MULTIPLE PERSPECTIVES OF DATA BREACHES IN HIGHER EDUCATION INSTITUTIONS (HEI): A CASE OF UNIVERSITIES IN SAUDI ARABIA

Haifa Almugamisi

degree of

Doctor of Philosophy

University College London

Department

Information Science

(DIS)

University College London

Declaration

I, Haifa Almugamisi confirm that the work presented in my thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

London,
AUGUST 2024

Abstract

This study investigates the significant risks posed by data breaches within Saudi organisations, with a particular emphasis on higher education (HE) institutions due to their extensive collection of personal data and early adoption of new technologies. It explores the multidimensional impacts of such breaches, including technical, organisational, and personal dimensions, as well as emotional aspects. The research aims to investigate the causes, risks, policies, mitigation strategies, and perspectives of a range of stakeholders concerning data protection. It seeks to understand the cultural complexities of data security in Saudi Arabia by utilising a convergent mixed-methods approach. The study examines two prominent universities for the case study contexts: King Saud University (KSU) and Taibah University (TaibahU). Through interviews with 15 managers and surveys distributed to 191 students and 70 faculty members, this research achieves a holistic understanding of personal data protection and captures the diverse risks and impacts of data breaches. Semi-structured interviews and a survey containing both closed and open-ended questions were used as data collection tools. The research was carefully designed to account for and mitigate power imbalances and potential researcher bias. In addition, it considered the challenges of collecting data on a sensitive and complex topic, namely, data security.

The findings reveal multiple risks in HE institutions, technical (e.g., malicious attacks and phishing), organisational (e.g., reputational damage), and personal (e.g., emotional responses including fear, anger, anxiety, shock) impacts. The study identified the critical impact of data breaches and the need for Saudi HE institutions to adopt the recently established national framework for data protection. This necessitates updating security policies, categorising data, engaging stakeholders in data processing, establishing structured protocols for managing breaches, and devising various mitigation strategies, such as offering compensation. Additionally, the research emphasises the importance of understanding personal risk, including the cultural significance of 'over trust', which influences the Saudi data security environment. Consequently, it proposes that universities should implement robust security protocols that

consider technical, organisational, and personal (emotional) aspects. A holistic response is required, including comprehensive data governance frameworks, clear response plans for data risks, and security training programmes at all organisational levels. The study highlights the importance of understanding cultural and social contexts when establishing data governance programmes. This work provides valuable insights for developing and delivering data protection and governance programmes within the Saudi context. Furthermore, it offers recommendations for the global university sector. Finally, the research framework presents new considerations for navigating across cultural boundaries and languages while addressing subject sensitivities.

Impact Statement

The contribution of this research lies in its novel, holistic exploration of data breaches within Saudi HE institutions. It offers a multidimensional perspective of the data security landscape in these institutions. This study incorporates insights from a diverse range of stakeholders, including students, faculty members, and managers. The findings identify the converging and diverging viewpoints among these stakeholders regarding data breaches and security management. It provides insights into the risks, vulnerabilities, and impacts, including technical, organisational, and personal (emotional) considerations related to data breaches. This knowledge will aid individuals and organisations in better understanding the data breach landscape and developing appropriate responses across stakeholders, thereby fostering a sense of shared responsibility as well as accountability for data governance and personal data protection in Saudi society.

The study's results have the potential to influence and improve the delivery of Saudi Arabia's digital transformation vision. This change and impact can be achieved through the adoption of its recommendations, especially regarding universities, leadership and governance structures, including training at all levels and resourcing. The research provides valuable information on data security in SA, an important country in the Middle East that increasingly offers global services, including hosting international universities and commercial businesses. Although the study focuses on a single geographical context, its implications are far wider and have the potential to impact beyond the Saudi context. The adage from a Saudi context, ‘We can find in the river what we cannot find in the ocean’ illustrates the significance of the context in which data is held. Nevertheless, there are also synergies to consider. Both contexts—local and global—must be understood. Every institution and country are susceptible to data breaches that affect them in various ways. In an increasingly interconnected world, particularly in the realm of digital services, it is essential to understand the perspectives of different cultures, sectors, and professions on data governance and the risks associated with data breaches.

Whilst this work has focused on HE, it has also evidenced important cultural and demographic trends, particularly regarding how, in SA, people tend to over-trust their systems and exhibit varied responses to breaches depending on gender and profession. It highlights the need to create support mechanisms for managers working in the data breach landscape as well as for all stakeholders affected by a breach. These findings extend beyond HE institutions into other sectors, including hospitals, banks, and schools. In addition, the study's results highlight the need for future research on cultural and emotional risks and impacts in different contexts. The impact of this study goes beyond its stakeholders, institutions, and even its cultural or global context; it is also valuable for researchers. The thesis offers key insights into employing a convergent mixed-method approach for data collection and analysis. It addresses linguistic challenges in navigating multilingual and multicultural research. Moreover, it considers power structures and ethical concerns related to data collection in a sensitive subject domain. The frameworks and cultural learnings used in this study hold value for future research endeavours.

Acknowledgements

I extend my deepest gratitude to all those who supported me throughout the challenging yet rewarding journey of conducting my doctoral research. Foremost, I am profoundly thankful for the divine guidance of God.

I extend my sincere thanks to my supervisory team, Dr. Elizabeth Lomas and Dr. Anna Sexton, for their invaluable guidance, support, and expertise throughout my doctoral research journey. Their mentorship has been instrumental in shaping the direction of my study and ensuring its success. I am also sincerely grateful to University College London for the invaluable support and resources it provides to researchers and doctoral students. Additionally, I would like to express my immense appreciation to the employees of the Department of Information Studies for their cooperation, generosity, and significant contributions in sharing ideas and fostering scientific research.

I am deeply grateful to King Saud University and Taibah University for graciously allowing me to conduct research within their institutions. Their collaboration and assistance were essential to the completion of this study, and I am truly appreciative of the opportunities they provided me as a researcher. Additionally, I extend my thanks to all those who contributed to the research, including managers, faculty members, and students, whose cooperation was fundamental to the success of this study.

I express my sincere gratitude to my family for their invaluable love and support, which have been steadfast pillars of strength throughout my journey. Their unwavering encouragement and patience helped me navigate both challenges and successes. In particular, I extend a heartfelt thanks to my dear father for his exceptional support. Additionally, I hold dear the memory of my mother, whose enduring spirit continues to inspire me daily. I am also grateful to my beloved sisters, brothers, and friends for their continuous encouragement.

Finally, I wish to express my gratitude to the Saudi Ministry of Education for its financial support, which made it possible for me to pursue my research aspirations. To all who contributed to this doctoral research effort in any capacity, I extend my heartfelt thanks.

Table of Contents

APPENDICES

LIST OF TABLES

LIST OF FIGURES

Chapter 1: Introductory Chapter

1-1 Thesis Overview

This thesis explores digital data breaches in higher education (HE) in the context of Saudi Arabia (SA). It is important to understand this geographical context and its cultures and positioning in the world. This chapter establishes the key contextual considerations of this study in terms of Saudi regulatory regimes, cultural considerations, and introductory information about respected universities included in this research. In addition, it contributes to broader data protection knowledge by clearly setting out the Saudi data protection position which is not widely discussed internationally. Chapter 2 presents the literature review, identifying the landscape of personal data security and understanding of data breaches and their impact on critical stakeholders. Chapter 3 outlines the methodological framework, and the findings of the work are delivered in Chapters 4, 5, and 6. More specifically, Chapter 4 details the qualitative data, Chapter 5 details the quantitative data and Chapter 6 integrates and discusses the findings in relation to the literature. Finally, Chapter 7 presents the overarching conclusions and summarises the novel contributions of this work.

1-2 Thesis Scope

This study explores data breaches in SA HE organisations. During the timeframe of this research project (2020_2024), SA, in line with other nations, has significantly increased the expectations for strong data governance and frameworks around the creation and protection of data. The threats to data security and the risk of breaches have been increasing year on year due to both cyber-criminal activity and state cyber warfare risks. In light of these developments, this research aims to explore personal data risks and data breaches in Saudi HE from multiple perspectives. It seeks to capture the technical, organisational, and personal impacts of data risks and data breaches in university settings in SA as well as the emotional consequences of data breaches.

To achieve the study's goals, the following critical research questions were drawn:

1- What are the causes of the data protection breach in SA HEIs?
2- How do SA HEIs tackle personal data risks, including personal data policies and processes?
3- What are the multidimensional impacts of data breaches on stakeholders technically, organisationally, and personally?
4- Why do stakeholders think their personal data should be protected? How would they like data management to change in terms of technical, organisational, and personal aspects?
5- How do SA HE mitigation strategies help to manage and recover from security breaches?

The research framework followed a convergent mixed methodology design. Interviews and surveys were conducted for two case studies at King Saud University (KSU) and Taibah University (TaibahU). The researcher is a Saudi citizen and academic from TaibahU with a scholarship enabling her to step away from this context for her PhD studies. This positionality is discussed in Chapter 3. A critical value of this work is establishing a greater understanding of not just the technical considerations of data breaches but also stakeholder perspectives, particularly those of stakeholders beyond the Western context. To date, much of the literature has taken a Western perspective; this work marks an important shift toward understanding different cultural stances and responses to data breaches from an Eastern perspective.

1-3 Thesis field

This research is primarily situated within the domain of information science, with a particular focus on three intersecting subfields: information management, information security, and information governance. Information science serves as the theoretical foundation and considers the nature of information and the methods by which it is organised and processed to ensure accessibility and comprehensibility. Information management translates these theoretical principles into practical applications, addressing the life cycle of information—including its collection, storage, dissemination, and utilisation—within

organisational contexts. Information security, as a specialised branch of information science, is dedicated to safeguarding information against threats such as theft, hacking, or corruption, by ensuring its confidentiality, integrity, and availability. Information governance, in turn, establishes the strategic framework for developing policies and standards to regulate information management and security, to promote compliance with legal and quality requirements. The interconnections among these subfields underscore an integrated approach: information science offers the theoretical underpinnings, information management ensures operational application, information governance provides the organisational structure, and information security delivers protective measures. Together, they facilitate the efficient and sustainable use of information within institutional settings.

This study investigates practices for managing data breaches within Saudi HE institutions, with a particular focus on individual perceptions of data processing and protection as a critical priority. The research extends beyond the technical dimensions of information security to include the policies, protocols, and ethical standards necessary for effective information governance and management. In essence, this thesis situates itself within the broader framework of information science, emphasising the roles of information management and security while integrating elements of information governance to present a cohesive regulatory and operational perspective. This synthesis highlights the symbiotic relationship between the theoretical constructs of information science and the practical frameworks that ensure sustainable and effective information practices.

1-4 University Stakeholders Included in the Study

Universities deal with a variety of stakeholders, both local and external. Local stakeholders include students and staff, while external stakeholders include entities such as government agencies, professional associations, parents, alumni, research participants, and others with whom the university interacts.

This study aimed to evaluate different levels of data security awareness and to understand the diverse security needs across key stakeholder groups. Given the wide range of stakeholders whose data universities handle, it is crucial to

identify those involved in this study. Stakeholders here refer to entities associated with the university and comprise three categories.

The first category is undergraduate students. Graduate students were excluded to focus on undergraduates, which constitute a larger segment of the student population. They enter the university with the most basic level of information security awareness, making them a more vulnerable population (Slusky & Partow-Navid, 2012).

The second category is faculty members from various academic specialisations without distinction between different ranks such as lecturer or assistant professor. Members of this category were expected to exhibit a higher level of information security awareness (Yerby & Floyd, 2018), with variations based on educational background, bachelor's, master's, or doctoral degrees. People in this category carry some level of responsibility for managing personal data held by the universities.

The third category is higher-level managers with additional responsibilities for data management or data security. Managers from multiple departments, including data security and information technology, as well as psychological and social departments, were included. People in this category represent a high level of information security awareness as stated by Albrechtsen & Hovden (2009).

Importantly, the critical stakeholders for this study are those whom the university holds data on, including staff, students, and research participants. Institutional approval was taken from the two included universities to participate in this study. As such, institutional channels were used to reach individuals for surveys and interviews. For a detailed explanation of the methodology, study participants, and findings, refer to Chapters 3, 4, and 5. These further establish the choices made in the study and the strengths and limitations of the approaches taken.

1-5 Saudi Arabia (SA) Global Context

SA is a significant economic power on the world stage, due in part to its substantial oil reserves. Beyond its significant oil wealth, comprising a quarter of the world's known crude oil reserves, the country's economic prominence is

evident as one of the top 20 global economies, and it is an active participant in the G20. Geographically, SA has a critical strategic position connecting three continents: Asia, Europe, and Africa. Culturally, it holds a distinguished status as the custodian of Islamic civilisation, with Mecca and Medina, the spiritual centres of Islam, underscoring its cultural and religious significance.

In recent years, SA has made extensive efforts to position itself in the global arena by hosting mega-events, notably the upcoming World Expo scheduled for 2030. Concurrent with this significant event, the country is poised to unveil a new strategic vision for the years 2030_2040, marking a substantial milestone in its global engagement and strategic planning. Despite criticisms, particularly regarding human rights and individual freedoms, the nation has implemented regulations to support personal freedoms, including the freedom of information and data protection law (Alwasil, 2010; Al-Rodiman, 2013).

Domestically, the nation introduced Vision 2030 in 2016 (VISION 2030, 2022), signalling a post-oil era with a focus on diversifying investments across sectors such as education, health, space, information security, and artificial intelligence. This initiative includes the completion of substantial government projects with costs ranging from 3.7 billion to 20 billion Saudi riyals. On a global scale, SA ranks 17th among 64 countries in competitiveness and stands 3rd in terms of G20, showcasing its economic prowess (Sokulski et al., 2022).

This research examines personal data management in SA, focusing on higher education institutions (HEIs) due to their role in creating, collecting, and processing personal data, along with their institutional ties to the state. Employing an intersectional approach, the study explores the multidimensional impacts of data breaches from diverse perspectives, including critical stakeholders. This chapter offers an introductory overview of personal data management and governance in SA, clarifying key laws and regulations through the interpretation of government directions. Additionally, it sheds light on relevant Islamic and social values, aiming to enhance understanding of the ethical and social background of Saudi citizens and their connections to privacy and personal data considerations.

1-6 Data and Information Regulations and Laws: An Overview

Data protection laws in SA are relatively new. The Personal Data Protection Law (PDPL), announced in 2021 and amended in 2023, is set to be implemented by mid-September 2024 (Meenagh & Tucker, 2023). This work therefore took place against a backdrop of change, with data being collected ahead of the implementation against knowledge that new laws were being formulated. Before the PDPL, various regulations focused on personal data management and information security, including the Cybersecurity Law and its related provisions, which govern the circulation of personal data and the rights of data subjects. Specifically, these laws include General Rules for Maintaining the Privacy of Users' Data, Anti-Cybercrime Law, and Electronic Transaction Law. Multiple authorities in SA oversee the implementation, compliance, and awareness of these regulations, notably the National Cybersecurity Authority (NCA), the Communications and Information Technology Commission (CST), and the Saudi Data and Artificial Intelligence Authority (SDAIA).

According to the CST, personal data includes any statement or piece of information, irrespective of its source or form, that singularly identifies or facilitates the identification of a user, either directly or indirectly. This inclusive definition spans a broad spectrum, including elements such as names, personal identification numbers, addresses, contact details, license numbers, records, personal property details, as well as financial information like bank account and credit card numbers. Additionally, it extends to visual elements like fixed or animated user photos and other data of a personal nature (CST, 2023). The main role played by the Saudi CST in the regulation of personal data management within SA is emblematic of the authorities' commitment to protecting individual privacy. The CST wields significant powers focused on privacy maintenance, coupled with the responsibility of overseeing the handling and governance of personal data.

This regulatory framework is reinforced by a series of documents published on the Authority's official websites, each addressing specific aspects of personal data privacy. These regulatory documents underscore the Authority's dedication to providing a structured and transparent framework for the management of personal data. The Authority's definition of personal data

reflects a nuanced understanding of contemporary challenges surrounding data privacy in the digital age. The all-encompassing nature of the definition acknowledges the multidimensional nature of personal information, capturing the diverse forms and sources through which individuals can be identified. The issue of regulatory documents further demonstrates a proactive approach to data management, ensuring that legal and ethical considerations keep pace with technological advancements. As the landscape of personal data evolves, ongoing scrutiny of these regulations will be essential to evaluating their efficacy, addressing emerging challenges, and maintaining a robust framework that respects individual privacy in the ever-changing digital world.

The following section provides additional information about the new PDPL, followed by details on other relevant regulations, such as General Rules for Maintaining the Privacy of Users' Data, Anti-Cybercrime Law, and Electronic Transaction Law.

1-6-1 Personal Data Protection Law PDPL

The issue of the PDPL in September 2021 marked a significant development in SA's regulatory landscape. The law, officially published in September 2022 by the Bureau of the Experts at the Council of Ministers (Experts Bureau, 2023a), signifies the Kingdom's commitment to safeguarding individuals' personal data. The enforcement, initially scheduled for March 2023, falls under the purview of the Saudi Data and Artificial Intelligence Authority, along with the Saudi National Data Management Office NDMO, ensuring a coordinated and comprehensive implementation. This legal framework sets conditions for processing personal data and represents a series of rights afforded to 'personal data subjects'. The document meticulously outlines data processing standards, the obligations of entities handling personal data, and the penalties for non-compliance within the nation. Notably, the law applies to the processing of personal data related to individual citizens/residents within or outside SA, extending even to data of deceased individuals if it reveals identifiable information about them or their family members (Baig, 2023).

Comprising 43 articles, the law extensively addresses various aspects of data protection, including privacy policies and procedures for data controlling

entities, which are entities collecting and determining the purpose of processing personal data. The emphasis on transparency is evident in the requirement for senior officials to approve and disseminate privacy policies, ensuring clarity regarding collection and processing purposes. The document accentuates the rights of data subjects (SDAIA, 2023a), incorporating the right to be informed about data processing, the right to access personal data, and the right to correct or destroy data. The explicit or implicit consent of individuals for data collection, use, or disclosure is a foundational principle, ensuring individuals have agency over their personal information. Data minimisation is a notable concept, underlining the necessity of collecting the minimum data required to achieve specified privacy notice purposes. The law prescribes severe consequences for non-compliance or breaches. For instance, unauthorised disclosure or publication of personal data with malicious intent carries imprisonment or fines. Provisions regulating and minimising the transfer of personal data outside SA are stringent, subjecting violators to imprisonment or fines unless they have been acting in compliance with international agreements or serving the Kingdom's interests under the terms of the laws. The potential for the judicial process to be engaged on an individual or institutional level, conducted by the public prosecution and competent courts, underscores the seriousness with which personal data protection violations are taken. Detailed duties of data controllers, guidelines for processing and disclosing personal data, conditions for transferring data internationally, and mechanisms for monitoring compliance further solidify the comprehensive nature of the law. This legal framework additionally represents a commendable effort by SA to align its data protection practices with international standards. The law's meticulous determination of rights, obligations, and consequences reflects a nuanced approach to balancing individual privacy with the evolving landscape of data usage and technology. The law has been a massive step forward in SA’s commitment to data protection which has rapidly evolved during the timeframe of this study.

1-6-2 General Rules for Maintaining the Privacy of Users’ Data

Preserving the privacy of users' personal data mandates compliance with several foundational principles (CST, 2023). Firstly, the processing of such data should be conducted systematically and transparently, with a commitment to

fairness to avoid any unwarranted negative impacts on user interests. Secondly, the processing of users' personal data must have explicit and well-defined purposes, emphasising transparency and user comprehension. Thirdly, collection of the minimum amount of personal data necessary for the intended purposes is paramount, necessitating a delicate balance between data utility and individual privacy. Additionally, the retention of users' personal data should be constrained within the period necessary to achieve its processing purposes, preventing prolonged identification possibilities. Finally, robust protection mechanisms are imperative to ensure the privacy of users' personal data, guarding against illegal access, leakage, tampering, or misuse, underscoring the meaningful role of cybersecurity in maintaining data privacy.

Obligations of Service Providers

Service providers bear several obligations to safeguard the privacy of users' personal data. Firstly, they are mandated to establish and execute a comprehensive privacy maintenance programme, encompassing the development, documentation, and implementation of policies and procedures about users' personal data privacy. This programme must gain approval from the service provider's senior official or their authorised representative, with submission to the regulatory authority for review and periodic updates. The service provider must assign responsibility for users' personal data privacy to an independent unit, ensuring adequate support and preventing conflicts of interest.

Additionally, service providers are obliged to formulate, endorse, and publish a privacy policy specifying the types, purposes, sharing practices, retention durations, protection procedures, and user rights concerning their personal data, along with instructions on how to exercise these rights. Furthermore, processing users' personal data outside the Kingdom necessitates written approval from the regulatory authority, emphasising localisation. Service providers must retain users' personal data for specified purposes and durations in accordance with regulatory instructions and promptly notify the authority of any data leakage through approved mechanisms and procedures (CST, 2023).

Users' Rights Regarding the Privacy of their Personal Data:

The following outlines the rights of users regarding the privacy of their personal data. These rights are designed to ensure transparency, control, and protection of user information throughout processing by service providers. The key principles emphasise user consent, accessibility, and the ability to manage and correct personal data. Below are the specific rights users hold:

- Users' personal data may not be processed without explicit consent, and users may withdraw their consent at any time, except for what is required by the relevant laws, regulations, and instructions.
- Users must be enabled to view the personal data privacy policy before processing of their personal data.
- Users must be able to access their personal data processed by the service provider at any time and to correct it when there is erroneous or inaccurate data.
- Users must be able to obtain a copy of their personal data in electronic form, as approved by the CST.
- The processing of users' personal data requires their explicit consent; users retain the right to withdraw at any point, except in cases mandated by pertinent laws, regulations, and instructions.
- Users should review the personal data privacy policy before the processing of their personal data.
- Users must have continuous access to their processed personal data, with the capability to rectify inaccuracies when discrepancies arise.
- Users should have the facility to acquire an electronic copy of their personal data, subject to the approval of the regulatory authority.

These points collectively underscore the importance of user consent, transparency, accessibility, and data accuracy in the processing of personal data by service providers (CST, 2023).

1-6-3 Anti-Cybercrime Law

The Anti-Cyber Crime Law of SA represents a comprehensive legal framework with the primary objective of protecting information security and upholding the

rights associated with legitimate computer and information network usage. Enacted under the jurisdiction of the CST in 2007, this legislation determines a set of cybercrimes along with their corresponding penalties in order to bolster information security in the ever-evolving digital threat landscape.

An essential feature of this law is the introduction of a tiered system of punishments, strategically tailored to the severity and nature of the cybercrimes committed. Individuals engaged in activities such as cyber espionage; unauthorised access to websites leading to their destruction, disruption, or alteration; infringement upon the privacy of individuals through technological means; or the dissemination of defamation and harm through information technology may find themselves facing penalties of imprisonment for a maximum period of one year, a fine not exceeding 500,000 Saudi riyals, or a combination of these sanctions. As crimes progress to a more stringent classification of cybercrimes, the law prescribes more substantial penalties. Offences like fraudulent acquisition of movable property or bonds, and illicit access to bank or credit data for the purpose of acquiring unauthorised data, information, funds, or services, could lead to imprisonment for up to three years, a fine not exceeding 2 million riyals, or a combination of these penalties. In the subsequent category, cybercriminals who gain unauthorised access to delete, destroy, leak, alter, or republish private data; disrupt or damage information networks; or obstruct access to information services may face penalties involving imprisonment for a period not exceeding four years, a fine not exceeding 3 million Saudi riyals or a combination thereof. The most serious categories of cybercrimes include offences encompassing the production, transmission, or storage of materials that transgress public order, religious values, public morals, and privacy through information networks or computers; the creation or promotion of websites facilitating human trafficking; the development, publication, and promotion of pornographic or gambling materials that violate public morals; and the distribution of materials related to the narcotic and psychotropic drug trade. Perpetrators of these crimes may be subject to the most severe penalties, which involve imprisonment for a term not exceeding five years, a fine not exceeding 3 million riyals, or a combination of these sanctions.

Lastly, the law stipulates the gravest penalties, including imprisonment for a period not exceeding 10 years and a fine not exceeding 5 million riyals, for individuals engaged in the creation or promotion of websites on the information network or computers designed to benefit terrorist organisations. These websites may serve purposes such as facilitating communication with the leaders or members of such organisations, providing financial support, propagating extremist ideologies, disseminating knowledge about the production of incendiary devices or explosives, or employing any other means utilised in acts of terrorism.

Additionally, unauthorised access to websites, information systems, or computers for the acquisition of data that poses a threat to the internal or external security of the state, or its national economy falls within this most severe category of cybercrimes. The law, through its meticulously structured framework of offences and corresponding penalties, is inherently designed to fortify information security, serving as a crucial deterrent against malicious actors who might engage in cybercrimes that have the potential to undermine the integrity of the digital realm, thereby contributing to the overall enhancement of information security and the maintenance of ethical standards in the digital world (Alabdulatif, 2018).

1-6-4 Electronic Transaction Law

The Saudi Electronic Transaction Law constitutes a comprehensive legislative initiative directed at the establishment of a meticulously structured regulatory framework for the world of electronic transactions and digital signatures. This legislation, as delineated by the CST in 2007, embodies an array of overarching objectives that extend their purview across both the private and public sectors. As its primary intent, the law aspires to standardise the legal parameters governing the deployment of electronic transactions and digital signatures, thereby concurrently advancing their integration through the facilitation of reliable electronic record-keeping mechanisms. The aim of this effort is to engender a state of uniformity in the legal and operational facets of electronic business transactions, instilling a sense of consistency and dependability in the electronic business environment.

Furthermore, the Saudi Electronic Transaction Law accords paramount importance to the preservation of the credibility and integrity of electronic transactions, digital signatures, and the associated record-keeping processes, thereby fostering a climate of trust and confidence within the digital domain. This is particularly critical in a landscape where traditional ink-and-paper signatures have been supplanted by electronic counterparts, and the law seeks to ensure that this transition does not compromise the trustworthiness and authenticity of digital transactions. The notion of credibility, therefore, emerges as a foundational element in the legislative framework, aiming to build a robust foundation for the digital world (Atim, 2020).

Moreover, this legislation is fundamentally designed to facilitate electronic transactions and the utilisation of digital signatures on a domestic as well as an international scale, for a diverse array of sectors, including government functions, commercial activities, healthcare practices, educational processes, and electronic payment systems. This ambitious scope reflects the law's commitment to transcending the confines of domestic borders and supporting the internationalisation of electronic transactions. By facilitating electronic interactions within and beyond national boundaries, the law aims to underpin the broader objective of fostering a globalised digital economy and reinforcing the global interconnectedness of various sectors, transcending geographical barriers.

As the fourth cornerstone of its objectives, the law is resolute in its effort to dismantle the impediments that may obstruct the smooth utilisation of electronic transactions and digital signatures. These impediments may include legal complexities, technical challenges, or administrative bottlenecks that hinder the adoption and implementation of digital transaction systems. By proactively identifying and mitigating such obstacles, the law seeks to expedite the assimilation of electronic transactions into daily business practices, thereby promoting efficiency and ease of use. The legislation assumes the role of an anticipatory guardian against potential misuse and fraud in the world of electronic transactions and digital signatures.

As digital spaces offer increased opportunities for illicit activities, safeguarding the integrity of these transactions has become critical. The law, in this regard, strives to establish mechanisms and legal frameworks that proactively deter and address instances of misuse and fraud, thereby erecting safeguards to protect the sanctity of electronic transactions. The Saudi Electronic Transaction Law stands as a pivotal legal edifice that transcends mere regulatory provisions. It not only functions as an enabler of electronic commerce but also operates as a custodian of values such as reliability, security, and ethical conduct within the burgeoning digital landscape. In an era defined by the acceleration of digitisation and the increasing prevalence of electronic transactions, this legislative initiative is positioned at the fulcrum of regulating, promoting, and protecting the domain of electronic interactions, underscoring its critical significance in contemporary society (Al-Ghathar & Al-Subaih, 2012).

1-7 Saudi National Data Management, Governance, and Personal Data Protection Framework

In addition to the legal protections described above, SA has established the PDPL specifically to protect personal information and enhance data security. Alongside this legislation, the country has implemented a national framework for data governance and protection to ensure the law's effective implementation and enforcement. The Saudi National Data Management Office (NDMO) has outlined a set of national principles concerning data management, governance, and personal data protection. The first edition of these principles was launched in August 2020, and this has since been updated five times, with the most recent revision in January 2021. It is important to highlight that the framework has been revised five times within a short span; this could be attributed to growing cybersecurity threats, necessitating updates to address new incidents and vulnerabilities as they emerge. The framework includes eight principles that are crucial for understanding the data management and governance system, which are detailed in the following tables.

Principle	Related Field
Data as a National Asset	Data governance.
Data Protection by Design	Personal Data Protection Data Classification Data Security and Protection
Open by Default	Open data
Ethical Data Use	Data governance.
Purposeful Design	Data Operations Data Sharing and Interoperability Data Architecture Reference and Master Data Management
Data-Driven Outcomes	Business Intelligence and Analytics Data Value Realisation
Learning Culture	Data Value Realisation Business Intelligence and Analytics Data Governance
Trusted Data	Data Quality Reference and Master Data Management Data Catalogue and Metadata Document and Content Management

Table 1 Information developed from data presented by NDMO

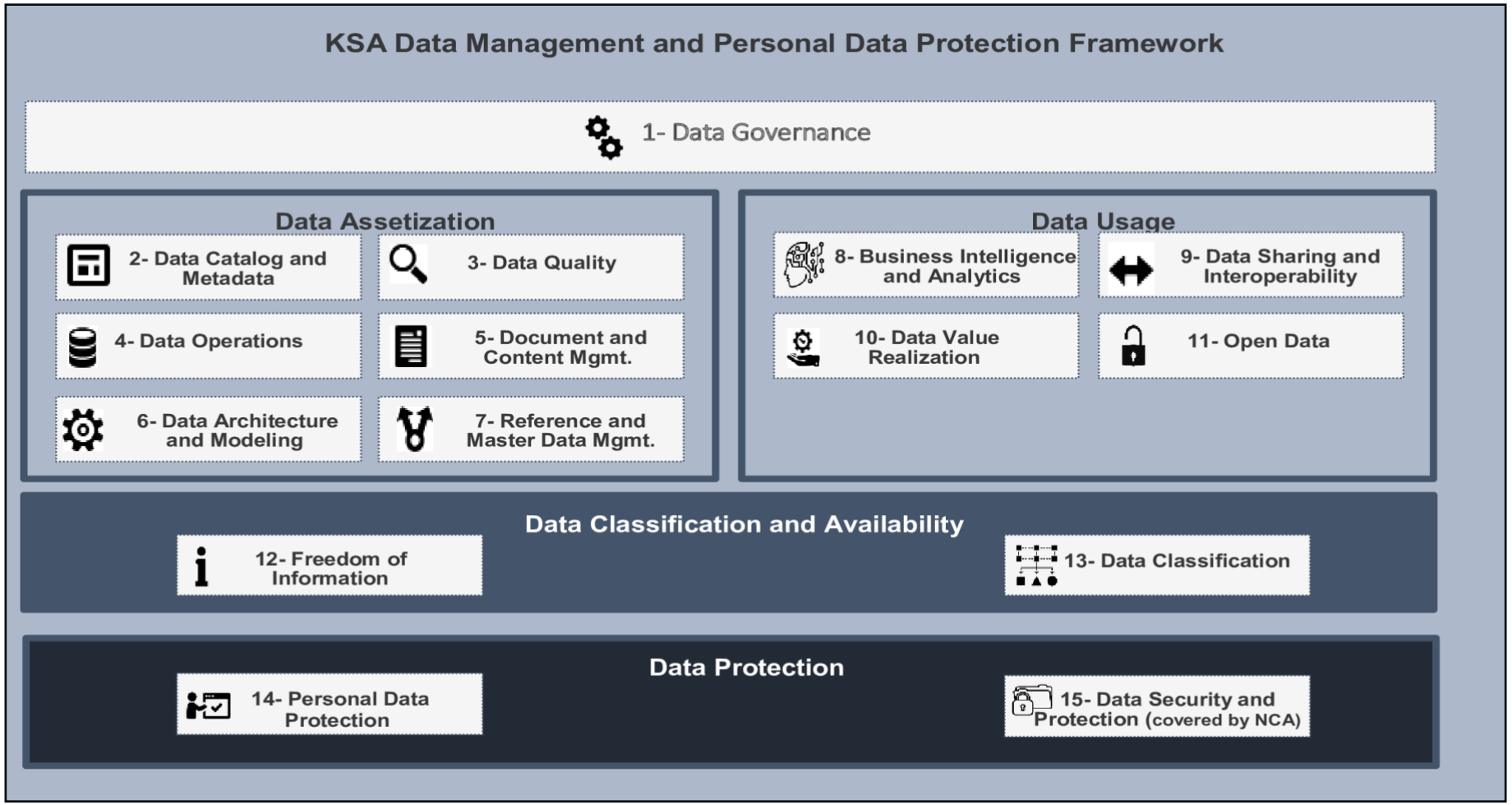

Figure 1 National Data Management and Personal Data Protection Framework developed by NDM, available on the following link https://sdaia.gov.sa/ar/Sectors/Ndmo/Pages/default.aspx

1-7-1 Data Governance

Globally the significance of data governance has been increasingly recognised, with data being understood as an asset. Data governance provides control mechanisms to both effectively manage data and enhance its value and mitigate associated risks (Abraham et al., 2019). Within the administrative framework of SA, data governance is defined as a structured set of practices and procedures aimed at ensuring the proficient management of data assets across organisations. This involves the formulation of a comprehensive data plan, the development and implementation of controls and policies, and commitment to compliance standards. The Saudi NDMO has instituted eight fundamental controls, including 28 specifications that delineate the management, control, and oversight of data assets (NDMO, 2023). These controls involve strategic planning, formulation of policies and guidelines, training and awareness initiatives, organisation of data management and governance structures, personal data protection measures, compliance examination frameworks, data lifecycle governance, performance management, and records management.

The NDMO directs each institution to articulate a strategy for data management, governance, and personal data protection. This strategy is expected to integrate the institution's data initiatives with those of other entities to serve public interests, ensuring alignment with the National Data Governance Strategy promulgated by the Office. Essential components of these strategies include specifications of internal and external requirements, challenges, visions, missions, goals related to data management and personal data protection, performance indicators, and an implementation budget. Policies and guidelines are to be developed collaboratively, following a flexible and coordinated approach between the institution and the NDMO. Institutions are mandated to establish policies and controls for data management, governance, and personal data protection, tailored to their specific needs in line with the controls stipulated by the office.

To execute and oversee the implementation of the national data management strategy, institutions are required to establish a dedicated data management

and governance office. This office assumes responsibility for training and awareness initiatives. The organisational structure of these data offices is outlined by the NDMO, with defined roles such as Data Office Manager, Data Governance Officer, Data Availability Officer, Compliance Officer, Personal Data Protection Officer, Business Data Representatives, Business Data Specialists, Data Technologists and Technicians, and Legal Counsel. These roles ensure a systematic and specialised approach to the management, governance, and protection of data within the institutional context.

1-7-2 Data Catalogue & Metadata

File catalogues and metadata catalogues play a vital role in data networks, helping to discover and locate data among many locations in the network (Waqar et al., 2013). Catalogues are utilised for storing information and require robust access control mechanisms to ensure data protection (Santos & Koblitz, 2008). Within the broader framework of data management and the protection of personal data, the second domain of emphasis pertains to the metadata data catalogue, which includes six main controls distributed across 20 specific facets. These controls consider crucial elements, such as strategic planning, policy formulation, training initiatives, comprehensive management of the data lifecycle, automation of data cataloguing processes, and performance monitoring within this domain. Key components integral to this facet include the prioritisation of data sources, the systematic structuring of metadata, establishment of protocols for organised data access, provision of training regarding data catalogue utilisation, systematic registration and periodic updating of metadata, evaluation and assurance of metadata quality, issuance of metadata certificates, facilitation of metadata notifications, rigorous auditing processes, and the formulation and application of performance indicators (NDMO, 2023). These elements collectively contribute to the systematic and effective management of metadata within the overarching paradigm of data governance and personal data protection.

1-7-3 Data Quality

Data quality stands as a foundational governance column crucial for the facilitation of effective data governance, with organisations across several sectors evidencing a keen commitment to ensuring the accuracy and reliability of their data (Data & Authority, 2021). This commitment is supported by the recognition of accurate data's vital role in informing analytical processes, thereby facilitating informed decision-making and contributing to the competitive edge of companies' actions predicated on the quality of their data and the soundness of their decisions (Shankaranarayanan & Cai, 2006).

The significance of high-quality data extends to its capacity to enhance strategic planning and fortify risk management within organisations. The Open Data Quality Standards Guide, as articulated by the SDAIA, defines data quality as a nuanced concept requiring evaluation of the suitability of data and its quality with respect to the intended context and purpose it is being used for. The quality of data is contingent upon various factors, including accuracy, completeness, reliability, importance, and the frequency of updates (SDAIA, 2023b). In contrast, the Saudi NDMO defines data quality as a comprehensive set of periodic operations undertaken to process data and ensure its validity, accuracy, and maturity to meet the purposes of the business requirements for which it is being used.

This domain of data quality governance includes four distinct controls, further delineated into 13 specifications. Firstly, the planning control incorporates critical aspects such as the prioritisation of data quality, the formulation of a comprehensive data quality plan, and the initial assessment of data quality. Secondly, the data standardisation process control entails the development of data quality rules, the establishment of monitoring mechanisms, the implementation of effective problem-solving strategies, the definition of service level agreements, and the integration of data quality tools. The third control, performance management, involves the specification of paths for data improvement and the resolution of data quality issues. Lastly, the data life cycle management control encompasses crucial facets including data quality verification points, the provision of support for data quality, and the incorporation of quality metadata. The orchestration of these controls and

specifications collectively constitutes a strategic approach to maintaining and enhancing data quality, an essential facet in the broader landscape of data governance and its multifaceted implications for organisational decision-making and operational efficiency (NDMO, 2023).

1-7-4 Data Operations

Data operations focus on data storage, which represents a critical domain that significantly shapes the landscape of data protection within the framework of data management and governance (Sarkar & Kumar, 2016). This sector within the Saudi framework involves five fundamental controls displayed in 15 specifications. Organisational procedures within this domain require the formulation of a meticulous data storage and preservation plan, considerations of storage capacity, prioritisation of data system requirements, evaluations of the database, and the establishment of policies governing storage and retention. Complementary executive procedures, constituting three controls, encompass database operations, business continuity, and performance management. Database operations entail essential components, such as continuous monitoring, access control mechanisms, data store settings, system upgrades, and service level agreements. The business continuity officer, in turn, is entrusted with necessary responsibilities, including overseeing backups, orchestrating disaster recovery protocols, and implementing stringent controls over data access.

Within the Saudi NDMO's regulatory framework (NDMO, 2023), each organisation is requested to formulate a comprehensive disaster recovery plan. Under this framework, key aspects of the plan are to

A. Establish a prioritised catalogue of information systems, delineating the specific sequence in which these systems are to be recovered, thereby providing a structured framework for efficient retrieval processes.
B. Allocate distinct roles responsible for managing incident response cases, ensuring a clearly defined distribution of responsibilities within the organisational context to enhance the efficacy of incident resolution.
C. Determine and articulate the procedural guidelines that dictate the activation of the incident response system, outlining the specific steps

and protocols to be followed in response to potential security incidents or breaches.

D. Define and assess the measures to be implemented to minimise damage and mitigate the consequences of unforeseen accidents on the critical operations of the organisation, fostering a proactive approach to organisational resilience.
E. Establish recovery point goals for each information system enlisted in the plan, stipulating the maximum permissible duration during which data loss can occur without causing adverse impacts on the business, thereby guiding data recovery strategies.
F. Specify recovery time goals for each information system incorporated in the plan, defining the maximum allowable period during which a database can remain inactive without detrimentally affecting the overall functionality of the business.
G. Identify and enumerate the distinct recovery activities, comprehensively detailing the strategic steps and actions to be undertaken for the restoration and resumption of normal organisational operations following a disruptive incident.

1-7-5 Document and Content Management

Document and content management systems assume a great role in upholding data security through robust mechanisms designed to mitigate potential threats from hacking activities (Patel et al., 2013). According to the Saudi framework, the domain of document and content management is structured around five overarching controls, further subdivided into 15 specific sections. This comprehensive framework is designed to effectively oversee the administration, preservation, and evolution of content and documents, employing strategies that involve digitisation and the facilitation of their exchange. The strategic approach within this field incorporates accurate planning, entailing the formulation of a plan for the management of content and documents. This plan extends to include digitisation processes and the establishment of policies to govern content management practices (NDMO, 2023).

Within the scope of implementation processes, various facets of content management are addressed, including critical aspects such as backup and recovery procedures, the identification of access rights pertaining to content and documents, the publication of metadata associated with content, the utilisation of content management tools, and the establishment of key performance indicators to assess the effectiveness of content management initiatives. The document digitisation plan adopts a strategic perspective, outlining measures such as the phased implementation of mechanisms for transitioning paper documents into digital formats. Concurrently, initiatives are promoted to reduce the production of physical documents, aligning with the case made for the increased use of digital tools.

Furthermore, this plan involves the precise determination of resources and budgets dedicated to the digitisation process. The incorporation of a ‘retention and deletion’ clause underscores the imperative of establishing secure mechanisms for the disposal or destruction of documents. This process is conducted under the careful supervision of the archive’s unit within the institution, ensuring compliance with archival standards and regulatory frameworks and thus reinforcing the commitment to responsible and secure document management practices.

1-7-6 Data Classification

There are diverse types of data, each demanding distinct levels of protection (Shaikh & Sasikumar,2015). Within the Saudi framework, the thirteenth domain within data governance authorised by the office focuses on data classification, including five foundational controls and 10 specifications. This domain divides data into distinct levels, establishing a mechanism to address them based on the severity of the impact ensuing from any unauthorised disclosure of data or its content. Organisations, as mandated by the office, are required to undertake the classification of the data they collect and accumulate, prioritising datasets and records classified within their systems.

The classification of data is contingent upon various controls, particularly security controls. Each institution is expected to appropriately allocate protection and processing controls tailored to each data classification group.

This allocation is devised to ensure the secure circulation, processing, sharing, and deletion of data in accordance with the policies stipulated by the NCA. As part of the office's directives, organisations are further requested to conduct a potential impact assessment in instances where data is disclosed or unauthorised access occurs. This assessment is integral to understanding and mitigating the potential impacts of such incidents. The potential impact assessment includes the following steps:

A. Identify the categories that can be affected by entities, individuals, people, and the environment.
B. The potential damage impact level for each category is chosen between 'High', 'Medium', 'Low', and 'None'.
C. Determine classification levels for data sets and records based on the level of impact specified:

- ✓ If the impact level is 'high', the data is classified as 'top Secret'.
- ✓ If the impact level is 'medium', the data is classified as 'Secret'.
- ✓ If the impact level assessment is 'low', the data are classified as 'Confidential'.
- ✓ If the impact level assessment is 'none/Insignificant', the data is classified as 'Public' (NDMO, 2023).

1-7-7 Personal Data Protection

The domain of personal data protection includes a structured framework of five controls and 10 specifications, constituting a comprehensive set of provisions and procedures designed to govern the processing of personal data (NDMO, 2023). This framework is carefully crafted to ensure the preservation of privacy for individuals while protecting their inherent rights. As per the directives of the NDMO, each organisation is obligated to formulate a personal data protection plan that aligns with both operational and strategic requirements, as outlined in the personal data protection policy issued by the NDMO. A key aspect of compliance entails the imperative for organisations to conduct training initiatives focused on personal data protection for all stakeholders processing personal data. This training aims to build a safe environment focused on data protection. The training programme necessitates covering essential elements, including an introduction to the significance of protecting personal data; an

exploration of its effects and consequences on both the organisation and data subjects; an illustration of the rights vested in data subjects; a determination of responsibilities for both the organisation/controller and data subjects; guidance on notifications and reporting procedures; and guidance on managing requests about the collection, processing, and sharing of personal data.

Within the scope of controls instituted to protect personal data, an essential measure is a protocol for 'notifying data leaks'. In this regard, individuals responsible for data control or data processing within the organisation bear the onus of promptly notifying the regulatory authority within 72 hours of a personal data breach. This timeframe is intended to speed up the resolution of a breach, ensuring compliance with established controls and fostering a swift and effective response to mitigate potential consequences.

1-7-8 Data Security and Protection

Under the directives acknowledged by the NDMO, the authoritative entity responsible for cybersecurity oversight in SA is the NCA (NCA, 2023). This regulatory body assumes the crucial role of supervising and monitoring compliance, including regulatory and operational aspects germane to data security and protection. The framework for data security controls and protection, as articulated by the NCA, includes a series of imperative components, notably information security governance, the architectural underpinnings of information security, the intricate processes of designing, developing, and testing information systems, protocols for identity management and access to information, measures ensuring the security of third-party suppliers, comprehensive training initiatives, awareness campaigns, and communication strategies within the purview of information security.

Additionally, the framework involves information asset management, information security operations coordination, information security incidents management, information security risk management, and information systems continuity management (NCA, 2023).

1-7-9 The Reality of Compliance in SA

The legislative and regulatory landscape for this study was developing during the timeframe in which data was collected and written up. There is a strength in the framework delivered but as yet it has not been fully realised and tested across all the domains set out above. This was a fast-moving scene during the study. As such, it is important to note that during the data collection period, which took place from April to July 2022, certain aspects of implementing the state governance framework or the new PDPL were in progress. According to the national framework for data protection, organisations, including universities, are required to establish dedicated data management departments. These departments were found to have been created, but upon visiting them, it was reported that they were new and had no significant tasks at that point in time.

Additionally, all institutions involved in the study had legal management departments, but preliminary discussions revealed a general lack of awareness about the data protection law, likely due to its recent introduction. Nonetheless, this does not imply an absence of regulations for data security management. As detailed later, each institution has its security policies and all adhere to existing regulations such as the General Rules for Maintaining the Privacy of Users' Data, the Anti-Cybercrime Law, and the Electronic Transaction Law. One of the critical gaps explored by this study is the organisational approach of universities to managing the security of personal data.

1-8 Values in SA

This section discusses social and Islamic values within the context of SA, a country where laws and regulations are based on Sharia law. The focus is on social values such as citizenship, freedom, equality, and social justice. These values have significant relevance to this research as it seeks to understand individuals' perspectives on personal data security management. This responsibility is shared by the state and relevant organisations, thereby linking data security management to the concept of citizenship especially in regulating individuals' privacy rights.

Regarding freedom, although the topic is specific and sensitive, the views expressed by individuals do not contradict the principle of freedom as a social

value in the state. Regarding equality and social justice, particularly gender equality, the study included both state-recognised genders: female and male. While efforts were made to include both, methodological limitations existed (see Chapter 3). Gender considerations also impacted the findings (see Chapter 6).

Islamic values, according to the Basic Law of Governance in SA, protect individuals' privacy rights, with data security management primarily based on systems, policies, and laws. Saudi systems are generally rooted in Islamic teachings. Therefore, key Islamic values believed to be directly relevant to the research, such as morals and ethics, honesty, integrity, and permission, are introduced, as they are fundamental to the data protection system (Andress, 2019).

1-8-1 Social Values in SA

The philosophical lexicon outlines the concept of value as a tangible characteristic intrinsic to the essence of words (within the domain of knowledge), actions (within the field of morals), and entities (about the arts) (Almutrajiy, 2021). Importantly, this inherent quality persists consistently and remains unaltered despite fluctuations in circumstances and contextual variables. The constancy of value is posited to endure as an immutable attribute if it is an inherent aspect of the nature of words, actions, and things. Social values constitute a complex framework of ideals, goals, objectives, and behavioural regulations shaping individual and collective conduct (Kinzig et al., 2013). The genesis of these judgments lies at the nexus of familial, immediate environmental, and societal interactions, subject to standards endorsed by the collective in accordance with religious, customary, and societal goals. Al-Qahtani (2010) contributes a nuanced perspective by characterising social values as a composite of psychological constructs, encompassing intellectual and emotional judgments shared among individuals. This conceptualisation posits these constructs as cognitive frameworks, directing and channelling individual motivations and desires within the intricate tapestry of social life to achieve communal objectives. This psychological lens offers insight into the intricate interplay between individual psychology and the broader social fabric. Cultural, historical, and geopolitical factors can subtly shape interpretations of

social values, necessitating a more nuanced exploration of the Saudi context. The interplay of religion, custom, and societal goals in shaping social values demands further critical analysis. The extent to which these factors harmonise or diverge in influencing values, and the potential conflicts that may arise, are crucial considerations. Therefore, it was necessary to outline the societal context under investigation within this research to achieve a better understanding of the research issue.

1-8-1-1 The Value of Citizenship

Citizenship constitutes the foundational link between an individual and the state and establishes a mutual relationship wherein one's rights are fulfilled in exchange for the execution of certain duties. Al-Attar (2017) underscores the inseparability of duties and rights within the construct of SA citizenship. Citizenship is conceptualised as a value that shapes desirable social behaviour aligned with societal values, aiming to cultivate individuals into responsible and contributing citizens. In essence, citizenship signifies an individual's connection to their national identity and country, entailing both rights enshrined by the state and one’s corresponding obligations and responsibilities toward the state.

The Saudi Vision 2030 places a spotlight on citizenship. It envisages an effective, transparent, and responsible government. Vision 2030 seeks to inspire societal engagement across all SA communities, urging citizens to actively participate in advancing the nation. It underscores the pivotal role of individuals, positioning them as the primary driving force behind the realisation of the nation’s goals. Thus, it emphasises the reinforcement of citizenship concepts and associated obligations as crucial elements in overcoming challenges and fostering collective success (Al-Maliki, 2023).

Addressing the contemporary landscape, a proposed vision for cultivating digital citizenship among university students is part of the SA Vision 2030. Albraithen's study examined the values of digital citizenship deemed essential for university students in SA. Employing a descriptive-analytical approach, the study identifies key values, including respect, education, and protection, emphasising sub-elements within each category, such as digital fitness, access, laws, digital rights, security, health, and safety (Albreathin, 2020). Critical

engagement with the study involves an exploration of the implications and potential challenges associated with instilling digital citizenship values in a rapidly evolving technological landscape. The role of universities in the delivery of Vision 2030 is critical if digital citizenship education is to be developed over time.

Furthermore, an examination of the recommendations and proposals emanating from Albreathin's study is important to gauge their practicality and alignment with the overarching goals of Vision 2030. The study's recommendation to strengthen cooperation among SA universities in addressing issues of intellectual security and citizenship introduces a dimension of societal responsibility. This underscores the role of universities not only in education but also in contributing to the broader cultural and social fabric. Critical analysis has yet to be fully explored in terms of understanding the potential impact of security events and initiatives on shaping a responsible citizenry, preserving cultural heritage, and addressing societal challenges.

The academic discourse surrounding citizenship, particularly in the context of Saudi Vision 2030 and digital citizenship among university stakeholders, necessitates critical examination. Although the role of universities in promoting digital citizenship has been discussed (Al-Otaibi et al., 2021; Amani Qalyobi, 2022), this study explores the perspectives of students, faculty members, and managers working specifically in the context of personal data security, reflecting their level of satisfaction and confidence with government digital services concerning data security management.

1-8-1-2 The Value of Freedom

Freedom, as a fundamental human right, occupies a vital position in shaping individual autonomy and decision-making. This expansive concept encompasses the freedom to make personal choices and dictates the way an individual shapes their life. Within the broader context of this research, freedom is examined as a crucial element underpinning an individual's right to control their personal data, particularly within the world of privacy. In SA society, the value of freedom is acknowledged as a cornerstone of rights, with the government playing a significant role in its promotion. Notably, the endorsement

of the Freedom of Information and Personal Data Protection Act signifies a legislative commitment to protecting individual liberties, emphasising the importance of privacy rights within the framework of personal freedom. This legislative step aligns with the broader principles of human rights, reinforcing the idea that freedom, including the right to privacy as a foundational aspect of an individual's rights, provides for well-being and self-determination (Experts Bureau, 2023a). The societal and human values entrenched in Saudi culture serve as a fertile ground for the cultivation of human rights. Rooted in the principles of Islamic Sharia, these values are integral to the cultural fabric, emphasising peace, goodness, and the inherent dignity of individuals.

In Article 26 of the basic law of governance, SA has shown its commitment to human rights through robust regulatory frameworks, legislation, and policies designed to ensure a decent life for its citizens and enhance their rights and freedoms (Experts Bureau, 2023b). Participation on the international stage further exemplifies SA's commitment to the promotion and protection of human rights. The active engagement in International Human Rights Day, marked by the slogan 'Dignity, Freedom, and Justice for All', underscores a global acknowledgement of the intrinsic dignity of all individuals and their equal and inalienable rights. The commitment to these principles is enshrined in the Basic Law of Governance, emphasising the right to freedom and dignity as fundamental to national systems (Saudi Press Agency, 2023).

However, within a critical academic framework, one must carefully scrutinise the practical implementation and realisation of these values. While legislative acts and international commitments demonstrate a dedication to the ideals of freedom and human rights, the effectiveness of these measures requires critical examination. Scholars might explore the lived experiences of individuals within Saudi society, assessing the extent to which legal and policy frameworks translate into tangible freedoms and protections in everyday life. The exploration of freedom in the Saudi context within the framework of human rights demands a nuanced and critical examination. Legislative strides and international engagement signal a commitment to foundational principles, yet scholarly inquiry should focus on lived experiences, shedding light on the complexities and differences in the organisation of freedom (individuals'

freedom in processing their data). This study explores the preferences of individuals affiliated with universities concerning data security management, including their inclination to reduce the collection of personal data. Chapters 4 and 5 provide detailed insights into these preferences within the framework of personal data security system requirements.

1-8-1-3 The Value of Equality and Social Justice

The foundational principles of equality and social justice are indispensable components in the construction of a perfect society, where the equitable distribution of wealth, resources, and opportunities stands as a paramount objective. The broader scope of social justice includes the imperative of ensuring impartial access to protection, opportunities, and the active participation of diverse stakeholders in decision-making processes (Eberlin & Tatum, 2008). Tackling these issues is essential not only for achieving economic balance but also for fostering a socially equitable environment that upholds the principles of fairness and justice.

The anticipated challenges arising from technological advancements and the evolving landscape of work underscore the potential for heightened vulnerability and subsequent inequality (Yusuf, 2021). Particularly noteworthy is the emphasis on gender equality and the integration of women into the workforce, underlining the critical importance of addressing gender imbalances as a central societal priority (Saleh, 2020). The intersectionality of these challenges demands comprehensive scrutiny and strategic interventions to mitigate the potential adverse effects on societal equity. In Arab countries, pervasive conflicts often find their roots in discrimination and marginalisation based on regional, ethnic, sectarian, gender, or origin-based factors. The intricacies of these issues, entangled with regional, ethnic, and sectarian dimensions, underscore the complexity of the challenges faced. Despite reforms aimed at rectifying injustices and ensuring equal rights, persistent institutional, legal, and cultural discrimination persists. The imperative for achieving equal rights remains a foundational requirement for fostering sustainable social and political peace, necessitating ongoing scrutiny, evaluation, and adaptive policy measures (Yusuf, 2021).

Within the Saudi context, the legal systems, grounded in Islamic Sharia, expressly reject racism and mandate justice and equality as foundational governance principles. The prohibition of all forms of racial discrimination is enshrined in national systems, aligning with the comprehensive goals and programmes outlined in Saudi Vision 2030. This transformative initiative places a significant emphasis on principles of equality, tolerance, and moderation as fundamental columns of societal progress, reflecting a commitment to addressing historical imbalances and fostering a more equitable future (Alzuhair et al., 2022). An outcome arising from the overarching vision aimed at justice attainment manifests in legislative amendments favouring women to actualise principles of gender equality. Up to 2016, Saudi women were barred from partaking in activities such as driving automobiles, aspiring to autonomous lifestyles, and having employment opportunities on equal footing with their male counterparts. Despite governmental initiatives and regulatory modifications, resistance to these transformative measures persists within certain Saudi households (Pilotti et al., 2021).

1-8-2 Islamic Values

1-8-2-1 The Value of Morals and Ethics

The concept of politeness, as expounded in the Islamic context, carries profound significance, including a holistic integration of virtues in an individual's conduct. This multi-faceted approach signifies a commitment to refining not only external behaviours but also the internal aspects of an individual, constituting a foundational principle for the well-rounded maintenance of human character. In Islamic teachings, morality is a necessary quality, refining the logic, speech, and overall conduct of individuals for the purification of souls, and fostering outward and inward beauty. The emphasis on good manners in Islamic discourse aligns with the directive in the Quranic, wherein God praises the dealing of Prophet Muhammad with people, '**It is by mercy from Allah that you were gentle with them. Had you been rude, hard-hearted, they would have dispersed from around you'** (The Qur'an,3: 159). God describes the manners of Prophet Muhammad in another place, saying: **'And indeed, you**

are of a great moral character' (The Qur'an,4: 68).[1] The nature of Islamic etiquette is rooted in the religion's emphasis on high moral standards, encapsulated in wise commands, sound guidance, and profound directives. Islam recognises varied levels of politeness, differentiating, for instance, the etiquette with the state, parents, scholars, peers, and others. The diversity of etiquette extends to various aspects of daily life, including eating, drinking, travelling, speaking, and even silence (Al-Kaysi, 2015).

1-8-2-2 The Value of Asking for Permission

Islam, as a comprehensive moral and legal framework, places great emphasis on benevolence and ethical conduct to regulate relationships within the family, society, and among individuals. Central to these ethical guidelines is the concept of asking for permission, which serves to sanctify homes, protect personal privacy, and promote disciplined and right behaviour among Muslims. This value is intricately woven into the fabric of Islamic teachings to ensure secure, reassured, and content communities where rights are respected, and social bonds are strengthened. This practice of permission stems from a profound understanding that homes are sacred spaces requiring preservation and protection. Islam, in its intricate details, codifies the etiquette of asking permission to ensure its proper implementation. Key aspects include waiting for an explicit acceptance from the homeowner before entering. Islam emphasises restraint in door-knocking, limiting it to three times with a brief interval between each, and underlining the importance of returning if explicitly requested to do so. As stated in the holy Qur'an, asking permission to access houses **'And if you find no one in them, do not enter them until you are given permission. And if it is said to you, 'Turn back', then turn back. That is more proper for you. Allah is aware of what you do'** (The Qur'an,24: 28).[2] Islam not only recognises the right to seek permission but also extends its concern to protecting the human right to privacy. The legal underpinning for the sanctity of private life within Islamic jurisprudence is established through the explicit

[1] All quotes from the Holy Qur'an were taken from the English version of the Qur'an website. You can browse the website at the following link https://www.corequran.com.

[2] All quotes from the Holy Qur'an were taken from the English version of the Qur'an website. You can browse the website at the following link https://www.corequran.com.

prohibition of activities such as spying, mistrust, and backbiting. Islamic doctrine explicitly prohibits spying, aligning with the divine injunction found in the Qur'an**: ‘O you who believe! Avoid most suspicion—some suspicion is sinful. And do not spy, nor backbite one another’** (The Qur'an,49: 12).

1-8-2-3 The Value of Honesty and Integrity

Honesty is seen as a crucial moral quality in Islam, playing a big role in its ethical framework. The teachings of various divine religions and positive sects converge on the emphasis placed on the virtue of honesty, a principle that Islam specifically prioritises (Almutrajiy, 2021). Manifesting in both word and deed, honesty is a pervasive theme in the Qur'an, where believers are admonished to' **O you who believe! Be mindful of Allah, and be among the truthful'** (The Qur'an,9:119). This Islamic ethical paradigm extends beyond honesty alone and includes the broader concept of integrity. In its simplest form, integrity is construed as the antithesis of betrayal, signifying an individual's unwavering commitment to assigned tasks, executed without betrayal, corruption, or negligence (Clarke, 2012).

Integral to the fabric of Islamic values, integrity is regarded as instrumental in fostering societal strength across various domains, thereby contributing to comprehensive and sustainable development. Islam not only calls for honesty and integrity in individual conduct but also underscores their application in all aspects of life. Quranic verses, such as the injunction to return trusts to their rightful owners and to judge between people with justice, epitomize the divine mandate for upholding integrity (Guellouh, 2023). The profound link between trust and faith is further articulated by Prophet Muhammad, who stated, **‘He who has no trust has no faith’**. Aligning with these core Islamic principles, the Kingdom of SA, in 2011, established the Oversight and Anti-Corruption Authority. This institutional framework seeks to safeguard integrity, promote transparency, and combat corruption comprehensively, exemplifying a proactive commitment to Islamic ethical values.

The recent initiation of the ‘Nazaha/ Integrity’ project by the Authority signifies a strategic effort to enhance citizen-government collaboration, allowing for the reporting of suspicions or breaches, whether in real or virtual environments, as

part of the broader mission to reduce corruption within the nation (Nazaha, 2023). Of course, there are many Islamic values, but these three were highlighted because they are believed to be particularly relevant to the context of data security research. For instance, the practice of obtaining permission concerning others' property is a fundamental Islamic value ingrained in Muslim individuals' upbringing. This aligns with one of the key strategies in data security management, which is obtaining consent.

1-9 An Overview of the Higher Education System in SA

HE plays an essential role in shaping the cognitive and cultural landscape of any country, and SA is no exception. HEIs provide individuals with the knowledge, skills, and competencies necessary to succeed in building a decent professional life. By providing access to diverse academic disciplines and specialised fields of study, universities enable students to explore their interests, hone their talents, and realise their full potential. Moreover, HEIs cultivate critical thinking, creativity, and problem-solving abilities, equipping graduates with the intellectual agility to navigate challenges and contribute meaningfully to society. HEIs also provide services for the advancement of society, and this is highlighted by the roles played by their libraries and research centres in preserving the means of learning and developing solutions, alternatives, and technologies in all fields (Smith & Abouammoh, 2013).

Saudi universities serve as engines of innovation, fostering research and development initiatives that fuel technological advancements, enhance productivity, and stimulate industry innovation across various sectors. HE plays a crucial role in fostering social cohesion, national identity, and cultural enrichment in Saudi society. Academic institutions serve as vibrant hubs of intellectual exchange, cultural dialogue, and social interaction, bringing together individuals from diverse backgrounds and fostering mutual understanding and respect (Aburizaizah, 2022).

The establishment of the Ministry of Education in 1975 marked a significant milestone in the organisational structure and governance of the education sector in SA. Over the years, the sector has witnessed substantial growth, with the establishment of 30 governmental universities and 15 private universities.

These institutions are strategically distributed across various regions of SA, reflecting a concerted effort to expand access to HE nationwide (Ministry of Education, 2020). Despite their affiliation with the Ministry of Education, both governmental and private universities in SA operate with a considerable degree of administrative and academic autonomy. This autonomy allows these institutions to develop and implement policies, programmes, and initiatives tailored to their specific needs and priorities. Consequently, governmental and private universities exercise a significant degree of independence in matters pertaining to governance, curriculum development, faculty recruitment, and student affairs.

SA's commitment to providing free education for its citizens represents a significant investment in human capital development and socioeconomic progress. Free HE ensures that all eligible students, regardless of socioeconomic background, have equal access to academic opportunities. This promotes social mobility and enables talented individuals to pursue their educational aspirations without financial constraints. While free HE offers numerous benefits, its sustainability relies on adequate funding and resource allocation. Maintaining high academic standards and quality assurance mechanisms is essential to upholding the credibility and reputation of Saudi universities (Alkhazim, 2003). HE in SA has undergone remarkable transformations in recent decades witnessing a rapid expansion of its infrastructure and the establishment of new universities, colleges, and research institutions across the country. The government's substantial investment in building world-class campuses and academic facilities has significantly increased the capacity to accommodate a growing number of students seeking HE opportunities (Aburizaizah, 2022). However, this increase may create challenges for HEIs. HEIs gather a considerable volume of data, rendering them prime targets for cybercriminals, as evidenced by a study revealing that government and education sectors collectively accounted for approximately 71% of cyberattack targets (Alzahrani, 2020).

Although the Communication and Information Technology Commission identified electronic crimes in SA as including blackmailing, privacy violations, and unethical content (Alzahrani, 2020), there is a paucity of investigations into

data breach incidents within the country's HE sector. Universities face a range of cyber threats, including phishing attacks via emails and deceptive web pages aimed at extracting sensitive information like passwords or credit card details (Al-Sadhan, 2020). Furthermore, Jerry (2015) who examined the efficacy of information security programmes in HE institutions revealed that 39% of reported violations were attributed to piracy or malicious programmes such as viruses, worms, Trojan horses, bots, backdoors, spyware, rootkits, keyloggers, ransomware, and browser hijackers.

Understanding the contexts and realities of breaches for HEI is important. Therefore, this research focuses on investigating data breaches at two prominent Saudi universities: KSU and TaibahU. Both institutions, operating as nonprofit public entities, are officially recognised by the Ministry of Education of SA. They offer a diverse range of academic programmes spanning undergraduate, graduate, and doctoral levels across various disciplines. Upholding Islamic principles, KSU and TaibahU maintain segregated campuses for male and female students, aligning with cultural norms. Admission to these universities is selective, involving entrance examinations and evaluation of academic records. International applicants are also welcomed, provided they meet requisite criteria. Alongside academic offerings, both universities provide comprehensive support services, including library resources, residential facilities, sports amenities, financial aid, and study-abroad opportunities. Embracing modern pedagogical approaches, they offer online and distance learning programmes to cater to diverse student needs.

1-9-1 King Saud University (KSU)

KSU, founded in 1957, is dedicated to fostering leadership and excellence in education to cultivate a knowledge-based society. It is committed to delivering distinguished education and conducting innovative research that serves societal needs and contributes to the development of the knowledge economy. This is achieved by creating an engaging learning environment that fosters intellectual creativity, utilises technology effectively, and fosters strong local and global partnerships (KSU, 2023). The university has established strategic objectives to guide its aims, including promoting creativity and innovation in scientific research, ensuring excellence in academic programmes and their outcomes,

engaging in community service to enhance the quality of life, implementing effective governance mechanisms, enhancing the efficiency of human resources, developing internal revenue sources, diversifying investments and asset growth, and ensuring prudent financial management for sustainability. The university includes various deanships and scientific departments dedicated to enhancing educational services and fostering scientific excellence (KSU, 2024a).

Among these entities is the Deanship of Electronic Transactions, which plays a crucial role in managing data breaches and risks. This deanship is responsible for delivering electronic services to university sectors and employees, as well as developing the necessary infrastructure to support the educational process. Additionally, it offers innovative electronic services in networking and digital communications, operates a data centre for information preservation and classification, and provides technical support for academic and administrative equipment to facilitate educational and administrative operations (KSU, 2024b). Moreover, the Deanship of Electronic Transactions and Communications, particularly through its Risk and Information Security Unit, is tasked with securing and safeguarding the university's network and data. This involves implementing policies and procedures aligned with global information security standards and cybersecurity controls mandated by the National Cybersecurity Authority. The unit also ensures compliance with these policies, raises awareness of security issues among university employees through awareness bulletins in collaboration with the Cybersecurity Guidance Centre, and strives to achieve the vision outlined in SA 2030. The Deanship supervises various units, including public relations, development and quality (comprising beneficiary care and development and quality), e-learning (including e-learning and distance education, digital content, and electronic courses), applications and projects (including project coordination, electronic portal, and electronic services), technical affairs (incorporating data centre, network, risks and information security, and digital communications), operation and maintenance, administrative affairs, and financial affairs. To maintain alignment with leading information security policies and practices for ensuring a secure technical environment, the Deanship has instituted several policies. These include risk

and information security policies, which are categorised as follows (KSU, 2024c):

- Policy for Physical and Environmental Security.
- Policy for Social Networking Site Security.
- Cloud Computing Security Policy.
- Access Management Policy.
- User Agreement.
- Non-disclosure Agreement.
- Human Resources Security Policy.
- Information Security Policy.
- Information Security Awareness Policy.
- Commitment Policy.
- Access Control Policy.
- Password Policy.

Moreover, the Deanship administers additional policies concerning E-Learning and Distance Education, Networks, Electronic Portal, Data Centre, Beneficiary Care, and Digital Communications.

In 2022, KSU founded a Data Management Office in line with Ministry of Education Resolution No. 59036. The primary objective of this office is to develop an advanced data management system aimed at governing, digitising, investing in, classifying, making available, and safeguarding university data in alignment with the strategic directions of the institution and the developmental objectives of the state. The Data Management Office of the University undertakes various responsibilities, including the formulation of systems and policies for managing university data, monitoring compliance with data management policies, designing training and awareness initiatives, managing data sharing requests, compiling statistics and reports, and establishing information repositories.

Since its inception, the office has a high workload with significant goals, set, including the inventorying and cataloguing of the university's data assets, as well as the development of organisational policies, plans, procedures, and guidelines. Notably, the office has approved plans and policies about data

classification, open data initiatives, data integration and sharing, protection of personal data, data freedom, data modelling and structuring, privacy notices, open data licensing, safeguarding children's personal data, and regulations governing the transfer of data outside the SA. Furthermore, the office has also approved strategies for managing reference and master data, ensuring data quality, maintaining a data directory, leveraging data for value creation, implementing business intelligence and analytics, and establishing protocols for data storage and preservation.

Additionally, the Office has been involved in the preparation of records and agreements and has facilitated the creation of an open data platform for KSU. The office has managed the delivery of a series of training programmes covering topics such as data governance, cybersecurity protocols, content and document management, digital transformation, data sharing best practices, utilisation of the data directory, data classification policies, and personal data protection policies. These training initiatives have benefitted 100 participants from 25 entities within the university. Furthermore, the office has organised numerous workshops focused on data management and information governance (KSU, 2024d). (Additional contextual framing is provided in Chapter 3).

1-9-2 Taibah University (TaibahU)

TaibahU compared with KSU, was initially founded in 2004 as a solitary College of Education. The university has operated under a clear mission to contribute to the advancement of a society fostering sustainable development and knowledge-based economies. This mission is achieved through the delivery of distinguished education, qualitative research, and collaborative partnerships with the community within an environment conducive to learning and innovation. Despite its humble beginnings, TaibahU has expanded significantly, now comprising 28 colleges spanning diverse fields of knowledge, alongside numerous deanships, secondary institutes, research centres, and support centres. In alignment with the national Vision 2030 agenda, the university has recently formulated a series of strategic objectives aimed at enhancing teaching and learning excellence, advancing scientific research and graduate studies, fostering genuine societal partnerships, continuously refining administrative and

financial structures, diversifying revenue streams, and bolstering the university's local, regional, and global standing (Taibah University, 2021).

The Deanship of Information Technology and Digital Transformation plays an essential role at TaibahU, responsible for providing technical support and electronic services to both administrative and academic stakeholders. This includes overseeing all aspects of information technology operations, from communications and network infrastructure to facilitating electronic transactions and e-learning initiatives. Additionally, the deanship is charged with supervising the university's information technology-related affairs, including the provision of educational, administrative, and financial systems, and research information bases, as well as establishing network infrastructure, and central operating systems, and ensuring information security measures are in place. Moreover, the deanship actively promotes technical awareness among university staff through tailored training courses. Within the Deanship of Information Technology, various departments and units are operational, covering aspects such as systems development, administrative affairs, electronic transactions support, data management, performance evaluation, technical support, beneficiary care, infrastructure management, planning, quality assurance, and technical project management (Taibah University, 2024).

TaibahU has also committed to establishing a Data Management Office in compliance with Ministry of Education No. 59766, tasked with managing and digitising university data to align with strategic objectives and ensure protection through relevant policies and controls. However, only select regulations regarding open data are currently available on the office's website (Taibah University, 2024a).

TaibahU has established a specialised Cybersecurity Department tasked with the oversight and governance of information security protocols. This department is responsible for implementing comprehensive security frameworks, policies, and procedures aimed at safeguarding the technical and information assets of the university. It is entrusted with managing potential information security risks and threats through the application of preventive technical solutions.

Furthermore, the Cybersecurity Administration is responsible for monitoring the operational performance of information security technologies and systems deployed within the university, ensuring their continual updating and development to address emerging threats. To mitigate cyber risks and fortify the security posture of technical and information systems against internal and external threats, TaibahU has instituted several policies. These policies include cybersecurity protocols, guidelines for the acceptable use of assets, and policies governing access and permissions management. These measures are implemented to uphold the confidentiality, integrity, and availability of information assets across the university's infrastructure (Taibah University, 2024b). (Chapter 3 provides additional context about the university).

Summary

This chapter introduced the general data security landscape in the Saudi context. It began by outlining the primary objective of examining the landscape of digital data breaches in HE organisations in SA and the societal and cultural context. This foundational chapter unifies this information on SA for the first time and is in itself a beneficial contribution for those wishing to undertake other studies regarding digital/data security in SA.

In terms of the legislative and regulatory landscape, the introductory section reviewed some information written in official government documents sourced from authoritative entities responsible for overseeing data security, such as the NCA, the SDAIA, and the CST. Special emphasis is placed on the NDMO at SDAIA, tasked with supervising data management and security across institutions in SA. This information explains data protection regulations such as PDPL and the national framework for data governance and protection in the country.

While the consideration of organisational dimensions is imperative for ensuring robust data security, the social aspect assumes a significant role in influencing the acceptance of administrative directives by both individuals and society at large. Consequently, it became essential to present a concise overview of prevalent social values. Therefore, values such as citizenship, freedom, equality, and social justice were presented. The presentation of these values

was required because of social and cultural constraints associated with this research methodology, as well as considerations regarding access to research subjects, particularly influenced by factors such as gender. The introduction also detailed key Islamic values as they form the foundation of legislation in SA. Islamic values such as ethics, asking for permission, honesty, and integrity were chosen due to their direct relevance to the principles of the information security systems.

Finally, the chapter provided a general overview of the two universities featured in the study, (KSU, and TaibahU), setting the stage for the subsequent detailed analysis and discussions in the following chapters. The next chapter, which is the literature review chapter, helps to develop the broader research landscape this work builds on. This frames the research by identifying gaps in existing literature.

Chapter 2: Literature Review

Introduction:

This mixed-method case study aims to investigate data breaches in Saudi HE, employing a comprehensive approach from different stakeholder perspectives, including students, faculty members, and managers. The objective of the academic literature review is to present a thorough critical synthesis, focusing specifically on the Saudi context and providing insights into data breaches on a global scale. It supports the design, delivery and analysis of the study's findings. Given the study's emphasis on Saudi universities, the academic literature encompasses scientific papers published in both Arabic and English. The initial search focused on peer-reviewed academic articles. To manage the wealth of information, a theoretical framework was developed, encompassing key facets identified as centrally significant to the core research question (Pickard, 2013).

This chapter of the literature review is structured to comprehensively explore various insights into digital data breaches and their causes/risks and impacts. It begins with an introduction, followed by an overview of data breaches. The subsequent section discusses technical risks, which include data breach levels, data breach types, and IT infrastructure and risks. The chapter then examines the gaps in organisational data risk, covering the lack of data security policies and processes, and human risk factors. It further examines organisational impact, addressing both reputational impacts and financial impacts. The review also explores personal impacts, particularly emotional impacts, and social data impacts.

Finally, the chapter concludes with a discussion on risk mitigation strategies, offering insights into addressing and reducing these risks. It is necessary to acknowledge that these headings were formulated based on the wealth of available sources, facilitating critical analysis within the literature. Figure 2 shows a concept map of the literature review that was developed to set out the critical lenses for the overarching landscape.

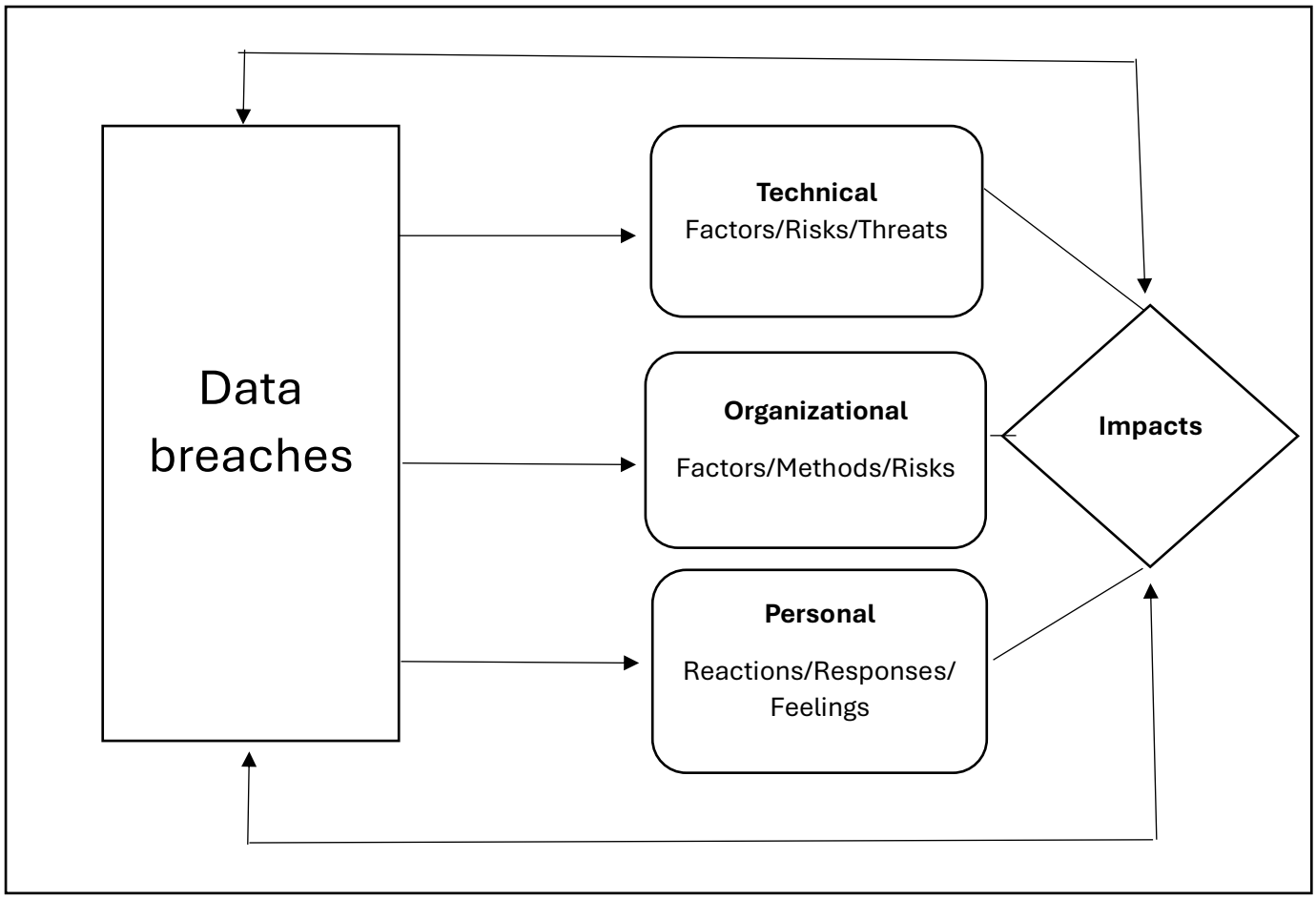

Figure 2 The concept map of the literature review

The collection of articles was predominantly sourced from prominent academic databases such as ProQuest Central, EBSCO, SAGE, SCOPUS, and databases accessible through the Saudi Library. The search strategy involved utilising specific keywords, including data breach, data security, educational data breaches, data protection, data security strategy, data security systems, cyber-attacks, cybercrime, data crime, data theft, individual privacy, personal data, university data, and Saudi data security. The data extraction process was based on various codifications, including authorship field, study objectives, geographical location, publication year, participants, key findings, and limitations. This rigorous review aimed to discern prevailing trends, patterns, and interrelationships within the academic literature, while also identifying existing gaps in Saudi research literature. The initial search yielded a

substantial number of papers, subsequently refined through sorting, and the resulting count is detailed in Table 2. These papers include types such as articles, books, reports, conference papers, and theses published by official channels within both the UCL and Saudi libraries.

Number of papers retrieved at initial searching						230
Number of papers removed after screening						63
Number of papers nominated for inclusion after the initial scanning						167
Number of papers excluded after intensive reading						18
Including Paper Numbers						149
Journal Articles	Website	Books	Reports	Conference Papers	Thesis	Total
107	20	4	4	7	7	137 sources
English 127				Arabic 22		

Table 2 The number of papers identified from the literature search

In addition, Table 3 shows that 20 websites have been incorporated into the literature review, including reports and news disseminated on these websites. The rationale for the inclusion of such sources is substantiated by the inherent value of the information they provide, as elucidated below:

- Official news sites: data breaches garner public attention, prompting official news sites such as the BBC to furnish real-time and comprehensive information about these incidents.
- Data protection institutions: entities tasked with overseeing data protection, such as the Information Commissioner's Office (ICO) and the Ministry of Communications and Information Technology (CST), routinely publish statistics and information on violations through their official websites.
- University publications: universities themselves contribute to publishing information regarding specific breaches, such as the University of Maine's communication of noteworthy incidents.
- Organisations specialising in data security; entities dedicated to data security, such as IBM Security, serve as valuable sources of information. These organisations often house a cadre of experts in the field of information security and publish annual reports.

Website	Description	Location
Venafi	Private cyber security company.	United States
BBC	News Service	United Kingdom
Modern Healthcare	News magazine	United States
College Consensus	A ranking site for colleges	United States
TitanHQ	Software company	Ireland
IBM Security	Private security consulting company	United States
ICO	UK's Information Commissioner's Office site	United Kingdom
CST	SA's Ministry of Communications and Information Technology site.	Saudi Arabia
NCSC	UK's National Cyber Security Centre site	United Kingdom
-	The world university rankings site of Times	United Kingdom
PRC	Privacy Rights Clearinghouse A non-profit organisation for privacy protection.	United States
The Economic	Newspaper	Saudi Arabia
University of Maine	A university site	United States

Table 3 A list of websites included in the literature search

Boolean searches constituted the methodological approach employed in this research, facilitating an exploration of the interplay between terms within the context of HE. Combinations of terms, utilising logical operators (such as 'or', 'and', and 'not'), were strategically employed to both refine and broaden the scope as dictated by the research objectives. The keywords and potential combinations implemented were as follows:

- Data breach: data security OR data crime OR cybercrime OR data theft OR cyber-attacks OR computer crime OR personal data threats OR attacks OR risks.
- HE institutions: university OR college OR higher learning OR educational provider OR educational unit OR academia.

- Emotional impacts/ effects: anxiety OR fear OR shock OR trauma OR depression OR frustration OR anger OR privacy concerns.
- Organisational impacts/ effects: operational OR policies OR strategies OR procedures OR regulations OR data AND Information.

The chain-searching strategy was employed to expand the research scope, particularly in the exploration of Arabic resources. The exhaustive review encompassed diverse perspectives on data breaches across international contexts, aiming to conduct a comprehensive examination of the existing literature and identify potential gaps in prior studies.

Data and information security is a rich topic, which is discussed and analysed across various disciplines, e.g., computer science, economics, and business. Articles were included according to the availability of academic research in the sector and its compatibility with the educational context. Some articles were selected due to their objective value in bridging the gaps in the educational sector. For instance, it was challenging to find investigations or classifications for types of data breaches specific to Arabic data security literature. To achieve coherence and address these gaps, the researcher adopted the classification systems used in other contexts, such as the UK (ICO, 2021) and the US (PRC, 2021). The main inclusion criteria are focused on the multidimensional risks and impacts of data breaches in the context of HE. The detailed inclusion criteria for the search are:

- ✓ Academic studies that describe the multidimensional impacts of data breaches or cyberattacks whether in education or other sectors to bridge the gaps.
- ✓ Academic papers that studied technical/ organisational/ personal risks of data security.
- ✓ Academic articles, reports, theses, conference papers, or websites that discuss the topic.
- ✓ The Saudi context is a primary consideration.
- ✓ The UK's context, the US's context, and other broader geographic contexts to enrich the review.
- ✓ Papers published in English and Arabic.

However, some of the retrieved articles were not included after reviewing their contents, such as the following papers:

- Studies that examined data security in an independent environment such as libraries.
- Articles that examined legal issues and data protection laws.
- Studies that focused on data security in terms of intellectual property, digital records
- Studies that focus on specific elements of data security management such as quality, digital rights

The flowchart illustrates the practical steps for conducting this review, starting from the research step to writing. This chart was developed based on (Creswell & Creswell, 2018, p.23) Instructions.

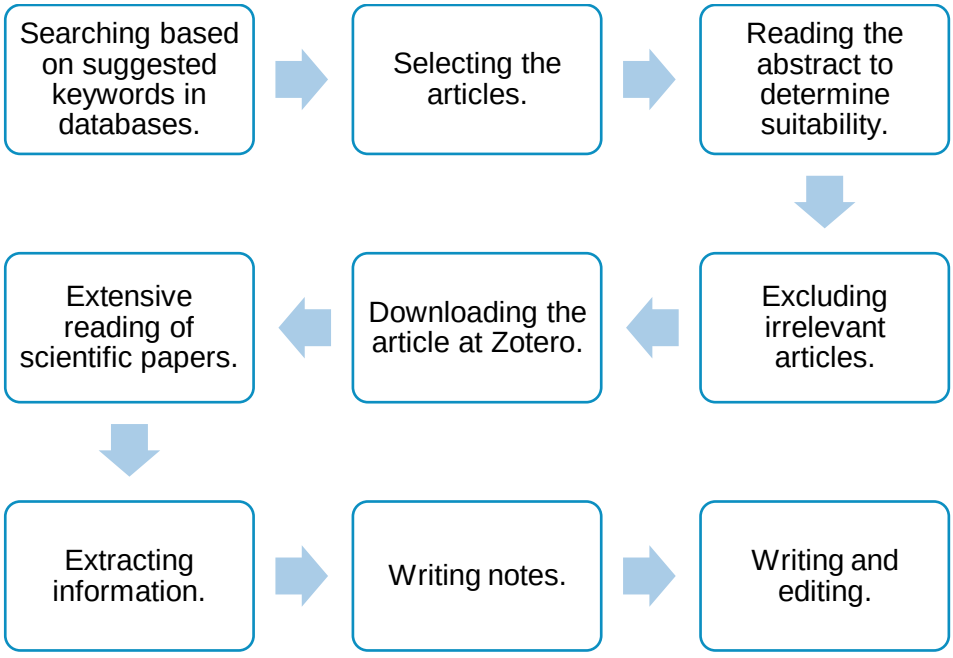

Figure 3 The literature review process flow

Through this approach to the literature gathering, it has been possible to categorise the literature gathered into an initial understanding of the nature and range of breaches across sectors and countries, the infrastructure that surrounds and influences the likelihood of breaches or exposure to data breaches, the broader organisational contexts, and impacts and then the human contextual considerations and impacts at play. It is to be noted that in

categorising and considering these issues, there are not always hard boundaries in the studies and realities of these issues where risk is at play.

2-1 Data Breaches

Data breaches affect individuals and threaten the survival of the organisation (Ayereby, 2018). These breaches take the form of attacks aimed at revealing the information stored across an organisation (Hassanzadeh et al., 2019). The literature has provided many definitions of the term ‘data breach’, which refers to the unintentional release of secure or personal/confidential information (Guha & Indurkar, 2020). Such sensitive, protected or confidential data may include personal health information, personally identifiable information, trade secrets, intellectual property and personal financial data (Sen & Borle, 2015). In this context, the focus will be on personal data stored in the organisation's databases and systems.

Within the General Data Protection Act in the UK (GDPR, 2021), the term ‘personal data’ in Article 4(1) is defined as 'any information relating to an identified or identifiable natural person who can be identified, directly or indirectly' in addition the term ‘personal data breach’ in Article 4(12) is defined to ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’. Veltsos (2012) also defined a data breach as information for distinguishing and tracing someone by data, such as name, address, SSN, date of birth, place of birth, parents' full names, and biometric records. The term ‘personal data’ is a broad term, and therefore, it must be noted that personal data breaches may involve ‘identity theft‘ as organisations collect Personally Identifiable Information (PII) about individuals. Whilst there are personal information and identity theft incidents that might result from non-technology channels such as lost or stolen wallets (Bisogni & Asghari, 2020), this work seeks to focus on digital breaches specifically.

Accordingly, this review will consider the data breaches and cyberattacks that organisations are exposed to. Cyberattacks are a global phenomenon. In the Saudi context, Alqurashi (2020) stated that the government administration in

SA was hacked by a succession of massive cyberattacks[3], which hindered the governmental operations temporarily. For example, in 2013, a source on the Ministry of Interior declared that several government websites in SA were sabotaged in a series of cyberattacks, disabling them for a short period until the attacks were repelled, including the website of the Interior Ministry, which was disabled by receiving a 'huge amount' of requests for service. However, it returned to work after less than two hours (Staff, 2013).

Another SA attack was reported by Al Amro (2017) who announced that the Saudi Ministry of Foreign Affairs was attacked and that this had led to the leak of essential and significant documents. He stated that this attack was caused by transmitting documents via e-mail. It is to be noted that not all attacks become public knowledge and as such there is not a complete picture of the range and nature of attacks in SA, not indeed globally.

2-2 Technical Risk

The assessment of technical risk is systematically structured into three critical sections. The first section, data breach levels, highlights the varying levels of data breaches across different countries. This section underscores the need for a deeper scientific understanding of the synergies, similarities, and differences in breach experiences globally. The second section, data breach types, explores extensive literature on the types of data breaches, categorising them by the nature of the breach or the targeted organisation. This section emphasises the various forms of attacks and risk exposures discussed in the literature. Finally, the third section, IT infrastructure and risk, examines the crucial role of IT infrastructure in an organisation's data security. It discusses

[3] In Al-Qurashi's study (2020), the author used the following terms 'cyberattack ', 'cybercrime', 'computer crime', He does not provide a specific definition of cyberattack. However it seems from the content of his paper, that Cyberattack is as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing infrastructure; or destroying the integrity of the data or stealing controlled information (CSRC, 2021) .

the vulnerabilities that arise from reliance on technology and the importance of robust IT infrastructure management in reducing security incidents.

2-2-1 Data Breach Levels

While some studies have been carried out on examining the landscape of data breaches (Garrison, 2010; Chapman, 2019), there is very little scientific understanding of the synergies, similarities, and differences of breaches between countries. However, the IBM Security Report (2020) offers some insight. The report's data was collected from 3,200 interviews in 524 organisations that experienced data breaches between 2019 and 2020 in 17 countries across the world. That report pointed out that the levels of attack vary from country to country, and sector to sector with different types of attacks dominating in different contexts. However, there is no strong explanation for the causes of the discrepancy, whether due to the varying levels of awareness of data security, protection systems, infrastructure, or reporting incidents. Table 4 below indicates the dominant types of attacks at the regional level.

Region	Attack level		Attack dominated type	Low attack type
	2019	2020		
Europe	21%	31%	Ransomware.	Hardware/software misconfiguration.
North America	44%	27%	Ransomware.	Credential theft.
Asia-Pacific	22%	25%	Data theft and leak.	Insider.
Central and South America	5%	9%	Business email compromise BEC tied with ransomware.	Fraud.
Middle East and Africa	7%	8%	Data theft and leak.	Hardware/software misconfiguration.

Table 4 The levels and types of attack by regions worldwide. The table contains data provided by the IPM report (IBM Security, 2021)

Based on the above statistics, there was an increase in the average of attack levels in all regions outside of North America between 2019 and 2020. It was also noticed that Europe, North America, and Central and South America experienced more ransomware events than Asia-Pacific, the Middle East, and Africa. Data theft and leaks, on the other hand, did significantly impact Asia-Pacific, the Middle East, and Africa. The report does not provide information about the reasons for the difference in attack levels, but it indicates that Middle Eastern countries, including SA, did suffer data breaches and leaks. It can be posited that there will be different cyber warfare and criminal factors at play, but no definitive data is publicly available from the SA perspective. As noted in this report and the wider literature, the levels of attacks may vary from place to place since the data security landscape is different everywhere. However, it should

be noted that there have been attacks on the HE sector. As an illustration, some universities in the United Kingdom, the United States, and Canada were attacked in 2019 by a ransomware programme that came through from Blackbaud. This is a cloud computing provider that provides education, fundraising, and financial management programmes. Indeed, the attack directly affected current and former students, as the stolen data included phone numbers, a history of donations, and information about events attended (BBC, 2020).

The outcomes and impacts of this event are not yet fully known. However, it can be inferred that educational institutions may be exposed to a breach of their data and information systems both directly and through third parties. This review seeks to further explore the range and nature of data breaches.

2-2-2 Data Breach Types

There has been a significant literature in research and practice focusing on the types of data breaches that occur (Collins et al., 2011; Posey & Ncube,2011; Holtfreter & Harrington, 2015; Hammouchi et al., 2019; Al-Mulhim et al., 2020). Some of these pieces of literature have classified data breaches based on the type of breach or the type of organisation against whom the breach is committed. Within this context, the literature has focused most typically on forms of attacks (risk exposures are further discussed within the later parts of this literature review).

Regarding the breach type, internationally, Hammouchi et al., (2019) provided an in-depth analysis of data breach types and trends in order to identify the most attacked sectors. They analysed approximately 12 billion records that were archived from 2005 to 2018 on the Privacy Rights Clearinghouse (PRC)[4] in the United States (US). The authors divided data breach types into various categories in accordance with the PRC classification, including unintended disclosure, hacking or malware, payment card fraud, insider, physical loss, portable device (lost or stolen), stationary device loss, and unknown. The following table provides definitions of the eight types of data breaches.

[4] Privacy Rights Clearinghouse (PRC) considers a non-profit organization in the USA for protecting privacy established in 1992 (PRC, 2021)

Source	Author's Methodology	Breach type	Type's definition	Effects according to the study
Hammouchi et al.,2019)	An analysis of over 9000 data breaches.	Unintended disclosure	It refers to posting sensitive information publicly to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax (PRC, 2021).	Financial and technical impact.
		Hacking or malware	It refers to hacking by an outside party or malware (PRC, 2021).	
		Payment card fraud	It means fraud resulting from debit and credit Cards (PRC, 2021).	
		Insider	It refers to insiders whether employees, contractors or customers (PRC, 2021).	
(Collins et al., 2011)	Description and observation using the Bayesian system.	Physical loss,	Paper documents that are lost, discarded or stolen (PRC, 2021).	Financial impacts
		Portable device (lost or stolen)	Involving any lost, discarded or stolen laptop, PDA, smartphone, memory stick, CD, hard drive, and data tape (PRC, 2021).	
		Stationary device Loss	Stationary Computer Loss includes lost, inappropriately accessed, discarded or stolen computers or servers not designed for mobility (PRC, 2021).	

Table 5 Definitions of data breach types

Collins et al., (2011) investigated these previous eight types of data breaches in the educational sector to assess the state of organisational data breaches within the US. Surprisingly, the authors found that seven of these previous types occurred in the educational environment in different proportions, except payment card fraud. They confirmed that the most common types of breaches that occurred in educational entities based on the available data were hacking or malware attacks, the unintended disclosure of information, and the theft or loss of a stationary device. Based on the data provided by Collins et al, payment card fraud was not identified in the educational sector. This may be due to the objective and methodological limitations of the study, as it focused on analysing incidents of data breaches reported in one place (Privacy Rights Clearinghouse (PRC)), limited by a certain period between 2005 to 2010, and conducted in a specific geographical location (US). Nevertheless, some universities confirmed payment card fraud incidents. In Lona College, for instance, an employee used stolen College credit card data for personal purchases estimated to total more than £525,000 (Parr, 2013). Hence, all eight types of data breaches are and might be experienced within universities.

According to the organisation type, Holtfreter and Harrington (2015) have sorted data breaches based on the organisation's type, whether financial and insurance services, businesses – retail/merchant, business – other, government and military, non-profit, educational institutions, and healthcare. Classifying data breaches according to the type of organisation provides information about the nature of targeted data, the level of data security in sectors and the present and potential impacts. For instance, Hammouchi et al., (2019) identify that the government and military data are targeted due to their security value, albeit that the strength of their protection systems makes this data difficult to attack compared with other sectors. However, military data is not entirely safe from breaches. For example, the BBC (2021) reported that the UK Ministry of Defense suffered a data leak which revealed the identities of 250 Afghan interpreters who were seeking relocation to the UK. According to the report, the data was sent by email and contained personal data, such as names, contact details, email addresses and victims' pictures. Based on the report, it is clear that this data leak might well have jeopardised the lives of translators still

living in Afghanistan. This incident shows that regardless of the type of sector, its importance and the sensitivity of its data and information, all institutions may experience data breaches. Nevertheless, such incidents may be rare in certain institutions and frequent in others depending upon their organisational type.

To explain further, a research study analysing data breaches reported in the US over five years from 2005 to 2009 and relating to six different sectors, including business, education, military, finance, government, and medicine, highlighted that there is a great difference in the number of data breach incidents according to the type of institution. In this context, the education sector had the largest number of penetration incidents. To illustrate, about 32.63% of breaches occurred in education, 19.43 % in business, 19.32% in government, 15.95 % in medical, 6.44 % in the military, and 6.23% in financial (Garrison & Ncube, 2011). Within this context, it was assumed that the reason for the high number of attacks on the HE sector was due to the production of valuable research data (Roman, 2014 cited in Bongiovanni, 2019; Chapman, 2019; Redscan Research, 2020).

Each unique type of data breach has a distinct and different level of impact on the organisation. A data breach in all forms is likely to affect the confidentiality and integrity of the data stored in the organisation's information systems. For example, malware and phishing may lead to data being lost, stolen, or damaged (McClurg,2015). Surprisingly, Hammouchi et al., (2019) indicated that the hacking or malware category represents a significant proportion of data breaches that occurred in HE based on an analysis of 9,000 breached records to determine the type of organisation. According to Edwards et al., (2016), the types of data breaches naturally fall into two groups, including breaches arising through ‘negligence’, such as loss of data and devices, and breaches arising through ‘malicious’ activities, such as attackers hacking into systems. Through analysing a dataset containing 2,253 breach incidents that span over a decade (2005 to 2015), they found that negligent breaches occur nearly twice as often as malicious breaches. However, malicious activities, as Atrews (2020) has argued, create gaps that can lead to damage to the security system and generate particular political or financial effects. An example from the SA context, Al-Mulhim et al., (2020) confirmed that Aramco, which is a Saudi oil company

that provides global services, was exposed to a virus in 2012; consequently, 75% of the company's data was destroyed and erased.

Further literature explores the relationship between organisational types and the breach types by investigating five types of breaches: exposed, hacker, insider, missing, and stolen. ‘Exposed’ means data that is publicly unprotected, and exposed either through email, over the Internet, or through disposal. ‘Hacker’ involves the unauthorised intrusion of systems and devices. ‘Insider’ refers to the accessibility to the data by employees or former employees. ‘Missing’ refers to data loss in the form of disks, files, computers, and servers, while ‘Stolen’ includes hardware and hard drive thefts. They found that educational institutions experienced the highest number of hacker, exposed, and stolen incidents; this may be attributable to the type /number of individuals who have access to sensitive data (Garrison & Ncube, 2011).

Beaudin (2017) identified different types of data breaches that occur in HE institutions, including hacking, physical theft, and vendors. It is likely that the author relied on this classification based on the source of the breach, either technical ‘hacks’, physical ‘thefts’, or operational ‘vendors’ which provided data management and storage services. In 2016, an example of hacking was the human resources information system at the University of Virginia, which was compromised by a phishing email, resulting in the disclosure of employees’ personal data.

Concerning the theft, in 2015 at the University of Maine, the laptop computer and media card used by a faculty member were stolen, which resulted in the exposure of the personal information of 941 students. These students' information included names, social security numbers, phone numbers, email addresses, grade data and course information (University of Maine, 2015). Thus, the theft of computers belonging to educational institutions is considered a form of physical theft that may lead to a data breach. Vendors are referred to in this context as a type of data breach, which refers to breaches that result from external dealings with vendors. As the author explained, some universities process, store and manage their data on the site by contracting with a third-party data supplier (which has been covered earlier as an added exposure).

The author demonstrated that the contracts concluded between the university and the third party include basic elements of protection such as the identification of personal information, the required level of security, data protection provisions, procedures in place for the detection and prevention of data breaches, a plan to respond to a data breach, the parties authorised to view the data. The author also presented an example of what happened at Southern New Hampshire University, the University's database was hacked, with more than 140,000 of the breach records becoming exposed (Beaudin, 2017).

The existing literature on data breach types has centred on global trends and specific sectors such as education, government, and healthcare in Western nations like the US and UK. Researchers like Hammouchi et al. (2019) and Collins et al. (2011) have extensively analysed datasets to categorise breaches into types such as hacking, malware, insider threats, and physical theft, typically within specific geographical or organisational contexts. However, there exists a notable gap in understanding data breach types within regions characterised by unique regulatory frameworks, cultural contexts, and distinct cybersecurity challenges, such as SA. The table below illustrates different types of breaches that happened in HE institutions as defined by the literature.

Source	Author's Methodology	Affected university	Breach type	Type's definition	Effects according to the study
(Beaudin, 2017)	Undefined	The University of Virginia (2016)	Hacking	It refers to illegal access to data, and it tends to be the most common data breach trend in HE(Beaudin, 2017., P 38).	- Unauthorised disclosure of data. -Institutional reputation -Financial costs
		The University of Maine, (2015).	Physical Theft	Physical theft of laptops, desktop computers, portable electronic devices such as smartphones, or hard drives(Beaudin, 2017., P 39).	
		Southern New Hampshire University (2015)	Vendors	Accidents that result from a third-party vendor (Beaudin, 2017., P 40).	
(McClurg, 2015)	A QUAL-Quan methodology. Questionnaire. Semi-structured interviews with Chief Information Officers and IT Officers in two universities in the US.	Unknown	Malware.	Software that is intended to damage or disable computers and computer systems (Kaspersky, 2015; McClurg, 2015)	Not specified
(Garrison & Ncube, 2011).	Analytical approach / The group of institutions, including educational in the US.	Undefined	Exposed	Unprotected data that may be publicly accessible via e-mail, regular mail, online and through disposal.	Not specified
			Hacker	It means unauthorised access to computers by cyber criminals.	
			Insider	The misuse of access/authority of computer usage by an employee.	
			Missing	Missing disks, files, hard drives, flash drives, tapes, laptops, computers, and servers.	
			Stolen	Stolen hardware like desktop computers, laptops, servers, drives etc...	

Table 6 Types of data breaches in educational institutions.

2-2-3 IT Infrastructure and Risk

Data is one of an organisation's most important assets. The risk of losing control over data reflects a serious problem that affects everyone (Juma'h & Alnsour, 2020). The heavy reliance on technology in organisations always creates the potential for both old and new technical vulnerabilities that may facilitate the occurrence of data breaches. These have been indicated in the forms of data breaches that occur. However, it is important to consider this within the picture of the technical landscape. The most prominent of these gaps is the lack of IT infrastructure. Although IT infrastructure can be seen as a strength, failure to manage each of its components is a weakness. The success of the organisation

in cyber data protection depends largely on the IT infrastructure used within the organisation. In addition, good management of the IT infrastructure reduces near-misses and the number of actual security incidents and their impacts (Irfandhi et al., 2016).

In the Saudi context, surprisingly, Al-Shanbari (1998) indicated that there is a lack of information systems infrastructure in Saudi HE. This includes financing, computer workstations, network expertise, appropriate computer applications, and information databases, which could mainly affect the processing of data and information. Al-Shanbari also emphasised that by comparing the infrastructures in SA and the United Kingdom UK, communication and information processing is a greater problem in SA than in the UK. HE in SA faces many challenges that are not limited to the information technology infrastructure but also challenges in the traditional infrastructure (Facilities and University Buildings). Al-Shanbari's work was referenced in this literature review to illuminate historical issues concerning the information systems infrastructure in Saudi HE. The current study examines whether these challenges related to infrastructure persist today.

When Alshammari (2017) examined, in his study, the challenges facing the university administration in Saudi universities from the perspectives of academic and administrative leaders. He stressed that Saudi universities have challenges within the traditional infrastructure, such as incomplete infrastructure suitable for administration and university work, inadequate specifications of existing facilities to support the educational process, outdated buildings and laboratories, and a lack of safety, maintenance and control requirements. However, Sheikha (2015) explained the weaknesses of the traditional infrastructure in Saudi HE as there has been a numerical focus driving the abrupt and quick establishment of universities in an unplanned manner, which has resulted in administrative confusion and a lack of operational infrastructure. Reference is made to the traditional infrastructure in order to obtain a clear picture of the resources in the Saudi environment and data management. It is not necessarily the presence of weaknesses in the traditional architecture that leads to a data breach. Indeed, the modern information technology infrastructure can expose data to greater risks. To

clarify, Kacha and Zitouni (2017) stated that there are many issues associated with data security in cloud infrastructure, such as loss of control over data, confidentiality and data integrity risks. Nevertheless, institutions use the same 'classic' solutions that are used in traditional data protection infrastructure, such as 'access control'.

Alaqla (2010) indicated that there are efforts being made in the SA to provide the infrastructure for information technology to adopt e-learning and electronic management in a secure environment with cybersecurity protections. Despite these efforts, there are still some challenges faced. Alsadhan (2015) has listed the difficulties facing the implementation of the e-learning system at Shaqra University from the point of view of specialists, and one of these difficulties was the weak infrastructure and the lack of regular maintenance services for devices. Similarly, AlAtiwi (2010) stressed that Saudi universities need to develop the information technology infrastructure, as they face a challenge in how to integrate information technology into the educational environment and ensure its continuity, review, and update. AlAwdah (2021) stated that the technical obstacles to the application of electronic administration in the General Administration of Education in Al-Ahsa in SA could be the threats to websites, risks of creating/ preserving/ protecting data, and poor communication infrastructure.

Alkhudary et al. (2020) conducted a comparative study between Saudi universities to verify the levels of cybersecurity and stressed that the cybersecurity risks in Saudi universities are focused on technical factors such as the lack of adequate protection programmes, which may lead to data destruction risks. In contrast, Alotaibi and Almufeez (2021) conducted a study to evaluate the level of information technology governance at Taif University using the Kuwait scale. They argued that information technology at the university provides critical governance dimensions, including the information infrastructure.

There is no one clear picture of this landscape. Denning (1999) divided the risks of technical failure into two main categories, which are systems threats (the lack of system functionality), and data threats (the loss of data integrity and

confidentiality). Similarly, Dillon and Paté-Cornell (2005) stressed the need to identify the technical risks to both data and information systems, which include: the unavailability of the system; the inability of the user to access it; loss of confidentiality of data; and loss of server integrity, which refers to improper data corruption or incorrect data or files added. They also suggested a set of developmental alternatives to enhance data and information security in organisations. For example, adopting additional firewalls, software operating system alternatives, different hardware configurations for multiple servers with rebooting, encryption tools, and detection systems, upgraded development and maintenance processes (including additional code reviews), further training, and automated software updates.

Organisations tend to link their control systems with commercial office software. Connecting reliable organisational systems with non-secure software, whether in a server or operating system, such as (Windows XP or Vista), or applications running on them (e.g., Office or PowerPoint), helps attackers to identify vulnerabilities in such programmes for hacking data (Perrow, 2011). Although this integration between the organisation's systems and commercial software provides advantages, it also raises several security issues. First, there is often insufficient knowledge among the organisation's IT experts about the interactions between the systems and programmes. Second, the safety of Commercial Off-The-Shelf (COTS) software in computers may be compromised, leading to cybersecurity errors that make the systems vulnerable to deliberate attacks

In HE institutions, Liu et al. (2020) argued that having clear management to regulate the interaction between information systems and technology in cyberspace may ensure that those systems and software can effectively address data breaches. They also claimed that IT personnel in universities often struggle to understand how IT subsystems interact with each other and how security risks are interconnected. Consequently, the ability to respond to cybersecurity issues is reduced in a more heterogeneous computing environment.

Regarding network risks, Dillon and Paté-Cornell (2005) confirmed that one of the serious technical impacts of breaches is the disruption of data and information systems both in current and future contexts. They suggested a framework designed to reduce the risks of different types of information systems failure. They also discussed three types of technical effects of disruption of university web servers, including low-impact technical faults that take seconds to resolve, medium-impact, which takes minutes, and high-impact, which takes hours to diagnose and resolve. These risks are not limited to only the disruption of web servers, but also extend to the risk of transmission and virtual storage of data, as many academic institutions have tended to use cloud services in storing and transmitting their data. As such, there are many risks to the process of data transmission and storage in the cloud storage system. Zhe et al. (2017) identified the security risks of storing data on the cloud, including data transmission risk, data storage risk, and cloud terminal risk.

Concerning the best strategies for data management, in a technical report published in 2018 by the UK National Cyber Security Centre (NCSC), there are 14 principles for guaranteeing cloud security: data in transit protection, asset protection and resilience, separation between users, governance framework, operational security, personnel security, secure development, supply chain security, secure user management, identity and authentication, external interface protection, secure service administration, audit information for users, and secure use of the service (NCSC, 2018).

Overall, there is a general agreement about the necessity of having the appropriate data technology infrastructure to manage and protect data (AlAtiwi, 2010; Irfandhi et al. 2016; AlOtaibi & AlMufeez 2021). Most studies in the Saudi context have only focused on investigating the IT infrastructure in some fields, e.g., E-learning and E-management (Al-Shanbari,1998; Alsadhan, 2015; AlAwdah, 2021). It has been argued that there is a pressing necessity for upgrading modern infrastructure across all sectors in SA, not limited to education (Alzahrani, 2020). Some research has discussed cybersecurity risks in Saudi HE institutions (Alkhudary et al., 2020), but extensive research has not been carried out on data breaches. Internationally, there is an examination of

the technical risks of data breaches, and their impact on systems (Perrow, 2011), networks (Dillon & Paté-Cornell, 2005), and data (Denning,1999). What is not yet clear is the impact of technical breaches on individuals in HE institutions. Also, although organisations need to provide adequate systems, programmes, and networks, they need to harness them to manage data and ensure its security and integrity (Ahmad et al., 2005). This indicates that software risks are not the biggest concerns in data management, as there are other elements that also play a role in data protection. That is what will be discussed in the following section.

In summary, the literature review emphasises the critical importance of robust information technology (IT) infrastructure in safeguarding data within organisations, particularly in Saudi HE. Historical perspectives, such as those by Al-Shanbari (1998), highlight enduring challenges like inadequate financing, limited expertise, and outdated facilities that continue to impact data processing and information management. Despite efforts to enhance the IT infrastructure for e-learning and administrative purposes (Alaqla, 2010; Alsadhan, 2015), significant gaps persist, including cybersecurity vulnerabilities (Alkhudary et al., 2020). However, there remains a need to understand individuals' perspectives regarding the risks and impacts of technical breaches within HE in SA, which this research aims to explore.

2-3 Organisational Data Risk

Information security is a major component in the planning and management of modern organisations (Chang & Ho, 2006). Within the HE sector, there is, as noted, a lot of data collected for the management of a university and the delivery of its research and education offerings. Increasingly, HE institutions rely heavily on information technology because of the learning environments where technology has acted as an enabler. However, the increased use of technology may lead to more security threats (Joshi & Singh, 2017). The term information management (IM) is generally understood to mean managing operations and systems associated with obtaining, organising, storing, distributing and using information (Detlor,2010). Information management in organisations involves managing a variety of information resources, ranging from data to information (Baltzan, Phillips, & Detlor, 2008; cited in Detlor, 2010).

Singh et al., (2014) identified several factors of organisational information security management (ISM), involving top management support, information security policy, training, information security awareness, security culture, information security audit, information security management best practices, asset management, security incident management, and security regulations compliance. Organisations consider these factors of data and information security to avoid organisational risks. Jourdan (2010) mentioned that the organisational information security risks are: human errors, espionage or trespass, extortion, vandalism, theft, software attacks, natural risks, quality of service deviations from providers, hardware errors, software failures, and technical obsolescence risks.

2-3-1 Lack of Data Security Policies and Processes

Universities need to put in place policies that promote the best security measures, as Fulford and Doherty (2003) stated that the information security policy should cover several areas including personal usage of information systems, disclosure of information, physical security, violations and breaches, viruses, worms, trojans, system access control, mobile computing, internet access, software development, encryption, and contingency planning. Furthermore, the data and information security policy may be designed in different forms. For illustration, a previous study examined university policy content critically in eight countries, including The United States, the United Kingdom, Australia, Canada, New Zealand, Hong Kong, Ireland, and South Africa. This study indicates that organisations could adopt one of three different principal forms of information security policy formulation. The first structure is to establish one comprehensive information security policy, containing detailed coverage of data security management issues and risks. The second way is to create a series of inter-related, cross-referenced, policies: (e.g., separate system, product, community, and corporate information policies). The third form is to create an information security policy, supported by several relevant guidelines and procedures, each guideline referring to a single specific part of security (Doherty et al., 2009).

The information security policy is considered essential for the success of information security in organisations. It represents an effective way to confront

breaches, make the organisation's workflow based on systematic institutional thinking, and limit individual errors. However, there are many factors that affect the activation of the data security policy. Sohrabi Safa et al. (2016) investigated different factors that influence information security organisational policy compliance. They asserted that information security knowledge sharing, collaboration, intervention, and experience have a significant impact on employees' attitudes towards compliance with organisational information security policies, except for attachment to the organisation.

The higher the cybercrime rates, the greater the value of security awareness and policy compliance. This point has been examined by Rajab and Eydgahi (2019), who argue that if HE employees perceive a lack of control over their information infrastructure and recognise that it is frequently targeted by daily attacks, their likelihood of complying with information security policies increases. This suggests a direct correlation between perceived vulnerability and adherence to security protocols. Moreover, Rajab and Eydgahi (2019) highlight that employees with higher levels of skills, confidence, and ability to respond to information security risks—such as phishing, unauthorised access, and infected files—are more inclined to comply with these policies.

In the Saudi HE framework, there is still a need to educate employees on correct practices that ensure the integrity and confidentiality of data. A research study was conducted to examine the extent of information security awareness of faculty members in Saudi universities through a case study of 'Majmaah University'. In that study, it was found that although the faculty members have an awareness of the fundamentals of information security, there are some harmful practices that may lead to a significant breach of privacy, such as opening messages and files that arrive through email from an unknown source or exchanging private passwords with colleagues (Al Omran, 2011).

Similarly, in Australia, researchers revealed that HEI employees were surprisingly lacking in security awareness, as more than half of respondents had unclear knowledge about the information security policy (Chan & Mubarak, 2012). On the contrary, a comparative study exploring information security awareness showed that employees at the University of Salford in the UK are

familiar with the university's information systems security policy and related information systems legislation in the United Kingdom (Marks & Rezgui, 2009). It is likely that the previous findings support the idea that compliance with information security policies differs between geographical contexts due to different laws, regulations, cultures, levels of awareness, and levels of risk.

Data and information security policies are not only limited to the commitment of the employees, but they also require the commitment of the universities themselves to the regulations and policies as stipulated, especially regarding data storage, transfer, destruction, etc. Universities store massive amounts of personal data that are identified, transferred, and accessed (Mukthar & Sultan, 2017). All colleges and universities hold data assets, and over the years, this data may become a heavy burden, thus universities decide to take measures to reduce this burden, either by replacing the data storage media with more capabilities or by getting rid of what is old.

Generally, it is noticeable that many institutions or organisations in developing societies are trying to keep pace with the technological development and growth associated with data security and protection, but there is still a clear deficiency and a great shortage, especially in establishing security regulations and forming the personnel who can supervise and monitor the data security policy (Abu-Taieh et al., 2018). Regarding data security professionals, a case study at King Abdulaziz University in SA, to identify the reality of information security, confirmed that the university is keen to provide a policy for information security and update it periodically, and is interested in developing training courses in the field of information security. However, it was noticed that the staff and users did not comply with the information security policy. As the university’s Information Security Department lacks an adequate number of professional workers in information security, most of the administration’s employees are not specialists in information security (Asel & Al-Aifan, 2014). The information security policy is being adopted on the organisation's needs and is linked to the risks by the concerned organisation. Users must understand the security policy and adhere to its application. Therefore, the current research focuses on exploring weaknesses and risks from both administrative staff and individual (students and faculty) perspectives, which are crucial for effective information

security policy implementation. There is a significant gap in understanding detailed views and concerns in Saudi HE. Al-Ghathar and Al-Subaih (2012) identified five elements that represent information security concerns in Saudi organisations in their study, which aimed to measure the state of application of information security in Saudi institutions as follows:

A. Failure to adhere to information security standards in the organisation.
B. The lack of specialised information security workers in the organisation.
C. Lack of adequate data protection practices.
D. Absence of good practices in choosing passwords.
E. Lack of financial support dedicated to information security.

According to these concerns, information security within Saudi institutions upholds five priorities: anti-virus programmes, firewalls, data loss prevention, user identity verification, and network access control. However, widely, in the absence of information security chiefs specialised in managing data security, keeping up with administrative and technological developments becomes meaningless, and it is difficult to achieve security quality and ensure the availability of international standards (Karanja, 2017).

Accordingly, it must be reiterated that information security is not only a technical matter that can be corrected and overcome by installing a firewall and protection software, but it also represents an administrative act. The workforce and other parties must acknowledge receipt of the information security policy report, pledge to apply the principles and standards it contains and accept strict measures in the event of failure to do so. For example, based on a case study of information security policy at Polytechnic University in Palestine, the researcher recommended several measures that decision-makers in universities should take into account in the information security policy, including (Saheb, 2013):

A. Establishing an administrative unit concerned with electronic information security.
B. Editing an information security document that includes a set of appropriate instructions and laws.

C. Educating staff, faculty members, and students about the importance of information security.
D. Providing the necessary equipment and software.
E. Providing training courses in the field of information security.

Literature indicates significant regional variation in security awareness and policy adherence, with developing countries often lacking in security regulations and specialised personnel (Al Omran, 2011; Chan & Mubarak, 2012; Marks & Rezgui, 2009; Abu-Taieh et al., 2018). Compliance with security policies is influenced by factors such as employee skill levels (Sohrabi Safa et al., 2016; Rajab & Eydgahi, 2019). In SA, persistent issues include inadequate policy compliance, insufficient specialised workers, and limited financial support for data protection (Al-Ghathar & Al-Subaih, 2012). Despite efforts to develop and update security policies, a gap remains in understanding the detailed views and concerns of individuals within Saudi HE (Asel & Al-Aifan, 2014).

This research aimed to investigate vulnerabilities and risks to data security from both managerial and individual perspectives within Saudi HE, providing a thorough insight into information security challenges. By examining the viewpoints of administrative staff and end-users (students and faculty), this study aimed to uncover participants' expectations regarding their personal data protection. Conducting research that prioritises beneficiaries' perspectives is crucial for developing targeted strategies aimed at enhancing data protection and compliance with regulatory standards.

2-3-2 Human Technological Linked Risk Factors

The human factor is a powerful element in supporting and delivering on the security process in any institution, as well as undermining the process if there is not a positive human focus on information and cyber security as areas of concern. Organisations allocate huge budgets and acquire the latest software to provide full protection against cyber-attacks (Dillon & Paté-Cornell, 2005). They also develop measures and policies to provide information security and disseminate these regulations and processes among employees to ensure roles and responsibilities are clear (Arutyunov, 2017). However, the highest levels of security are not achieved unless each individual is actively aware of

their role and responsibilities within the security system. Unfortunately, there are some poor practices that threaten data security, as some information security incidents are related to human errors and human behaviours (Evans et al., 2019a ; Evans et al., 2019b).

Password exchange is the most common weak practice among Saudi HE employees since passwords represent an individual activity for each user, defining the employee's authority in a standardised way. Although passwords are usually applied to control access to information systems, very few employees are aware enough of password security and the fact that passwords should not be shared with others. In her examination of information security at Qassim University in SA, Alsheety (2014) confirmed the common use and exchange of passwords among users of the university's information system, whereby 48.6 % of participants reported that this risk may happen every month. The spread of this practice among university employees can lead to a breach of the security of data and information systems (Al Omran, 2011).

The international context shows that organisations use multi-factor authentication techniques as an additional solution to enhance data security. multi-factor authentication (MFA) creates multiple verification layers to verify a user's identity in addition to the password with targeted individual checks (Bhargav-Spantzel et al., 2007). Although this mechanism greatly enhances security, the same cannot be said about users' acceptance of these security tools where choices are in place (Das, 2020).

From the Saudi general perspective, Abu Musa (2004) discussed the risks that threaten the security of data and information in Saudi organisations and indicated that the biggest security risks relevant to human actions involve the intentional and unintentional introduction of incorrect data by employees, the sharing of passwords among employees, and unauthorised data disclosure. By contrast, globally, Hughes-Lartey et al., (2021) analysed data breach incidents attributed to human error and reported in the United States from 2009 to 2017. They found that data loss, improper disposal, unauthorised access or disclosure, and hacking may occur through human failures. They identified that

employees share protected information with unauthorised persons, browse malicious websites, open spam, and click on malicious links.

The causes of human errors have been considered in the literature. According to Carlton and Levy (2015), users' errors in IT range between 72% and 95% of security threats to organisations due to poor cybersecurity skills. Badie and Lashkari (2012) also highlighted that security accidents linked to human behaviour could arise from factors such as a lack of awareness, insufficient motivation to follow security procedures, risky beliefs, dangerous behaviour, improper use of technology, and pressures associated with workload. Metalidou et al., (2014) examined five of these human factors in the higher education sector, including inadequate motivation, employee beliefs, behaviours, lack of understanding of potential attacks, and improper use of technology. They found that all five human factors were significantly correlated with a lack of awareness. An important factor that has not been fully explored in higher education, even in previous studies, is workload and stress. Many human errors result from insufficient time to detect and correct mistakes, as well as the repetitive nature of tasks (Evans et al., 2019b). Table 7 provides examples of data breaches primarily caused by human error in the educational sector

Date	Affected university	Country	Breach	Source
February 2019	University of Washington	US	Almost 1 M personal health records from the Medicine department were exposed due to internal human error.	(Olenick, 2019; (Bongiovanni, 2019).
June 2014	Riverside Community College District	US	Data of over 30,000 students were exposed by an employee who emailed records via a non-secure system to an incorrect email address.	(Hunt, 2021)
July 2014	Park Hill School District	US	A former employee accessed over 10,000 sensitive student and employee data. subsequently, the data was inadvertently published on the Internet.	(Hunt, 2021)
August 2018	Strathmore College	Australia	An employee at Strathmore College accidentally published more than 300 students' records on the school's intranet.	(Bisson, 2020)
February 2018	Pennsylvania Department of Education	Pennsylvania	With the misassigned permissions, an administrative employee is allowed to access the personal information of 360,000 current and retired teachers for users.	(Bisson, 2020)
May 2019	Oregon State University	US	Personal identifiable information (PII) of 636 students and their families were compromised due to an employee falling prey to a phishing scam.	(Clark, 2019)
December 2018	University of Connecticut	US	The personal data of 326,000 patients were compromised from employees' emails.	(Cohen, 2019)

Table 7 Data breach cases caused by human errors.

From the previous table, it is evident that a significant number of data breaches in higher education (HE) are attributed to human errors. However, there are no examples of human errors found in the Saudi context due to the lack of sources that investigate data security incidents caused by such errors. As the table shows, a single instance of human error can have a substantial impact on a large number of individuals. For instance, a single human error led to a data breach involving nearly a million records at the University of Washington, affecting almost a million individuals (Bongiovanni, 2019). An employee should not be held accountable if they have not received the relevant training. Al-Dunaibat et al. (2020) pointed out that employees in Saudi universities (included in their study) acknowledged that they had not received any data security training upon being hired. Training in information security at universities was often limited to staff within the Information Technology (IT) department, rather than extending to all employees. This lack of comprehensive training helps explain the weak practices mentioned earlier.

Furthermore, a lack of knowledge in handling various technological risks represents a key obstacle to providing cybersecurity in SA, as the greater technological advancement, the greater the diversity of attackers' strategies (Alqahtani, 2019). Numerous studies have examined data and information security awareness among staff and students and found that there is a significant need to enhance their skills regarding data security (Marks & Rezgui, 2009; Chan & Mubarak, 2012; Yerby & Floyd, 2018; Al-Qahtani, 2019).

By way of illustration, a study was conducted to examine employees' behaviour concerning data and information security in King Saud University Hospitals. The study showed that the application of information security among hospital staff posed high levels of threats to patient data privacy and confidentiality (Albarrak, 2011). Nadim (2014) also surveyed the awareness of female faculty members in Saudi universities to identify security issues when using social media websites. The study indicated that approximately 12.8% of Saudi academics had been exposed to privacy violation incidents on social media apps. Additionally, 69.8 % of participants were not checking the privacy settings of the social sites. Furthermore, an investigation of 2,325 participants, examining the awareness of information security among undergraduate students in SA,

revealed a lack of awareness of basic information security. The study showed that 92% of the participants had not received any kind of security training (Alzahrani & Alomar, 2016). Areishi and Aldossary (2018) claimed that HE institutions need to adopt a set of roles to raise awareness of information and data security. These roles include educating individuals about the dangers of information crimes and how to deal with them. They conducted the study on three universities in SA: King Saud University, Princess Noura University, and Imam Muhammad bin Saud University, to assess the role of HE institutions in promoting awareness of information and data security.

In summary, despite significant investments in technology and policies, effective data security remains elusive without active human awareness and adherence to security protocols (Dillon & Paté-Cornell, 2005; Arutyunov, 2017). Human errors, such as password sharing and inadequate security practices, continue to pose substantial risks in educational settings, as evidenced by studies on Saudi universities (Al-Sheety, 2014; Al Omran, 2011). Moreover, global analyses highlight the prevalence of data breaches stemming from human error, emphasising the need for enhanced awareness and training across educational institutions (Hughes-Lartey et al., 2021; Carlton & Levy, 2015; Badie & Lashkari, 2012). However, existing literature on data security in Saudi HE lacks a comprehensive exploration of factors such as workload-related stress and the adequacy of training programmes, which significantly influence human error rates (Evans et al., 2019b; Al-Dunaibat et al., 2020). Hence, an important goal of this study is to explore the perspectives of students, faculty members, and managers on the causes of data breaches and the potential links between vulnerabilities in the data security system and human actions.

2-4 Organisational Impact

It has been mentioned earlier that data breaches affect individuals emotionally, such as their feeling of anger reflected by posting negative messages on social media about the organisation. These reactions can affect the reputation of the organisation negatively. Hence, institutions afford many costs to enhance the reputational aspects. What is not clear yet is how organisations can change the previous attitudinal outcome as I think the change in general attitude might lead

to a change in behaviours. I previously stated that organisations use multiple strategies to mitigate the effects of data breach incidents, such as deterrence, compensation, etc. Nevertheless, organisations not only face the burden of the breach, but they also bear the consequences of the breach. Therefore, it is necessary to review the reputational and financial effects of data breaches on organisations to create a comprehensive picture of the implications and organisations' responses to these impacts.

2-4-1 Reputational Impacts

Despite the increase in the number of emerging universities in SA, students are enrolled in universities of great and distinguished reputation, and this is reflected in their first choice to enrol in reputable universities (Alshammari, 2017). Reputation is not only an attractive element for individuals but also for institutions, as institutions (Abu Musa, 2004), especially institutions of HE (Areishi & Al-Dossary, 2018), are keen to confront data and information security threats in order to preserve their reputation. Al Shelash, (2020) analysed the strengths, weaknesses, opportunities, and threats, in his study that examined the reality of competitive advantages in Saudi universities and colleges to achieve comprehensive quality and strategic planning. The researcher suggested applying remedial strategies to improve competitive advantages in universities, for example, improving academic and administrative reputation to attract students. and defensive strategies using its resources (human and technical), reputation and prestige to reduce external threats that will affect it. The reputation of universities can be affected by data breaches. According to Chapman (2019), although university incidents are not massive enough to attract media attention, they have consequences that affect the reputation of universities and trust in their data security measures. Reputational consequences are the loss of alumni donations, research grants, or partners, or a drop in student applicants (Ulven & Wangen, 2021b). This is fully consistent with Hewitt et al., (2019) report aims to measure students' opinions about data security in the UK HE institutions, which showed that 65% of respondents asserted that the university’s weak security reputation affects their decisions to enrol it.

In general, organisations are keen to build an exemplary reputation in the environment in which they operate (Haleblian et al., 2017). Of course, the company's reputation and market value will be significantly affected if it is exposed to a data breach. Wang and Johnson (2018) stressed that the effects of data breaches quickly turn into a crisis for companies in terms of protecting their reputation during and after the data breach incident. They reviewed three strategies that help mitigate the impact of reputational damage, which are denial, diminish, and rebuild. in more detail, (denial) through using a scapegoating strategy or denying the existence of the crisis, (diminish) by minimising the impact of breaches and the organisation's responsibility, (rebuild) by providing compensation or apologies for the breach.

However, using any of the above strategies should be done deliberately, as Coombs et al., (2016) have found increased reputational damage and stakeholder anger if the organisation denies responsibility for the crisis in the event that it is later found to be responsible for the breach. Specifically, an analysis of Twitter posts conducted by Syed and Dhillon (2015) examining the information security reputation (ISR) dimensions of organisations indicated that 48% of tweet content condemns organisations for data breaches. However, Bentley and Ma (2020) found that (rebuilding) by apologising and providing compensation for data breaches has significant reputational implications for the compromised organisation and can positively impact future purchase intentions.

IMPACT		Reputational impacts		
Focus area	**Source**	**Methods**	**Location**	**Field**
Social Media Data Breach	Syed and Dhillon (2015)	Analysis of Twitter postings.	Unspecific	Cybersecurity
Crisis Management	Coombs et al., (2016)	Undefined	US	Industry
Management	(Haleblian et al., 2017)	Quantitative research	Unspecific	Industry
Data Breach Mitigation	Wang and Johnson, (2018)	Case study	US	Industry
Cybersecurity Risks	(Ulven and Wangen, 2021a)	A review	General	Higher education
Data Breach crisis.	Bentley & Ma, (2020)	Online experiment	Unspecific	Industry

Table 8 Summary of studies that discussed the reputational impacts of data breaches.

2-4-2 Financial Impacts

In HE, although universities spend their budget on investing in data security, they bear a responsibility to protect data in the event of damage in the open environment (Joshi & Singh, 2017b). As a fine result of such costs, the University of Greenwich had to pay £120,000 for holding data on an unsecured server (Chapman, 2019). According to the BBC report (2018) the personal data of 19,500 staff and students were affected by a hacking breach in 2016. Noting that the University of Greenwich was also attacked by a previous attack in 2013, Curtis (2018) claimed that the hackers used the same vulnerability to access the university web server. However, the cost of data security penalties varies from country to country unless there is standard regulation (Ishii & Komukai, 2016).Therefore, determining the value of costs, whether on security or breaches, varies based on the regulations in force in the country. Kim (2017) stated that the more rising of cyber threats, the more awareness and funding for better prevention and security.

Another report examining students' priorities for protecting their personal data indicated that 83% of students think that protecting passport photos or their contact details is very important (Hewitt et al., 2019). While universities deal with third parties, such as banks, training companies, etc. Rationally, these parties perhaps have the authority to access the personal data of university employees and students (McClurg, 2015).

According to Silverman (2007), institutions should contract with third parties that hold the same practices and procedures to ensure data security whenever personal information is disclosed. Additionally, according to the Data Protection Act (DPA) in the UK, the process of personal data management needs to consider some requirements concerning its security, storage, and destruction (Jenkins & Potter, 2007). The following table summarises some examples of data breaches in universities with their costs.

Institution	Affected records	Breach date	Estimated cost	Country	Source
University of Hawai'i	90,000	from 2009 to 2011	$550,000	USA	(Beaudin, 2017)
University of Greenwich	3,500.	2016	£120,000	UK	(Chapman, 2019)
Washington State University	Unspecified.	2017	$4.7 million	USA	('Essential Guide to Higher Education Data Breaches', 2021)
South & City College Birmingham	It was undefined yet but the college has around 13,000 students.	2021	Unspecified, but the settlement will be approximately £3,500	UK	(South & City College Birmingham, 2021)

Table 9 Examples of data breach costs in universities.

In general, the literature shows no consensus on the financial costs of data breaches conclusively, as the determination of the actual cost relies on several factors including the extent of the damage, the type of breach, the amount of data breached, etc (Acquisti et al., 2006). Fowler (2016) debated how to prepare for data breaches, and categorised the financial implications of data breaches in organisations into direct effects (costs of managing the breach), indirect effects (costs of time and effort), and systemic costs (costs of breach evaluation). Davidoff (2019) discussed the impact of payment card data breaches on various parties, including consumers, banks, payment processors, merchants, and card brands. The author argued that both banks and merchants reduced their data breach costs by increasing product prices and transaction fees, which affects the consumer negatively. Moreover, Angelis and Miller (2020) discussed the financial impacts of data breaches on organisations, they showed that the cost of a lost or stolen record costs roughly $200 i.e., 141-pound sterling per record. Although it is difficult to determine the costs of data breaches, there is some effort in estimating the costs of breaches (MCIT, 2013; Riek et al., 2016; IBM, 2019). The table below illustrates the average total cost of a data breach by country or region estimated by the IBM report which

analysed a sample of data breaches in various fields, including education breaches (IBM Security, 2020).

Region	The average total cost of a data breach	
	Measured in US$	Measured in the Local Currency
United States	$8.64 million	8.64 million US$
Middle East	$6.52 million	24.251.786 Riyal
Canada	$4.50 million	5.639.265 CA Dollar
Germany	$4.45 million	3.750.215 Euro
Japan	$4.19 million	460.288.260 Japanese yen
France	$4.01 million	3.378.976 Euro
United Kingdom	$3.90 million	2.820.252 GBP
Italy	$3.19 million	2.687654 Euro
South Korea	$3.12 million	3.609.434.400 KRW
Asian	$2.71 million	3.637.158 Singapore Dollar
Australia	$2.15 million	2.890.320 AU Dollar
India	$2.00 million	146.231.800 INR
Turkey	$1.77 million	14.662.149 Turkish Lira

Table 10 The average total cost of a data breach by region was published by the IBM security report.

2-5 Personal Impacts

Some studies have indicated universities are exposed to breaches due to the nature of their possession of rich data resources (Gupta & Sharman, 2012; Aliyu et al., 2020). Borgman (2018) reviewed two unique types of data collected by universities. The first is research data, which includes scientific and critical data collected by universities within the framework of the research field. The second is grey data, consists of personal, academic, administrative, and educational data related to individuals that universities collect for operational purposes, whether for education, libraries, travel, health, student services, and others. The author stressed that regardless of the type of data, universities bear four responsibilities towards that data: supervision and governance, protection of privacy, academic freedom, and intellectual property. Universities are also interested in providing open data for all (Zubcoff et al., 2016). Students, academics, staff, and visitors regularly access university IT infrastructures to use data (Bongiovanni, 2019). Thus, it is necessary to intensify the process of data security (Ulven & Wangen, 2021a). Due to this widespread use of university systems and the value of their data, exploring the implications of data

breaches in the educational setting is considered significant. Below, it will review below how much data breaches affect individuals and organisations.

2-5-1 Emotional Impacts

The literature has focused on covering the financial and administrative consequences of data breaches on universities, such as the costs of providing a secure environment for data and the costs of mitigating their breaches (Malavet, 2017). However, individuals' feelings that might arise after experiencing a breach such as the effects of trust and loyalty are often overlooked. It is potential, as Angelis and Miller (2020) argued these impacts are very nebulous. Hence, investigating these unstudied effects on individuals is significant, as they are the ultimate victims of data breach effects when their data is breached (Coffey, 2019).

Trust is an example of one of these emotional impacts, Bilgic et al., (2019) stated that although building trust is an emotional process linked to feelings of security and protection, this significant emotional aspect is often overlooked in security studies. Zhang and Gupta (2018) also argued that there are strong relationships between issues of security and trustworthiness, which need to be addressed urgently. In this review, trust can be defined as a stakeholder's expectation that the organisation will deal with integrity and reliability towards them (Morgan & Hunt, 1994). Trust is created by two components, a cognitive element dependent upon the consumer's knowledge of the organisation and its capabilities, and the emotional element, which represents the emotional bond between individuals and their institutions that strengthens over time (Dowell et al., 2015). HE institutions are keen to achieve trustworthiness, as Penberthy (2020) investigated the effectiveness of several strategies that universities undertake to reform students' confidence levels after violating their privacy. He emphasised that the best way to repair students' confidence is for HEIs to apologise for breaching student data. Given the competition between universities, a data breach may affect students' or staff's confidence in the university. Although this point is not clear in the educational sector, it is common in the industry sector. A study conducted to establish the effects of data breaches on commercial companies' trustworthiness indicated that even if companies are surrounded by security and have confidence in their safety, data

breaches negatively affect consumers' confidence who are dealing with the company (Curtis et al., 2018).

The greater the confidence in security methods, the fewer privacy concerns individuals might have. Pirim et al., (2008) revealed that individuals in academia whether they were faculty staff or students, perceive a high need for security and data privacy. They aim to control the dissemination of their confidential data by releasing the information to parties who achieve a high level of trust, or a low expectation of misuse. Therefore, the authors argued that if an individual feels a high need for privacy, their need for security should also be high.

Padyab and Ståhlbröst (2018) studied the factors affecting users' perceptions of privacy concerns regarding Internet of Things (IoT) use situations and found that despite the importance of the developments in the field of the IoT, researchers know little about individuals' thoughts and feelings about privacy issues in the IoT. Therefore, they advocated for developing ways that should be found to alleviate concerns arising from data mining and analytical practices applied to individuals' data collected via IoT devices. In SA, the adoption of big data in Saudi universities revealed several security concerns, especially in protecting the personal data of individuals (Ahmed, 2005).

Moreover, Alhubaishy and Aljuhani (2021) examined the challenges hindering the success of digital services in Saudi universities and showed that the fear of change resulting from privacy concerns is one of the factors that hinder students and teachers from adopting digital services. Additionally, Mollick (2006) investigated the effects of privacy and security concerns on students' feelings of alienation resulting from their university's wrong practices regarding errors in data and access to personal data, by surveying 187 students at a large U.S. University. The study results revealed that students' concerns about data collection and the use of the collected data by their universities strengthen their feelings of alienation toward their university. They also stated that alienation related to privacy concerns could affect the extent of the student's cooperation with the university and their identity as a member of the university community.

The alienation that arises from these threats may affect the academic level of students, as Muhammed (2000) discussed psychological alienation and its

relationship to creativity among university students. He stated that the feeling of alienation can be accompanied by multiple negative feelings such as lack of belonging, aggression, and anxiety. He concluded that alienation cannot be removed, but it can be mitigated and transformed into positive energy. Furthermore, a research study examined the university brand prestige in HE institutions and students' supportive behaviours towards the university and showed that students who strongly identify with the university engage in positive behaviours for university improvement due to their trust, loyalty and satisfaction (Heffernan et al., 2018).

Regardless of the sector of the institution, research indicates that the impacts of data breaches are significant on individuals (Sen & Borle, 2015; Coffey, 2019). These impacts from a cybersecurity perspective, refer to the consequences that come after breaches (NICCS, 2021). Agrafiotis et al., (2018) argued that psychological damage is the most common type of damage, where individuals feel various negative feelings after the leakage of their data and information, including confusion, discomfort, frustration, and anxiety. They emphasised that determining the extent of the damage depends on the environment in which the attack was carried out. Similarly, Bada and Nurse (2020) pointed out that the psychological impact of cyber-attacks can be understood through the extent of the social impact, referred to as a social disorder. These social and psychological effects include aspects such as anxiety, anger, depression, and loss of confidence in cybersecurity. They also argued that information security behaviours, for example, avoiding opening an anonymous email, necessitate individuals to make daily decisions that may cause anxiety. Elhai and Hall (2016) examined anxiety and stress resulting from electronic data breaches by exploring anxiety in response to ten specific types of hacking incidents, including IM interception, email hacking, cloud storage account hacking, social media account hacking, personal information being posted by others on the internet, sensitive photos being posted by others, theft of internet account passwords, financial account hacking, computer/phone access, and GPS tracking without permission. They stated that the sample reported significantly more anxiety from most electronic data breaches compared to resting anxiety.

Labrecque et al., (2021) explored the impact of stress and perceptions of social contract violation on consumer protection behaviours after a data breach. They demonstrated that stress positively impacts consumers to spread negative word of mouth (WOM) on social media, switch to another business, and practice consumer protective measures such as complaining. Additionally, Cheung-Blunden et al.,(2019) investigated the feelings of individuals in terms of anxiety and fear caused by cyber threats. They found that although fear may not make individuals gravitate towards vigilance and cybersecurity monitoring, anxiety may attract individuals to seek cybersecurity solutions. However, they emphasised that there is no significant difference between fear and anxiety functionally in motivating toward Information Security protection. On the other hand, some individual effects, such as anger, are difficult to mitigate. For example, Chatterjee et al., (2019) examined consumers' consumers' reactions to the information scope (the number of people affected by a data breach) by focusing on two unique emotions: fear and anger. They discovered that fear makes stock market reactions sensitive to the scope of a data breach, while anger makes stock market reactions insensitive to the scope of a data breach.

In more detail, fear and anger elicit very different cognitive assessments. Fear affects consumers by decreasing their purchasing intentions, though it can be reduced by using appropriate mitigation strategies. However, mitigation strategies do not change the feelings of angry individuals, nor do they alter their assessment of the situation (data breach). The researchers also recommended further studies to measure the impact of data breaches, given that individuals experience a variety of emotions, such as surprise. This highlights the need to explore the impact of trauma as an emotional response of individuals after experiencing a data breach. While few studies have addressed cyber risks and recovery from trauma in the digital world, they often focus on violence, digital abuse, and cyberbullying (Hamby et al., 2018; Paat & Markham, 2021). From the broad scope of data breach impacts, regardless of the sector type, the emotional effects can be summarised in the following table:

SOURCE	IMPACT	Study's field	Impact investigation focus
(Labrecque et al., 2021)	Stress	Industry	Essentially
(Elhai & Hall, 2016)	Anxiety	General	Essentially
(Paat & Markham, 2021)	Trauma or shock	Internet crimes	Narratively
(Malavet,2017)	Trust	Education	Unessentially
(Angelis & Miller,2020)	Trust, Loyalty	Industry	Unessentially
Pirim et al.,(2008)	Privacy Concerns	Education	Unessentially
(Padyab &Stohlbrost, 2018)	Privacy Concerns	General	Essentially
(Mollick,2006)	Feeling of Alienation	Education	Essentially
(Abdelbaset, 2015)	Feeling of Alienation	Education	Essentially
Agrafiotis et al., (2018)	Complex emotions Confusion, Discomfort, Frustration, and Anxiety.	Cybersecurity	Unessentially
(Bada & Nurse, 2020)	Complex emotions Anxiety, Anger, Depression, and Loss of Confidence	Cybersecurity	Essentially
(Cheung-Blunden et al., 2019)	Anxiety and Fear	Cybersecurity	Essentially
(Chatterjee et al., 2019)	Fear and Anger	Industry	Essentially

Table 11 Emotional impacts of data breaches.

It can be observed from the previous table that the emotional impacts of individuals were investigated if they were exposed to a risk affecting their personal data. There has been interest in discussing these feelings in industry, given the important role that individuals (customers) play in the economic system. Researchers investigated individuals' emotional responses by focusing essentially on specific emotions such as anxiety or focusing on narrating the effects without directly investigating them (i.e., non-essential treatment) (Agrafiotis et al., 2018).

The reviewed studies have examined emotional responses following a data breach in two primary ways: by focusing on a single behavioural reaction, such as anxiety (Elhai & Hall, 2016), or by analysing multiple behavioural reactions, such as fear and anger (Chatterjee et al., 2019). In the context of HE, research has primarily explored behavioural and attitudinal outcomes such as feelings of alienation, privacy concerns, and trust issues. However, the scope of current

studies does not fully address all actual and potential behavioural responses. Therefore, a comprehensive exploration of these emotional effects is essential to understand the broader impact of data breaches on individuals.

2- 6 Social Data Impact

Navigating through the literature on social risks associated with personal data breaches in SA has proven challenging, with a predominant focus on investigating the goals, motives, effects, and awareness levels of information crimes within the societal context. Alghadyan (2018) conducted a comprehensive study, examining the manifestations of electronic blackmail crimes, their underlying motives, and the ensuing psychological repercussions from diverse perspectives, including educators and psychological counsellors. Employing three scales to identify cybercrime images, motives, and psychological effects, the study found prevalence in financial, emotional, sexual, revengeful, and entertainment-related cybercrime images, with sexual motives garnering substantial attention. The researcher concluded that anxiety, fear, nervousness, excessive sensitivity, and feelings of guilt and self-blame emerged as the foremost psychological effects resulting from electronic crimes and blackmail.

In addition, a qualitative, descriptive, and analytical study focused on a cohort of young individuals aged 18 to 35 aimed to elucidate the social factors contributing to Saudi youth falling victim to cybercrimes (Al-Mukhaita, 2021). Utilising interview and observation tools, the study revealed an escalating victimisation rate correlating with the proliferation of diverse cybercrime forms, encompassing various hacking incidents. Notable social factors contributing to the vulnerability of young individuals included familial disinterest and lack of awareness regarding their children's activities, a penchant for curiosity, experimentation, and exploration of novel aspects, electronic communication patterns with friends, unwarranted confidence leading to unguarded responses, technological ignorance and unfamiliarity with fraudulent methods, and excessive leisure time. Collectively, these factors rendered young individuals susceptible to cybercrimes, highlighting the multifaceted nature of the challenges faced in the Saudi context.

Furthermore, Al-Qahtani (2021) conducted a study assessing the impact of social services in mitigating the risks of cybercrime among a cohort of participants from Princess Noura University. The findings revealed that, from the perspective of faculty members, key social factors contributing to the cybercrime commission included the widespread presence of anonymous electronic links, limited awareness among internet users regarding criminal responsibility, and a general lack of social consciousness regarding the perils of social networking. Consequently, the researcher advocated for an active role of social services in preventing cybercrimes in Saudi society. This involvement encompassed initiatives such as raising awareness among community members, especially adolescents and young individuals, about the inherent dangers of cybercrimes and fostering a culture of caution. The study emphasised the imperative need for remedial measures, suggesting engagement with experts in crime prevention programmes, modification of negative attitudes among victims, and active family participation in shaping the behaviour of those impacted by cybercrimes. Mitigation strategies were proposed, including the provision of counselling services to victims, alleviation of negative emotions, assistance in rebuilding confidence, and the formulation of educational plans within curricula to enhance awareness of electronic environment perils and effective strategies for crime prevention.

Saeid (2019) conducted a survey study aimed at assessing the level of community awareness regarding cybercrimes among students at Imam Muhammad bin Saud Islamic University. The study addressed four fundamental elements, including the identification of cybercrime forms, factors contributing to the cybercrime commission, the risks associated with cybercrimes, and the role of the university in enhancing community awareness. The findings indicated that participants believed information crimes include the dissemination of extremist ideas and violence on the Internet, offences such as insult, defamation, and sexual blackmail, the spread of viruses on devices, data falsification, and bank card crimes. Factors contributing to cybercrimes included a misunderstanding of religious matters, increased internet usage, inadequate deterrent laws and legislation, and societal pressures. As perceived by students, prominent risks associated with cybercrimes encompass the

propagation of extremist ideas, the publication of pornographic materials, the spread of corruption, and family disintegration. The study concluded by emphasising the pivotal role of universities in raising awareness. It urged university professors to educate students and disseminate knowledge about the dangers of information crimes.

In a study conducted by Al-Mutawa (2020), the aim was to identify the level of awareness among students in the College of Education at Shaqra University in SA regarding the system for combating cybercrimes. Utilising a descriptive methodology, including survey and inductive methods, the results indicated agreement among participants with statements related to the terms mentioned in the cybercrime prevention system. However, a considerable number of students exhibited limited awareness of these terms, particularly concerning the principles of eavesdropping, illegal website entry, and privacy exposure within the system. This knowledge gap was attributed to the students' limited understanding of the system's functionalities. Consequently, the study highlighted educational measures to enhance awareness among students. Recommendations included informing students about the nature and dangers of cybercrimes, fostering a sense of responsibility and moral values, and safeguarding them from social factors that may lead to engagement in or endorsement of cybercrimes. Furthermore, the study advocated for the development of control and prevention measures, leveraging the available material, human, and technical resources at the college.

It is important to acknowledge that the primary focus of this research is to explore personal aspects rather than social perspectives. However, during the literature review, several studies were found that discussed personal issues such as anxiety and fear, albeit from a social standpoint. For example, research conducted by Alghadyan (2018) and Saeid (2019) highlighted the psychological distress experienced by victims, including feelings of anxiety, fear, and emotional vulnerability resulting from cybercrimes like cyber-extortion and the dissemination of extremist content. Therefore, it was crucial to include these studies in the literature review to gain a comprehensive understanding of the personal impacts of cybercrimes.

2-7 Risk Mitigation Strategies

The issue of breach mitigation has been considered globally in a range of contexts. Padayachee (2013) claimed that maleficence caused by insider threats is more damaging than outsider threats. He reviewed five controls to mitigate the internal threat that can positively reduce the opportunities of insiders, as follows:

A. Raising the security effort by installing firewalls, controlling access to utilities (authentication), screen exits, and controls via networks (hiding IP addresses).
B. Using intrusion detection systems, prepare reports and policies, and enhance formal oversight through audit and recording reviews.
C. Reducing polling information, removing information and disconnecting devices, identifying properties by watermarking, and encryption.
D. Reducing provocations by reducing frustration and stress, avoiding conflicts, reducing emotional excitement, and neutralising peer pressure.
E. Establishing clear rules such as user agreements, posting instructions, reminders of conscience (code of ethics), compliance assistance, and training in Internet ethics.

Theoretically, there are some countermeasures and strategies adopted by security experts to reduce information and data systems risk, including data breaches, which consist of four unique activities, namely: deterrence, prevention, detection, and recovery (Straub & Welke, 1998). For an example of deterrence effectiveness, Wilson et al., (2015) investigated the role of a surveillance banner in an attacked computer system in determining system trespassers' engagement with the system. They found that the presence of a surveillance banner in the attacked computer systems reduced the probability of commands being typed into the system during system trespassing incidents.

In addition, Densham (2015) suggested three strategies to mitigate the impact of data breaches, namely response in-depth, 360-degree security, and coconut and avocado. According to the author, response in-depth means the ability to find and apply the right technologies, logging capabilities, and monitoring

solutions for warning of the early stages. If an organisation can identify threats early, then appropriate action can be taken. The author, therefore, suggests using the RID model to implement a depth response plan, which consists of six steps involving detection, aggregation, analysis, response, and improvement.

The second strategy is called 360-degree security, valuable assets are identified, and then the correct controls are put in place to confront the threats. This stage includes identifying the assets (including data) of value, securing the assets by providing controls, processes, and technology to protect them, and conducting a simulation test for all forms. Simulated attacks may provide information about the types of attacks, as well as continuous improvement through risk management, monitoring the response process for data breach incidents, and the extent to which security methods are followed within the organisation.

The third strategy is called coconut and avocado. Traditionally, organisations would have hardened their perimeter in order to offer a level of security and safety – to use an analogy, a bit like a coconut. However, this has been proven to be ineffective when faced with today's sophisticated attacks. Hence, the author stated that accepting a certain level of risk on the Internet and email environment to enable the free flow of information as needed is considered a more effective approach. Instead, the author explained that there should be a solid core without a connection to the Internet that opens at all.

This solid core contains the most valuable data, and this model is like an avocado. As the author confirmed, organisations must safeguard critical data, key processes, applications, and systems within a hard core.

Stokes (2015) explained the necessity for HE institutions to find best practices to mitigate data breaches by adopting an incident response plan, which considers a systematic action plan designed to reduce the damage caused by a data breach. This plan has many benefits for HE institutions when preparing and dealing with a data breach. Incident response plans provide organisations with a structured and detailed action plan to utilise during a data breach, including roles assigned to response team members and the chain of command to executive management during a data breach event. An enterprise incident

response plan also helps mitigate the costs incurred by a breach by putting in place a sequence of events as soon as a breach is discovered.

Stokes (2015) explained that universities with large budgets tend to invest in responding plans to mitigate data breaches, as they are targeted by hackers because of the size of their data. They need to prepare for these attacks through planning to preserve their reputation and confidence in dealing with them. The plan for responding to data breaches and mitigating their effects should be clear and focused, Jaeger (2013) explained, that an effective response policy to data breach incidents should not exceed 30 pages to allow flexibility within the organisation, due to the changing IT environment constantly, the approaches to dealing with data also need to change.

Pranggono and Arabo (2021) conducted a research study to examine cybersecurity issues that occurred during the coronavirus (COVID-19) pandemic and suggested some practical approaches that can mitigate the risk of cyber-attacks, such as user education, a virtual private network (VPN), enabling multi-factor authentication (MFA), updating all device firmware, keeping anti-malware software up to date, activating a strong company online policy, segmentation and separation[5], and physical security. They mentioned some cyber-attacks that the HE institutions were subjected to during the coronavirus pandemic. For instance, in March 2020, the Brno University Hospital as one of the COVID-19 testing laboratories in the country was hit by a cyber-attack and was forced to shut down its entire IT network. Similarly, in June 2020, the University of California San Francisco (UCSF), which was working on the COVID-19 vaccine, was targeted by a ransomware attack and forced to pay $1.14 million to cybercriminals called ‘Net walker’. There are other strategies used in HE institutions, such as compensation for those affected. For example, in 2013, the University of Maryland (UMD) suffered a breach in its data systems, resulting in the loss of Social Security numbers for 310,000 individuals. Consequently, to mitigate the impact of this breach, the university

[5]Segmentation and separation mean is not used networks and devices in the institution for a single purpose. ‘Segmentation’ refers to breaking down the organisation's network into different trusted zones. ‘Separation’ refers to isolating the IoT devices on a separate network to control access (Pranggono & Arabo, 2021).

provided credit monitoring services to victims free of charge for five years, at an estimated cost of more than $ 6 million (Stokes, 2015).

The compensation strategy is commonly used in marketing to reduce the effects of data breaches, where Kude et al., (2017) investigated the effectiveness of compensation to mitigate data breaches, by measuring customer reactions. Some personality traits, such as compatibility, conscientiousness, emotional stability, extroversion, and openness were examined[6], and it was found that there are positive moral effects of perceived compensation.

McClurg (2015) examined the overall effectiveness of information security programmes in higher educational facilities by conducting a case study of two universities in the southeastern United States. The researcher evaluated cybersecurity monitoring in universities and the extent to which stakeholders are involved in cybersecurity risk management through the following points:

A. Establishing formal committees to oversee the information security function.
B. Managing third-party risk and embracing outsourced technology service providers.
C. Allocating funds to mitigate cyber risk.
D. Ensuring key stakeholders understand the legal ramifications associated with FERPA, PCI DSS, HIPAA, and GLBA violations.
E. Monitoring and maintaining sufficient awareness of threats and vulnerabilities.
F. Establishing and maintaining a dynamic control environment.
G. Purchasing cybersecurity insurance.

[6] The selection of emotional elements in the study relied on the five-factor model (FFM) of personality, which is considered a prominent theory in personality research. ‘Openness’ means the individual tends to be tolerant and open to new ideas. ‘Conscientiousness’ demonstrates that the individual is planning, organized, and active. ‘Extraversion’ indicates that the individual tends to be cheerful, optimistic, and friendly. ‘Compatibility’ shows that a person is kind, and compassionate, accepts the help of others, and expects help in return. ‘Emotional stability means an individual's sense of security, and emotional instability represents the feeling of fear and anxiety (Kude et al., 2017).

H. Developing and testing business continuity and disaster recovery plans that incorporate cyber incident scenarios.
I. Subscribing to a real-time threat analysis feed.

Summary

The purpose of this chapter is to review the literature on data breaches. This literature review aimed to describe the landscape of data breaches and their effects on HE institutions more specifically. The review included a presentation of previous studies in various sectors and geographical areas, with a view to focusing on the issues for HE institutions as a sector, and Saudi intellectual production as a geographical area. Because the subject of data breaches in Saudi HE institutions was largely overlooked, the literature in different sectors and regions was included.

This chapter has explored various aspects of data breaches and their risks and impacts. It began with an introduction setting the stage for understanding the significance of data breaches. It then covered types of data breaches, and technical risks including breach levels, types, and IT infrastructure's role. The discussion extended to organisational data risk, focusing on challenges like security policies, processes, and human risk factors. It also addressed the impacts on organisations and individuals, including reputational, financial, emotional, and social dimensions. Lastly, effective risk mitigation strategies were discussed to consider how it is possible to enhance data breach prevention and response measures.

The review highlights several significant elements within the context of data breaches, including both domestic and global perspectives. Notably, numerous Saudi institutions, including those affiliated with the Ministry of Interior (2013), the Ministry of Foreign Affairs (2017), and Aramco (2012), have reported instances of security breaches. This pattern is not exclusive to SA, as institutions globally, spanning diverse sectors, have encountered data breaches. In the field of HE, a diverse set of data breaches has been observed, reflecting the vulnerability of institutions to various cyber threats. Cyber-attacks, targeting multiple universities across different geographical locations simultaneously, are rationalised by the adoption of consistent technical

methodologies in data security. This uniformity extends to the use of similar information systems and engagement with common suppliers.

A notable disparity exists between developed and developing countries in terms of data protection systems. Developed nations, exemplified by the UK and the US, have instituted stringent frameworks for protecting personal data and issued annual reports scrutinising data violations. In contrast, developing countries such as SA face imperatives for research, driven by deficiencies in personal data and information regulations, reporting mechanisms, and available statistical data. However, it is important to note that both developed and developing countries still face challenges in confronting and mitigating the impact of data breaches.

Within HE institutions, technical risks are pervasive, manifesting in vulnerabilities within information systems and employees' understanding of the systems environment. System integration with software introduces significant vulnerabilities, making institutions attractive targets for cybercriminals. Additionally, the prevalent use of cloud storage tools poses an additional threat, particularly noteworthy in the context of SA's acknowledged weakness in information technology infrastructure.

Studies have brought to light weak practices among employees in Saudi Higher Education Institutions (HEIs), including the exchange of passwords. These practices stem from poor security awareness and insufficient training programmes, rendering employees unaware of the applied security policies within their respective universities. The literature also shows that data breaches have significant reputational and financial impacts on organisations, including universities, affecting their ability to attract students, secure donations, and maintain trust.

Research shows that data breaches can significantly affect stakeholders' confidence, making it essential for organisations to implement effective strategies, such as issuing apologies, to rebuild trust. Data breaches can also significantly affect privacy concerns. Based on the literature, in an academic context, high privacy needs correlate with high-security needs, influencing individuals' willingness to share personal information. Concerns about data

misuse can lead to feelings of alienation, affecting students' cooperation with their universities and their sense of belonging. Despite existing research exploring the effects of students' feelings of alienation in an educational context, there remains a need for further investigation into other emotional impacts, such as fear, anger, anxiety, and surprise. Notably, within the Saudi context, there is a noticeable lack of research addressing the emotional effects in the context of data breaches within HE. These emotions can lead to various behavioural changes, including spreading reputational damage such as through negative commentaries, switching institutions (universities), and decreased stakeholder cooperation. In business, for example, fear and anger as a result of data breaches elicit distinct cognitive responses, fear reducing purchasing intentions and anger leading to indifference toward mitigation and sometimes hostile actions.

The literature suggests that while business-focused research has extensively examined these emotional responses, the educational sector has explored issues of trust, privacy concerns, and alienation but not as full a range of emotional responses. This indicates a gap in understanding the full range of emotional impacts within HE. In addition, it was notable that limited consideration was given to cultural contexts and responses. This is in spite of the known high numbers of international students that shift countries and continents to conduct their studies. To bridge this gap, this research seeks to provide a comprehensive understanding of the emotional and psychological effects of data breaches, considering both actual and potential behavioural responses of individuals. By understanding these emotional consequences, universities can develop more effective strategies to support their communities and enhance overall cybersecurity resilience.

In conclusion, the literature extends to social data impacts and risks, particularly focusing on studies conducted in the Saudi context. These studies shed light on the social factors contributing to cybercrime vulnerability among people and capture some significant personal impacts. Additionally, the review underscores the strategies employed by organisations to mitigate data breaches, such as deterrent measures and compensation protocols. The data breach landscape is a complex one. Nevertheless, to fully understand, it is necessary for some

studies to try to surface this complexity. The literature reviews do evidence the need for a holistic understanding of this space and for frameworks that address the interlinked complexity of this space. The literature review provided three critical lenses for the research to focus on namely looking at technological, organisational and personal impacts. Building on the literature review, Chapter 3 discusses how a research framework was developed to navigate and surface these complexities in the SA context.

Chapter 3: Research Methodology

Introduction

This chapter sets out the methodological framework used for exploring the landscape and impacts of educational data breaches within the Saudi HE context. To lay the foundation for this chapter and establish the research approach, careful consideration was given to the intricacies of educational data breaches through the underpinning literature review. The chapter seeks to provide a roadmap for the research while also offering a thorough exploration of the underlying rationale guiding the researcher's methodological choices. Consequently, a nuanced understanding of the research's positionality and her alignment with the broader research objectives is established.

In addition, it has been important to acknowledge that data breaches are a sensitive issue. As identified in the literature, review there are gaps in the available evidence presented. Organisations are sensitive about revealing the data breaches they have suffered, near misses or their security vulnerabilities, particularly when there is no regulatory requirement to report these. In addition, it was known that potentially employees and students would be wary of criticising their host institutions. This is particularly the case in a more hierarchical and respectful culture as discussed in relation to SA in Chapter 1.

In addition, this work sought to develop a picture of personal responses to data breaches including emotional responses. This necessitated participants to open up and engage with the research. This was an important facet of the research and a domain where work to date has been largely undertaken through a Western lens. This framing is important, if ambitious, as focusing solely on technical considerations misses the potential to provide a more holistic picture of data breaches which occur and impact in complex ways.

The sensitive and challenging nature of this research emphasised the need to carefully design the approach for this study. Nevertheless, there was significant public value in undertaking this study as the exploration provides the opportunity for making improvements moving forward. In addition, the researcher felt her affiliation with a prestigious Saudi university gave her a privileged opportunity to explore this phenomenon. It gave her a potential

network and route to access universities and a deeper initial understanding of the context under study, which enhanced the potential to plan, manage, and mitigate the sensitivity surrounding the issue of data breaches.

It was known that this data breach landscape and associated risks are shifting rapidly with new technological tools and advancements emerging year on year. As such, a conscious effort was made to acknowledge both the strengths and limitations inherent in any chosen approach and those selected in this instance. Recognising the multifaceted nature of educational data breach impacts, the research sought to strike a balance between methodological rigour and flexibility to manage the sensitivities, ensuring the robustness of findings whilst remaining responsive to the dynamic and sensitive nature of the research context. This chapter explains the methodological underpinnings of the research, providing not only a detailed account of the strategies employed but also a reflective assessment of the considerations that inform these choices.

3-1 Research Questions

The research aimed to explore personal data risks and data breaches in Saudi HE from the perspectives of students, faculty members, and managers. Therefore, the focus was to capture the technical, organisational, and personal impacts of data risks and data breaches in university settings in SA. The following critical research questions were drawn:

1- What are the causes of the data protection breach in SA HEIs?
2- How do SA HEIs tackle personal data risks, including personal data policies and processes?
3- What are the multidimensional impacts of data breaches on stakeholders technically, organisationally, and personally?
4- Why do stakeholders think their personal data should be protected? How would they like data management to change in terms of technical, organisational, and personal aspects?
5- How do SA HE mitigation strategies help to manage and recover from security breaches?

3-2 Research Framework

A research design provides a framework for the collection and analysis of data (Bell et al., 2022). According to Grix (2010), the starting point for all social science research is an ontology, which is linked to the epistemological and methodological positions of the researcher. Blaikie and Priest (2019) define ontology as 'the nature of social reality', while epistemology has been defined by a group of researchers as a philosophical belief system about how research proceeds and what counts as knowledge (Harding, 1987; Guba & Lincoln, 1998; cited in Leavy & Hesse-Biber,2006). This research was constructed with the belief that an independent reality exists; the philosophical basis here is that the world exists and can be known and that approaches can be used to discover that reality (Cohen et al., 2002).

On the other hand, there can be the recognition of the existence of a constructive reality with different social perceptions: Tuli (2010) stressed that the philosophical basis for an explanatory constructive truth lies in the idea that facts arise through individuals, so meaning is derived from investigating social facts and interpreting them in a descriptive and qualitative manner. To address these tensions, the researcher chose to investigate the impacts of data breaches by employing mixed methods within a single research logic in which all methods are framed within a consistent ontology, as suggested by Blaikie and Priest (2019, p.167). Her stance is that of a pragmatist as discussed and developed below.

3-2-1 Research Paradigm

According to Teddlie and Tashakkori (2009, p.84), a paradigm can be defined as 'a worldview, together with the various philosophical assumptions associated with that point of view'. A variety of philosophical paradigms and worldviews exist, each developed with differing perspectives on their appropriateness. These include, but are not limited to positivism, post-positivism, interpretivism, constructivism, transformationalism, and pragmatism (Denscombe, 2008). This research deploys a mixed-methods approach that brings together quantitative and qualitative research methods, taking a 'pragmatic' approach as pragmatism is accepted as a philosophical underpinning for mixed-methods research

(Creswell & Creswell, 2018). Consequently, the researcher has adopted a single-paradigm stance, namely the pragmatist stance.

3-2-1-1 Pragmatism

According to Parvaiz et al. (2016), the main concern in pragmatism is ‘what works’, and therefore the research question or problem is the primary focus. Pragmatism, an American philosophy developed by Charles Sanders Peirce, William James, and John Dewey, is regarded as an 'accepted model or pattern' within the research paradigm, as quoted from Kuhn (1962, p.23) by Feilzer (2010,p.7). Pragmatism is compatible with mixed methods, as it does not adhere to a single philosophical framework. Onwuegbuzie and Leech (2005) characterise pragmatism as a flexible paradigm that mitigates the distinctions between quantitative and qualitative perspectives.

Morgan (2007) and Maarouf (2019) argue that pragmatism denotes the ‘intersubjective’ nature of the pragmatic paradigm, indicating that the researcher embodies both subjective and objective elements. To mitigate subjectivity, a methodological design has been formulated. Methodology is defined as the approaches a researcher employs to ascertain knowledge or reality (Miller, 2017). Given that the researcher's ontological position is rooted in the existence of a single reality in a specific context at a particular time while acknowledging multiple perceptions of this reality, a convergent mixed-methods approach has been chosen to explore the landscape of data breaches (reality) and to identify the multidimensional impacts (i.e., technical, organisational, and personal) on stakeholders in Saudi HEIs. Consequently, the researcher believes that the convergent design significantly reduces potential bias.

The utilisation of multiple methods is advantageous for gaining insight when studying an issue; in this context, the term ‘triangulation’ becomes relevant to data analysis across the data collected. According to Graham (2005), triangulation typically involves a multi-methods approach to data collection to mitigate potential errors and biases present in any one methodology. By adopting a convergent mixed methods design (i.e., triangulation), the researcher accrues numerous benefits, including leveraging the strengths of qualitative and quantitative approaches and minimising biases.

The case study design has been utilised as the HE sector is very broad and can be classified into old and new institutions. The researcher selected two respected universities, each representing a layer of that classification, namely KSU (old) and TaibahU (new). The assumption is that differences between these institutions would reflect a wider range of experiences and perspectives about the reality of data breaches. The target population includes students, faculty members, and senior managers because the researcher aims to explore the technical, organisational, and personal perspectives of data breaches in Saudi HE settings. Senior managers, in particular, contribute to capturing information regarding both technical and organisational perspectives that students may not be able to provide. Faculty members offer a better understanding of the personal and technical impacts of data breaches, in addition to their role in processing personal data. Students provide a broader lens for capturing personal impacts and potentially represent a stakeholder group with more limited power in the context of data management choice, albeit new legislation and rights have been framed. The researcher then compares three levels of awareness resulting from the three categories of participants to present their perspectives on the multidimensional impacts of data security breaches.

The researcher conducted semi-structured interviews with managers (data security and information technology managers as well as managers in the departments responsible for social and psychological aspects) in the two universities, while simultaneously distributing an online questionnaire to students and faculty members. The fact that the researcher is an integral part of this reality does not negate her ability to reach an objective understanding of reality (i.e., being one of the stakeholders in SA HEIs). Cohen et al. (2002) assert that understanding the social world is contingent on the perspective of individuals actively engaged in the ongoing actions being investigated. This is because researchers exploring a specific issue within the same community as the research problem possess a heightened familiarity with the background of the problem. The next section clarifies the researcher’s position in the Saudi educational sector.

3-2-2 Researcher's Positionality

The research aims to explore multiple perspectives on the issue of data security and information protection in Saudi HE. The researcher is a Saudi citizen with the cultural and linguistic background from this context. In addition, she has a specific lens in the HEI sector. She has an information science bachelor's degree and a master's degree, both studied in SA. In these contexts, she has previously investigated the behavioural patterns of stakeholders in processing their personal information and exploring the needs of these stakeholders within the information system. This expertise forms a critical underpinning assumption that enables her to better engage with the intricacies of the data and information protection system, particularly concerning policies and systems governing the processing, utilisation, access, and security of data and information as well as stakeholders' perspectives. The examination of this issue adopts a multidimensional approach, including personal (e.g., social and psychological factors), technical, and organisational aspects related to personal information protection. However, the researcher's scientific and administrative expertise remains a crucial lens through which this topic is approached.

Moreover, the researcher has been a faculty member in the Department of Information and Learning Resources at TaibahU since 2010, and for two years, she served as an assistant to the head of the department in the female section at the same university. These roles have enriched her administrative and scientific knowledge and skillsets. The research methodology employs a case study approach, with the selection of two Saudi universities (TaibahU and KSU) to explore the identified issue. While acknowledging her affiliation with TaibahU, the researcher actively mitigates potential bias by including another case, namely KSU, to ensure a balanced and comprehensive investigation was conducted.

Additionally, this research constitutes part of the researcher's pursuit of a PhD. from University College London UCL in the United Kingdom. Recognising the distinctions between the societal context from which data was collected and the British environment in terms of language, culture, regulations, etc., the researcher affirms her belonging to Saudi society—the sample under investigation. Despite sharing the same cultural background as the research

sample, she situates herself as a researcher at UCL to challenge some culturally engrained perspectives, leveraging her Arabic knowledge and linguistic capabilities to interpret research findings from a British perspective. The researcher acknowledges the potential for bias arising from environmental contexts or translation limitations between Arabic and English. However, she diligently worked to minimise these biases to uphold the credibility and objectivity of the research outcomes.

It is worth noting that in establishing the research framework, it was initially anticipated that the researcher would have more privileged access to open participants at TaibahU. TaibahU did support and provide access permissions. However, KSU offered just as open a response. Potentially the participants were more aware that at TaibahU they were giving data to someone who would re-enter their systems. It was made clear at TaibahU that the data and knowledge would be limited to the research domain. At TaibahU reaches were acknowledged which may evidence trust in the researcher. The ‘insider’ and ‘outsider’ dynamics of the researcher’s positionality need to be carefully navigated and are not always clear-cut but are often complex when dealing with such a complex and sensitive research space. Clearly, the researcher's SA nationality and ability to speak Arabic were critical advantages in the delivery of the research.

To mitigate potential or intentional biases, the researcher implemented several measures, which are detailed as follows:

Study Design and Methodology: The study adopted a multi-convergent methodology, assigning equal value to different types of research data and employing triangulation to enhance the credibility of the results.

Sample Design: The research sample was systematically designed to minimise biases introduced by the researcher. A stratified sampling approach was used, comprising three groups: students (random sample), faculty members (random sample), and managers (purposive sample). Random selection within the student and faculty strata helped reduce bias and ensure diversity. For the managers, purposive sampling was deemed more appropriate

due to their small population size and critical role in data security. This approach effectively balanced the need for inclusivity with the research objectives.

Pilot Testing of Tools: A pilot test was conducted on the survey instruments to assess clarity, neutrality, and suitability. Feedback from the pilot informed several adjustments, including rephrasing ambiguous questions, shortening the questionnaire introduction, and refining the overall format. These refinements enhanced the tool's reliability and usability.

Minimising Interview Bias: To reduce bias in the qualitative phase, the researcher intentionally selected managers from diverse roles and departments to ensure a broad representation of perspectives related to data security. Semi-structured interviews were chosen to allow flexibility, and open-ended, non-directive questions were used to encourage honest and diverse responses without leading participants.

Reducing Bias in Analysis: During data analysis, identifiers and qualitative contributions from interviews were anonymised and coded using NVivo software to ensure objectivity. For survey data, no personal identifiers were collected, and responses were analysed using statistical software. Reliability and validity checks were performed on the quantitative data, including the use of Cronbach’s alpha, with a validity level of 95% established.

Ethical Considerations: Ethical standards were rigorously followed, with informed consent obtained from all participants. The researcher ensured participation was entirely voluntary by providing clear, transparent information about the study’s purpose, along with assurances of confidentiality and the right to withdraw at any time without consequences. These measures supported the credibility and ethical integrity of the research.

Translation and Linguistic Accuracy: To minimise biases arising from working across Arabic and English, the researcher translated the survey instruments and interview questions with careful attention to both linguistic accuracy and cultural relevance. Sensitive topics were framed to respect the cultural norms and values of participants. The researcher’s deep understanding of both languages and cultures helped prevent misunderstandings or misinterpretations that could have introduced bias into the responses.

3-2-3 Research Methods

The study approach was a convergent mixed-method design. This study used the definition written by Given (2008) which defines the mixed methods approach as research that relies on collecting and analysing data, merging results, and drawing conclusions using qualitative and quantitative methods in a single study. The rationale behind the choice of mixed methodology was to reflect the complexity of personal data breaches, drawing the wide range of impacts on both the organisational context of the HEI and the broader stakeholder landscape. Due to the perceived difficulty in understanding the research problem related to the privacy of individuals, this approach was applied to bring into play a better understanding of different perceptions.

McKim (2017) argues that researchers, by using a mixed-method approach, can procure a deeper and broader understanding of the phenomenon under investigation. Alexander et al. (2008) also describe these researchers as wanting to know more about the phenomenon by hearing different voices and drawing multiple constructions that reflect the complexity of the problem or area under exploration. Routsis (2020) for example, has employed a mixed methods approach to examine information privacy in a socio-historical context with the aim of discovering the behaviours, perceptions, and concerns associated with online communication. In essence, a qualitative analysis of internet content and a quantitative analysis via a complex survey construction were used to study the behaviours of individuals regarding self-disclosure and privacy.

In this research, a mixed methods convergent design has been taken because of the value of integration and mixing results. What is meant here by integration was implemented at the levels of research, design, methods, interpretation, and preparation of reports, to confirm or refute the results of both types of data (quantitative/ qualitative). O'Cathain et al. (2007) emphasise that integration gives readers more confidence in the results and conclusions drawn from the study. The quantitative approach was well-suited to achieve objectivity, control, and precise measurement (Leavy, 2017). In contrast, the qualitative approach was well-fitted to describe the meaning of the phenomenon and subjective people's experiences (Clark, 2019). The approach sought to enable not only an

integration but also a balancing of quantitative and qualitative data. This is called ‘offset’ in the philosophies of scholars such as Greene, Caracelli, and Graham (1989) and Bryman (2006) cited in Croswell (2018). The researcher gains added value and understanding through the combination of quantitative and qualitative research to offset their weaknesses and benefit from strengths in both. The multi-method study is superior to mono-method studies in exploring data security from multiple perspectives (Johnson & Onwuegbuzie, 2004), due to the qualitative differences in the target community, which includes students, faculty members, and managers. These qualitative differences required the application of a greater variety of tools and techniques to reach an appropriate amount of information that can deliver results.

To illustrate, a qualitative approach could provide in-depth descriptive information that helps understand why data breaches occur and is unlikely to clarify the potential multidimensional effects of those breaches. Since the effects differ from one person to another, therefore the wider the scope of the research, the more effects the researcher would capture. Likewise, when relying on the quantitative approach itself, it can capture a larger number of effects that can be explained by statistical graphs and tables, but it would not provide detailed qualitative data on the data breaches provided by the interview participants. The mixed-methods study is characterised by the possibility of analysing contrasting types of data (Creswell & Creswell, 2018). Using multiple approaches can produce diverse results, which are seen as beneficial for capturing the impacts/risks of data breaches and enhancing data security practices.

3-2-3-1 Convergent Mixed Methods Design

Regarding the design, there are many forms of mixed research designs, as these designs can be divided in terms of the purpose of the study (e.g., exploratory), or in terms of the relationship between methods (e.g., a parallel or sequential relationship), it can also be divided in terms of the role of quantitative or qualitative methods in the study, (e.g., leadership design or follow up) (Clark & Ivankova, 2016). The main object for choosing mixed methods was to compare different perspectives from quantitative and qualitative data perspectives in an integrated way. This comparison can be done by merging

the two databases to show how the data converge or diverge, data similarity or difference to generate new visions about the Saudi data security landscape.

The convergent mixed methods design was defined by Creswell (2018) as a design that relies on collecting and analysing quantitative and qualitative data simultaneously, but separately and then comparing the results to see if the results confirm each other. Fidel (2008) explains that convergent design enables collecting data by using suitable data collection tools that are used in each approach separately, then analysing and interpreting the data using appropriate analysis and coding techniques for each type separately, and then combining qualitative and quantitative data to produce appropriate results and findings.

The convergent design was chosen because of its advantages, particularly its suitability for the research context and the limitation of site access. Croswell (2011) describes this design as efficient, logical, and intuitive. The convergent design allows the researcher to smoothly collect data and independently analyse each type of data using traditional techniques associated with each type. The following section explains in more detail why the convergent design was valuable to apply.

1- The Nature of the Convergent Design

In a convergent design, two types of data are collected concurrently. Following data collection, the analysis is also conducted simultaneously. The diagram below shows an overview of the convergent design framework cited from (Creswell & Creswell, 2018):

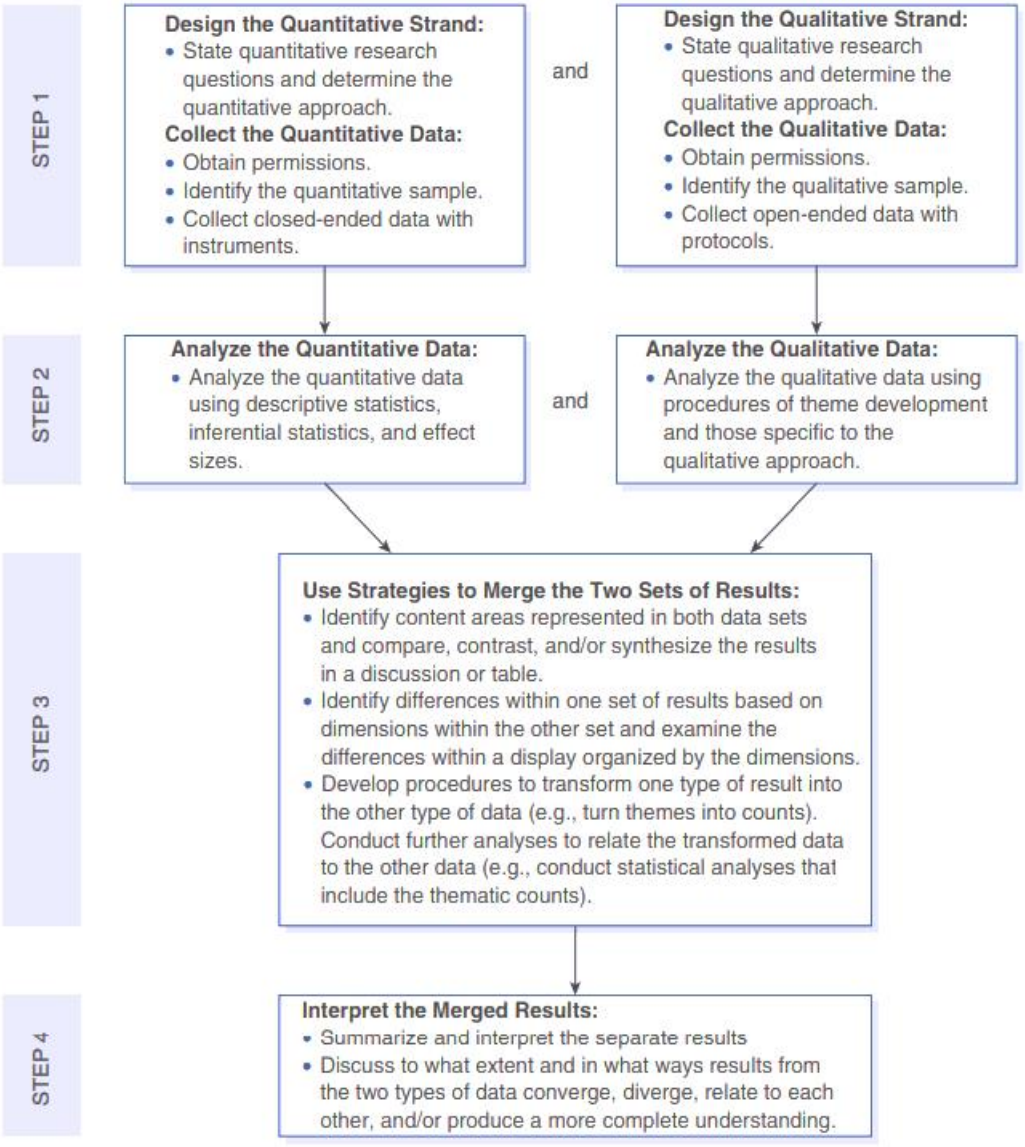

Figure 2 The convergent design framework that was drawn by Creswell (2018).

2- The equal priority of qualitative and quantitative data

The researcher perceives equal value in both qualitative and quantitative data concerning the primary purpose of the research problem and its associated questions. Assigning priority to either type of data in the collection and analysis process does not fundamentally alter the comprehension of the current research problem aimed at exploring multiple perspectives. In contrast to mixed-sequential designs, where assigning value and priority to a specific type of data (either quantitative or qualitative) significantly influences the collection, analysis, and reporting of results, the convergence approach is distinguished by a more balanced treatment of both data types.

3- The Possibility of Reducing Bias

The significant objective underlying the utilisation of the convergent mixed-method design was to mitigate certain aspects of bias arising from sampling, transcription, translation, and coding. Unlike other designs such as explanatory and exploratory, which introduce intervals in data collection, the convergent design minimises the potential influence of signals that may emerge during such time gaps. Implementing alternative designs, such as conducting interviews followed by surveys or vice versa, has the potential to impact the design and analysis of the tool employed in the second stage. The second tool is likely to be significantly influenced by the experiences of the first tool, affecting sample selection, formulating a second set of questions, translation, coding, and analysis. It is to be noted that the coding was inductive, and no prior assumptions and frameworks were placed on the research design and delivery. Therefore, the application of a convergent design serves to diminish potential biases, whether intentional or unintended.

4- Aligning Design with Research Limitations

This study was commenced and planned at a time of great uncertainty due to the global pandemic. It was started in September 2020 when travel was difficult and in addition the ability to get approval for research overseas was complex. There were periods when no travel was permitted and when it was UCL required additional risk assessments ahead of travel, taking into account the UK government advice. In addition, the research had to be planned to take into account the SA rules on travel and work during this timeframe. It took considerable time to obtain the necessary permissions from the universities included in the study to collect the data during this difficult period where health concerns were the priority. A further complexity was that the data needed to be collected from different areas (universities) in SA. If the researcher collected data within two stages, that would have consumed time and cost to travel twice between the two countries (the UK and the SA) and the cities within SA to reach the universities. This was difficult to plan at this time.

As noted, the primary process of communication and negotiation with the universities took a long time, over 4 months, to persuade them to participate. When the permits were granted, they were valid for a specific period of time. Further permits would have been needed for additional data collection. Therefore, one immersive visit was deemed to be the least risky approach. The convergent design enabled the researcher to conduct the research within a reasonable cost of time and money. The pragmatic rationale does not negate the strength and ultimate rationale for the choice. As previously mentioned, the main reason for choosing the convergent mixed methods was to collect and analyse two types of data and merge the results to identify the extent of convergence or divergence of the data. Although this design has advantages such as bias control, it creates a challenge for the researcher in how to successfully integrate different data sets (Hands, 2022). This challenge has been described by Clark (2019) as achieving meaningful integration of the quantitative and qualitative perspectives, methodologies, data sources, and data analyses.

Assumptions and Requirements of the Convergent Mixed-Methods Design:

A mixed-methods approach assumes that integrating quantitative and qualitative data provides a more comprehensive understanding of complex issues than either method alone (Creswell & Plano Clark, 2018). In the context of this research, which explores the causes, impacts, and mitigation strategies for data breaches in Saudi Higher Education Institutions (HEIs), the mixed-methods approach enabled a multidimensional exploration of the issue. The convergent design, specifically, assumes that quantitative and qualitative data are complementary, allowing for independent collection and analysis before integration to produce richer insights (Teddlie &Tashakkori 2009). Key requirements include a clear rationale for combining methods, alignment of research questions with both qualitative and quantitative data, synchronised data collection, and careful integration of findings during analysis. Meeting these requirements is essential to ensure that the insights from both methods contribute effectively to addressing the research questions.

To achieve these requirements, this study employed surveys with students and faculty members to capture measurable data on their awareness of data risks, experiences with breaches, and perspectives on data security practices. Additionally, semi-structured interviews were conducted with managers to gain deeper insights into institutional policies, organisational challenges, and strategies for mitigating data breaches. This approach addressed the issue from multiple angles and ensured that both broad trends and nuanced stakeholder perspectives were included (Bryman, 2016). Data collection for both methods was conducted concurrently, ensuring temporal alignment and enabling robust integration during analysis. Findings were synthesised through thematic analysis to draw meaningful connections between quantitative patterns and qualitative narratives (Fetters et al., 2013). Methodological rigour was upheld through the use of validated survey instruments, systematic coding of qualitative data, and member checking to validate interpretations. These considerations ensured a comprehensive exploration of the technical, organisational, and personal dimensions of data protection in Saudi HEI.

3-2-3-2 Case Study Design

The choice of exploring the impacts of data breaches in HEIs rather than other types of institutions, given that HEIs are characterised by openness, and provide access to a large set of personal data that makes them an easy target for hackers (Chapman, 2019). Trying to explore the impacts of data breaches in a large population consumes time and effort as well. In addition, taking too large a population out of context would potentially not enable the nuanced understanding of data breach impacts to be properly understood. Therefore, the case study method was applied, as a strong fit for the research aim and objectives. In order to answer the research questions accurately and appropriately, a multiple-case study design was chosen. Case studies enable in-depth investigations of a complex phenomenon (Yin, 2014; Cresswell, 2007). The approach that includes multiple cases would help in generalising the results, as the focus is on studying contextual issues and not on describing a topic or the circumstances of a certain case (Yin, 2009, cited in Yin, 2012, p. 4).

There are typically understood to be three types of case study, namely the intrinsic case study, the instrumental case study, and the collective case study. Due to the need to study the contextual topic and undertake comparisons to gain nuanced insights into the effects of data breaches, two cases were included, therefore, this research falls under the collective case study, which is used to describe a research study that targets more than one case to examine a particular phenomenon (Pickard, 2013). In this study, the collective case consists of KSU and TaibahU, but each case is treated as a single case in collecting and analysing data before undertaking comparisons. The researcher also attempted to contact a third institution, King Abdulaziz University, but was unable to include it in the study due to permission issues. The primary goal was to gain insight into how universities handle personal data management, necessitating the inclusion of more than one university for comparative purposes. Further information on these case context choices is below.

3-2-4 Data Collection

Population

There are two bodies in the SA responsible for education (Smith & Abouammoh, 2013a). The Ministry of Public Education, established in 1952, supervises basic education in its three stages (primary, intermediate, and secondary). The Ministry of HE, established in 1975, is responsible for university education. However, to achieve interdependence and integration, reduce the gap between public and HE, and improve educational outcomes, the two ministries were merged into one in 2015, forming the Ministry of Education. University education has received generous support, reflected in the establishment of new universities and substantial financial allocations in the budgets. As of today, SA has twenty-five public universities, nine private universities, and thirty-four private colleges, offering scientific and applied specialisations in various fields (Ministry of education, 2021). In the following table, data on public and private universities in SA are provided.

Type of institution					
Public			Private		
Institution's name	Date of establishment	Region	Institution's name	Date of establishment	Region
Imam Muhammad Bin Saud Islamic University	1974	Riyadh	Prince sultan university	1999	Riyadh
King Saud University	1953	Riyadh	Yamamah University	2001	Riyadh
Princess Nourah Bint Abdulrahman University	2004	Riyadh	Dar Al Uloom University	2008	Riyadh
Saudi electronic university	2011	Riyadh	Knowledge University	2009	Riyadh
King Abdulaziz University	1967	Jeddah	Riyadh Elm University	2004	Riyadh
King Saud bin Abdulaziz University for Health Sciences	2010	Jeddah	Effat University	2009	Jeddah
Jeddah University	2014		Dar Al-Hekma University	1999	Jeddah
Shaqra University	2010	Shaqra	Prince Fahd Bin Sultan University	2003	Tabuk
Taif University	2004	Taif	Mustaqbal University	2002	Al Qassim
Islamic University	1961	Madinah			
Taibah University	2003				
Imam Abdulrahman Bin Faisal University	1975	Dammam			
King Fahd University of Petroleum and Minerals		Dhahran			
King Faisal University	1975	Al Ahsa			
King Khalid University	1998	Abha			
Qassim University	2004	Al Qassim			
University of Hail	2006	Hail			
Al Jouf University	2005	Sakakah			
Jazan University	2005	Jizan			
University of Tabuk	2006	Tabuk			
Albaha University	2006	Albaha			
Najran University	2006	Najran			
Majmaah University	2010	Majmaah			

Table 12 Data about public and private universities in SA

3-2-4-1 Sample Selection

The first case study is King Saud University (KSU)

KSU is the first university in SA, it was established in 1957 in the capital, Riyadh. It is considered the largest university in the Kingdom and offers a wide range of courses in sciences, humanities, and professional studies. It includes several libraries and two university hospitals and provides educational opportunities for local and foreign students. Undergraduate programmes are taught in English, except for Arabic and Islamic studies (KSU, 2021a).

There is no fee for admission of Saudi students to the university. In 2010, the university was ranked 221 in the Times Higher Education - QS World University Rankings - the highest ranking of any Arab university (Smith & Abouammoh, 2013). KSU contains many departments in five major colleges as follows, science colleges, community colleges, women's colleges, health colleges, and humanitarian colleges. The university focuses on preparing graduates at a high level, developing their skills and talents, as well as helping them to make a contribution to the development of the local and international community (KSU, 2021b).

In 2020, it was ranked as the second-best university among Saudi universities, according to Academic Ranking of World Universities (ARWU) (ARWU, 2021). The number of students enrolled in 2019 in the university is roughly 62,771 students in various programmes including intermediate diploma, undergraduate, and postgraduate programmes. Moreover, the university employed about 7159 academic personnel, while 13,504 administrative and technical personnel (GASTAT, 2019).

The second case study is Taibah University (TaibahU)

TaibahU, one of the newly established Saudi universities, was established in 2003 and is located in Medina. The university is divided into 28 different colleges, covering subjects as diverse as law, medicine and humanities, engineering, business administration and the arts. It offers education for free to citizens who meet the admission requirements similar to the other Saudi public

universities, as it offers 156 academic programmes, including 94 graduate programmes.

TaibahU has achieved full and unconditional institutional accreditation from the National Assessment Authority (Taibah University, 2021). In 2020, it was ranked the sixth-best university in SA (U.S.News, 2021). Despite its recent establishment, it is considered one of the largest universities in terms of student capacity, as the number of students registered is about 69357 students in many academic programmes such as undergraduate and postgraduate. Furthermore, the number of faculty members is estimated at 3159, and 3013 administrative and technical staff in the university (GASTAT, 2019). The table below shows information about the two cases.

	King Saud University (KSU, 2021a)	**Taibah University** (Taibah University, 2021)
Foundation	1953	2003
Location	Riyadh	Medina
The total of undergraduate students	48,788	63,122
The total faculty members	7159	3159
Saudi Ranking (U.S. News & World Report ,2020)	3	5

Table 13 Contextual information about the two case study universities.

The table demonstrates that some points would help to compare between the universities as follows:

- ✓ Foundation: By including old and new established Saudi universities to examine the range of experience. Among the most important considerations is experience, which is believed to play a role in the organisational field to deal with security breaches. That means the institution has sufficient experience to address all data security and protection issues. According to Garrison (2010), universities need to learn from their experience in the security violations they are exposed to, as a good number of hacked records in universities were the result of errors, negligence, and lack of enforcement of policies by both the user and IT staff.
- ✓ Location: To reflect whether cultural and social differences between individuals play a significant role in the size and extent of the impact of data breaches.
- ✓ IT Infrastructure: Infrastructure is represented as an essential factor to consider for avoiding data breaches and managing personal data effectively. As mentioned by Irfandhi et al., (2016), the success of universities depends largely on the IT infrastructure used in them. Therefore, the researcher chose a university located in the capital, which represents the best Saudi cities in terms of infrastructure compared with other universities (Garba, 2004). It also reported a data breach incident in 2012 (Alqurashi, 2020).

Besides the previously mentioned differences, another important factor influencing the selection was obtaining ethical permissions. The researcher contacted three universities for permission, but only two agreed to participate.

3-2-4-2 Sample Size

KSU and TaibahU have been engaged because of the differences between the two universities, which could provide a larger lens for educational data breaches. In the academic community, there are many groups, such as students (undergraduate/ postgraduate) and employees (technicians /managers/ academics). The focus has been on students and faculty members as categories that receive data security services. It is expected that their perspectives regarding data security are different according to the varying

levels of awareness among them. Managers, such as senior managers, IT managers, social workers, and psychologists, were included as they were security services facilitators within the university. The surveys were chosen as a method of collecting data from students and faculty members, A c.10% study sample was the aspiration for this work. The interviews were selected to be conducted with managers, and the maximum number of interviews was 20 participants, but this number depends on the response of the participants to the researcher.

Selecting the Sample Size:

1- Managers

The qualitative sample for the study's manager group was selected using purposive sampling. Initially, the research aimed to conduct 20 interviews, with 10 interviews at KSU and 10 at TaibahU. However, the final sample consisted of 10 interviews at KSU and 5 at TaibahU. The difference in the number of interviews conducted at each university can be attributed to the size and structure of their administration. KSU, as the largest university in Saudi Arabia with 13,504 administrative personnel, has a larger pool of potential interviewees, TaibahU employs 3,013 administrative staff, limiting the number of available managers. Consequently, while the original plan was to conduct 10 interviews at each university, the smaller number of administrative staff at TaibahU resulted in only 5 interviews being conducted there. In addition to the data security departments, the study also aimed to include managers from psychological and social departments, who may have insight into data protection from a student support perspective. However, at TaibahU, managers from the psychological and social departments did not participate. Despite this, the exclusion of these departments did not significantly impact the quality or breadth of the information gathered, as the data security managers at TaibahU provided valuable insights into the personal (emotional) perspectives.

2- Faculty Members

The faculty group was selected using stratified random sampling to ensure representation across different academic disciplines and varying levels of experience. This approach aimed to capture diverse perspectives and reflect the variety of roles faculty members play in safeguarding and managing student data. A total of 70 faculty responses were received, comprising 41 responses from KSU and 29 responses from TaibahU. The expected sample size was approximately 10% of the faculty population (7,159 faculty members at KSU and 3,159 at TaibahU). While the actual sample size was smaller than anticipated, statistical analysis, including a t-test, confirmed its adequacy for identifying significant trends and differences in faculty responses between the two universities.

3- Students

For the student group, stratified random sampling was also utilised to ensure a wide range of representation from various academic programs, levels, and backgrounds. This approach allowed the study to capture the diverse views of the student population effectively. A total of 191 student responses were collected, with 42 responses from KSU and 149 responses from TaibahU. The anticipated sample size was also 10% of the total student population (48,788 students at KSU and 63,122 students at TaibahU). Although the response rate was below expectations, the collected sample is diverse and representative. A t-test was employed to verify the adequacy of the data, ensuring the study's reliability and ability to identify significant trends and patterns.

However, the lower-than-expected response rate can be attributed to several challenges. The COVID-19 pandemic significantly impacted participation, as remote learning and working arrangements reduced accessibility and engagement. Additionally, participation was entirely voluntary, which may have further limited responses. Despite these constraints, the diversity and randomness of the sample ensured that the data remained valuable and reflective of the broader population. Statistical analysis, including t-tests, confirmed that the sample size was sufficient to meet the study's objectives and uphold its validity.

3-2-4-3 Data Collection Instruments

Two research methods were employed to collect primary data involving semi-structured interviews and online surveys. This section explains each of these instruments.

3-2-4-3-1 Semi-Structured Interviews

Interviews were picked out to collect qualitative data from key stakeholders responsible for protecting personal data within selected universities to present their perspectives in terms of the data security framework offered by their corporation to prevent data breaches. The stakeholders in the qualitative approach were the managers in the selected universities. (McKim, 2017) believes that the qualitative approach generates new information, therefore the researcher adopted this approach with managers due to the significance of their position, and the valuable information retrieved from them. According to (Al-Habadan, 2021), managers are the essential element in achieving the university's goals and objectives that relate to efficiency and effectiveness in management. Directors of departments related to the organisation and management of data and information technology and managers of social, psychological and legal aspects in universities were reached.

Due to the wide scope of HE, the principle of multiple case studies was adopted, which is largely compatible with purposeful sampling. Gentles et al., (2015) encouraged the use of purposive samples in the case studies, and they stated that purposeful sampling means selecting study participants based on their expected experience and the important information they provide related to the research questions. Regardless of sampling purposefully, semi-structured interviews SSI were used to diminish the leading of questions during interviewing participants (Newcomer et al., 2015). The use of the semi-structured interview does provide many advantages to the researcher, such as flexibility, and the ability to interact with the interviewees and explore the topic in further depth, opening up the questions and discussions to unanticipated content and ideas. Nevertheless, the structured components allow for some cross-analysis between the participants focusing on particular important themes. In this way, this method enabled the researcher to collect a high volume of comprehensive and in-depth data on manager experiences of data breaches

in their respective Universities to determine the current state of data breaches in the Saudi HE context. This also helped the researcher to come up with effective response strategies on how Saudi Universities can mitigate existing data breaches in Saudi Universities. Semi-structured interviews also gave the participants more freedom to express themselves during the interview process, thereby enabling the researcher to yield a comprehensive dataset (Gill et al., 2008).

In addition, owing to the fact that the current research seeks to explore the multiple perspectives of data breaches, the semi-structured interview method was suited for the exploration of the perceptions and opinions of respondents regarding complex and sometimes sensitive security issues (Louise & While, 1994). It enabled a rapport and trust to be built between the participant and the researcher as part of the consent process, and then the conversational exchanges that can occur in interviews. Regarding the content of the questions, the researcher designed a set of questions that were directly related to the research questions.

As Galletta and Cross (2013) recommend, in their book on mastering the semi-structured interview, that questions should be open, of a theoretical nature, to elicit data based on the participants' experiences. Additionally, a review of the literature helped the design and development of the interview protocol for the qualitative data of this study. The literature was examined for themes which related to the purpose of the study and the research questions. Thus, the interview protocol was developed based on the effects discovered through the literature review. Interview questions were focused on exploring the multidimensionality of data breaches and their effects. (See Appendix G for a list of interview questions). The researcher developed a broad guide which includes several aspects that are shown in the following table:

	Discussion themes
1	Background information about participants' responsibilities within the university.
2	Technical considerations of data breaches in terms of their causes, effects, and risks.
3	Regulatory procedures and policies, and their effects in reducing data breaches.
4	Reflection of the emotional reactions toward security breaches, limitations, and challenges.

Table 14 Interview discussion themes.

Although the researcher designed a list of critical questions for the three technical, organisational, and emotional dimensions, the background of the interviewee was respected. In the sense that it identified basic questions, and they were directed to all participants regardless of their knowledge, but the researcher tried as far as possible not to lead the interview, especially in the emotional aspects. For example, the interviews conducted with managers of psychological and social fields depended heavily on making the interviewer talk frequently about data security and the emotional effects of the breaches. Talking about emotional responses by psychological and social managers who dealt with many psychological cases provided fruitful information for understanding these emotions. According to both Holmes (2015) and Dempsey et al. (2016), the interviews might yield rich and meaningful data to capture the emotionally sensitive aspects. Furthermore, due to the situation of COVID-19, the meetings were organised carefully to be face-to-face interviews and online interviews were held if the participants refused the physical interaction. Permission was taken from the participants to record the interview. Although many abstained from the audio and video recording of the interview, there were those who agreed. Interviews were recorded with UCL recording/storage media (Microsoft Teams).

3-2-4-3-2 Online Surveys

The survey served as a tool for gathering data. The survey design was clearly considered. According to (Larini & Barthes, 2018), the survey should include an introduction, a body, and a conclusion. The survey was to ensure the provision of quantitative information on the effects of data breaches by involving a reasonable proportion of the original community. To reach a larger number of respondents, an online survey application was chosen, which provides the appropriate data at the lowest costs (Creswell & Creswell, 2018).

The survey contained questions that included various themes to find out the effects, based on what was discovered in previous studies. The questions focused on exploring the personal aspects mainly, and the participants were asked about some technical and organisational aspects from their perspectives. The questionnaire was based on open and closed questions addressed to two categories in the educational context of students and faculty members. The tool design did enable for some qualitative data to be collected anonymously from different participants as well as for quantitative data to be gathered.

The survey employed a 5-point Likert scale (strongly agree to strongly disagree). There is a debate among specialists about the appropriateness of adopting the Likert scale in social research, as there are those who believe that it is the optimal measure to use in social studies (Croasmun & Ostrom, 2011), as it is very useful to measure an individual's attitude toward social issues (Likert, 1932). On the contrary, there are those who believe that its use is fraught with some challenges in terms of reliability (Subedi, 2016). However, ؘthere is a consensus that it is appropriate to collect emotional data(Guilford, 1954) Croasmun & Ostrom, 2011;Subedi, 2016) .

To determine emotions, the Integrated Management Crisis Mapping Model (ICM) was relied on, given that data leakage is a crisis facing the organisation (Jin & Pang, 2010) (Kim & Cameron, 2011). The model contains four negative elements (i.e., anger, sadness, fear, and anxiety) that the crisis may arouse in the hearts of individuals. A fifth element was included in the model, which is the

feeling of (surprise), and an option (other) was added to enable participants to write any other response feelings. The purpose of expanding (the ICM) module was that the researcher wished to capture a greater number of emotions. For example, Jin et al. (2014) developed a model of 13 items to measure people's reactions to a company crisis, including anger, anxiety, apprehension, confusion, contempt, disgust, embarrassment, fear, guilt, sadness, shame, surprise, and sympathy. The decisions around these choices were made based on the underpinning literature review.

The students' questionnaire included a total of 41 questions. The faculty members' questionnaire contained a total of 42 questions. Both surveys were quite similar, the only difference was in exploring the job level of the faculty. The surveys were designed to be distributed over the Internet, from the university's official outlets. Opinio software was used for designing surveys. The questionnaire was distributed in both universities simultaneously in a way that serves the study methodology. (See Appendix F for the questionnaire format).

Surveys are an effective method of data collection in research, offering several key advantages. Firstly, they enable efficient gathering of data from a large number of participants, enhancing the representativeness and generalisability of the results. By widely distributing surveys, it can access a diverse sample, providing a broader perspective on the research topic. Additionally, surveys can be administered through various means, such as online platforms, which improve accessibility and minimise logistical challenges. Thus, utilising questionnaires was particularly suitable for overcoming access restrictions imposed by the COVID-19 pandemic, such as social distancing and other related measures. In addition, surveys allow for anonymous comments and as such the potential for free and frank responses. This was deemed to be particularly important in the context of the sensitivities of discussing data breaches both in terms of personal experiences and organisational sensitivities.

Surveys, despite their advantages, come with some limitations that must be considered. One significant drawback is the potential for response bias, where participants may consciously or unconsciously provide answers that they believe are more socially acceptable or desirable. This bias can distort survey

results, leading to inaccurate conclusions. For example, participants may overestimate their consent against university data security systems or underreport certain unwanted behaviours. However, surveys are carefully designed to minimise response bias through clear and neutral wording of questions and answer options. Another tool, the interview, was used to balance the bias that both methods might introduce.

3-2-4-4 Convergent Design for Data Collection

In addressing the research inquiries, a convergent mixed-methods design was employed to comprehensively investigate the multidimensional impacts of data breaches. Data collection was simultaneously conducted through interviews and surveys, facilitating an expansive exploration of the impacts of data breaches and an understanding of their evolving nature and trends. The integration of methods helped to gain benefits. The inclusion of qualitative data was deemed instrumental in presenting unforeseen insights and enriching the depth of understanding of the issue. The collection of quantitative data was beneficial to knowing the discerning prevalent trends and recurrent patterns in participants' answers. This methodological synthesis ensured a comprehensive investigation of the research issue, affording multiple perspectives through the concurrent employment of both qualitative and quantitative lenses. The following table shows the integration of the research inquiries.

Research Questions	Themes	Interview Questions	Survey Questions
What are the causes of the data protection breach in SA HEIs?	Experience a data breach	*Any university in the world is likely to be exposed to a data breach event, has your respected university experienced such an event before? What sort of data breach was it?	*Have you ever experienced a data breach incident within your university? (Q9 in employees survey / Q8 in students survey). *Have you ever experienced a data breach incident outside a university context? (Q10 in employees survey / Q9 in students survey). *If you have experienced a data breach, please describe the incident in more detail. What caused it and what steps could have been taken to avoid it? (Q11 in employees survey / Q10 in students survey). *Did you manage a personal data breach within your university? (Q12 in employees survey / Q11 in students survey). *If you have managed a data breach, then can you select what sort of data breach it was? (Q13 in employees survey / Q12 in students survey *Can you identify which of the following emotional responses you felt when your personal data had been breached? (Q15 in employees survey / Q14 in students survey).
		*What are the barriers? *What are the critical risks for the universities?	To what extent do you agree with the following statements: *I think that technical failings are the main cause of data breaches. (Q28 in employees survey / Q27 in students survey).

	Risk of data breaches	*What are the technical risks? *Could you tell me about the personal risks of data breaches?	*I think that weak employee practices are the main cause of data breaches. (Q29 in employees survey / Q28 in students survey). *I support this statement 'A frustrated employee/student presents a potential threat to breach data security by performing malicious acts'. (Q38 in employees survey / Q37 in students survey). *From your perspective, what are the following most common practices among employees/students that may lead to technical risks, which may cause data breach incidents? (Q in employees survey / Q29 in students survey). *From your perspective, what is the most harmful aspect of data breaches? (Q40 in employees survey / Q39 in students survey).
How do SA HEIs tackle personal data risks, including personal data policies and processes?	Data security policies	*Could you tell me the university regulations for data protection? *What can be done to support accessibility rights/ sides? *What can be done to manage the responsibility and accountability aspects effectively for protecting data?	*Do you know how your personal data is collected and processed by the university? (Q17 in employees survey / Q16 in students survey). *Do you know the data security policies adopted by your university regarding data breaches? (Q18 in employees survey / Q17 in students survey). *Do you know how you can make a complaint if your personal data has been leaked or disclosed to unauthorised individuals by the university? (Q19 in employees survey / Q18 in students survey). *Did you receive data security training when you were employed at the university? (Q20 in employees survey / Q19 in students survey).

		*Would you tell me about your university's IT infrastructure? What are the pros and cons? *Do university policies cover the personal aspects?	*In case you received training on data security from your university, select the type of training. (Q21 in employees survey / Q20 in students survey). *To what extent do you agree with the following statement 'I think that the data and information security awareness programmes provided by my university are sufficient'. (Q22 in employees survey / Q21 in students survey). *I believe that the technical tools adopted by my organisation are appropriate to minimise data breaches. (Q26 in employees survey / Q25 in students survey).
What are the multidimensional impacts of data breaches on stakeholders organisationally, technically, and personally?	Data breaches Impacts	*How does a data breach influence technically institutions and individuals? *Can you describe the organisational impacts of data breaches whether on the university or stakeholders? *What are the emotional consequences and impacts? Why do data breaches affect individuals emotionally? *Have you ever recognised any emotional reactions within	*To what extent do you agree with this statement 'I think that the information systems and networks used in my work environment are managed to reduce the impact of data breaches and information security incidents'. (Q27 in employees survey / Q26 in students survey). 'I am afraid that my personal data may be leaked to unauthorised persons, which may expose me to fraud, extortion, or anything that offends me as a result of that leak'. (Q32 in employees survey / Q31 in students survey). 'I have no concerns about the privacy of my data and personal information that I have provided to my university'. (Q33 in employees survey / Q32 in students survey). 'I think the emotional responses (reactions) of individuals such as anger, fear, anxiety…etc., represent negative consequences of data

		previous data security investigations?	breaches, which should be considered'. (Q34 in employees survey / Q33 in students survey). 'Too much provocation in the work environment increases employee anger and may result in intentional or unintentional data leakage'. (Q35 in employees survey / Q34 in students survey). 'I agree with this statement 'People who have enough security awareness would not be shocked if s/he experiences a data breach event'.(Q36 in employees survey / Q35 in students survey). 'It is usually an unpleasant experience for me when I have to disclose my personal data to the university due to trust issues'.(Q37 in employees survey / Q36 in students survey). 'I am interested in tracking rumours that some universities are facing data security problems, especially tracking data breach incidents in universities'. (Q39 in employees survey / Q38 in students survey). ' The level of my trust in the institution has changed after my personal data was breached. (Q16 in employees survey / Q15 in students survey). *How would you describe the technical impacts of data breaches? (Q31 in employees survey / Q30 in students survey).
			*What do you understand about data breaches? (Q6 in employees survey / Q5 in students survey).

Why do stakeholders think their personal data should be protected? How would they like things to change in terms of organisational, technical, and personal aspects?	Data breaches Awareness	*What do you understand when I talk about a data breach? [Then you might want to give an explanation of what you mean].	*Can you explain how data breaches happen? (Q7 in employees survey / Q6 in students survey). *One definition of a data breach is that it is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. Please indicate the extent to which you agree with this definition of a security breach. (Q8 in employees survey / Q7 in students survey). *I am interested in tracking rumours that some universities are facing data security problems, especially tracking data breach incidents in universities. (Q39 in employees survey / Q38 in students survey).
	Data protection needs and wishes	*What works well in terms of the data protection systems that are in place? *What could be done better? What would facilitate doing things better? *What can be done to improve these obstacles? *How your university IT infrastructure could be developed? *What needs to improve to reduce the impacts of such a breach?	*Which of the following aspects do you think are important for developing the process of protecting your personal data that you would like your university to adopt? (Q41 in employees survey / Q40 in students survey). *What are the changes you wish to see to improve the process of data security, and your personal data protection? (Q42 in employees survey / Q41 in students survey).

		*What could be changed, and why do we need to undertake this change? How would that be helpful? *What guarantees the best to boost data security?	
How do SA HE mitigation strategies help to manage and recover from security breaches?	Data breaches mitigation	*What is needed to recover from data breaches? *What can be done to diminish the emotional impact? *What can be done better to deal with victims of data breaches to repair trust?	*Do you think strategies to mitigate the impact of data breaches at the university are appropriate? (Q23 in employees survey / Q22 in students survey). *How would you prefer your university to treat you in case you are exposed to a data breach to mitigate the breach's effects? (Q24 in employees survey / Q23 in students survey).

Table 15 The combination of quantitative and qualitative questions.

3-2-5 Data Analysis

After the qualitative and quantitative data were collected, they were analysed to investigate personal data security dimensions in SA. The general method of analysis was thematic (Fugard, 2020) since the researcher aims to draw a series of themes and concepts from the data that identify the technical, organisational, and personal implications of data breaches and help to come up with response strategies for these impacts in Saudi HEIs. As previously mentioned in the research design, the convergent design was used. therefore, three phases were carried out for analysing data respectively 1- Qualitative data analysis by coding and classifying topics 2- Analysing quantitative data in terms of statistics 3- Analysing mixed methods data by merging the two databases.

The researcher was dependent on a side-by-side comparison approach, which practically means the researcher will first present the qualitative results (such as the topics) and then discuss the quantitative results (such as statistics) that confirm or oppose the qualitative results, that is interpreted as a comparison procedure within the discussion (Creswell & Creswell, 2018). Both design analysis methods and techniques are significant. However, the researcher was keen to analyse the data fruitfully and fairly to answer the research questions and find meaningful comparisons from a critical viewpoint.

3-2-5-1 Interview Analysis

To achieve the critical analysis, thematic content analysis and descriptive statistics were implemented after coding the data. Coding often adheres closely to qualitative data because of the complex and nuanced nature of the information gathered. For example, when analysing interview transcripts, specific themes and patterns must be carefully identified and categorised, which requires a detailed understanding of the context and subtleties in the participants' responses. Quantitative data could also be derived from qualitative data techniques in coding and analysing. Both qualitative and quantitative data were coded in a principled way after the types of data were identifiable (qualitative data/ texts) and (quantitative data/ nominal and ordinal data/ texts). Data Methods of analysing were organised and probed to present patterns and perspectives of data breaches in the Middle East.

Thematic coding was conducted on the interviews detailed in each case study. Initially, open coding was employed as the primary method of analysis, involving the segmentation of data into discrete parts and the creation of corresponding codes to label them (Khandkar,2009). Subsequently, axial coding was utilised to explore the connections between various concepts and categories that emerged during the open coding phase, aligning with the approach recommended by Vollstedt and Rezat (2019). Finally, selective coding was employed to integrate all the categories into a cohesive framework centred around a core category (Kaiser & Presmeg 2019).

NVivo was the software package used for data analysis in general, as it is a widely used package for analysing qualitative and quantitative data, as well as helping to code and classify topics that support the researcher while writing results. After the translation of interview texts, data were transcribed, coded, explicated, and analysed using thematic content analysis in NVivo (Version 12). (Refer to Appendix H to see an example of coding by NVivo). The quantitative survey data were coded into SPSS. As an additional tool, Excel was used for calculating a few mathematical operations and designing charts. All these programmes were chosen regarding their analytical makings as well as activable support to both Arabic and English languages. The table summarises the data techniques involved in this study.

Collected method	Data type	Analysis method	Coding method	Analysis app
Interviews	Transcribed text	Thematic Analysis	Open coding ê Axial coding ê Selective coding	NVivo (Fundamental) ê SPSS (Essential) ê Excel (Optional)
Surveys (Closed questions)	Nominal and Ordinal Data	Descriptive Statistics		
Surveys (Open-ended questions)	Transcribed text	Thematic Analysis		

Table 16 Data analysis

Interview Coding

All interviews were transcribed, and then all interview transcripts were translated into English, furthermore, the original copies of the interviews were preserved in Arabic. Transcripts were meticulously compiled using Microsoft Word, and each file was anonymised for confidentiality. To facilitate a systematic comparison between the two university cases under investigation, interview files for each case were aggregated into distinct matrices. The subsequent coding procedure was initiated using Nvivo12, a tool selected for its adeptness in efficiently managing and organising qualitative data, as advocated by Maher et al., (2018) and Jackson (2019).

In the initial phase of analysis, the researcher has undertaken several steps, including (1) transcribing and translating the participants' answers, (2) creating a new project within NVivo, (3) importing the participant responses, (4) creating the nodes, (5) reviewing and moving the content to the appropriate node. Participants' names were encrypted, and unique identifiers were given to records of their contributions after the interviews were translated and transcribed. The first letter of the interview file name stands for the first letter of the university name, KSU (S) and TaibahU (T), to discriminate the interview names among cases (universities), as these interviews were convergently translated and transcribed. Different inductive codes have been developed by using NVivo for each case, according to their relevance to the data. Some of the main codes were split into subcodes according to the broadness of the code and the amount of information provided by interviewees. Table 17 shows the file names for each case.

University Name	Interviews' Files Names
KSU	SAA, SAM, SDA, SHA, SLI, SMJ, SMO, SNO, SSA, and STG
TaibahU	TAD -TBV, THM, TMO, and TSA

Table 17 Files names.

In the open coding phase, raw data was broken into discrete elements, allowing the researcher to identify key concepts and patterns. For example, at King Saud University (KSU), issues like technical risks (e.g., DoS attacks, hacked USBs) and organisational risks (e.g., low budgets, lack of qualified staff) were identified, capturing the core concerns of the university. Similarly, at TaibahU, open coding revealed risks like human factors and lack of budgets under organisational risks, and software updates, external attacks, and human errors under technical risks. This demonstrated the different nuances and challenges faced by each institution. Axial coding followed, grouping these open codes into broader categories and exploring how they were interconnected. For instance, at KSU, human errors were grouped under technical risks, while the lack of qualified staff was linked to organisational risks, helping to clarify the relationships between different risk factors. At TaibahU, external attacks and human errors were organised under the technical risks category, while human factors and budget issues were categorised under organisational risks, showing a similar but distinct set of organisational concerns. Finally, selective coding synthesised these findings by identifying overarching themes, such as personal data management risk, which served as a central focus for both KSU and TaibahU. Through this coding strategy, the researcher was able to develop a clear and focused thematic structure for the qualitative analysis chapter, ensuring that the findings were both comprehensive and precise. The systematic organisation of data allowed the researcher to present key insights and establish connections between themes, facilitating a deeper understanding of the research topic and supporting comparative analysis across cases (Kaiser & Presmeg 2019).Tables 18 and 19 show the coding in both cases.

Coding		
Case	King Saud University KSU	
Selective codes	**Axial codes**	**Open codes**
Stakeholders	Managers	Data security, networks, social worker, psychologist, administrative, user services, electronic transactions.
Data breaches awareness	Data	Data centre- General data- Personal Data- Research data- Sensitive data.
	Data breach	Access attempt- Data leak- Data loss- Deliberate penetration- Digital applications- Digital Era- Fraud- Non-deliberate penetration- Theft.
	Breach causes	Digitisation of information services- Financial causes - Hackers- Psychological causes - Social causes.
	Breach reporting	Audio record- Chat- Video call.
Advantages of personal data management	Strengths	Awareness emails- Codified permissions- Determine responsibilities. - Electronic crime system- Fighting the exchange of passwords- Following up Identity authentication- Laws- NCSA Commission- Passion- Promote belonging- Suitable programmes- Systems
	NCSA roles	Instructions- Mandatory notification- Periodic inspection- Software standardisation- State regulations- Workshops
Personal data management risk	Organisational risks	The absence of qualified- Low budget- Poor management of the breach.
	Technical risks	Limited technical skills- Sharing passwords -Weak passwords- Human errors- Dos attack- Hacked USB- C & C attack- Hardware failure- System updates from Microsoft.
	Personal risk	Empathy- Over trust.
	Difficulties	Awareness- Commitment.
Organisational personal data management landscape	Policies	Access permissions- Access rights- Personnel policies- Responsibility and accountability- Sanctions- Student policies- Visitor policies.
	IT Infrastructure	Antivirus software- Compatibility and proportionality- Firewalls- Intrusion deterrent programme- ISO Standardisation- Ongoing support.
	Organisational effects	Budget- Performance- Reputation- Service.

Data breaches impact		
	Emotional effects	A feeling of insecurity- Anger- Anxiety- Depression- Disappointment- Distrust- Embarrassment- Lose confidence- Negative effects- Panic- Sadness- Shock.
	Emotional impact factors	Age- Awareness- Culture- Experience- Level of education- Social situation.
Social data security landscape	Islam culture	Integrity- Honesty- Permission- Privacy.
	Community traits	Customs and traditions- Modern families- Negative perceptions- Society's perception- Traditional families.
Data breaches management	Mitigation	Acknowledgement- Containment- Diagnosis- Isolation- Offender recovery plan- Mitigating Plan- Repairing Trust- Responsibility- Treatment- Understanding - Victim recovery plan
	Plans	Compulsory Training- Data management- Proactive plans- Update passwords Updating data.
Personal data management needs and aspirations	Technical needs	Software maintenance- Software development- System maintenance- Firewalls.
	Organisational needs	Training - Personnel qualifications- Subspecialties- Monitoring (control giving permissions) - Courses (awareness sessions- cyber security- protect personal data identifying sources of risk)- Raising awareness.

Table 18 Codes for KSU.

Coding		
Case	TaibahU	
Selective codes	**Axial codes**	**Open codes**
Stakeholders	Managers	Data security, infrastructure, beneficiary Care, administrative.
Data breaches awareness	Data breach	Access- Illegal use- Personal data- Privacy- Private data- University's data
	Breach causes	Exploitation- Bullying- Defamation- Extortion
Advantages of personal data management	Strengths	DPL Law- Integration- Multilayers Protection- National Access Service- Presence of the NCSA.
	NCSA roles	Cloud storage -Reporting -Supervision -Updated instructions
	Platform	Haseen

Personal data management risk	Organisational risks	Human factors, lack of budgets
	Technical risks	Software Update- External attack- License renewal- Human Errors-
	Difficulties	Vulnerabilities- phishing- policies resistance
Organisational personal data management landscape	Policies	Safe use of assets- identities- Access- cybersecurity- commitment test- penalties- COVID-19
	IT Infrastructure	Antivirus software- Cooperation- Firewalls- Intrusion Prevention System – licenses
Data breaches impact	Emotional effects-	Anger- Depression- Destruction- Discomfort- Fear - Sadness- Shock
	Organisational effects	financial implications- Assets loss- recovery cost- Reputation- budget- Disable service.
	Emotional impact factors	Awareness- Breach's cause- Education- Social acceptance- Environment
	Breach causes	Exploitation- Bullying- Defamation- Extortion
Data breaches management	Mitigation	Blacklist- Cleaning- Containing- Investigation- Isolation- Notification- Tracking
	Plans	Breach dealing plan- Digital transformation plan - Collaborative programmes
Personal data management needs and aspirations	Technical needs	Backup - Permissions -Software- Systems.
	Organisational needs	Awareness- Unified Framework- Training-

Table 19 Codes for TaibahU.

It is noticed that the number of codes (138) in the first case (Table 18) was higher compared with the second case (78 codes) (Table 19). This was due to the high number of interviewing participants (10 participants) in the first case compared to the second (5 participants). Where the participants expressed a variety of keywords in the description. However, this is unlikely to influence the answers to the study's questions in the second case due to its completeness as the responses reached data saturation.

3-2-5-2 Survey Analysis

The data analysis was mainly performed using IBM SPSS version 26. Excel was used to enter data and design tables, and NVivo qualitative data analysis software was employed for open-ended questions. Various statistical tests were performed to study the relationships between variables and to determine the probability of associations between the two cases (groups). Because the aim of the investigation was to explore data breaches in two Saudi universities, the independent t-test was used to determine the differences between the two groups (cases/universities). The chi-square test and the Kruskal–Wallis H test were used to determine the level of probability of associations and the relationships between variables. The significance or confidence level was set to 0.05 for all statistical tests.

The data was analysed using a simple statistical description by first calculating the percentage frequencies. Then, an independent t-test was performed to identify the differences between the two groups (universities). The independent-sample t-test is defined as, 'a test that compares the means between two unrelated groups on the same continuous, dependent variable'(Daines, 2023). The survey answers were also analysed using cross-hypotheses to determine the differences in perceptions according to gender and age. These two variables are important indicators that can reveal societal aspects in the awareness of data breaches and their potential impacts.

In the section on analysing the contributions of faculty members, the variable of job level was measured in addition to the variables of gender and age. The job level variable was calculated to detect any potential differences in the awareness level between participants depending on their jobs. Because the age variable carries nominal data, a Chi-square test was used. The chi-square test is one of the Karl Pearson family, as explained by Franke et al., (2012) 'A test is used to examine independence across two categorical variables and to assess how well a sample fits the distribution of a known population (goodness of fit)'. While with the variables of job level and age, a Kruskal–Wallis H test was used because it contains ordinal data. The Kruskal–Wallis H test is one of the

nonparametric tests to examine the two-sample Wilcoxon–Mann–Whitney rank (Dai, 2017). The following mind map explains the analysis mechanism.

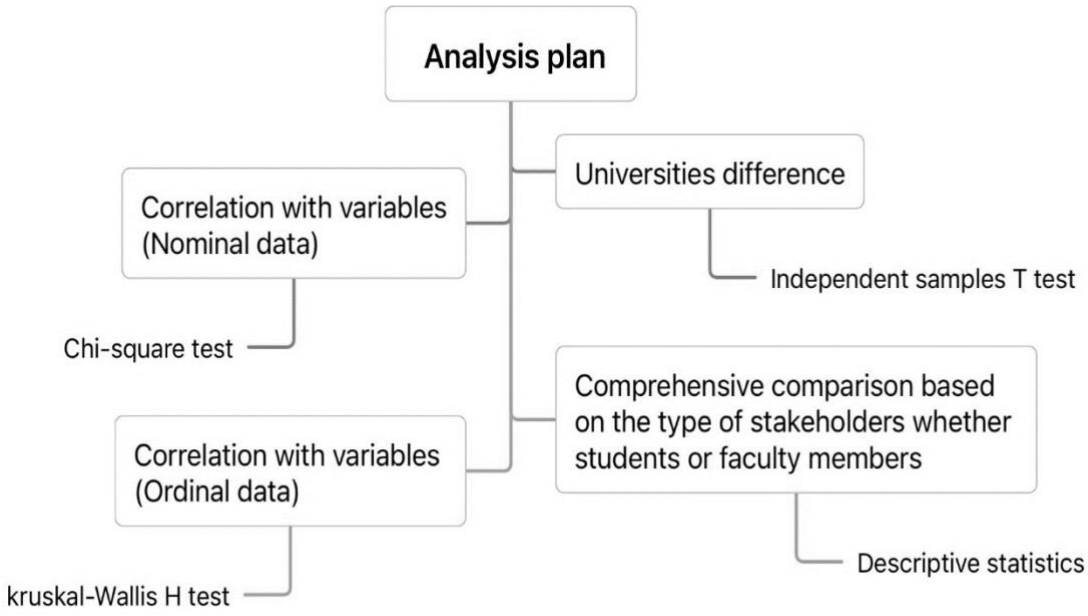

Figure 3 Analysis method and statistical tests used in the research.

Cross-responses were discussed and then compared statistically for the variables of gender and age to determine the relationships between them and to reveal any differences that contribute to the perceptions of personal data security investigated in the current research. The results for the faculty members are given first because they are part of the system in which students operate within the university, after which the results for the students are given. (For an in-depth analysis, refer to Chapter 5).

Statistical Tests Used

Several statistical tests were employed in the quantitative study to ensure a robust analysis of the collected data. Each test was chosen based on the type and distribution of the data and the research objectives:

1. **Independent t-test**: This parametric test was used to compare the means of two unrelated groups (the two universities). It assumes normal distribution of the dependent variable and equal variances between the

groups. The test provided insights into whether significant differences existed in the awareness levels of participants across the universities (Field, 2013).

2. **Chi-square test**: This nonparametric test was employed to examine relationships between categorical variables, such as gender and age. It is particularly useful for assessing independence between variables and determining how well the observed data fits expected distributions (Franke et al., 2012).

3. **Kruskal–Wallis H test**: As a nonparametric alternative to one-way ANOVA, this test was applied to assess differences among more than two groups for ordinal data, such as job level and age. It is appropriate when the assumptions of parametric tests (e.g., normality) are not met (Dai, 2017).

These statistical tests were complemented by descriptive analyses, including percentage frequencies, to summarise the data and provide an overall understanding of the key trends and patterns in the responses.

Survey Coding

The survey consisted of seven open-ended questions, which were analysed using NVivo software. Following a qualitative analysis approach, the texts extracted from the questionnaires were examined. Each question's responses were gathered separately and coded based on the topic. For example, the code for (academic discipline) included a variety of responses from 60 faculty members. Analysis revealed that these faculty members represented 42 different departments across two universities: 24 departments at KSU and 18 departments at TaibahU. (Refer to demographic data in Chapter 5).

The coding process for the questionnaires differed from that of the interview texts, with seven selective codes developed, including academic discipline, data breach concept, causes of data breaches, data breach experience, breach management, technical impacts, changes, and aspirations. This approach was taken to prevent issues with inconsistent coding of open-ended questions (Zhang et al., 2023).

Open-ended questions						
Code	**Faculty members' survey**	**Number of responses**	**Words count**	**Students survey**	**Number of responses**	**Words count**
Academic discipline	(Q4)	60	120	(Q4)	180	300
Data breach concept	(Q6)	41	218	(Q5)	81	340
Causes of data breaches	(Q7)	49	599	(Q6)	111	329
Data breach experience	(Q11)	32	500	(Q10)	67	592
Breach management	(Q14)	17	175	(Q13)	56	495
Technical impacts	(Q31)	9	53	(Q30)	43	259
Changes and aspirations	(Q42)	20	327	(Q41)	57	680

Table 20 Open-ended question codes.

3-2-5-3 Comparative Analysis

It is necessary to clarify the goal of the researcher in adopting a convergent mixed design, quoted from Morse (2000, p.122) ‘to obtain different but complementary data on the same topic’. Creswell (2018) advised analysing the two sets of qualitative and quantitative data separately and independently of each other using typical qualitative and quantitative analytical procedures. Therefore, the researcher relied on the recommended qualitative analysis tools in the sources of her scientific field, which is the field of information science. Pickard (2013) emphasises that qualitative analysis requires deep interaction with primary data and analysing it either line by line or word by word. The researcher consequently focused the qualitative analysis on understanding the experience and interpreting abstract words that she believed have a role in describing (managers) perceptions.

In the quantitative analysis, the researcher aimed to capture statistical perceptions from students and faculty members, providing quantitative data about these breaches, their effects, strategies for managing personal data security, and the needs and desires to reduce violations and enhance data security.

Following the analysis of interview transcripts and open-ended survey questions using NVivo software, and the closed-ended survey questions using SPSS software, the researcher gathered two sets of data: qualitative and quantitative. These data sets were integrated to achieve triangulation (Creswell & Plano Clark, 2006), enhancing the understanding. This approach captures the varied perspectives of managers, students, and faculty within the university context and enables comparisons between different university environments. For insights into the integration of both datasets in practice, reference should be made to Chapter 6.

3-2-6 Ethical Considerations

This research was approved by the UCL Research Ethics Committee under project number 21595.001. Alongside this, the researcher obtained the necessary permits to conduct the research at the two chosen Saudi universities from the Saudi Ministry of Education. (See Appendix A for permission letter).

According to (Pickard, 2013), the most transparent way to achieve informed consent is to prepare a formal informed consent form that is read, understood, and signed by all parties involved in the research. Therefore, the research objectives were explained to the universities, and they were given an initial copy of the survey and interview questions.

An information sheet was designed to explain all aspects of the research to participants (See Appendices C and E for the participants' information sheets). Additional details were attached to the information sheet, namely an interview consent form, indicative interview questions, faculty members' survey, students' survey, invitation form, and survey announcement. The researcher explained aspects of applying her research methods, such as the samples that will be taken and how to collect and analyse data, which can be summarised in the following points:

- ✓ Qualitative data was collected from managers (interviews), and quantitative data was collected from students and faculty members (online surveys).
- ✓ Participation in the research was voluntary, and the qualitative participant has the right to withdraw after one month of conducting the interview.
- ✓ The interview was scheduled with the participant according to the appropriate time and method (online / in person).
- ✓ The interviews were recorded after taking the participants' permission, and all texts were transcribed and stored in the data storage services at UCL.
- ✓ Participants were informed of the data preservation policy at UCL, and all data will be kept until one year after the completion of the PhD (September 2025), and the interview consent forms will be kept

until 5 years after the completion of the PhD and then will be destroyed in September 2029.

- ✓ Participants were informed of the contact information in case they wish to inquire or file a complaint.
- ✓ Participants were associated with pseudonyms to keep their data anonymous and to be referred to within the search based on public identifiers, for example, students, faculty, manager, technical, personal, etc.
- ✓ Participants understood that some of their answers would be used as quotations after being carefully screened.
- ✓ A cover letter was attached to the survey, and the Participant acknowledges his/her consent by continuing and accepting participation in the study.
- ✓ Surveys were distributed through university channels to avoid any irrelevant responses.
- ✓ All transcription and translation operations were carried out by the researcher.
- ✓ The participants were informed that the results of the research will be published in presentations and local and international conferences.
- ✓ Institutional approvals and individual approvals (written or electronic signatures) were obtained.

Every effort was made to explain the research to the participants and to take care that any data provided in this work does not expose the participants to any negative outcomes, for example, consequences if they did criticize their university. For this reason, all participants were speaking with organisational approval. Their responses were carefully anonymised in any outputs.

A risk assessment was conducted within UCL, and it was agreed that it is not expected that this research may cause damage to the reputation of the participating universities. On the contrary, it was suggested that by seeking solutions and understanding the issue of data breaches and their effects, the universities could potentially mitigate and minimise any potential breaches.

Nevertheless, it was noted to be important that the researcher did not include any sensitive information that might reveal weaknesses in university systems.

In relation to potential health risks, the research was conducted during the Covid-19 pandemic, but not during the lockdown. Therefore, the researcher respected all the instructions of the Saudi Ministry of Health regarding wearing masks and keeping social distance, took the necessary vaccinations before starting to collect data and presented the vaccination certificate granted by the British Ministry of Health.

Steps Taken to Protect the Personal Data of Interview and Questionnaire Participants

To ensure the protection and confidentiality of personal data, several precautions were taken to safeguard the privacy of participants and comply with ethical guidelines. The following actions were implemented to protect the personal data of interview and questionnaire participants:

- A risk assessment was conducted to ensure that all safety precautions were followed.
- Informed consent was obtained from all participants before the interviews and surveys.
- Participants were provided with detailed information about the research, its purpose, and the voluntary nature of participation.
- Personal data were anonymised by assigning a unique identifier to each participant to ensure their identity was not revealed in the data.
- Audio recordings of interviews were made only with the participants' consent and were securely stored.
- Interviews were transcribed and anonymised, removing any identifying details from the transcripts.
- All collected data, including audio files, transcripts, and survey responses, were stored on secure, password-protected systems at UCL.
- Data were stored separately from identifying information, further minimising the risk of identification.

- The data were retained according to UCL's data retention policies: interview transcriptions will be kept for one year post-PhD, while survey consent forms will be kept for five years.
- After the retention period, all data, including audio recordings and electronic files, will be securely destroyed in compliance with UCL's data disposal protocols.
- All data were used solely for the research study, ensuring that all participants were aware of how their data would be used.

3-2-7 Research Strengths

The researcher's knowledge, professional, and linguistic skills represent a strength of this research. Bland & Schmitz (1986) emphasised that knowledge and professional skills are priceless, given that the academic researcher is characterised by peer support/environment, and professional communication. The researcher's experience working in the educational sector, in addition to her scientific knowledge in information management, made understanding and interpreting data security aspects easier. The researcher designed a research framework in two completely different languages. (See Appendices C and E for the participants' information sheets available in English and Arabic). At each stage of the research, she converted words and sentences from English to Arabic. The process of transformation does not mean translating literally those words and sentences, but rather a deeper process that reflects the links between language and culture (Caminal & Di Paolo, 2019). Morel and Radic (2016) argued that language is a system for communicating ideas and feelings understood by a given society to the world. The researcher's language skills present an additional advantage to adapting and transferring the reality of Saudi data security from the Arabic language and culture to another language and culture.

Another strength of the research was the subject itself. According to Alzamil, (2018), although there are no statistical studies revealing security breaches and incidents in SA, information security threats are constantly increasing. In universities particularly, the possession of a large amount of personal data resulted in an increase in data breaches (Beaudin, 2015). Therefore, exploring

data breaches in Saudi HE and their impacts could be helpful in understanding and mitigating these breaches. By reviewing the literature, it has been found that there is a lack of studies discussing the multiple dimensions impacts of data breaches in the education sector, not only in SA but globally too. Despite the prevalence of data breach incidents in universities, there is a gap in coverage of the topic. In the UK, for example, several UK universities reported a data breach to the Information Commissioner's Office ICO in 2019 (ITProPortal, 2020). Therefore, this was a much needed and important study and as such, this was used to leverage sponsorship and then case study support.

The culture of the community was also a strength of the research. This study primarily examined a set of opinions and perspectives that emerged from the unique backgrounds, experiences, and ideas of individuals regarding data security within a particular community. The research aimed not only to explore the landscape of data breaches in terms of regulations, principles, and impacts but also to convey cultural perceptions of personal data protection. It tried to find paradoxes and approaches that are expected to create a kind of originality. For instance, the study highlighted the differences in personal influences and emotional responses based on gender, which enriched the understanding of data security issues within the distinct context of SA.

The mixed-methods implementation enriched the results because it provided quantitative and qualitative datasets. Although the study’s design was a case study, the quantitative statistics helped to generalise some results, and the qualitative findings developed a more nuanced understanding of the phenomenon. The mixed approach results helped to clarify personal data management in a complex environment, such as SA. The use of a convergent mixed methods design was chosen to diminish bias as much as possible due to the synchronisation and convergence of all stages.

Furthermore, the choice of the institution type boosted the ability to investigate different types of individuals/ perspectives who deal with multiple data risks in non-profit companies with varying capabilities and budgets, such as public universities. In this complex environment and with shrinking budgets,

universities are highly recommended to recognise the importance of data security and the need for continuous protection (Garrison, 2010). As universities have to play a lot of roles in the activation of the community partnership, and one of their duties is to secure personal data, hence, explaining the personal data protection strategies in educational institutions may inspire other types of institutions.

In addition, access to a sensitive sample as the participants in the interview (managers) represented a high category of members of the academic community. This sample was perceived to be disengaged in research due to the strength of their positions and the sensitivity of their responsibilities within universities which make reaching them extremely hard. In essence, the ability to reach and question managers and use their information brought an advantage to the results of the research.

In general, the research provided valuable information about data protection regulations in a developing country, which highlights an important aspect to the world about the state of data security in countries that are not covered mainly in scientific production. As the overall structure of the study takes the form of seven chapters, one of these chapters considers the Saudi data security landscape.

3-2-8 Research Limitations

This research is ambitious in the breadth of coverage and as such it could not go into as great a granular depth as would have been possible if it had been further focused. This choice was made in order to try and evidence the holistic connections of technological, organisational, and personal impacts. Legal considerations were a backdrop to these spaces. The work focused only on digital breaches. It would have been possible to broaden it out further to information security which would have drawn in physical security. The initial size and challenge of the literature review evidenced that confining the work to digital parameters was a sensible choice for a thesis.

Sampling posed a considerable challenge for the researcher given the expansive nature of Saudi HE. Consequently, the researcher opted for a multi-

case strategy to either present divergent findings or anticipate analogous results that substantiate specific scenarios about data security. Although there are over thirty public and private universities in SA, the study focused on two public universities, selected based on fundamental distinctions between them.

Additionally, the original community within the two cases encompassed various segments, including students, academic staff, technicians, managers, and others with a stake in good data management. Among students, distinctions were made between undergraduate and postgraduate students. Similarly, faculty members were categorised into lecturer, associate professor, assistant professor, professor etc. The study, however, concentrated solely on undergraduate students due to their representation of a substantial segment of the student population. In the case of faculty members, no discrimination was made among various ranks such as lecturer and assistant professor.

While these decisions regarding sample selection imposed limitations on the research, they served to enhance the researcher's awareness of the constraints inherent in the final sample when discussing the nature and implications of the research results (Pickard, 2017). Other studies could concentrate on a specific category of participants, studying more profoundly one effect of a data breach within that targeted group. Variables such as gender, age, school stage, occupational position, and awareness level may play diverse roles in understanding the effect.

15 interviews were conducted while the target was 20 interviews according to the theoretical contexts in the qualitative research (Morse, 2000; Pickard, 2013). Mason (2010) argues that studies that apply more than one method require fewer contributors. Thus, this type of research focuses on providing new information and avoids the repetition of data that could be made available by the higher number of qualitative interviews (Marshall et al., 2013). The researcher faced challenges in balancing the number of qualitative and quantitative samples across multiple cases. The inability to reach a comparable number of students, faculty members, and managers in one case compared to another was attributed to constraints related to time and response. The Covid-19 situation in addition limited reaching out to some candidates. The researcher

was flexible to work under the COVID-19 circumstances, as the research was conducted in line with appropriate safety guidance. All research was conducted on campus in line with each universities' safety protocols, e.g., social distancing, masks, and ventilation. However, the researcher could not achieve wider communication to reach participants.

There were difficulties relating to the topic area because disclosure of security concerns may conflict with individuals' privacy. Developing research on a sensitive area means considerably more than just getting some permits. Clear interview protocol, fair recruitment of participants, and appropriate methods of application were pondered to deal with the sensitivity of the topic. The risk assessment has been done within the UCL under the reference number (RA053567/1) before the results were achieved to reduce the likelihood of risks. All ethics papers have been approved by UCL. The research objectives and expected results have been explained to the included universities, and consent was obtained from both universities. The potential risks and consequences associated with this research have been considered through official approvals as well as logistical operations during all stages of research. Interviews have been designed under protocol including a list of questions that were reviewed before conducting interviews. Participants were contacted by their official email addresses for the invitation. (See Appendix B to read the invitation form). A questions list and research information sheet were sent to them before scheduling interviews to allow them to understand how data will be possessed, protected, and published. The researcher informed participants in advance of all the paramount details of the study objectives, expectations, time commitments, and how their data will be used and explained these elements twice at the beginning of the interview. Participation in the research was optional, and the participant could withdraw within a month from the date of the interview. (See Appendix D to review the consent form for managers). Participants were purposefully recruited by listening only to individuals who were already familiar with the different functions and politics operating within their universities.

The researcher introduced her identity to add a kind of credibility and clarify her profession to the participants. During the dialogue, the researcher created a

safe dialogue space by asking a general question and leaving the interviewer the freedom to answer and to dwell or not. The researcher relied on the participant being the one who leads the dialogue because of its great benefit in freedom of expression and storytelling. The researcher left time at the end of the interview for the participant in case s/he has information/inquiries that would like to add or put forward. The principle of navigation during the dialogue was adopted when the researcher felt that the participant did not want to talk about a topic due to its sensitivity. Thus, some qualitative answers were not given that the researcher thought were important. Surveys allowed free and frank anonymised data. The researcher was unable to know who exactly filled out the survey, and therefore she may get random answers that are likely to affect the accuracy of the results.

Furthermore, working across two languages brought some disadvantages to the research. Since the general context of the research was the discovery of the security organisation of the data in SA, it was relied on collecting some Arab sources to explain this context from its primary sources. In addition, the study community was an Arab community, as the study questions and data collection were conducted in Arabic. Arabic is widely considered one of the most difficult languages to deal with in a localisation context, based on data related to Arabic language use collected by, for example, Cote (2009); Haeri (2000), and Khalaila (2013), in terms of languages. They pointed out that the concept of the Arabic language includes three categories, such as Standard Arabic, Modern Standard Arabic, and Colloquial Arabic. However, to reduce the effects of dialect diversity, which may affect the success of communication, universities were selected in areas where the researcher understands the diverse dialects.

Interview Limitations:

Even though semi-structured interviews are valuable for gathering data and stories about data breach incidents, they provide insights into the causes, risks, and impacts of these breaches from a limited number of participants' perspectives. The interviews were conducted only with university managers who are expected to be highly trained in dealing with security aspects. However, stakeholders in universities are diverse, and not all are expected to have the

same level of awareness and experience in dealing with data breaches as qualified managers. Semi-structured interviews could be useful in capturing further effects if applied to other groups of stakeholders within the educational context. Nonetheless, if interviews had been conducted with students or academic staff, it would not have reduced the level of bias where the university would choose their representatives in participation.

The bias is likely not only due to participant selection but also to biases arising from the researcher's positionality, as mentioned earlier. The interviewer's interpretations and biases can influence question formulation, guide the flow of conversation, and impact how responses are understood, potentially undermining the reliability and validity of collected data. Moreover, the depth of information obtained from each participant may vary (Creswell & Creswell, 2018), leading to uneven coverage of perspectives on data breaches. Moreover, the logistical challenges of conducting interviews, especially during the COVID-19 pandemic, were significant. Access to participants required careful planning and coordination due to pandemic-related restrictions. Therefore, incorporating quantitative methods alongside interviews was crucial to minimise biases and ensure a well-rounded collection of primary data considering the COVID-19 pandemic.

Considerations for Gender-Specific Interview Settings

Several restrictions impacted the interviews, including whether they were conducted in person or remotely. In SA, female workplaces are often separate from male workplaces. Consequently, the researcher conducted in-person interviews with female managers and remote interviews with male managers. In total, the researcher conducted 15 interviews—10 with female managers and five with male managers. Of these five interviews with male managers, only one was conducted in person, while the remaining four were conducted remotely. The researcher favoured in-person interviews over remote ones, as they offered a more comfortable setting for participants to discuss the topic. In-person interviews also allowed for a better understanding of the interviewee's body language, which was particularly crucial when delving into the emotional repercussions of data breaches.

Another significant limitation noted was that at KSU, the researcher was required to have a third person present during female interviews, solely as an observer without interfering in the conversation. Even though the third party's role was passive, their presence might have consequences, possibly making participants less comfortable sharing their thoughts particularly if they have experienced personal breaches of privacy. However, equally, it was felt that the female participants valued the opportunity to meet and become comfortable interacting with the researcher.

Survey Limitations:

The surveys provide quantitative data that help explain some trends in data breach threats and impacts but do not reflect the overall landscape of educational data violations. Distributing online surveys may bring some errors in the sample, which may reduce the credibility of the results. Distributing the questionnaire also during the COVID-19 pandemic posed significant challenges. Social distancing measures and institutional closures hindered the effectiveness of distribution efforts, even with an online survey. Despite the universities' attempts to disseminate the survey via email to all members, participation rates remained low. To address this, the researcher employed multiple strategies to increase engagement and reach a broader audience. These included posting flyers at university locations, hanging them in various departments, manually distributing the survey link at university sites, and requesting faculty members to share the link within student groups. Additionally, a notable number of survey responses were incomplete, likely due to technical issues such as slow internet speeds or survey platform malfunctions. There were huge pressures on the internet infrastructure at this time. As a result, incorporating another data collection method was crucial to achieving a balanced approach during the pandemic in order to make reliable comparisons and conclusions, help achieve a variety of goals, and provide a complete description of cases (Sandelowski, 2000).

In summary, while interviews offer in-depth qualitative insights but are prone to researcher bias and logistical challenges during a pandemic, questionnaires provide a broader data set with less interviewer bias but are susceptible to

response bias and may not capture the same level of detail. Both methods have their place in research, and their combined use can provide a more comprehensive understanding of the research topic.

Impact of COVID-19 on the Study Design and Findings

The COVID-19 pandemic significantly impacted the early stages of this study, particularly the process of obtaining ethical approvals from the universities. Due to the health and safety restrictions imposed by the pandemic, the process of obtaining necessary ethical clearances was delayed. With universities transitioning to remote work and adjusting to new operating procedures, the approval process took longer than expected. In addition to the delays in ethical approvals, the pandemic also affected the researcher's interactions with the universities. Face-to-face communication was limited, and much of the correspondence had to occur through virtual channels, further contributing to the delay in obtaining permissions and coordinating with university departments. Despite these initial setbacks, once the ethical approvals were secured, the study proceeded, and the data collection process was carried out with the necessary precautions.

As for data collection, the researcher initially intended to conduct face-to-face interviews with managers, but the pandemic required a shift to conduct some virtual interviews using Microsoft Teams. While this adjustment ensured that the research could continue, it did alter the dynamic of the interviews by limiting non-verbal communication and face-to-face rapport-building. Additionally, while the researcher was able to distribute the surveys manually at the universities, the shift to remote learning meant fewer students and faculty were physically present on campus. This reduced the available pool of participants for in-person survey distribution. Despite these challenges, electronic distribution methods were used to gather responses, though the number of responses was smaller than initially anticipated.

While the pandemic affected the early stages of the study, including delays in obtaining ethical approvals and challenges in data collection, the analysis and interpretation of the data proceeded without disruption. The findings provide valuable insights into data protection practices in Saudi HEIs, and the impact

of COVID-19 was limited to the data collection phase. The study's later stages, including data analysis and writing, were conducted smoothly, ensuring the results remained robust and meaningful.

3-2-9 Alternative Methods

Human and social research is a fertile field for applying a variety of methodologies. Choosing the appropriate approach depends on many considerations such as the research objective, the level of accuracy, the form of the results, the method of analysis, and the target audience (Creswell & Creswell, 2018). This research can be conducted with alternative approaches to present and describe the events from different insights. The use of 'a qualitative approach can be highly suggested to capture individual perceptions and experiences of data breaches in university settings (Cohen et al., 2017). Qualitative research allows the researcher to fully understand the cultural and social complexities of a specific context. The researcher can take advantage of the strengths of qualitative research to build a philosophical dialogue that critically explains the research problem (Bloomberg &Volpe, 2008). The researcher can reduce weaknesses in qualitative research by applying multiple qualitative instruments. However, opting for a qualitative approach in the present study raises challenges, as the researcher would face difficulties in controlling bias stemming from her position within the university. Moreover, limitations may arise from the universities themselves in selecting representatives who may potentially present curated narratives.

It is also possible to select a specific event and conduct 'an event study approach' to measure the effects of a certain event on a group of people affected. This methodology is extremely effective in capturing the actual effects, whether technical, organisational, or emotional. However, it cannot be applied to the current research because the researcher was unable to access incidents officially reported by universities where data security management mechanisms are currently under development in the country. In addition, it is believed that focusing on a particular event inside the university would bring reputational risks to the university. It is believed that this method is very successful in institutions with superior capabilities to detect incidents of data breaches and inform stakeholders thereof. Thus, the researcher adopting this method can track the

event and evaluate the effects, the level of influence, and the change rates efficiently and comfortably. Although this approach is strongly used in various fields, such as business (Jeong et al., 2019), some researchers in social fields have adopted it to investigate the security risks of data breaches in HE by examining reported breaches between two time periods (Garrison, 2010). Therefore, this approach would be suitable for tracking the effects of data breaches if it fulfils the element of reporting incidents, which cannot be guaranteed within the scope of the current research.

The ‘experimental approach’ can also be employed by designing an experiment to measure emotional effects, following the steps outlined below:

A. Select a category of stakeholders in the educational sector, such as ‘students’, ensuring homogeneity in their characteristics.
B. Formulate two groups, an experimental group, and a control group, to discern differences.
C. Introduce the experimental variable (independent) by exposing them to a simulated data breach incident.
D. Isolate the independent variable from the control group and subsequently inquire about their feelings if they were subjected to a breach.

In both groups, observation serves as a data collection tool by gauging differences. It is strongly believed that emotions such as fear, anxiety, shock, sadness, frustration, joy, and sympathy can be externally observed in individuals' behaviour (Kim & Cameron, 2011). This observation encompasses aspects like the disorder of individual movements, and changes in facial coloration, among others. The two experiments could be recorded, and the behaviour of individuals analysed using programming languages such as Python to identify distinct behaviours. However, the drawback associated with applying this approach lies in its considerable expense and the necessity for a diverse research team with backgrounds spanning social research, psychology, and technical expertise.

Summary

The methodology for investigating personal data breaches within the settings of Saudi (HEIs) was outlined in this chapter. The research design and the selected methods for the study, including semi-structured interviews and online surveys, were described. Two case studies, KSU and TaibahU, representative modules of public Saudi universities, were characterised, providing general information about the study participants at each institution. The study employed a convergent mixed method. The chapter explains the methods used for data collection and analysis and provides an overview of the ethical considerations, strengths, and limitations of the study. Finally, alternative methods for studying data security issues were suggested for future research.

Chapter 4: Qualitative Analysis of Interviews

Introduction

This chapter qualitatively studies the landscape of Saudi data breaches and the multidimensional impacts of these breaches, from perspectives that draw in the technical, organisational, and personal impacts. This investigation focused on two specific cases within the Saudi HE context, namely KSU and TaibahU. An analysis of primary qualitative data was conducted using a sample of 15 participants, involving managers (data security and information technology managers, social workers, and psychologists) from two respected Saudi universities. As detailed previously in Chapter 1, this research stakeholders are divided into three categories: managers, students, and faculty members.

For the qualitative data, the focus was on the category of managers, with input from 15 managers. Chapter Five will introduce quantitative data including a wider group of stakeholders, namely students and faculty members. The examination centres on the data security issue, investigating various facets, including breach risks, vulnerabilities, and challenges, as well as the landscape of IT infrastructure. Additionally, the chapter explores the multidimensional impacts resulting from breaches, including their technical, organisational, and personal dimensions. It further investigates breach management and mitigation strategies, elucidating the responses to and resolutions of data breaches. Moreover, the chapter sheds light on the aspirations of managerial stakeholders for organisational change in the context of data security.

This chapter began by analysing the findings from KSU and then TaibahU, maintaining a flow of themes. These themes encompassed awareness of data breaches, experience and management, technical, organisational, and personal (including emotional responses) perspectives of managers on data breaches, needs and wishes, and breach mitigation. It concluded with a comparative discussion of the findings from both cases.

4-1 The Language Issue in Analysis

One part of the learning from this study was the complexity of providing understanding across cultures and languages. This finding emerged most particularly through the interview analysis and as such is presented here. The researcher worked across two languages to analyse the primary qualitative data. As the work analysing the interviews evolved, this revealed the challenges of working across cultures and languages. She acknowledged some challenges in situating Arabic cultural concerns into English, particularly in terms of language. Although all of the participants' texts were translated, there are some words that the researcher could only translate literally.

Descriptive names, such as those associated with Saudi projects, like the 'Haseen' platform and its English synonym 'immune,' have not been translated. If the English synonym is used, it cannot refer to the ‘Haseen’ platform. Similarly, the term 'Kollona Amn' platform, which means 'we are all safe' in English, has not been translated. Some Arabic words have a synonym in English but are used extensively with Arab pronunciation, even among some English readers interested in Arab culture. For example, the words 'Alhamdulillah' and 'Mashallah'; the first might be used with a specific adjective to convey complete satisfaction, and the second is employed to express someone's admiration for something. Although the researcher can exclude these words because they do not significantly affect the answer, they do impact a full understanding of the participant's position on a particular question. The researcher's goal was to investigate different perceptions, encompassing satisfaction or dissatisfaction, as well as satisfaction or dissatisfaction with personal data security management at the level of a system, programme, law, or service.

One of the challenges that the researcher also faced was the issue of syntactic differences related to the syntax/structure of the two languages. This can change the emphasis and meaning. The fact that Arabic and English are completely different is illustrative. There are some syntactic differences:

Word Order: English and Arabic follow a Subject-Verb-Object (SVO) order, but in Arabic, the verb often precedes the subject and object.

- Arabic (VSO)e.g., يمكن أن الانتهاك (Could a breach).
- English (SVO) e.g., 'A breach could'.

Verb Conjugation: Arabic Verbs are conjugated based on the gender, number, and person of the subject while English verbs are less inflected often involving just the addition of 's' for the third person singular.

- Arabic e.g., يُعتبر تأثير انتهاك البيانات خطيرًا جدًا
- English e.g., The impact of a data breach is very serious.

Pronouns: Arabic pronouns are attached to verbs, prepositions, or conjunctions but English pronouns are generally standalone words.

- Arabic e.g.,تراعي الجامعة أهمية حماية بياناتها
- English e.g., University considers the importance of protecting its data.

Moreover, another challenge that has been considered revolves around the issue of equivalence. As emphasised by Akan et al (2019), equivalence constitutes a fundamental concept in any language. Kashgary (2011) demonstrated that certain Arabic words possess multiple hyponyms, presenting a scenario where English lacks corresponding equivalents.

- Arabic e.g.,تصنيف البيانات وفقًا لأهميتها
- English e.g., Classifying data according to its importance.

As literal a translation as possible was provided for the quotes given in this chapter. Sometimes this means that the translated quotation in its literal form does not emphasise the professional and critical capabilities of the person being quoted. In a professional context, language is most normally edited to present education and professionalism, but this can create a loss of meaning across languages. It is important to highlight the expertise of the managers who took part in the interviews. In a wider research context, the global language of science has been English and yet the shifts that occur in translations are often not a part of the presentation of research articles. However, literal translations can potentially mean that countries not operating in English appear somewhat less expert in a domain under discussion, which is certainly not the case. Properly drilling down into and understanding these considerations is important

in terms of thinking through the analysis and findings. The work on this is an important part of the development of the value of this research.

4-2 Interviews Participants

The interview participants for this study were carefully selected to represent a diverse group of managers from two prominent Saudi universities. This sample consisted of 15 individuals (10 from KSU and 5 from TaibahU) holding key positions, such as presidents, data security and information technology managers, social workers, and psychologists. The age distribution of the participants ranged from 25 to 54 years, with 26.6% aged 25-34, 53.4% aged 35-44, 20% aged 45-54, and a median age of 35.8 years. Gender-wise, the sample was predominantly female, with women constituting 66.6% of the participants, a reflection of the researcher's easier access to female workplaces due to the separation between male and female departments, while men accounted for 33.4%.

Educationally, the majority held advanced degrees, with 80% having completed a master's degree and 20% holding a bachelor's degree. The participants also represented a broad range of academic disciplines, with 20% from Computer and Information Sciences, and 13.3% each from Business Management, Sociology, Computer Engineering, Cyber Security, and Computer Information Systems, while 6.7% each were from Psychology and Software Engineering. This diversity in scientific disciplines suggests a variety of scientific experiences among participants. Notably, 20% were specialists in computer and information sciences, and 46.6% had subspecialties within computing. This indicates a trend of appointing individuals with technical backgrounds to leadership positions in information and data security, often supplemented with administrative training to manage diverse responsibilities. This diverse and highly educated group of managers provided valuable qualitative data, offering a comprehensive understanding of the perspectives and experiences within their respective fields. Table 21 summarises the demographic data of interviewees at both universities.

Characteristic	Category	N	%
University	KSU	10	66.6 %
	TaibahU	5	33.4 %
Age	25-34	4	26.6%
	35-44	8	53.4 %
	45-54	3	20 %
Gender	Men	5	33.4 %
	Women	10	66.6 %
Highest level of education completed	Bachelor's degree	3	20 %
	Master's degree	12	80 %
Discipline	Business management	2	13.3 %
	Sociology	2	13.3 %
	Psychology	1	6.7 %
	Computer and Information Sciences	3	20.1 %
	Computer engineering	2	13.3 %
	Cyber security	2	13.3 %
	Software Engineering	1	6.7 %
	Computer information systems	2	13.3 %

Table 21 Demographic characteristics of participants.

4-3 Qualitative Findings

4-3-1 King Saud University (KSU) Results

Ten managers were interviewed at KSU, comprising six technical directors, two social workers, one psychologist, and one administrative director. Their perspectives were categorised into 7 themes to achieve the research objectives, including awareness of data breaches, perspectives on technical, organisational, and personal impacts (emotional) in terms of causes, risks, and effects of breaches, suggestions for enhancing data security measures, and strategies for mitigating breach impacts.

4-3-1-1 KSU Managers' Awareness of Data Breaches

Five participants at KSU defined the concept of a data breach as unauthorised access to a university's data system and unfair use of data for various purposes. The purposes of breaching could be categorised into five responses: (1) data theft, as mentioned by three managers; (2) data alteration, damage, or destruction, as stated by two managers; (3) data possession and ownership, as noted by two managers; (4) data exploitation, as indicated by two managers; and (5) data loss, as mentioned by one manager. Additionally, one manager highlighted that the data stored in their university systems could include administrative, research, or personal information and that data types potentially shift the nature of the data breach.

The differences in the professional roles and experiences of the participants did reveal insights into different views in terms of the concept of a data breach. One technical manager described a data breach as follows: ‘Accessing university information systems to either destroy, steal or possess sensitive data by unauthorised persons’. Technical managers described a data breach’s impact on a system or the organisation, whilst managers with differing experiences described impacts more related to individuals. This is evidenced by a psychologist, ‘A data breach is entering a person's privacy or swimming into a world other than yours, and you have no right to enter’.

This highlights the differing views on defining data breaches among managers at KSU. Technical managers emphasised technical and operational impacts, whereas managers with social and psychological backgrounds concentrated on the violation of personal privacy and its ethical and individual consequences. However, regardless of these differing perspectives, the concept of a data breach remains flexible. As a social worker noted, ‘A breach is a broad term’. Therefore, this term included unauthorised access to data, alteration, destruction, damage, possession, exploitation, loss, theft of data, and violation of individuals' privacy. These differences can be explained by understanding the responsibilities of each of these positions and therefore their role preoccupations. Nevertheless, it is important for the roles to have as full an insight as possible into the nature and impact of data breaches.

4-3-1-2 KSU Managers' Experience and Management of Data Breach Incidents

Six managers discussed topics related to the experience and management of data breaches. Three of them were IT managers who outlined challenges at the university that could potentially facilitate a data breach. One director addressed issues involving command and control attacks and malware, another highlighted network issues like Windows problems and updates to personal IDs, and a third director mentioned concerns related to third-party interactions and unauthorised access to university systems.

None of the participants explicitly confirmed having direct experience or knowledge of any data breaches but rather reported some risks that they faced in managing data security. One participant stated that ’during my period of work, we have not been exposed to a data breach, like other universities, we are facing some activities that may potentially create vulnerabilities in the security of systems’. Another manager described the university's response to a data breach, mentioning that ‘Data protection support personnel may work over 24 hours to deal with and solve the problem’. This position was repeated in interviews with participants beyond the technical domain, where likewise, there was no direct knowledge of data breaches occurring. One social worker mentioned, ‘I have not previously dealt with an individual who has experienced a data breach within the university’.

Overall, the statements from the six managers at KSU presented diverse viewpoints on experiencing and managing data breaches in theory, acknowledging them as a real threat. As such, although none of the managers explicitly reported a data breach, they highlighted ongoing challenges and risks that pose potential threats to data system security. These include issues like command-and-control attacks, malware, network vulnerabilities, and concerns related to interactions with third parties.

4-3-1-3 KSU Managers' Technical Perspectives on Data Breaches

By asking about the information technology infrastructure at KSU, the researcher observed participants' satisfaction with the IT infrastructure and confidence in the systems. There were responses that indicated this satisfaction, as one of the participants commented, ‘we have a good infrastructure’. Likewise, others stated the following: ‘I think the IT infrastructure is very suitable’, ‘We have suitable programmes’, and ’the IT infrastructure at KSU is quite suitable’. One of the managers justified her positive opinion due to the presence of backups, as she commented that, ‘we have backups of everything’. Another stated, ‘we can always refer to the backups and control the data through the data centre’. Technicians, regardless of the teams they supervised, felt confident in the sufficiency of the university's IT infrastructure. The participants named some of these programmes that justified this position, e.g., the Organisation Development Programme ODP, Firewalls, and Incident Deterrence and Response (IDR).

Some technical risks encountered by the university's data systems were reported, such as malicious viruses and DDoS attacks. After tracing the attack's sources, they explained that those attacks occurred due to internal sources (e.g., poor practices). According to responses from four managers, poor technical skills pose a significant risk, leading to various security threats such as clicking on phishing email links, username issues, sharing passwords, setting weak passwords, and using virus-laden USB devices. One of the technical managers acknowledged that such viruses could disable access to the university's servers and networks until the repair is completed. One of the technical participants talked about a specific attack as follows: ‘we were constantly exposed to attempts to hack into our data

systems, like Command-and-Control attacks(C&C), a device controlled by an attacker that sends commands to the university system by using malicious vulnerability (malware) to seize our data’.

It was noted that at KSU, four participants explicitly mentioned the use of ‘backup copies of everything’ as a safeguard against potential data breaches or natural data loss scenarios, such as power outages. One participant emphasised the role of backups in ensuring operational continuity, stating that the data centre's redundancy systems allow for immediate recovery and restoration following incidents. This proactive approach aligns with compliance audits conducted by the NCA, demonstrating the institution's commitment to maintaining robust recovery mechanisms. Additionally, KSU participants highlighted the role of backups in their broader incident response plans. For instance, during breach attempts, strategies such as isolating compromised networks and identifying attack sources depend heavily on maintaining reliable backups to minimise data loss. This reliance underscores the integral role of backups in preventing operational disruptions and safeguarding sensitive information.

Overall, there was satisfaction and confidence with the information technology infrastructure, including the programmes and protection systems at KSU. In practice, the absence of actual data breaches would seem to indicate a basis on which the participants were able to be confident in their systems. However, several technical risks impact data security, such as cyberattacks, viruses, and insufficient technical skills. This gap between the perceived adequacy of the infrastructure and the ongoing security threats highlights the necessity for continuous improvement and diligence in cybersecurity practices. A manager said ' If not dealt with these technical issues professionally, these may lead to a breach of data, systems, and networks'. The following table summarises an analysis of KSU of the managers’ technical perceptions.

Aspect	Summary
Backup Systems	Backups of data.
Programmes and Protection Systems	Organisation Development Programme (ODP), Firewalls, Incident Deterrence and Response (IDR),
Technical Risks Reported	Malicious viruses, DDoS attacks, internal poor practices
Security Threats Due to Poor Technical Skills	Phishing email links, username issues, sharing passwords, setting weak passwords, virus-laden USB devices.
Impact of Viruses	Disabling access to the university's servers and networks until repairs were made.

Table 22 An analysis of KSU of the managers' technical perceptions.

4-3-1-4 KSU Managers' Organisational Perspectives on Data Breaches

KSU operates within special regulations and policies for data protection. One participant described these policies as, 'excellent, Mashallah'[7]. The university has policies for accessibility and accountability, to define aspects that regulate data access permissions and accountability for data protection delivery. One participant stated that 'Authorities in the university are considered to define aspects of responsibility and accountability'. The university also follows strict procedures to control data availability, according to one manager, 'The data

[7] 'Mashallah' is a frequently used term in an Islamic context, expressing appreciation, admiration, or gratitude for something good or beautiful. It holds deep significance within Islamic culture, commonly spoken when praising achievements, blessings, or physical appearance. The phrase embodies humility and gratitude by attributing all goodness to Allah's will. Originating from Arabic, 'Mashallah' combines 'Masha', meaning 'to will' or 'to wish', with 'Allah', meaning God. Together, it translates to 'What Allah has willed' or 'What Allah has desired', reflecting a profound acknowledgment of God's blessings (Mohsin & Main, 2024).

access process takes a long scenario to verify identity and authentication to provide data security'.

Five respondents commented that the data security policies are straightforward and updated frequently. Managers used the names of particular data security policies during their interviews to justify their knowledge of university regulations, such as the policy for accessing, the policy for using email, and the policy for accessing networks. One participant said that there are data security policies for each category served by the university, whether students, faculty, or visitors. Another mentioned that the university has a policy for third parties in terms of using the university data as follows: 'We require the third party to sign a contract that spells out various terms... so, that we can provide protection for the stored data and control over availability and accessibility'.

KSU appears to have developed robust data protection policies and procedures. This positive reception underscores KSU's proactive approach to protecting data through accessible and accountable regulations. For instance, the policy outlining consequences if confidential data is mistakenly sent via email within the organisation emphasises a culture of responsibility. A manager stated, 'If recipient 'Y' receives such data due to sender 'X's error, 'Y' also bears accountability for any subsequent disclosure'.

All participants were satisfied with the data and information protection systems at the university. One manager said that these security regimes 'work well', another manager mentioned that they are 'strong', and another stated that they are 'excellent'. The participants each identified that they had a sense of safety due to the presence of the NCA, which directly supervises all Saudi institutions to guarantee their compliance with specifications and guidelines in terms of data security. One participant optimistically stated the following: 'The best development is the presence of the Authority, which supervises the digital transformation of our assets'. Another mentioned that the role of the Authority was as follows: 'Its role was not limited to a supervisory entity, but also as an educational entity' through courses offered to employees. Here the Authority directs them to deal with breaches of personal data, as well as to follow-up and audit annually with the university to ensure the validity of its

procedures and plans. As confirmed by one participant, ‘There are periodic visits and evaluation tours by the Authority’.

In addition, one participant explained a significant step has been taken by the state regarding data security, such as the ‘Kollona Amn[8]’ platform developed by the Ministry of Interior. This platform allows individuals to report breaches, impersonations, and any other threats. Furthermore, KSU follows strict procedures to verify the identity of the user, as an example of this, a manager explained that she uses a system developed by the university called ‘Tasks’, and said, ‘I use this app every working day, and each time I log in, I receive an automated call on my official number to verify my identity’.

Organisational risks include the lack of budget, the absence of qualified specialists, and insufficient technical awareness of both staff and individuals. Nine participants agreed with the seriousness of the human factor, as one participant indicated, ‘In my opinion, individuals are the main obstacle … in the data security system’. There were responses that pointed toward a blaming of individual users for the occurrence of a vulnerability where one participant responded, ‘Some individuals click on phishing links in spam email’, while another responded, ‘A user attempted to log into our data system incorrectly several times’. Others also reported some poor practices, such as sharing passwords between users, appointing weak passwords, and plugging breached (USB) drives into the university PCs, which could spread malware and other types of computer viruses to the university's system. In contrast, one manager rejected the idea that individuals were the biggest risk when managing data security when he responded, ‘The biggest obstacle to data protection is the progress of technology and the emergence of many viruses’. However, it is important to note that in an information security threat landscape, it is not just the biggest risks that matter but in fact every weakness within the system.

[8] A Saudi electronic platform that allows citizens and residents to submit security and criminal reports, reports related to personal life, threats, impersonation, and others, provided by the Saudi Ministry of Interior, available at the following link.
https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/

Regarding the organisational impacts, three managers highlighted a significant organisational impact of data breaches: data loss. Data is considered crucial for any organisation or university, and its loss can result in financial and reputational repercussions, affecting decision-making, resource allocation, and long-term planning at the university. A manager stated, 'The university loses part of its databases and data assets as a result of a data breach'. Additionally, data breaches disrupt information services and suspend university networks, severely affecting daily operations. This disruption hampers faculty, staff, and students' access to essential systems and resources, causing productivity losses and delays in educational services, particularly critical in today's reliance on virtual classrooms and distance education systems. A manager explained, 'Data breaches influence institutions and individuals by disrupting information and data services provided by the university'.

Moreover, data breaches cause reputational damage. Negative publicity from security incidents undermines trust among students, faculty, alumni, and funding bodies, potentially harming the university's reputation. Rebuilding trust post-breach requires substantial effort and resources. A manager stated, ‘Repairing trust after a data breach takes a long time'. For organisational implications, please refer to the following table.

Organisational impacts		
Impact	Data loss	Disable information services
Participant Identifier	SHA- SSA- STG	SAA- SMO
Impact	Drain the organisation's budget	Impact on university performance
Participant Identifier	SHA- STG	SAA
Impact	Network suspension	Reputational impacts
Participant Identifier	SMJ- SMO- SSA	SHA

Table 23 An analysis of KSU of the managers’ organisational perceptions. The identifiers (e.g., SHA, SSA, etc.) are anonymised codes assigned to participants to ensure confidentiality.

4-3-1-5 KSU Managers' Perspectives on Emotional Impacts of Data Breaches

This theme explored the emotional effects of data breaches. Each participant described the emotional impact of data breaches on individuals. The table below presents the various emotional reactions of individuals from the perspective of each manager.

Emotional impacts					
Impact	Anger	Anxiety	Depression	Disappointment	Embarrassment
Participant Identifier	SAM- SLI- SNO STG	SDA- SLI SMJ- SAA STG- STG	SDA- STG	STG	SLI- STG
Impact	Fear	Alienation	Distrust	Panic	Shock
Participant Identifier	SDA/ SLI SAA/STG	SLI SHA	SHA.STG	SDA/ SLI	SAM- SDA- SLI SMJ
Impact	Uncontrol Anger	Trauma	Discomfort	Sadness	Guilt
Participant Identifier	SDA	SDA- SLI	SDA- SLI- SMJ	SDA-SLI- SNO- STG	SNO

Table 24 Effects of emotional data breaches on individuals from KSU managers' perspectives. Participant identifiers (e.g., SHA, SSA) are anonymised codes assigned to protect interviewees' privacy.

Eight participants agreed that the emotional impact varies based on several factors, such as the type and extent of the data breach, the confidentiality and sensitivity of the data, the level of education, and the level of family openness. The latter represents a particular SA response to thinking about data breaches which would perhaps not be as evident in a Western response. A social manager presented the point of cultural understanding as follows: 'I believe the emotional impact is particularly strong on families that adhere to customs and traditions compared to moderate families. Traditional families are often fearful of society's opinion and concerned about negative perceptions that may affect their reputation. For example, the spread of a photo of a female victim without her hijab, resulting from the hacking of her personal data, has more negative effects on those who adhere to family values and societal norms'.

Another participant explained that these negative feelings are somewhat complex and described them as follows: ‘I believe these negative feelings can be prolonged and accumulate. The initial emotional risk is experiencing shock. After going through trauma, feelings of frustration and a loss of confidence may intensify, leading to anxiety. This anxiety can further escalate and develop into a persistent psychological state, either situational depression or chronic depression, which is considered a very distressing feeling’. Another participant expressed her feelings after being exposed to a data breach that she could not manage, but she strongly suspected that the breach happened outside of the scope of her university. She emphasised that ‘At that time, I felt shocked and became suspicious of all my dealings’.

Another participant described fear as an emotional response to a data breach, stating, ‘The feeling of fear can spoil the beauty of life. For example, if I were to imagine that there is a person in the department who hacks into my data, the fear would intensify daily. It would multiply even more when this fear is accompanied by the threat of exploiting my data’.

Another participant explained that exposure to a data breach can induce significant stress in individuals, making them highly reactive and prone to overreacting to minor incidents, much like a powder keg ready to explode at the slightest provocation. To illustrate this point, she said, ‘when a person is already under stress, it can cause him/her to explode from any situation. For instance, if you ask your sister, mother, or housemaid to make you mint tea and they forget to add the mint you specifically requested, you might refuse to drink the tea and become angry. It's not because they forgot the mint, but because your internal stress levels are very high, and your emotions are exaggerated and stretched to the breaking point’.

A manager addressed the issue of decreasing loyalty following the experience of data breaches, saying that ‘a data breach affects the level of student or employee loyalty, resulting in decreased loyalty. For example, the student may feel a lack of belonging to the university, and the employee may not perform their duties as expected’. It is important to emphasise that

‘loyalty’ holds significant value, supported by numerous studies confirming its importance among students and employees towards their universities.

The analyses conducted indicated the presence and significance of the emotional impact of data breaches as being well understood. One participant stated as follows: ‘For me, the breach of my data and theft is like a home breach and theft. The resulting emotional pain is the same regardless of whether the incident occurred in the virtual world or the physical world’.

In summary, emotional effects included responses such as anger, anxiety, carelessness, depression, disappointment, discomfort, disloyalty, embarrassment, fear, feelings of alienation, guilt, loss of confidence, panic, sadness, shock, trauma, and uncontrolled anger. In addition, these responses were both personal but intensified where there were additional organisational and family consequences. The findings show that the emotional impact varies based on factors such as the type and extent of the breach, data confidentiality, sensitivity, education level, and family openness.

4-3-1-6 KSU Managers' Needs and Wishes for Data Protection

To enhance the security of personal data, KSU does need to develop additional data security training programmes, raise awareness more widely amongst those with the benefit of understanding better how data is protected, and inform them of the sources of risk. KSU should consider proactive maintenance of systems, software, and hardware. In addition, it is important that clear processes are in place to notify affected people if their data has been breached, including considering the support that is put in place, given the noted emotional impacts of data breaches. KSU in addition needs to customise the accessibility of data. A technical manager explains this point of levels of permissions for staff, ‘Permissions are very important for data security and are distributed in different stages and levels. For example, technical personnel must not be classified to the same degree and have the same authority’. Additionally, two KSU managers suggested a desire to continuously develop backup systems to align with evolving cybersecurity threats. Advanced technologies, such as cloud-based backups and automated redundancy checks, were identified as

potential areas for improvement to ensure consistent data recovery and protection.

There were demands from managers at the technical level, such as qualifying technicians, updating protection systems, adopting new systems to deter viruses, and pushing employees to obtain Cisco certifications. All participants expressed concerns about the level of individual awareness, accordingly, from their perspectives it was necessary to increase workshops related to data security. However, in addition, there were demands from managers at the entertainment level, such as holding workshops that adopt activities to reduce the pressures of life and digital dealings, such as free writing to express concerns and encouraging the practice of some spiritual exercises like yoga. Considerations of staff and individual well-being are often not a part of data breach responses and systems. Therefore, these were innovative findings with the potential to improve data breach responses.

4-3-1-7 KSU Managers' Insights on Mitigation of the Impact of Data Breaches

Participants explained that the university has plans to reduce the impacts of data breaches. One manager revealed that ‘we have plans to deal with a data breach, before, during, and after the breach, we have plans in place to deal with any potential breaches’. As soon as a violation occurs, the responsible authorities of the university meet to manage and investigate a breach. These committees include members from the Deanship of Electronic Transactions and members from the department in which the event has occurred. They communicate with the University's Department of Senior Management to make the appropriate decision and to inform the NCA Authority. This was reflected in one of the manager’s answers, ‘You know that the HR Department deals with personal data related to employees' salaries, etc., or data linked to the civil service in the state. Consequently, mitigation will be a collaborative effort, involving affected committees meeting, assessing the situation, and discussing the appropriate measures for mitigation’.

For mitigating the effects of data breaches on individuals, the participants suggested some mitigating methods, such as acknowledging and apologising

for the breach, informing those affected by the breach, and compensating them. One manager confirmed, ‘Those affected by data breaches need to hear positive messages, such as that the system has been reformed, or strong passwords have been adopted’. To reduce the emotional effects on individuals and repair trust, participants mentioned that commitment to work within data security systems and regulations on actions that can then better guarantee future trust and repair damaged relationships.

The psychological and social participants mentioned that they would provide remedial plans for both the victims of a data breach and the perpetrators if the cause of the breach was an internal source, an employee, or a student. Participants revealed that dealing with the perpetrator is completely different from dealing with the victim. The methods of treating the emotional and psychological affected included (1) containing the victim, (2) helping him/her to understand the crisis, (3) explaining the reasons and possible solutions such as filing a complaint, and (4) clarifying the methods of dealing with the event in the respect of any future threats it might pose.

The offenders' treatment plan includes (1) understanding the offender's personality and the reasons for data penetration, (2) diagnosing the case, and (3) determining psychological sessions to get rid of criminal thoughts. However, it was important to clarify that while this treatment plan was presented by the psychologist, the university's primary strategies involved implementing administrative systems, security policies, and technical programmes designed to protect, prevent, and deter intruders and hackers from breaching the university's information systems. When looking at the offender’s treatment plan, it is important to understand if the offender is part of any larger systems that present a potential for further attack or if the offender is representative of others who might commit offences. The different levels at which the system and impacts need to be understood are complex.

4-3-2 Taibah University (TaibahU) Results

At TaibahU, five managers were interviewed, including four technical managers and one administrative manager. Despite differences in the flow of information, the data presentation followed the same semi-structured format as used at the

previous university which whilst providing comparative data equally provided for new insights to emerge.

4-3-2-1 TaibahU Managers' Awareness of Data Breaches

At TaibahU, the responses more critically focused on the element of access in defining the concept of a data breach. One participant specified that a data breach means access to the university's data and information systems. Two participants agreed that access to the university's data and information systems for the purpose of using them is illegal and unauthorised. One of the previous participants continued to describe this unauthorised access to any information owned by the university, whether in the form of assets or documents, data kept in databases, and information stored on systems or web pages.

Another participant considered a data breach to mean access to data that is unavailable publicly. By contrast, the participant from the Beneficiary Care Department linked data breaches to a breach of privacy. She stated the following: ‘In my opinion, a data breach is a breach of the privacy of beneficiaries by violating the privacy of their data and unauthorised access to personal data’. This range of definitions illustrates that managers' interpretations of data breaches are influenced by their specific roles and experiences, shaping their perception of breaches as either technical intrusions or privacy violations.

4-3-2-2 TaibahU Managers' Experience and Management of Data Breach Incidents

When asked about whether the university had previously been subject to breaches, one participant explained that the university had tested some of the attempts that were monitored and then closed the vulnerabilities that existed at the time. An example of such attempts was provided by a different participant, who reported an email phishing attempt that was an ‘external attack’ targeting employees' email addresses through spam messages. The hacked email had been blacklisted.

Another participant confirmed that she had previously supervised the management of a data breach for a user who communicated with her

department: ‘I remember one of the users raised an inquiry as he received a threatening message from a hacked account not on his official email, but on his private email’. She gave the victim the necessary support and directed him on how to deal with the threat as she wanted to educate the affected person and prevent the virus from being transmitted to the university systems.

Justifying the motivating driver for the breach from the perpetrator’s perspective, she asserted that ‘The hacker was asking for money’. While the university's response to these incidents demonstrates a strong response to the way these vulnerabilities were handled, which includes providing support in quite broad circumstances, it nevertheless reveals a reliance on addressing issues post-occurrence, i.e. reactively rather than proactively preventing them.

The distinction between official and personal email usage in security incidents highlights a need for more comprehensive security policies that bridge personal and institutional boundaries given the potential porous links between the two when individuals move across multiple spaces. Improving proactive measures and integrating user education with robust preventative strategies would likely improve overall resilience against such breaches.

4-3-2-3 TaibahU Managers' Technical Perspectives on Data Breaches

TaibahU has protection programmes, firewalls, antivirus software, an intrusion deterrence system, and monitoring systems. The Director of Infrastructure at the university described these systems as working ‘Alhamdulillah and good’. He continued by describing them as some ‘of the best systems in the world’ for providing data security, as the university cooperates with the Ministry of Education to provide some of them. In Arabic culture, the word Alhamdulillah[9] means complete praise and thanksgiving to God, while good in this context means good performance.

[9] ‘Alhamdulillah’ is an Arabic phrase commonly used by Muslims, which translates to ‘Praise be to Allah’ or ‘All praise is due to Allah’. It signifies gratitude and

Therefore, the researcher deemed the use of the two words together Alhamdulillah and good to indicate this manager's high satisfaction and confidence in the current security systems in terms of performance. On the other hand, the same manager explained that although these systems have the potential to provide security, they are extremely expensive as the university bears a high budget for the renewal of licences for those systems. He stated the following: 'Sometimes if a licence expires at the level of support or a specific service in the system, we have to work around the service'.

Additionally, three participants discussed backups more implicitly, referencing business continuity plans and alternative service provisions during potential disruptions. These measures suggest that backup systems are a foundational component of the university's recovery strategy, even if not always explicitly discussed. Furthermore, participants highlighted ongoing efforts to enhance technical infrastructure, implying a reliance on modern technologies with integrated backup and recovery features. For example, discussions around cloud services and localised data storage hint at the university's efforts to maintain redundancy and ensure data protection.

However, the coding analysis of the qualitative data indicated several technical risks that pose significant challenges to TaibahU, including external attacks, system and software updates, and the license renewal budget. A manager highlighted ongoing efforts to mitigate external threats by noting the email phishing incident, stating, 'We have addressed the email phishing (spam) issue'. Another participant mentioned, 'Some sensitive systems in the university cannot be upgraded'. These insights reveal the need for undertaking additional security steps.

---

acknowledgment of Allah's blessings and serves as an expression of appreciation to improve well-being (Hamim & Rosyidah, 2023).

4-3-2-4 TaibahU Managers' Organisational Perspectives on Data Breaches

An absolute consensus existed among the participants that it was the presence of the NCA that works well in managing data security in SA and reflects positively on the performance of universities. According to their responses, the NCA Authority is assigned to lead the wheel of change, development, and supervision to enhance data security in Saudi. One of the managers mentioned that the Authority checks the types of data stored by his university and periodically evaluates its security. He described it as ‘a comprehensive and massive review’ and also spoke about the Authority's effective guidelines regarding data handling and storage using cloud services’.

Another manager mentioned the Commission's role in directing the university to protect its data systems and information networks, as he felt that this role is ‘a very good role’. The ‘Haseen’ platform, an initiative by the NCA for sharing incidents of data breaches among Saudi institutions, exemplifies a proactive approach to cybersecurity. This platform's emphasis on transparency and knowledge sharing aims to elevate the overall security awareness and response capabilities of organisations. One manager's reference to the Aramco violation incident as an illustrative example underscores the platform’s value in disseminating critical information and best practices for incident management and containment.

Additionally, the involvement of the National Access Service provided by the Ministry of Interior, which manages the digital identities of citizens and residents, further enhances the security ecosystem. TaibahU’s implementation of this service, as noted by one of the directors, represents a strategic move to safeguard personal data and reduce the risks of identity theft and hacking. The digital management of passwords, where even employees cannot view new passwords, exemplifies a stringent approach to protecting user credentials, consequently reinforcing trust in the system's integrity.

Internally, TaibahU has implemented some policies for data security, such as the safe use of information assets and the management of identities, access, and powers. A manager stated, 'we have policies for the safe use of access and a policy for controlling access identities'. Another explained other policies, 'we have a policy that supports aspects of responsibility, such as generalisations for passwords'.

The strengths of the data security policies at the university are evident in their comprehensiveness in terms of policies and processes as well as their adherence to the standards that come from the state. A participant noted that the university reviews and updates its policies as necessary. Another participant evidenced this by talking about the university's introduction of special controls for cybersecurity for remote working in the immediate wake of the COVID-19 pandemic: ‘After the pandemic, to reduce threats and vulnerabilities, we introduced special controls for cybersecurity’.

Another participant mentioned that the data security policies, whether local or imposed by the authority, are ‘very excellent’. In contrast, the security policy gap identified was the resistance of individuals to adhere to them, as noted by one participant who mentioned, ‘the lack of clear commitment by some to follow security policies’. This commitment was crucial for ensuring the effectiveness of policies and addressing data breach threats, according to the participants' views. The acknowledgement by four managers of insufficient individual awareness further underscored a critical vulnerability on the organisational side.

Additionally, opinions differed about the impacts of data breaches. The first manager linked the type of data to the amount being affected by the breach, where he argued that financial data leakage leads to financial losses, and personal data compromise leads to social problems. The second manager considered that data breaches directly impacted individuals financially. The researcher was aware that this focus on the financial impact may have resulted from the active movement of data breach incidents in the Saudi banking sector recently which was a backdrop to this research.

In contrast, the third manager shared the impact of data breaches on the organisation in terms of losing its technical assets and wasting its budget, as he said, ‘recovery of data systems may be more expensive than the initial cost of construction’. Therefore, protective operations, despite their potential expense, yield long-term benefits. This ensures that the organisation avoids losses exceeding the value of the incurred cost. The fourth manager only assessed the degree of influence as follows: ‘The leakage of such data represents a high-risk event in terms of influence’. The fifth manager described the impacts of such incidents as extremely disturbing.

4-3-2-5 TaibahU Managers' Perspectives on Emotional Impacts of Data Breaches

Due to the absence of sociologists and psychologists from TaibahU, the investigation into the emotional impact was relatively limited. The emotional effects identified included anger, anxiety, destruction, fear, isolation, and shock. It was also observed that these emotional effects varied based on several factors: (1) the level of awareness of security measures; (2) the differing social acceptance and environmental context of the breach; (3) the extent of damage caused by the breach, such as exploitation, bullying, defamation, or extortion; and (4) the individual's overall awareness.

Two participants agreed that data breaches affect the level of trust in the university, which will affect its reputation. While the other two managers agreed that the emotional impact is related to the perception and social acceptance of the data breach event, and the accompanying emotional reactions of the victim, such as shock, fear, and isolation from society, one of them commented that and said, ‘There are some people who may be destroyed by the experience of data breaches, and there is the opposite according to the environment, there are those who expose to shock, fear, and isolation from the surroundings, and doubts abound within themselves’.

Another manager argued that the emotional impact is related to the level of awareness a person has at the point of attack. Therefore, a person with low awareness who does not take action may feel fear and guilt during an attack, whereas a person who is aware and takes the right security measures may feel

greater anger. The following table presents the range of impacts and risks associated with data breaches at TaibahU.

Emotional impacts			
Impact	Anger	Anxiety	Destruction
Participant Identifier	TMO	TBV	TMO
Impact	Fear	Isolation	Shock
Participant Identifier	TBV- TMO- TAD	TBV	TAD

Table 25 Emotional impacts associated with data breaches at TaibahU. Participant identifiers (e.g., TBV, TMO, TAD) are anonymised codes assigned to protect interviewees' privacy.

4-3-2-6 TaibahU Managers' Needs and Wishes for Data Protection

The interviews revealed a consistent emphasis on the critical need for raising awareness among individuals regarding data security. The recurrent statements, such as 'The subject of awareness we need', 'This lack of awareness represents a great danger to users of university systems', and 'awareness then awareness', emphasised a pervasive concern about inadequate understanding of security threats and prevention methods among university users. This concern is further highlighted by the call to educate the university community about hacker methods and the repeated emphasis. A manager's suggestion to implement collaborative awareness programmes involving various cultural institutions in Saudi society reflects an insightful approach to addressing this gap. The manager's recommendation to utilise multiple channels—such as universities, television, social media, and malls—indicates a recognition of the need for a multiple strategy to reach diverse audiences effectively. However, while these insights point to a significant consensus on the need for enhanced individual awareness, they also highlight a potential gap in the implementation and consistency of such security training which the university should embrace. Moreover, one TaibahU manager explicitly expressed a need for enhanced backup strategies to complement their broader data protection frameworks. Specific areas of focus included

improving redundancy protocols and investing in scalable storage solutions to support the growing demands of digital transformation.

4-3-2-7 TaibahU Managers' Insights on Mitigation of the Impact of Data Breaches

A technical manager explained the plan for dealing with the data breach at the technical level, which includes (1) isolating all services that may be affected by the breach, (2) isolating affected systems, (3) changing passwords and usernames. (4) cleaning up, (5) informing the NCA, (6) restoring systems and supervising their operation, and (7) testing the services and then restoring the service. Likewise, another director confirmed a plan to deal with a data breach includes steps, such as (1) containment, (2) defining responsibilities, (3) informing the national authority, (4) rectifying the situation, and (5) investigating the incident. For investigating a breach incident, the director mentioned in terms of responsibility and accountability, ’Of course, if the person responsible for the breach is identified, he will be referred to the state’s regular investigation, where the cybercrime law will be applied to him’.

Moreover, one project currently adopted by the university is a digital transformation project linked to Saudi Vision 2030. A participant spoke about this project as follows: ‘We are still conducting an ongoing study to list all the university's needs to draw a roadmap for a successful digital transformation plan, some projects related to cybersecurity have been released’. Another participant agreed with the promising outlook for the future and described the changes that have taken place in terms of data security as follows; ‘The change in data protection whether at the university or in SA did not happen suddenly, but happened gradually, to ensure that it is properly coped with’.

These detailed plans for managing data breaches at both technical and administrative levels underscored a structured approach to incident response and accountability. However, while the integration of cybersecurity measures within the broader digital transformation project aligned with Saudi Vision 2030 was promising, the gradual nature of data protection improvements suggested a need for continuous adaptation to emerging threats.

4-4 A Comparison Dissection

This section examined several critical themes related to the management and protection of personal data in Saudi HE institutions, focusing on a comparative analysis of KSU and TaibahU. It began by addressing the risks associated with personal data management, revealing multiple vulnerabilities in data security.

Following this, the regulation of personal data security was explored, with a focus on the policies and processes implemented by Saudi universities to mitigate risks and prevent breaches. The comparison between KSU and TaibahU offered insights into the effectiveness of these regulations and their impact on enhancing data security. The analysis also considered the multidimensional impacts of data breaches, particularly from an administrative perspective. Critically, it also explored the need for improvements in personal data management security.

Lastly, the section discussed mitigation methods for managing and recovering from data breaches, identifying best practices and innovative approaches to enhance outcomes in the event of security breaches. The comparison between KSU and TaibahU highlighted the diverse strategies employed by each institution. These themes align with the research objectives, which sought to investigate the causes of data breaches, understand security policies and processes, uncover the implications for stakeholders, identify desired changes, and explore strategies to mitigate or improve outcomes from security breaches.

4-4-1 Theme 1 Risks of Personal Data Management

The comparative analysis between KSU and TaibahU revealed significant insights into the organisational, technical, and personal risks associated with personal data security management in Saudi universities. This section draws out the discussion across the universities. It is worthy of note at this point that potentially if the researcher had gone back to conduct a further round of interviews with the findings from the counterpart university there would have been a shift and development in some of the discussions. However, it is right to highlight the priorities and landscape that are evidenced in these independent interviews.

Technical Risk

Both universities identified human errors as one of the technical risks, underscoring a common vulnerability inherent in the interaction between technology and human factors. It is crucial to acknowledge that while there is a minor divergence in perspectives regarding the human factor as a primary risk, this aligns with empirical research emphasising the significance of human behaviour and awareness in improving cybersecurity practices (Clark, 2019; Beeson, 2020; Hunt, 2021).

Some of the perspectives provided suggest that technological risks are the main threat, whereas 13 managers identify human errors as the primary risk, with two others considering technological advancements as the principal threat. KSU's focus on the inadequacy of technical skills among personnel highlights a training and competency gap that could exacerbate these risks. Conversely, TaibahU's emphasis on software and system updates, license renewal budgets, and external attacks indicates a broader scope of technical challenges.

Organisational Risk

At KSU, the emphasis on the lack of professionals and budget constraints highlighted a fundamental resource deficiency that may impede effective data security management. This scarcity of skilled personnel and financial resources suggested an underlying structural issue that may hinder the university's capacity to implement and sustain robust data security measures.

In contrast, at TaibahU, the significant role of individual awareness was underscored, reflecting a cultural and educational gap that may impact data security practices. The shared concern across both institutions about individual non-compliance and resistance to policies underscored a pervasive challenge in enforcing data security protocols. This resistance points to potential deficiencies in training, communication, and perhaps the cultural context within which these policies were introduced and enforced.

Personal Risk

KSU's identification of over-trust and excessive empathy as social risks reflected a cultural trait that could potentially be exploited in data security breaches. This insight into the cultural dynamics of Saudi society points to a need for targeted awareness and training programmes that address these specific vulnerabilities. Although TaibahU lacked input from psychological and social perspectives, the identification of risks such as data exploitation, defamation, bullying, and extortion by technical perspectives suggested these issues were recognised at multiple levels within the university. The classification of these risks as social causal risks by the researcher was significant, as it indicated a broader understanding of the social dynamics that contributed to data breaches. Table 26 summarises the risks of personal data management in the two universities.

Case	Organisational	Technical	Personal
KSU	Lack of professionals	Insufficient technical skills	Over Trust
	Lack of budget	Human Errors	Excessive Empathy
	Non-compliance with security policies		
TaibahU	Lack of awareness	Software Update	Exploitation
	Resist policy enforcement	Systems Update	Bullying
		External attack	Defamation
		License renewal budget	Extortion
		Human Errors	

Table 26 Data management risk.

4-4-2 Theme 2 The Regulation of Personal Data Security

The examination of the second theme underscores the regulatory landscape of personal data security management within Saudi educational institutions. Both universities expressed strong optimism about advancements in data security, largely attributed to the establishment of the Cyber Security Authority in 2018. This enthusiasm reflects a broader institutional confidence in the authority's role in enhancing data security frameworks across SA. A critical element of this development is the ‘Haseen’ platform, designed to manage cyber services and solutions nationally. This initiative signifies a strategic effort to bolster cybersecurity infrastructure and establish a coherent framework for data protection.

KSU's policies are praised for their excellence, with feedback highlighting them as ‘excellent, Mashallah’. Likewise, TaibahU's policies were considered ‘very excellent’, adhering to state standards and adapting to emerging challenges like remote work during the COVID-19 pandemic.

However, the observed differences in the naming and specific focus of data security policies between KSU and TaibahU reveal important nuances. At KSU, policies such as the access policy and the email use policy were noted, while TaibahU's policies included the secure use of information assets and identity and access management policy. While these differences might appear significant, they may largely reflect superficial variations rather than substantive divergences in policy content or effectiveness. The distinct terminologies used may be attributed to institutional preferences or historical practices rather than fundamental differences in the security measures themselves.

A deeper understanding of the actual content and implementation of these policies, beyond their nomenclature, is essential for evaluating their effectiveness. (Refer to Chapter Five to understand the level of awareness among students and faculty members regarding the data security policies at the two universities). The following table shows these policies in each university.

KSU Policies	TaibahU Policies
Access policy	Safe use of information assets policy
Email use policy	Managing identities, access, and powers policy
Network access policy	The cybersecurity controls.

Table 27 Data security policies in universities.

4-4-3 Theme 3 The Multidimensional Impacts of Data Breaches

4-4-3-1Technical Impacts of Data Breaches

TaibahU primarily faced challenges from external attacks and email phishing, whilst KSU contended with more diverse threats including, malicious viruses, DDoS attacks, and Command and Control (C&C) attacks.

External Attacks

Qualitative analyses highlighted external attacks at TaibahU as a significant technical impact of data breaches. This observation aligns with Bodin (2017), who notes that universities are vulnerable to such attacks. The prevalence of external threats at TaibahU underscores the need to enhance security measures, including upgrading threat detection systems and conducting regular security assessments, to better safeguard data against external threats.

Email Phishing

Email phishing has emerged as a critical technical issue at TaibahU, revealing a significant vulnerability in its cybersecurity practices. Phishing attacks exploit deceptive emails to trick users into disclosing sensitive information or downloading malware, which can lead to unauthorised access and data breaches. To mitigate this risk, the focus should be on fortifying email security protocols and implementing comprehensive user awareness training.

Malicious Viruses

Malicious viruses have posed a severe technical threat at KSU, confirming the widespread nature of this issue in academic institutions. McClurg (2015) supports this view, indicating that universities are susceptible to such threats.

Addressing this requires robust antivirus software, regular updates, and vigilant security practices to prevent malware infiltration.

DDoS Attacks

Distributed Denial-of-Service (DDoS) attacks have had a notable technical impact at KSU, leading to significant service disruptions by overwhelming network resources with excessive traffic. This incident highlights the need for effective mitigation strategies, such as traffic filtering and network strengthening, to maintain service availability and resilience against such attacks.

Command and Control (C&C) Attacks

Command and Control (C&C) attacks experienced by KSU represent a technical consequence. Attackers gained control over the university's systems to issue commands and extract data, underscoring the need for advanced threat detection and response capabilities. Monitoring for unusual network activity and preventing malware from establishing control are crucial for defending against these complex attacks.

4-4-3-2 Organisational Impacts of Data Breaches

The analysis of the information on data breaches at both KSU and TaibahU identified a set of organisational consequences as set out below.

Reputation Damage

Both KSU and TaibahU agree that data breaches adversely impact the university's reputation. This finding aligns with the literature, which highlights reputation as a critical asset in organisational trust and credibility (Beaudin, 2017; Alshammari, 2017; Areishi & Al-Dossary, 2018). The degradation of institutional reputation can have long-lasting effects on stakeholder trust, student enrolment, and research opportunities. The agreement between the universities on this point underscores the widespread recognition of reputation damage as a fundamental consequence of data breaches.

Disruption of University Services

Both universities also identified the disruption of university services as a major impact of data breaches. This is consistent with Dillon and Paté-Cornell (2005) findings, which emphasise the operational disruptions caused by data breaches. Such disruptions can affect teaching, research, and administrative functions, leading to inefficiencies and interruptions in academic and administrative processes.

Financial Drain

The financial implications of data breaches are another agreed-upon impact, with both universities acknowledging that breaches result in significant financial costs. Chapman (2019) supports this view by documenting the financial burden associated with data breaches. The financial drain explained by both universities illustrates the substantial economic impact of breaches.

Additional Impacts

KSU reported that breaches affect the quality of university performance and data loss, this second impact aligns with findings from Garrison and Ncube (2011), who emphasise that data loss can undermine organisational efficiency and compromise sensitive information. While TaibahU noted the cost of recovery as a significant impact. These findings add depth to the understanding of the organisational effects of data breaches. The quality of performance reflects how breaches can impair the institution's ability to deliver on its mission and objectives, potentially affecting academic and research outcomes.

Meanwhile, recovery costs increase the burden on universities, as confronting data breaches requires huge budgets to provide the necessary security hardware and software. overall, the comparison of organisational impacts between KSU and TaibahU, as summarised in Table 28, reveals that while both institutions share common concerns about reputation, service disruption, and financial strain, they also experience unique challenges related to performance quality, data loss, and recovery costs.

Case	Organisational Impacts	
KSU	Data loss	
	Disable information services	Drain the organisation's budget
	Impact on university performance	Reputational impacts
TaibahU	Reputational damage	Service crashes
	The high cost of recovery	Wasted budget

Table 28 The organisational impacts of data breaches on universities.

4-4-3-2 Emotional Impacts of Data Breaches

The qualitative analysis captured four common emotional responses among managers at both universities:

Fear

The analysis revealed that seven principals identified fear as a primary reaction to data breaches, with four from KSU and three from TaibahU. This indicates that fear is generally the dominant emotional response. One of those managers attributes this fear to concerns over the potential misuse of personal information and the broader implications for personal and academic safety. This emotion is often heightened by privacy concerns, as highlighted by Al-Hubaishi and Al-Juhani (2021), who discussed fears related to privacy and the adoption of technological means in Saudi universities, though not specifically focusing on data breaches.

Anger

Anger emerged as the second most prevalent emotional response to data breaches. According to the analysis, six managers, five from KSU and one from TaibahU, viewed anger as a reaction to the breach. According to three managers, this emotion often extends beyond the initial breach incident, persisting through the investigation period as individuals become aware of the breach's specifics and vulnerabilities.

Anxiety

Anxiety was another significant emotional impact, as indicated by five principals, with four from KSU and one from TaibahU. The emotional bond and trust individuals have with their organisation, as described by Doyle et al. (2015), can be severely damaged by a data breach, leading to depressive symptoms.

Shock

Four managers (three from KSU and one from TaibahU) noted that shock is a common immediate reaction to data breaches, highlighting the unexpected and unsettling nature of these incidents. Based on one of the comments, The sudden violation of privacy and security can lead to a state of shock, underscoring the need for organisations to manage and report breaches effectively to mitigate this initial emotional impact.

Compared with the review findings (refer to Chapter 2), this study presents unique findings on the emotional aspects of data breaches. Based on managers' responses, data breaches have profound emotional effects that impact individuals' well-being. Among the common responses recorded in the two universities were fear, anger, depression, and shock, along with other emotional responses.

At KSU, where there was strong recognition of the emotional impacts on staff and data stakeholders, there is a need to develop approaches to better surface and manage these impacts. This included some quite innovative potential responses such as holding workshops that adopt activities to reduce the pressures of life and digital dealings. Ideas were expanded to include free writing to express concerns and encourage the practice of spiritual exercises such as yoga. See the following table for specific responses from managers regarding the emotional repercussions of data breaches on individuals.

Case	Emotional Impacts					
KSU	Responses And Reactions	Anger	Anxiety	Depression	Disappointment	Embarrassment
		Fear	Alienation	Lack of confidence	Panic	Shock
		Uncontrol Anger	Trauma	Discomfort	Sadness	Guilt
TaibahU		Anger		Fear		Isolation
		Anxiety		Destruction		Shock

Table 29 The emotional Impacts of data breaches.

4-4-4 Theme 4 Things That Need to Change within Data Management

The identification of these needs reflected a comprehensive approach to managing data security within both universities. The common needs explained the fundamental elements of a robust data security framework, emphasising the importance of financial investment, skilled personnel, and continuous education and training. By addressing these common needs, both institutions can build a more solid foundation for their data security strategies, ensuring resilience against potential breaches.

However, the distinct needs of each university highlighted the unique challenges they faced. TaibahU's focus on upgrading outdated technologies and ensuring data backups indicated a need for modernisation and risk mitigation. These steps might be crucial for creating a more secure and reliable IT infrastructure that can withstand contemporary cyber threats. The emphasis on data backups also pointed to a proactive approach to protecting against data loss, which is essential for maintaining academic and operational continuity. In contrast, KSU's specific needs, such as enhancing problem-solving skills and

establishing a clear breach reporting process, reflected a more tactical approach to data security. By improving problem-solving capabilities, the university aimed to empower its staff to respond effectively to security incidents, reducing the impact of breaches. A breach reporting process was critical for timely intervention and minimising the damage caused by data breaches. Additionally, the focus on software maintenance highlights the importance of keeping security systems up to date to counteract new and emerging threats.

The emphasis on training programmes by six managers (4 from KSU and 2 from TaibahU), explained a significant angle of data security that extended beyond technical solutions. This focus on training revealed an understanding that while technological advancements are essential, they are insufficient on their own to effectively mitigate data breaches. This recognition was supported by the assertion that robust training programmes are necessary to empower individuals with the knowledge and skills needed to protect their data and navigate potential security threats. Other hoped aspects can be summed up in Table 30.

Needs	Cases
Converting systems that operate on old technologies	TaibahU
Distribution of powers	Both Cases
Financial support	Both Cases
Having copies of the data	TaibahU
Hire qualified personnel	Both Cases
Permissions control	Both Cases
Problem-solving skills	KSU
Raise awareness of the risks	Both Cases
Reporting data breaches	KSU
Software development	Both Cases
Software maintenance	KSU
Systems maintenance	Both Cases
Training	Both Cases
Workshops	Both Cases

Table 30 Universities need to develop personal data management.

4-4-5 Theme 5 Mitigation Methods for Managing and Recovering

The examination of mitigation strategies employed by KSU and TaibahU revealed distinct approaches tailored to their respective contexts. Both institutions demonstrated a commitment to managing data breaches effectively, but their strategies reflected differing priorities and methodologies.

At KSU, the mitigation strategy included a formal apology, notifying affected individuals, and offering compensation. This approach suggested a focus on accountability and reparative measures, aiming to address the immediate concerns of those impacted by the breach. In contrast, TaibahU prioritised containment of the breach and support for affected individuals as its primary mitigation strategies. This approach emphasised immediate actions to limit the extent of damage and provided direct assistance to those impacted. Containment efforts were aimed at stopping the breach from spreading further, thereby minimising potential harm. Support mechanisms focused on addressing the needs of individuals affected by the breach, aligning with a more preventive and supportive stance rather than a reparative one.

Despite these differences, both universities agreed on the importance of taking responsibility for the breach. This shared understanding reflected a common commitment to accountability and reinforced the idea that addressing data breaches involved more than just technical solutions; it required acknowledging and managing the broader implications of such incidents. Both universities had established protocols for managing data breaches, involving notification to the (NCSA) once the breach's extent and impact were assessed. Each institution had designated departments responsible for handling various aspects of the breach, including technical, psychological, and social support.

At KSU, these protocols involved both technical and counselling departments, which provided psychological and social support. In KSU the need to deal with over-trust in particular was an important observation with particular pertinence to consider for organisations more broadly in SA. At TaibahU, although direct interviews with social and psychological directors were not conducted,

information from the Beneficiary Service Department indicated that the university also had systems in place for addressing security crises through psychological and social counselling.

In addition, backups are integral to the recovery strategies at both universities. KSU's incident response plans heavily rely on backups to restore systems and protect data, as noted by multiple participants. TaibahU's business continuity measures, mentioned by three participants, imply their use in maintaining operations. Both institutions could benefit from further investment in advanced backup technologies, such as automated cloud-based systems, to enhance their resilience against data loss.

Summary

In this chapter, qualitative data from data collected from KSU and TaibahU in SA. The research targeted managers from various departments, addressing technical, organisational, and personal aspects within the universities. The results were explored through two distinct lenses: first, by separately detailing the qualitative data obtained from semi-structured interviews, and second, by comparing this data across the two institutions.

In the individual analysis, the data for each university were presented through seven key themes to ensure alignment with the context of the research and to correspond with the statistical results from the survey (refer to Chapter Five for context). These themes covered: managers' awareness of data breaches, experiences and management of data breach incidents, technical perspectives on data breaches, organisational views on data breaches, emotional impacts of data breaches, needs and desires for data protection, and strategies for mitigating the impact of data breaches. In the comparative analysis, five primary themes emerged, providing insights into the convergences and divergences between KSU and TaibahU. These themes included: the identification of risks associated with personal data management, the regulation of personal data security, the multidimensional impacts of data breaches, the need for improvement in data management, and the mitigation methods employed by each university.

The qualitative findings indicated that both universities faced common

challenges and distinct issues related to data security. KSU struggled with budget constraints and a shortage of skilled personnel, while TaibahU highlighted issues related to individual awareness and resistance to security policies. Organisational aspects at both universities were addressed, with both institutions showing confidence in the advancements brought by the National Cyber Security Authority (NCSA) and the 'Haseen' platform. Although there were differences in policy names and focuses between KSU and TaibahU, these differences were largely superficial, reflecting institutional preferences rather than fundamental divergences in security measures. The impacts of data breaches were also examined, revealing both technical and organisational consequences. TaibahU faced external attacks and phishing, while KSU encountered a broader range of threats including viruses, DDoS attacks, and Command and Control attacks. Both universities reported reputation damage, service disruption, and financial strain, with additional unique challenges noted by each university.

The study identified common needs for enhancing data security, such as financial support, skilled personnel, and ongoing training. However, specific needs varied: TaibahU required updates to outdated technologies and robust data backup systems, while KSU focused on improving problem-solving skills and breach reporting processes. Mitigation strategies differed between the universities, with KSU emphasising reparative measures such as apologies and compensation, and TaibahU prioritising containment and support for affected individuals. Both institutions agreed on the importance of taking responsibility for breaches and had established protocols for managing them, including notifying the NCSA and providing both technical and psychological support.

Support was identified as needing to be for all stakeholders and KSU proposed some potential innovative approaches to considering the future evolution of processes, including workshop formats. In addition, the research has found that potentially there is a cultural issue of over-trusting others; this was observed at KSU. This is an important cultural finding which deserves further examination. This chapter has focused on manager perspectives. The next chapter discusses the quantitative data collected in tandem, which draws on a broader pool of stakeholders.

Chapter 5: Quantitative Analysis of an Online Survey

Introduction

This research investigates people's opinions and experiences of personal data protection in the Saudi context both in terms of their knowledge about protecting from breaches and then their perspectives on breaches. The researcher created two surveys directed at the two participant categories (faculty members and students), to investigate the multiple perspectives of data breaches in the university case examples. Data was collected through Opinio as the survey tool. This is a UCL-designed piece of software, which is approved as a source tool. The data collected was then downloaded into an Excel spreadsheet which was imported into the SPSS. Statistical analysis was undertaken to establish relations and connections between the data. Coding was undertaken on the open-ended questions. The closed answers were designed to enable a set of multiple-choice answers, depending on the context of each question.

The researcher drew on the existing literature to determine the potential answers to each question. For example, the emotional responses to the questions on responses to data breaches were defined by the existing literature on attitudes and emotional responses to breaches. To examine the landscape of Saudi data security, the researcher used a nominal scale (Goddard & Villanova, 2006), with questions on age, gender, security training, weak practices, etc. Although the nominal scale is useful for generating basic nominal data for a data security landscape, it is recognised that it has some limitations. Nevertheless, it does provide a modest amount of mathematical processing. A decision was made to use Likert scales with a five-point scale (Croasmun & Ostrom, 2011), to investigate the participants' opinions and perspectives. This scale enabled the researcher to gain insights into respondents' feelings and opinions and to understand the degree of their agreement with different security statements. It can be described as follows:

1. Strongly Agree: Indicates the highest level of agreement, a definitive positive stance.
2. Agree: Reflects agreement, but with less intensity than “strongly agree.”

3. Neutral: Represents a neutral stance, where respondents neither agree nor disagree with the statement, often used when respondents have no strong opinion.
4. Disagree: Indicates disagreement, but less intense than “strongly disagree.”
5. Strongly Disagree: Reflects a strong level of disagreement with the statement.

In the context of data security and data breaches, the Likert scale provides a nuanced understanding of respondents' attitudes towards the university’s data protection strategies, their concerns about potential breaches, and their perceptions of the effectiveness of current measures. For instance, it helps to measure how much participants agree or disagree with statements like ‘I trust the university's data protection methods’ or ‘I am concerned about the security of my personal data’.

Additionally, another scale consisting of five elements (yes definitely, yes to some extent or partly, no, don't know, prefer not to say) was used to identify further experiences and opinions regarding data violations and their multidimensional effects as follows:

1. Yes, definitely: Indicates strong agreement or certainty, representing a clear affirmative stance.
2. Yes, to some extent or partly: Reflects a moderate level of agreement, indicating some but not total certainty or agreement.
3. No: Represents strong disagreement, a clear rejection of the statement.
4. Don’t know: Reflects uncertainty or lack of knowledge, where the respondent does not have enough information to provide a firm opinion.
5. Prefer not to say: Indicates a desire to remain neutral or withhold a response, often due to privacy concerns or lack of willingness to engage.

This scale focuses on participants' awareness and understanding of data security practices. It helps to identify whether respondents are familiar with how to report a breach, whether they have received training, or whether they

understand the risks associated with data leaks. This scale captures certainty about topics such as whether respondents know how to file a complaint or whether they believe they have adequate protection from data breaches.

Furthermore, descriptive statistics were supplemented with statistical tests to identify associations between key factors and participants' responses. The Chi-square test was used to explore associations between gender and participants' responses to various survey questions. Gender is an important factor to consider in studies of data security because perceptions and experiences of data protection may differ based on societal roles, expectations, and access to resources (Anwar et al., 2017). For instance, men and women might exhibit differing levels of trust in institutional data protection strategies or varying concerns about the consequences of data breaches. By examining the role of gender, this study aimed to identify patterns that could inform targeted awareness programmes or interventions (Sommestad et al., 2014).

The Chi-square test was also employed to examine associations between job level and participants' responses. Job level is a critical factor because individuals' roles within a university can influence their exposure to data protection issues, their awareness of security protocols, and their responsibilities for safeguarding data. Faculty members in senior positions may possess more knowledge about institutional policies, whereas junior faculty may face different challenges. Understanding these associations helps to identify specific training or support needs tailored to individuals at various employment levels (Chua et al., 2018)

To explore associations with age, the Kruskal-Wallis H test was used. Age is a key demographic factor that can shape how individuals perceive and respond to data security challenges. Younger participants may be more tech-savvy but less aware of privacy risks, while older participants might be more cautious but less familiar with digital platforms (Ugwu et al., 2021). Measuring age provides insights into generational differences that could affect attitudes toward data breaches, trust in institutional safeguards, and preferences for mitigation strategies. Examining gender, job level, and age provides a multidimensional perspective on the data, enabling a deeper understanding of how demographic

and contextual variables influence participants' views and behaviours. These analyses can uncover disparities, highlight areas for improvement, and inform tailored interventions designed to address the unique needs of different groups.

It's important to note that the questions are organised by thematic relevance rather than numerical order. This arrangement improves the coherence of the data, facilitating a better understanding of how different aspects of the topic are interconnected. The analysis starts with employee survey data, followed by student data.

5-1 Faculty Members' Survey Findings:

5-1-1 Employees Demographic

Although the surveys were distributed in the same way in both universities, the response rate of academic staff at KSU of 58.5% (n = 41) was higher than that of the staff at TaibahU of 41.4% (n = 29). The response rate of females (55.7%, n = 39) was slightly higher than that of males (40.0%, n = 28), and 4.2% (n = 3) of participants preferred not to specify their gender. It is important to note that the Saudi system categorises people very clearly with gender separations men and women. In SA contexts it is not culturally normal to provide for non-binary choices and this can offend. Academic staff were asked which age group they belonged to, with five age groups offered that covered the ages of employment in the Saudi employment system, the youngest group being 18–24 and the oldest group being 55 and above.

The most common response was the age group of 35–44 with a rate of 42%. This result is reasonable given that the appropriate age for youth falls within this category. In contrast, the least common response was the age group of 18–24, at approximately 4%. Regarding the participants' employment level, the most common responses were 'lecturer' (35.7%) and 'assistant professor' (28.5%), with both 'associate professors' and 'assistant' accounting for 12.8%, and professors accounting for 4.2%. The response of 'lecturers' dominated at TaibahU, whereas 'assistant professors' dominated at KSU. Consequently, a high proportion of participants had a master's degree (80.9%), and more than two-fifths had a PhD (45.5%).

Q	Socio-demographic characteristics		N	Fi %
Q1	Select your university	KSU	41	58.6%
		TaibahU	29	41.4%
Q2	Select your gender	Male	28	40.0%
		Female	39	55.7%
		Prefer not to say	3	4.3%
Q3	Select your age	18-24	3	4.3%
		25-34	22	31.4%
		35-44	30	42.9%
		45-54	9	12.9%
		55 and up	6	8.6%
Q5	What is your current job level?	Professor	3	4.3%
		Associate Professor	9	12.9%
		Assistant Professor	20	28.6%
		Lecturer	25	35.7%
		Demonstrator	9	12.9%
		Prefer not to say	4	5.7%

Table 31 Socio-demographic characteristics of KSU and TaibahU participants.

In summary, at KSU the rate of female responses was slightly higher than male responses, the most common age group was 35–44. At TaibahU, the rate of female responses also was higher than male responses, and the most common age groups were 25–34 and 35–44. The most common level of employment at KSU was assistant professor (34%), while at TaibahU, it was lecturer (41%). The academic disciplines who participants are detailed in Table 32, which evidences the slightly different research and educational programmes offered by the two universities.

Case (1)		Case (2)	
KSU	**Disciplines Number**	**TaibahU**	**Disciplines Number**
• Arabic Language • Biomedical engineering • Business Management • Computer Sciences • Curricula and methods of teaching forensic sciences • Dentistry • Development and Quality • Education • Educational Leadership • English Language • Geographical Information Systems • Health Informatics • Law • Libraries and information science • Linguistics • Management Information Systems • Medical Sciences • Nursing • Nursing Administration and Nursing Education • Psychology • Social Service • Sociology • Syllabuses, and teaching methods • Translation	55	• Arabic Language • Business Management • Computer Science • English Language • Information Science • Information Technology • Islamic culture • Islamic studies • Journalism and digital media • Law • Media • Nutrition • Psychological Health • Psychology • Quranic studies • Radio and television • Sociology - Social service • Special Education	23

Table 32 Academic disciplines of staff participants.

5-1-2 Employees' Awareness of Data Breaches

This section examines the level of awareness among faculty members of the concept of data breaches and their understanding of how they occur. This title was covered by three questions (Q6, Q7, Q8). Question 6 was analysed by NVivo and coded with the question number (Q6), in line with the approach taken for qualitative questions provided in the survey. In this question, participants were asked about their comprehension of data breaches, to which they responded that such breaches involve unauthorised access and unlawfully obtaining data. The reasons given by participants as potential motivating drivers for unauthorised access to personal data were hacking, assault, theft, tampering, intrusion, impersonation, and manipulation of data to defame or monitor another person.

They also elaborated that hacked data is often used illegally and undesirably, such as to commit fraud. Some of the definitions provided by the participants described ways to access data, such as by hacking cloud storage services, social media accounts, systems, devices, computers, and mobile phones. One of the definitions was as follows: '**Data breach is the violation of privacy and access to data by unauthorised persons, it is the irresponsible use of data that can be classified as a form of social engineering'**. Overall, the responses indicated a level of understanding of the nature of data breaches with additional knowledge of the forms and drivers for data breaches.

In question 7, participants were asked more explicitly to describe how data breaches occur. Many responses indicated that data breaches occur as a result of either technical factors or regulatory factors. Technical factors included issues like inadequate systems vulnerable to advanced viruses and technical vulnerabilities, such as inefficient encryption algorithms that could be exploited to access data. Regulatory factors involved inadequate compliance with data security policies within the university, such as data privacy protocols, or human errors like clicking on unsafe links, which result in breaches of personal data. One participant's response exemplified this, stating: **'Data breaches occur due to an unprofessional design structure of IT-related data/systems, and/or through hacking processes'.**

To ensure faculty members were fully informed about the concept of a data breach on an international scale, they were asked to express their agreement with a specific definition. This definition, drawn from the GDPR UK guidelines, describes a data breach as any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The researcher opted for this definition due to the ambiguity surrounding data breaches in the Saudi context and because the study, conducted at UCL, would be presented to UK readers. Despite finding a similar definition provided by the Saudi National Cyber Security Authority, which uses the term 'compromise', the researcher focused on the UK perspective to gauge awareness of the concept of data breaches. Among participants, approximately half strongly agreed with the UK definition (48.6%), while 41.4% agreed, and 10% neither agreed nor disagreed.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
One definition of a data breach is that it is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. Please indicate the extent to which you agree with this definition.	Strongly Agree	23(32.9%)	11(15.7%)	34(48.6%)	0.480
	Agree.	14(20.0%)	15(21.4%)	29(41.4%)	
	Neither Agree or Disagree	4(5.7%)	3(4.3%)	7(10.0%)	
	Disagree	0(0.0%)	0(0.0%)	0(0.0%)	
	Strongly Disagree.	0(0.0%)	0(0.0%)	0(0.0%)	
	Prefer not to say	0(0.0%)	0(0.0%)	0(0.0%)	

Table 33 Distribution of percentages and frequencies from the employees' survey for question 8, a data breach definition awareness.

Sex and age correlations

The relationship between responses regarding awareness of the data breach definition and age groups was analysed using the chi-square test. With a Pearson chi-square p-value of 0.6, there is no indication that awareness of the data breach definition varies significantly across age groups. Figure 5 visually represents this correlation. Similarly, gender was found to have no significant impact on awareness of the data breach definition, as indicated by a Pearson chi-square p-value of 0.7. While the number of females agreeing with the definition exceeded the number of males, statistical analysis rejected the presence of a relationship with gender, affirming gender as an independent variable. Figure 6 illustrates this relationship.

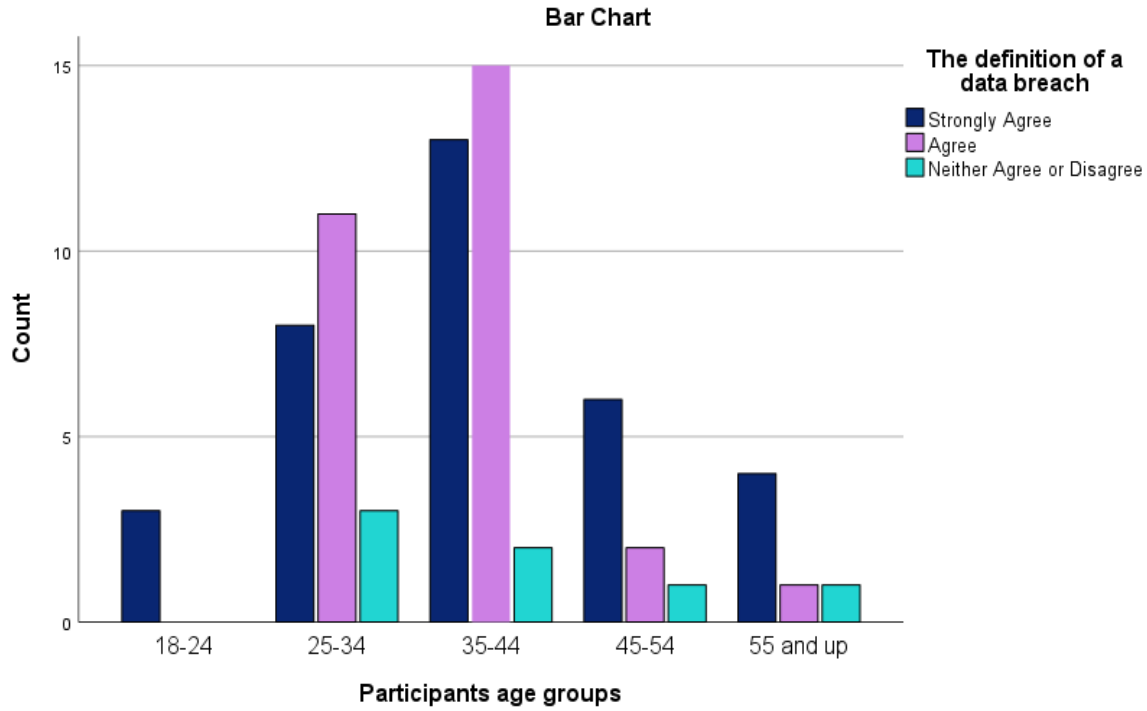

Figure 4 The correlation between data breach definition awareness (Q8) and the age groups.

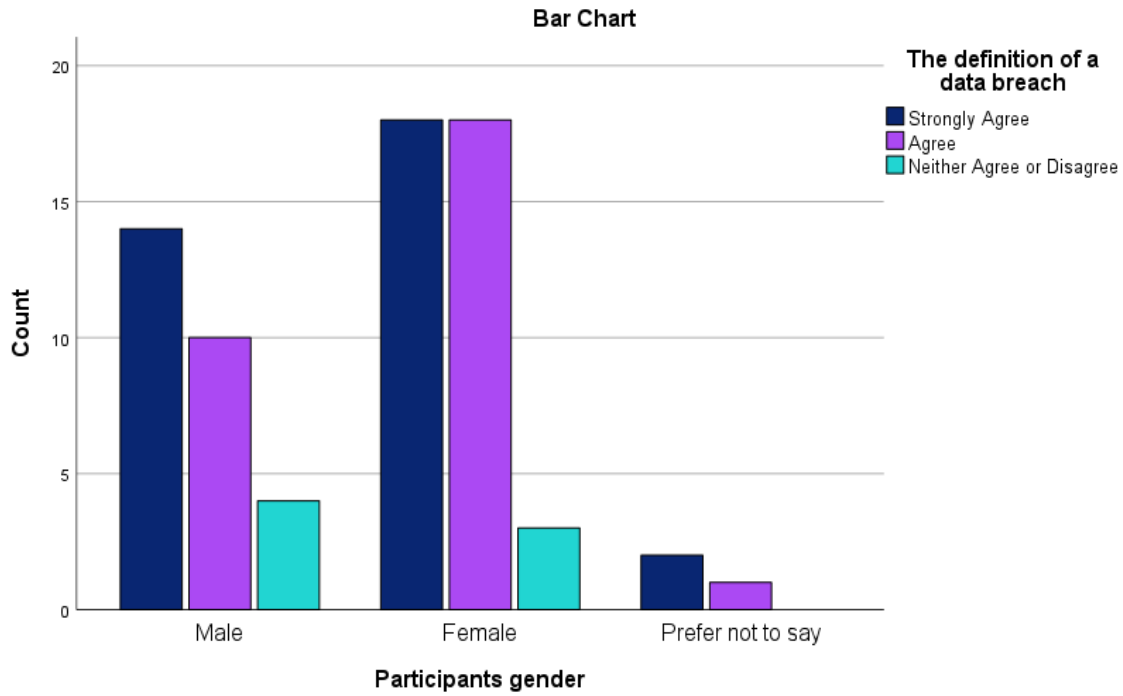

Figure 5 The correlation between data breach definition awareness (Q8) and the gender variable.

5-1-3 Employees' Experience and Management of Data Breach Incidents

Several questions were included to gather insights into participants' encounters with data breaches, specifically Q9, Q10, Q11, Q12, Q13, Q14, Q15, and Q16. Surprisingly, a significant number of participants opted not to respond to Q9, which aimed to explore instances of breach incidents within their university facilities. This reluctance to answer might stem from a sense of loyalty to their workplace, with participants hesitant to tarnish their university's reputation. Conversely, Q10 inquired about participants' experiences of data breaches outside their university. Results showed that nearly half (48.6%) reported no breaches of their personal data, while 45.7% confirmed experiencing data breaches outside their workplace. Regarding the management of breaches (Q12), the majority of participants from both universities (84.3%) stated they had not managed a data breach, with only a small proportion of employees (5.7%) indicating partial involvement in managing a breach. Further detailed statistics for these questions are presented in Table 34.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q9: Have you ever experienced a data breach incident within your university?	Yes	0%	0%	0	0,015
	No	0	1 (1.4%)	1 (1.4%)	
	Prefer not to say	29	40	69 (98.6%)	
Q10: Have you ever experienced a data breach incident outside a university context?	Yes	21 (30%)	11(15.7%)	32 (45.7%)	0,657
	No	18 (25.7%)	16 (22.9%)	34 (48.6%)	
	Prefer not to say	2 (2.9%)	2 (2.9%)	4 (5.7%)	
Q12: Did you manage a personal data breach within your university?	Yes, definitely	0	0	0	0,673
	Yes, to some extent or partly	1(1.4%)	3(4.3%)	4(5.7%)	
	No	36(51.4%)	23(32.9%)	59(84.3%)	
	Don't know	3(4.3%)	2(2.9%)	5(7.1%)	
	Prefer not to say	1(1.4%)	1(1.4%)	2 (2.9%)	

Table 34 Distribution of percentages and frequencies from the employees' survey for questions 9,10, and 12.

In Q11, participants were asked to provide detailed descriptions of data breaches they experienced. Most responses indicated participants' belief that their emails and mobile numbers had been hacked, as they received random and advertising emails. However, it is not possible to conclude whether such incidents were workplace violations because participants did not specify whether their emails were official or personal. Some participants also reported incidents of financial data theft involving personal data such as their mobile number and email address. Two particularly interesting responses were noted. One employee mentioned, '**I have a graduate student whom I supervise, who illegally used his colleague's personal data'**, while another stated, **'A university employee leaked my personal information to others'.**

Additionally, the researcher inquired about the type of data breach managed by respondents who had experienced a breach in question 13. A drop-down list was provided in the survey, including prominent types of data breaches identified in the literature review. This list comprised accidental disclosure, hacking or malware, payment card fraud, insider attack, physical loss of data, data theft, hardware loss, unknown, or another type. Based on the collective calculation of results, the most common response was 'unknown' at 41.3%, followed by 'other' at 17.4%. 'Hacking or malware' and 'payment card fraud' each had a frequency of 8.6%, 'unintended disclosure' and 'data stolen' each had a frequency of 6.5%, and 'insider attack' and 'physical loss of data' each had a frequency of 4.4%. Table 35 illustrates this information.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q13: If you have managed a data breach, then can you select what sort of data breach it was?	Unintended disclosure	1(2.2%)	2(4.3%)	3(6.5%)	0,636
	Hacking or malware	2(4.3%)	2(4.3%)	4(8.6%)	
	Payment card fraud	3(6.5%)	1(2.2%)	4(8.7%)	
	Insider attack	1(2.2%)	1(2.2%)	2(4.4%)	
	Physical loss of data	1(2.2%)	1(2.2%)	0(4.4%)	
	Data stolen	2(4.3%)	1(2.2%)	3(6.5%)	
	Device loss	0(0.0%)	1(2.2%)	1(2.2%)	
	Unknown	11(23.9%)	8(17.4%)	19(41.3%)	
	Other	4(8.7%)	4(8.7%)	8(17.4%)	

Table 35 Distribution of percentages and frequencies from the employees' survey for question 13 data breach sorts.

In Question 14, participants were asked to describe how they had managed a data breach if they had experienced one. The answers included that they had contacted technical support services at their university. To avoid hacking,

participants provided tips, such as creating strong passwords and downloading security software. One of the responses relating to mitigating breaches was as follows, '**Establish a national data protection act for academic institutions'**.

After experiencing a breach, 25.8% of employees felt anger, 25% of them suffered from anxiety, 16.9% of them felt fear, and 12% were sad and surprised. This information was shown in Q15, which captured the emotional responses after experiencing a data breach. The following chart illustrates these effects.

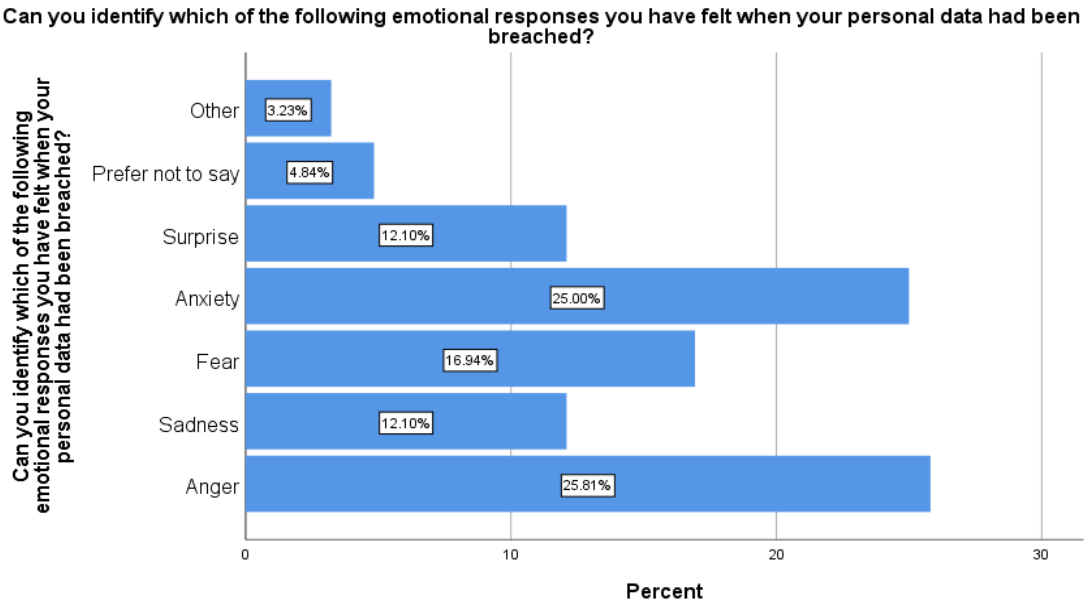

Figure 6 Emotional responses after experiencing a data breach incident in question 15.

Sex and age correlations

A significant correlation ($p = .016$) was found between gender (Q2) and emotional impacts (Q15) of data breaches. Figure 7 illustrates that females experienced greater emotional effects from data breaches compared to males. Emotional responses, ranked by statistical significance, were fear (1), sadness (2), anger (3), and anxiety (4). Notably, anger was more prevalent among males, while proportions of fear, sadness, and anxiety were more evenly distributed. Additionally, a Kruskal–Wallis H test revealed a significant difference ($p = .000 < .05$) between age groups (Q3) and the emotional effects of data breaches (Q15), indicating that age influenced emotional responses. Emotional effects increased significantly in the age groups 25–34 and 35–44,

while decreasing in the age groups 18–24 and 55 and above. Anger was observed across all age groups.

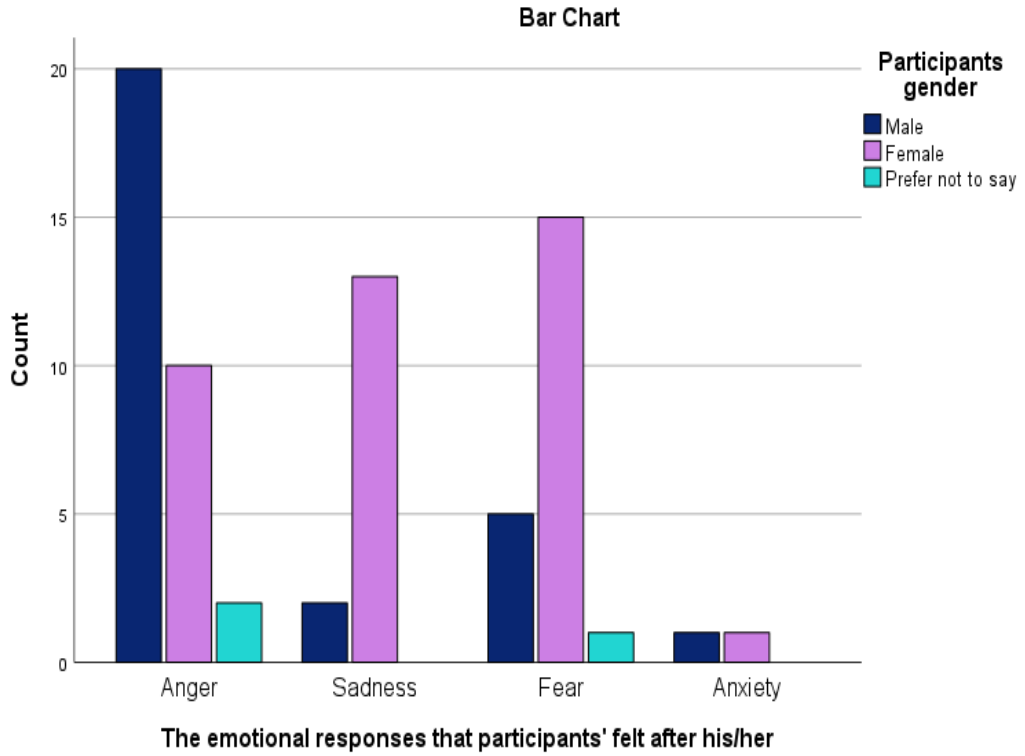

Figure 7 The correlation between question 15 the emotional impacts of data breaches and the gender variable.

In Question 16, both KSU and TauibahU employees reported a significant change in trust following a personal data breach. At KSU, 34% strongly agreed and 29% agreed with the statement, indicating a total of 63% who experienced a change in trust. At TaibahU, 24% strongly agreed and 31% agreed, totalling 55% who reported a shift in trust. Thus, while both universities show a considerable impact on trust due to the breach, KSU employees expressed this change slightly more intensely compared to their TauibahU counterparts.

5-1-4 Employees' Technical Perspectives on Data Breaches

To comprehensively analyse the impacts of data breaches, participants' technical proficiency was assessed through six questions. Four questions presented technical statements using a five-point Likert scale, gauging participants' perceptions. Regarding satisfaction with technical tools for minimising data breaches (Q26), the most common response was 'neither agree nor disagree' (38.5%), followed by 'agree' (20%), 'disagree' and 'strongly

disagree' (both 8.5%), and 'strongly agree' (7.1%), with 17.1% preferring not to provide an opinion.

Statistical differences between the two universities were evident. Although percentages under the 'disagree' scale were similar, KSU had more 'strongly disagree' responses, indicating some employees believe that technical tools are insufficient to limit data breaches. For the statement on whether workplace information systems and networks were managed to reduce the impact of data breaches (Q27), 35.7% chose 'neither agree nor disagree', and 27.1% agreed. Significant differences between the universities were observed, with TaibahU participants more neutral, and KSU participants expressing confidence in their systems.

Regarding technical failings as the main cause of data breaches (Q28), almost half (47.1%) agreed, while 4.2% disagreed. Similarly, for poor technical practices of employees as the main cause (Q29), 45.1% agreed, while 7.1% disagreed. Statistical analysis did not reveal significant differences, but the highest response at KSU was 'neutral', while at TaibahU, it was 'I agree' regarding technical malfunctions as a major cause. Participants from both universities agreed that poor employee practices contribute to data breaches.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q26: I believe that the technical tools adopted by my organisation are appropriate to minimise data breaches.	Strongly Agree	4(5.7%)	1(1.4%)	5(7.1%)	0.013
	Agree.	8(11.4%)	6(8.6%)	14(20.0%)	
	Neither Agree or Disagree	12 (17.1%)	15(21.4%)	27(38.6%)	
	Disagree	3(4.3%)	3(4.3%)	6(8.6%)	
	Strongly Disagree.	6(8.6%)	0(0.0%)	6(8.6%)	
	Prefer not to say	8(11.4%)	4(5.7%)	12 (17.1%)	
Q27: I think that the information systems and networks used in my work environment are managed to reduce the impact of data breaches.	Strongly Agree	5(7.1%)	2(2.9%)	7(10.0%)	0.005
	Agree.	12 (17.1%)	7(10.0%)	19 (27.1%)	
	Neither Agree or Disagree	10 (14.3%)	15(21.4%)	25 (35.7%)	
	Disagree	1(1.4%)	1(1.4%)	2(2.9%)	
	Strongly Disagree.	4(5.7%)	0(0.0%)	4(5.7%)	
	Prefer not to say	9(12.9%)	4(5.7%)	13(18.6%)	
Q28: I think that technical failings are the main cause of data breaches	Strongly Agree	3(4.3%)	5(7.1%)	8(11.4%)	0.202
	Agree.	12 (17.1%)	13(18.6%)	25 (35.7%)	
	Neither Agree or Disagree	13(18.6%)	7(10.0%)	20(28.6%)	
	Disagree	2(2.9%)	0(0.0%)	2(2.9%)	
	Strongly Disagree.	1(1.4%)	0(0.0%)	1(1.4%)	
	Prefer not to say	10 (14.3%)	4(5.7%)	14(20.0%)	
Q29: I think that weak employee practices are the main cause of data breaches	Strongly Agree	8(11.4%)	4 (5.7%)	12 (17.1%)	0.359
	Agree.	10 (14.3%)	10 (14.3%)	20(28.6%)	
	Neither Agree or Disagree	12 (17.1%)	8(11.4%)	20(28.6%)	
	Disagree	2(2.9%)	3(4.3%)	5(7.1%)	
	Strongly Disagree.	0(0.0%)	0(0.0%)	0(0.0%)	
	Prefer not to say	9(12.9%)	4(5.7%)	13(18.6%)	

Table 36 Distribution of percentages and frequencies from the employees' survey for questions 26,27,28, and 29.

Question 30 explored employees' perceptions of the most common bad practices among employees. The two most common answers among employees were opening anonymous emails and clicking on unknown links (both 20.8%), followed by choosing simple or not updated passwords and sharing them with others (17%), the shared use of computers among employees (14.2%), browsing malicious websites on internal university

networks (13.2%), and using private computers for work and accessing university systems through them (10.4%).

The most widespread bad practice among employees in TaibahU was considered to be clicking on unknown links (22.1%), while in KSU opening anonymous emails was the most common answer (20.4%). Moreover, participants were asked to describe the technical implications of data breaches (Q31), but they briefly described the technical impacts, e.g., one participant linked the effect to the ‘destruction of devices’, while other responses explained the inability to describe these impacts e.g., ‘I don’t know’.

Sex and age correlations with technical questions:

The correlation between gender and the employees’ perceptions of the most common practices (Q30) resulting in a data breach was examined. A statistically significant difference was found between gender and faculty members’ perceptions ($p = .02 < .05$) through the chi-square independence test; thus, a link was found between gender and perceptions of bad practices. Males had a slightly stronger perception than females that the practice of 'opening anonymous emails' was common among employees. According to the result of the Kruskal–Wallis test, there was no relationship between age and perceptions of poor practice ($p > .05$). The Kruskal–Wallis test was used because the data type of the variables was ordinal.

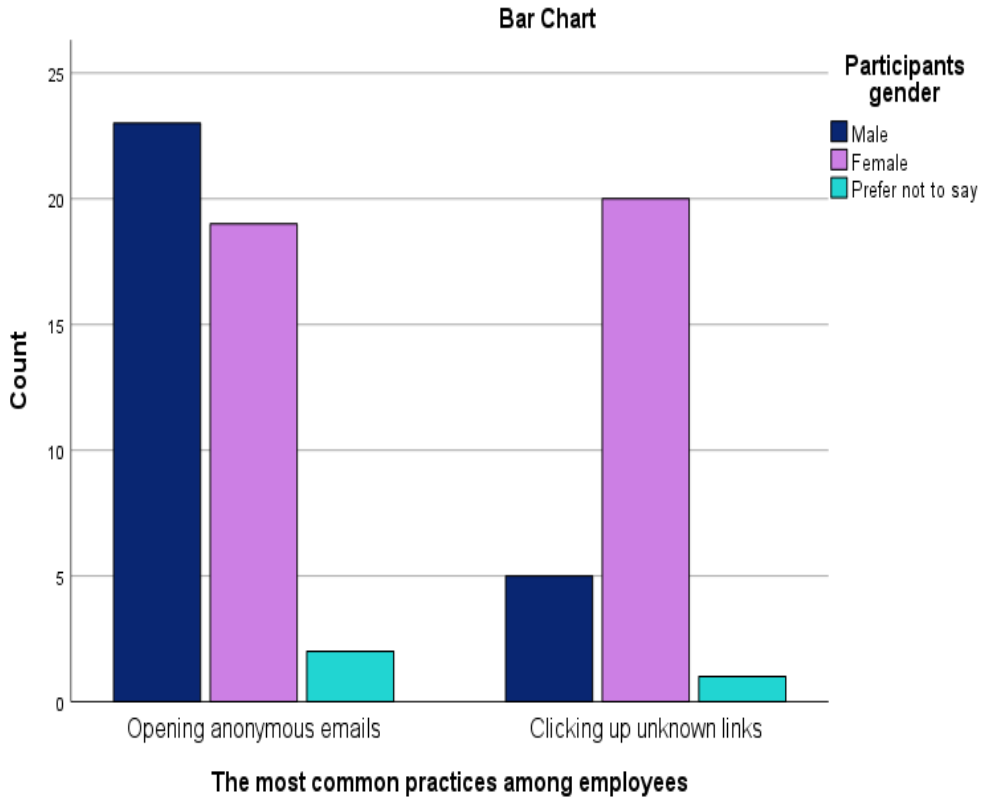

Figure 8 The correlation between question 30 the most common practices and the gender variable.

5-1-5 Employees' Organisational Perspectives on Data Breaches

One objective of this study was to explore the organisational dimension of data security and employees' perspectives on managing data breaches within their respective universities. Several questions (Q17-Q22) were designed to uncover participants' perceptions in this regard. In Q17, participants were asked about their understanding of how their universities handle their personal data. The results showed that 38.6% of employees answered 'No', indicating that they did not understand how their personal data is processed, while 14.3% responded with 'I don't know', indicating some hesitation in their understanding of the subject or their awareness of how their personal data is processed. Additionally, 21.4% had partial knowledge, and 8.6% had full knowledge of how their data is managed. Notably, a higher percentage of employees at KSU had partial knowledge of data processing compared to those at TaibahU. Conversely, a greater proportion of employees at TaibahU reported having no understanding of how their personal data is handled compared to their counterparts at KSU.

In Q18, participants were asked about their knowledge of the data security policies implemented by their universities regarding data breaches. The results showed that 44.3% of employees answered ‘No’, indicating they were unaware of these policies, while 15.8% responded with ‘I don’t know’, suggesting uncertainty or a lack of familiarity with the subject. Additionally, 17.1% had partial knowledge, meaning they were aware of the existence of such policies but did not fully understand their content or application. Only 5.7% had full knowledge of their university’s data security policies, while 17.1% chose ‘Prefer not to say’.

Although the distinction between ‘No’ and ‘I don’t know’ is clear in this context, there may be some ambiguity between ‘I don’t know’ and ‘Partial knowledge’ when interpreting responses regarding data security policies. Therefore, recognising this distinction is crucial for accurate analysis. ‘I don’t know’ reflects a complete lack of awareness, indicating that these respondents were either unfamiliar with the concept of data security policies or uncertain about whether their university had such policies in place. In contrast, ‘Partial knowledge’ suggests that respondents were aware that these policies existed but did not fully grasp their specifics, scope, or practical implementation. These findings highlight a significant gap in employees’ awareness of data security policies, with a considerable proportion of respondents either unaware or uncertain about them. The relatively low percentage of employees with full or partial knowledge suggests a need for improved communication, training, or better accessibility to policy information to ensure staff are well-informed about institutional data breach protocols. This result is particularly noteworthy given that most respondents were assistant professors or lecturers, roles in which employees are typically expected to have a good understanding of university policies. However, statistical analysis did not indicate a significant relationship ($p = .09 > .05$) between employment level and awareness of data security policies. While awareness levels were generally similar between the two universities, a higher percentage of employees at KSU reported being unaware of these policies compared to those at TaibahU.

In Q19, participants were asked whether they knew how to file a complaint if their personal data had been leaked. The results highlight a concerning gap in awareness, with 37.1% answering ‘No’, indicating they were certain they did not know the complaint procedure, and 11.4% selecting ‘I don’t know’, suggesting uncertainty about whether they possessed this knowledge. The distinction between these responses is critical. ‘No’ reflects definite unawareness, while ‘I don’t know’ implies hesitation or an incomplete understanding.

Only 10% were fully aware of the complaint process, while 25.7% had partial knowledge, indicating that even among those with some familiarity, clarity was lacking. Additionally, 15.8% preferred not to respond, which may suggest discomfort or a lack of confidence in discussing data breach complaints. These findings point to significant deficiencies in institutional communication and training regarding complaint procedures for personal data breaches. Given the increasing importance of data protection, universities must ensure that employees are adequately informed about their rights and the appropriate channels for reporting breaches. Table 37 provides the percentages for Q17, Q18, Q19, Q20, and the number of respondents.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q17: Do you know how your personal data is collected and processed by the university?	Yes, definitely	3(4.3%)	3(4.3%)	6(8.6%)	0.123
	Yes, to some extent or partly	10(14.3%)	5(7.1%)	15(21.4%)	
	No	12(17.1%)	15(21.4%)	27(38.6%)	
	Don't know	8(11.4%)	2(2.9%)	10(14.3%)	
	Prefer not to say	8(11.4%)	4(5.7%)	12(17.1%)	
Q18: Do you know the data security policies adopted by your university regarding data breaches?	Yes, definitely	2(2.9%)	2(2.9%)	4 (5.7%)	0.413
	Yes, to some extent or partly	7 (10%)	5 (7.1%)	12 (17.1%)	
	No	17 (24.3%)	14 (20%)	31 (44.3%)	
	Don't know	7 (10%)	4 (5.7%)	11 (15.8%)	
	Prefer not to say	8 (11.4%)	4 (5.7%)	12 (17.1%)	
Q19: Do you know how you can make a complaint if your personal data has been leaked?	Yes, definitely	5 (7.1%)	2 (2.9%)	7 (10.0%)	0.935
	Yes, to some extent or partly	6 (8.6%)	12 (17.1%)	18 (25.7%)	
	No	18 (25.7%)	8 (11.4%)	26 (37.1%)	
	Don't know	4 (5.7%)	4 (5.7%)	8 (11.4%)	
	Prefer not to say	8 (11.4%)	3 (4.3%)	11 (15.8%)	
Q20: Did you receive data security training when you were employed at the university?	Yes, definitely	1(1.4%)	0(0.2%)	1(1.4%)	0.158
	Yes, to some extent or partly	6(8.6%)	3(4.3%)	9(12.9%)	
	No	25(35.7%)	22(31.4%)	47(67.2%)	
	Don't know	1(1.4%)	0(0.2%)	1(1.4%)	
	Prefer not to say	8(11.4%)	4(5.7%)	12(17.1%)	

Table 37 Distribution of percentages and frequencies from the employees' survey for questions 17,18,19, and 20.

A concern raised by the results of the survey is that, according to Q20, more than half of the participants (67.2%) had not received any training on data security, whereas 1.4% had been fully trained and 12.8% had received partial training. From Q21, it was found that 20.5% of those who had received training had undergone formal training, 17% had undergone web-based training, 14.7% had undergone self-study, and 5.8% had undertaken mandatory formal training. In the final question of the survey on the organisational aspect of data security, the participants read a statement (Q22) indicating their satisfaction with the data and information security awareness programmes provided by their universities. It was found that 31.4% neither agreed nor disagreed with the statement, 27.1% disagreed, 17.1% preferred not to answer, 12.8% agreed, 10% strongly

disagreed, and only 1.4% strongly agreed with the statement that the data security awareness programmes in their universities are sufficient.

5-1-6 Employees' Emotional Perspectives on Data Breaches

Although data breaches are caused by technical vulnerabilities, technical awareness is not the only area that should be prioritised. Eight questions about emotional responses and the impacts of breaches were formulated. The questions focused on the emotional reactions identified in the literature review. Question 32 focused on measuring the fears of faculty members.

Question 32 focused on measuring the fears of faculty members. It was found that 40% strongly agreed with their fear of having their data leaked, and 32.8% agreed with the scenario. A small number of participants (5.7%) neither agreed nor disagreed, while 1.4% each disagreed and strongly disagreed.

Question 33 explored privacy concerns regarding the personal data provided by the beneficiaries to the university. About half (49.9%) of participants expressed concerns about the privacy of their data, 8.5% had no concerns, and 21.4% gave a neutral response. While statistical analysis did not show significant differences between the two universities for Questions 32 and 33, noteworthy data emerged: participants from both universities expressed concerns about data privacy and the possibility of unauthorised data access. This may stem from their lack of knowledge about data processing and storage, as well as a lack of awareness of security policies within their university settings, as revealed by the organisational axis results.

In Question 34, respondents indicated their anticipated emotional responses to data breaches, including anger, fear, and anxiety. Specifically, 25.7% strongly agreed that they would experience these emotions, 22.8% agreed, 27.1% neither agreed nor disagreed, 2.8% disagreed, 1.4% strongly disagreed, and 20% did not provide a response. Question 35 inquired whether pressure and provocation in the work environment could lead to an angry employee causing intentional or unintentional data leakage. The findings revealed that 41.3% of participants agreed with the statement, 19.9% rejected it, 18.5% provided a neutral response, and 20% preferred not to answer. The statistical analysis revealed no discernible differences between the two universities in Questions

34 and 35. In Question 34, it is notable that there was a remarkable similarity in the percentages of ‘strongly agree’ responses, highlighting a consensus among participants regarding the adverse nature of emotional reactions, such as anger, fear, and depression, arising from data breaches. However, in Question 35, 22.8% of participants from TaibahU showed a slightly higher level of agreement compared to their peers from KSU, who had an 18% agreement rate. Their concurrence focused on the notion that excessive provocation within the work environment can lead to an escalation in employee anger, potentially resulting in damage to the data security system.

Concerning the emotion of shock, it was associated with the level of security awareness regarding handling data breaches. Participants were asked whether they agreed that a security-aware individual would not be traumatised if they experienced a breach of their personal information (Q36). The responses displayed similar frequencies in both universities, with 25.6% of participants agreeing, 29.9% disagreeing, 24.2% providing a neutral response, and 20% not providing a response. In Question 37, 37.1% of participants acknowledged feeling uncomfortable when required to disclose their personal data to the university due to trust concerns, while 17.1% expressed neutrality on the matter.

Furthermore, participants were questioned about whether employees' feelings of frustration might pose a threat to the organisation through an intentional or unintentional data breach (Q38). The most common response indicated that such a threat existed (47.1%), while 5.7% of participants believed no such threat existed. The percentages indicated a notable level of awareness among employees regarding the monitoring of rumours concerning data breach incidents at universities (Q39), as there was a predominant preference for responses on the ‘neutral’ and ‘disagreement’ scales in relation to tracking such rumours.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q32: I am afraid that my personal data may be leaked to unauthorised persons, which may expose me to fraud.	Strongly Agree	14(20.0%)	14(20.0%)	28(40.0%)	0.546
	Agree.	15(21.4%)	8(11.4%)	23(32.9%)	
	Neither Agree or Disagree	3(4.3%)	1(1.4%)	4(5.7%)	
	Disagree	0(0.0%)	1(1.4%)	1(1.4%)	
	Strongly Disagree.	0(0.0%)	1(1.4%)	1(1.4%)	
	Prefer not to say	9(12.9%)	4(5.7%)	13(18.6%)	
Q33: I have no concerns about the privacy of my data and personal information that I have provided to my university.	Strongly Agree	3(4.3%)	3(4.3%)	6(8.6%)	0.834
	Agree.	0(0.0%)	0(0.0%)	0(0.0%)	
	Neither Agree or Disagree	11(15.7%)	4(5.7%)	15(21.4%)	
	Disagree	13(18.6%)	11(15.7%)	24(34.3%)	
	Strongly Disagree.	5(7.1%)	6(8.6%)	11(15.7%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q34: I think the emotional responses (reactions) of individuals such as anger, fear, anxiety...etc., represent negative consequences of data breaches.	Strongly Agree	9(12.9%)	9(12.9%)	18(25.7%)	0.796
	Agree.	10(14.3%)	6(8.6%)	16(22.9%)	
	Neither Agree or Disagree	11(15.7%)	8(11.4%)	19(27.1%)	
	Disagree	1(1.4%)	1(1.4%)	2(2.9%)	
	Strongly Disagree.	1(1.4%)	0(0.0%)	1(1.4%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q35: Too much provocation in the work environment increases employee anger and may result in intentional or unintentional data leakage.	Strongly Agree	5(7.1%)	4(5.7%)	9(12.9%)	0.605
	Agree.	8(11.4%)	12(17.1%)	20(28.6%)	
	Neither Agree or Disagree	9(12.9%)	4(5.7%)	13(18.6%)	
	Disagree	7(10.0%)	4(5.7%)	11(15.7%)	
	Strongly Disagree.	3(4.3%)	0(0.0%)	3(4.3%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q36: People who have enough security awareness would not be shocked if s/he experience a data breach event.	Strongly Agree	3(4.3%)	3(4.3%)	6(8.6%)	0.771
	Agree.	5(7.1%)	7(10.0%)	12(17.1%)	
	Neither Agree or Disagree	11(15.7%)	6(8.6%)	17(24.3%)	
	Disagree	12(17.1%)	8(11.4%)	20(28.6%)	
	Strongly Disagree.	1(1.4%)	0(0.0%)	1 (1.4%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q37: It is usually an unpleasant experience for me when I have to disclose my personal data to the university due to trust issues.	Strongly Agree	5(7.1%)	5(7.1%)	10(14.3%)	0.856
	Agree.	14(20.0%)	12(17.1%)	26(37.1%)	
	Neither Agree or Disagree	9(12.9%)	3(4.3%)	12(17.1%)	
	Disagree	3(4.3%)	4(5.7%)	7(10.0%)	
	Strongly Disagree.	1(1.4%)	0(0.0%)	1(1.4%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q38: A frustrated employee presents a potential threat to breach data security by performing malicious acts.	Strongly Agree	0(0.0%)	4(5.7%)	4(5.7%)	0.921
	Agree.	18(25.7%)	15 (21.4%)	33(47.1%)	
	Neither Agree or Disagree	11(15.7%)	4(5.7%)	15(21.4%)	
	Disagree	3(4.3%)	1(1.4%)	4(5.7%)	

	Strongly Disagree.	0(0.0%)	0(0.0%)	0(0.0%)	
	Prefer not to say	9(12.9%)	5(7.1%)	14(20.0%)	
Q39: I am interested in tracking rumours that some universities are facing data security problems, especially tracking data breach incidents in universities.	Strongly Agree	2(2.9%)	3(4.3%)	5(7.1%)	0.494
	Agree.	3(4.3%)	1(1.4%)	4(5.7%)	
	Neither Agree or Disagree	11(15.7%)	11(15.7%)	22(31.4%)	
	Disagree	15(21.4%)	7(10.0%)	22(31.4%)	
	Strongly Disagree.	1(1.4%)	1(1.4%)	2(2.9%)	
	Prefer not to say	9(12.9%)	6(8.6%)	15(21.4%)	

Table 38 Distribution of percentages and frequencies from the employees' survey for questions 17,18,19, and 20.

5-1-7 Employees' Needs and Wishes of Data Protection

This section examines the aspirations and needs of faculty members from the data security system in their universities. The participants answered four questions on this topic. In question 40, participants in the survey identified technical aspects (36.1%) as the primary detrimental factor of data breaches, followed by organisational factors (35.2%), and then personal implications (25%). At KSU, views were evenly divided between the organisational and technical aspects of damage caused by data breaches followed by the personal implications. Conversely, at TaibahU, technical issues took precedence, followed by organisational concerns, and finally personal implications. Question 41 enquired about the needs and aspirations of the participants from the data security system. Employees prioritise the development of organisational aspects (37.4%) over technical aspects (34.8%) and personal considerations (22.6%). Despite variations in percentages, all employees from both universities agreed on the same order of development aspects, showing consistent prioritisation regardless of numerical disparities. Free comments were possible for Q41 and Q42, through the 'other' option, but no comments were given. Table 39 plots the distribution of ratios and frequencies for Q40 & Q41.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q40: From your perspective, what is the most harmful aspect of data breaches?	Technically.	22(20.4%)	17(15.7%)	39(36.1%)	0.498
	Organisationally.	22(20.4%)	16(14.8%)	38(35.2%)	
	Personally.	16(14.8%)	11(10.2%)	27(25 %)	
	Other	2(1.9%)	2(1.9%)	4(3.7%)	
Q41: Which of the following aspects do you think are important for developing the process of protecting your personal data that you would like your university to adopt?	Technical protection tools	21(18.3%)	19(16.5%)	40(34.8%)	0.209
	Organisational procedures	22(19.1%)	21(18.3%)	43(37.4%)	
	Personal aspects	16(13.9%)	10(8.7%)	26(22.6%)	
	Prefer not to say	2(1.7%)	2(1.7%)	4(3.5%)	
	Other aspects	2(1.7%)	0(0.0%)	2(1.7%)	
Q25: Do you think that your personal data should be minimised? Should your university keep less personal information about you?	Yes, definitely	17(24.3%)	11(15.7%)	28(40.0%)	0.087
	Yes, to some extent or partly	7(10.0%)	11(15.7%)	18(25.7%)	
	No	5(7.1%)	1(1.4%)	6(8.6%)	
	Don't know	4(5.7%)	2(2.9%)	6(8.6%)	
	Prefer not to say	8(11.4%)	4(5.7%)	12(17.1%)	

Table 39 Distribution of percentages and frequencies from the employees' survey for questions 40,41 and 25.

As illustrated in Table 39, Question 25 investigated whether faculty members desired a reduction in the collection of their personal data. Approximately 40% of participants indicated a definitive 'yes', while 25.7% responded with either 'yes' or 'to some extent'. Similarly, the frequencies for 'no' and 'don't know' were both 8.6%. Question 42 explored the modifications employees wished to see for enhancing data security and safeguarding their personal information. The most common responses included increasing employee awareness, implementing protective measures, and enhancing training programmes. Additionally, the following response was provided: ‘That the data protection system be standardised nationally according to approved protocols and a unified university charter for security and information exchange {...}, with an initiative to identify vulnerabilities and develop innovative, efficient, and dependable crisis management solutions’.

5-1-8 Employees' Insights on Mitigation of the Impact of Data Breaches

Many of the questions revealed some of the effects of data breaches. Universities therefore should consider developing ways to mitigate data breaches. For Q23, which explored the appropriateness of mitigation strategies to reduce the consequences of data breaches, 37.1% of the participants in both universities answered that they did not know, 17.1% considered the strategies to be appropriate, 24.2% considered that they are appropriate to some extent, 4.2% considered them to be definitely appropriate, and 12% preferred not to answer. For Q24, participants stated that they preferred 'compensation' as a mitigation strategy (48.3%), followed by an apology (32.9%). A few participants (10.9%) preferred other strategies, such as 'promising to protect data', 'punishing the hacker', 'raising the quality of security', and 'recognition of the breach event'. No statistically significant differences were observed between the two universities for questions 23 and 24. See Table 40 which provides information about percentage distribution and frequencies in Q23 & Q24.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q23: Do you think strategies to mitigate the impact of data breaches at the university are appropriate?	Yes, definitely	3(4.3%)	0(0.0%)	3(4.3%)	0.127
	Yes, to some extent or partly	9(12.9%)	8(11.4%)	17(24.3 %)	
	No	7(10.0%)	5(7.1%)	12(17.1 %)	
	Don't know	14(20.0%)	12(17.1%)	26(37.1 %)	
	Prefer not to say	8(11.4%)	1(1.4%)	9(12.9%)	
Q24: How would you prefer your university to treat you in case you are exposed to a data breach to mitigate the breach's effects?	Apology	17(24.3%)	13(18.6%)	30(42.9 %)	0.500
	Compensation	22(31.4%)	16(22.9%)	38(54.3 %)	
	Prefer not to say	2(2.9%)	0(0.0%)	2(2.9%)	
	Other	0(0.0%)	0(0.0%)	0(0.0%)	

Table 40 Distribution of percentages and frequencies from the employees' survey for questions 23 and 24.

Gender and age correlation:

When gender- and age-related differences in preferred strategies for mitigation (Q24) were compared, it was observed that males preferred ‘apologising’ (56.7%), while females preferred ‘compensation’ (71.1%). However, no statistically significant correlation was found ($p > 0.05$). Regarding the age groups, ‘apologising’ and ‘compensation’ were the most popular responses for the 35–44 and 25–34 age groups, respectively.

Job level correlation:

The Kruskal–Wallis test was conducted to examine the relationship between Q4 and Q24. A significant relationship was observed ($p = 0.01 < 0.05$). 40% of the assistant professors but only 6.6% of demonstrators favoured ‘apology’ as an appropriate mitigation strategy. Conversely, 44.7% of lecturers but only 7.8% of associate lecturers chose ‘compensation’. These may be due to the differences in the participants’ income regarding their employment levels.

5-2 Students' Survey Findings:

5-2-1 Students Demographic

Nearly 433 students were approached for data collection in this study, among them 242 started the questionnaire but not all completed it. Completed data was obtained from a total of 191 participants with 149 (87%) from TaibahU and 42 (22%) from KSU. The age range was 15 to 35 and upwards. In Table 43, the demographic characteristics of the respondents were presented with their corresponding universities. In sum, 52.9 % (n = 101) were male and 45.5 % (n =87) were female. Most of their age was 18-24 (90%, n = 172), and only 8.4 % (n = 16) were 25-34. The number of male and female students was found to be higher at TaibahU compared to KSU. The number of students whose ages ranged from 18-24 was comparatively higher among TaibahU participants. That is an expected result, given that the appropriate age for bachelor's students falls within this category.

Variable name		**King Saud University (%)**	**Taibah University (%)**	**Total (%)**
Gender	Male	9 (4.7)	92(48.2)	101(52.9)
	Female	33 (17.3)	54 (28.3)	87 (45.5)
	Prefer not to say	0(0)	3(1.6)	3(1.6)
Age	18-24	29(15.2)	143 (74.8)	172 (90)
	25-34	10 (5.2)	6 (3.1)	16.(8.4)
	35 and up	3(1.6)	0	3 (1.6)
	Prefer not to say	0	0	0

Table 41 Socio-demographic characteristics of KSU and TaibahU students' participants.

Students participating in the questionnaire were from various scientific disciplines, including social service, accounting, architecture, biology, business management, chemistry, communication and information, computer networks and communications, computer science, early childhood education, English language, family guidance and correction, geography, health, heritage resources management and tourist guidance, history, information science, information systems, Islamic studies, journalism, languages and translation, law, marketing, mathematics, occupational therapy, physics, public relations,

qur'anic studies, respiratory therapy, sociology, software engineering, sports science, and tourism and hotel management.

5-2-2 Students Awareness of Data Breaches

This section reviews the findings from the students' questionnaire to determine their awareness of the concept of data breaches and their perceptions of how they occur. Q5 and Q6 were open-ended to give students more freedom to express their opinions, while Q7 was closed-ended (five-point Likert scale) to assess students' agreement with the definition of the term provided by the UK Data Protection Compliance Act.

In terms of Question 5, 30 responses acknowledged that they could not identify the concept of a data breach. Other responses, which offered a definition, focused on a narrow view of the term. These responses concentrated on hacking and stolen data, data espionage, data editing and modification, or unauthorised access to data. For instance, one comment described 'intentional or unintentional editing of secure or private information,' while another referred to 'stealing someone else's data.'

Some students considered the definition more comprehensively. For example, one participant stated that a data breach is 'bypassing the privacy of individuals,' while another explained it as 'any act that breaches data systems.'

Question 6 aims to explore participants' awareness in describing how data breaches occur. Thirty-five responses indicated an inability to describe data breaches, e.g., one student's response was, 'I don't have the knowledge to answer this question.' Most of the other perspectives revolved around the occurrence of violations through spam links and fraudulent links.

One student explained a data breach scenario: 'The data is hacked through spam sent from a fake company, and the person is deceived into updating their data through {please click on the link}, after which the data is leaked.'

Regarding the extent of students' agreement with the UK definition of data breaches question 7, table 42 shows that most of the participants 87 (46.5%), and 80 (40.7%) 'agreed' and 'strongly agreed' with the definition of the security

breach. In contrast, 4(2.1%) and 2 (1.1%) were ‘disagreed’ and ‘strongly disagreed’, and 7(3.7%) preferred not to say.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q7: One definition of a data breach is that it is a ‘breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data’. Please indicate the extent to which you agree with this definition.	Strongly Agree	19(10.1)	61(30.6)	80 (40.7)	0.265
	Agree.	21(11.2)	66 (35.3)	87 (46.5)	
	Neither Agree or Disagree	1 (0.5)	10(5.4)	11 (5.9)	
	Disagree	1(2.4)	3 (2)	4 (2.1)	
	Strongly Disagree.	0 (0)	2 (1.1)	2(1.1)	
	Prefer not to say	0(0)	7(3.7)	7 (3.7)	

Table 42 Distribution of percentages and frequencies of students’ survey for question 7

5-2-3 Students’ Experience about Data Breach Incidents

In this axis, Q8, Q9, Q10, Q11, Q12, Q13, Q14, and Q15 will be displayed from the students' questionnaire. Table 43 evidences that statistically most of the participants 168 (89.8%) have not experienced a data breach incident within their university (Q8), among them 138 (73.8%) at TaibahU, and 30 (16) at KSU. However, it is noteworthy that a significant proportion of students had experienced a data breach (3.2 %). Among these students, 4 (2.1%) were at TaibahU, 2 (1.1%) at KSU, and 13 (7%) preferred not to respond.

The same table also represents the findings of Question 9, where 137 (71.7%) participants reported not experiencing a data breach incident outside their university. Among them, 112 (58.6%) were from TaibahU and 25 (13.1%) from KSU. In contrast, 38 (19.9%) of the participants stated they had experienced a data breach incident outside their university, including 28 (14.7%) from TaibahU and 10 (5.2%) from KSU. By conducting a t-test, statistical differences were observed between the results of the two universities for Q8 and Q9, where the p-value was < 0.05.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q8: Have you ever experienced a data breach incident within your university?	Yes	2 (1.1)	4(2.1)	6(3.2)	0.000
	No	30(16)	138(73.8)	168(89.8)	
	Prefer not to say	9(4.8)	4(2.1)	13(7)	
Q9: Have you ever experienced a data breach incident outside a university context?	Yes	10(5.2)	28(14.7)	38(19.9)	0.016
	No	25(13.1)	112(58.6)	137(71.7)	
	Prefer not to say	7(3.6)	9(4.7)	16(8.4)	

Table 43 Distribution of percentages and frequencies of students' survey in questions 8 and 9.

Question 10 was an open-ended question for students who had experienced a data breach. They were asked to describe the incident in detail and the steps taken. The questionnaire recorded 67 responses, with 20 participants describing an incident that happened to them. These incidents included data leakage through physical theft, spam, and hacking of social media platforms such as WhatsApp and Instagram.

Two out of the 20 respondents reported that they did not know how to avoid the breach. A student at KSU stated, 'I do not know the appropriate steps to avoid the breach.' Another student at TaibahU admitted that the hack occurred due to their mistake, saying, 'The hack happened unintentionally, as I gave the hackers my personal data.' Students' responses focused on steps to avoid such incidents, including not clicking on random links, setting strong passwords, and keeping them up to date.

Although the percentages were low in Q8 and Q9 regarding the experience of data breaches, whether inside or outside the universities, the researcher believes that the actual number of exposures to data breaches may be higher than the reported rate in these questions. This may be due to the sensitivity of the issue, which participants may have been reluctant to discuss. For example, in Q10, one participant remarked, 'I prefer not to reveal it.'

In question 11, the students were asked if they had managed a data breach. Table 44 represents that most of the participants 125 (67.6%) did not manage

a personal data breach within the university, among them 97 (52.4%) at TaibahU, and 28 (15.1%) at KSU, while 38(20.4%) of them don't know whether they were managed a personal data breach within the university or not, on the other hand, only 9 (4.9%) of the participants had definitely or partly managed a personal data breach within the university, and 4(2.2%) preferred not to say.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q11: Have you ever Managed a personal data breach within the university?	Yes, definitely	4(2.2%)	5(2.7%)	9(4.9%)	0.089
	Yes, to some extent or partly	2(1.1%)	7(3.8%)	9(4.9%)	
	No	28(15.1%)	97(52.4%)	125(67.6%)	
	Don't know	6(3.2%)	32(17.2%)	38(20.4%)	
	Prefer not to say	0(0%)	4(2.2%)	4(2.2%)	

Table 44 Distribution of percentages and frequencies of students' survey in question 11.

Students who experienced a data breach were asked to specify the type of breach in Question 12. Table 45 shows that 68 (59.6%) of the participants suffered from an unknown data breach, including 56 (49.1%) at TaibahU and 12 (10.5%) at KSU. This was followed by 15 (13.2%) of the participants who reported experiencing unintended disclosure, among them 11 (9.6%) at TaibahU and 4 (3.5%) at KSU. Meanwhile, 13 (11.4%) reported that they had experienced hacking or malware, with 9 (7.9%) from TaibahU and 4 (3.5%) from KSU. Additionally, 13 (11.4%) reported experiencing data theft, including 12 (10.5%) at TaibahU and 1 (0.9%) at KSU. On the other hand, 6 (5.3%) of the participants reported experiencing payment card fraud or device loss, including 1 (0.9%) at TaibahU and 5 (4.4%) at KSU.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q12: If you have managed a data breach, then can you select what sort of data breach it was?	Unintended disclosure	4(3.5%)	11(9.6%)	15(13.2)	0.377
	Hacking or malware	4(3.5%)	9(7.9)	13(11.4%)	
	Payment card fraud	1(0.9%)	5(4.4%)	6(5.3%)	
	Insider attack	0(0%)	1(0.9%)	1(0.9%)	
	Physical loss of data.	0(0%)	1(0.9%)	1(0.9%)	
	Data stolen	1(0.9%)	12(10.5%)	13(11.4%)	
	Devices loss	1(0.9%)	5(4.4%)	6(5.3%)	
	Unknown	12(10.5%)	56(49.1%)	68(59.6%)	

Table 45 Distribution of percentages and frequencies of students' survey in question 12.

Participants were asked to describe how the data breach was managed in Question 13, which recorded 56 responses. Most of the responses were related to two themes: either denying the management of the data breach or providing advice that was followed during its handling, such as intensifying protection methods and changing passwords.

Question 14 examined emotional responses. Among the students who experienced a data breach, Figure 6 shows that slightly more than half of the sample (52.7%) reported feelings of anger, followed by 48% reporting feelings of anxiety, 28% reporting surprise, while 24.7% reported sadness, and 15.3% preferred not to respond.

Data breaches not only had an emotional impact on participants but also affected their level of trust in universities. This was evident in question 15, where participants were asked to indicate their agreement with a statement regarding changes in their trust following a personal data breach. As shown in Table 46, among the 191 participants, 88 (50.9%) and 40 (23.1%) 'strongly agreed' and 'agreed', respectively, that their trust in the institution had changed. Meanwhile, 22 (12.7%) remained neutral, selecting 'neither agree nor disagree'. A smaller proportion, 9 (5.2%) and 2 (1.1%), 'disagreed' and 'strongly

disagreed', respectively. Additionally, 12 (6.9%) preferred not to disclose their stance.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q15: To what extent do you agree with this statement ' the level of my trust in the institution has changed after my personal data was breached'	Strongly Agree	22(12.7)	66(38.2)	88 (50.9)	0.278
	Agree.	10(5.7)	30(15.7) 17.3	40(23.1)	
	Neither Agree or Disagree	3(1.8)	19(9.9) 10.9	22(12.7)	
	Disagree	1(0.6)	8(4.2) 4.6	9(5.2)	
	Strongly Disagree.	0(0)	2(1.1)	2(1.1)	
	Prefer not to say	0(0)	12(7.0)	12(7.0)	

Table 46 Distribution of percentages and frequencies of students' survey in question 15.

Sex and gender correlations with the axis.

The study did not record any statistical links between the gender variable and the experience of data breaches inside (Q8) or outside (Q9) the university context. However, a statistical relationship was identified between the age variable and the experience of data breaches outside the university context, with a p-value of 0.03, indicating statistical significance.

This relationship suggests that age influences the likelihood of experiencing data breaches outside the university environment. For instance, older participants may be more susceptible to breaches due to factors such as greater online exposure, reliance on legacy systems, or reduced familiarity with modern cybersecurity practices (Pacheco, 2024). Conversely, younger participants might exhibit lower susceptibility, potentially due to their more frequent use of advanced protective tools and heightened awareness of digital privacy (Ugwu et al., 2021). Prior studies have noted similar trends, where age correlates with variations in digital literacy and cybersecurity behaviours, thereby influencing data breach experiences (Herbert et al., 2024).

The chi-square test did not show any statistically significant differences between the gender variable and Questions 14 and 15. However, it was noted that three emotions dominated among the students in Q14: anger, fear, and sadness.

As shown in Figure 9, male students predominantly felt anger after their data was leaked, while female students expressed a greater sense of fear.

The Kruskal-Wallis H test similarly found no statistical relationships between the age variable and Questions 14 and 15.

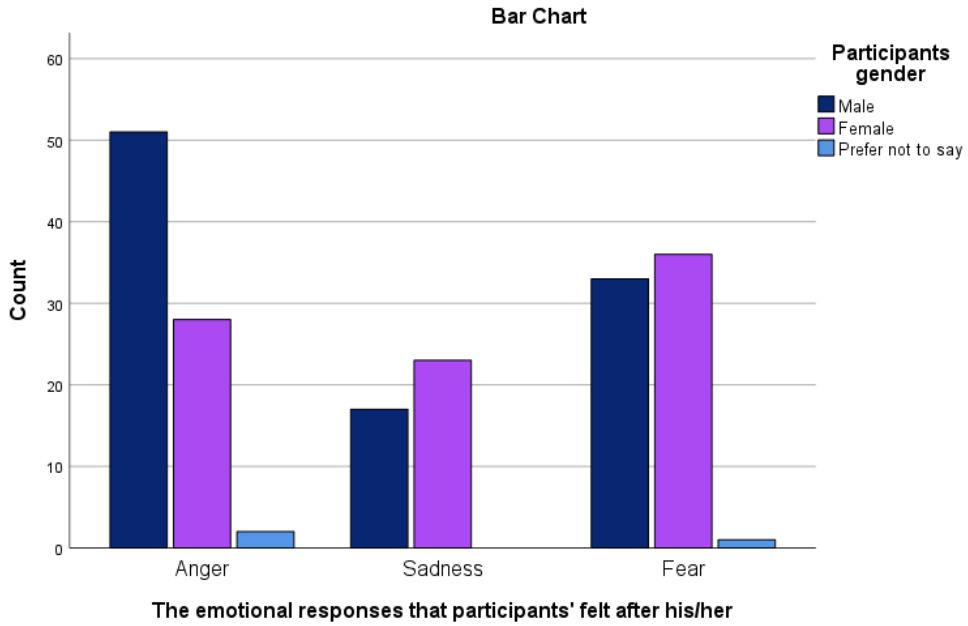

Figure 9 The correlation between question 14 the emotional responses and the gender variable.

5-2-4 Students' Technical Perspectives of Data Breaches

This section presents six questions from Q25 to Q30, with Table 47 summarising the preliminary analysis of responses to questions 25, 26, 27, and 28. For question 25, students were asked whether they believed that the technical tools implemented by their universities were effective in minimising data breaches. The findings indicate that 45 (23.9%) of students remained neutral, selecting 'neither agree nor disagree', while 65 (34.3%) agreed, and 52 (27.7%) strongly agreed. In contrast, 9 (4.9%) and 2 (1.2%) disagreed and strongly disagreed, respectively. Additionally, 15 (8.0%) preferred not to disclose their stance.

Beyond the effectiveness of technical tools, students also expressed their perceptions of how well information systems and networks were managed to control data breaches (Q26). Specifically, 73 (38.5%) agreed that their university's information systems and networks were well managed to mitigate the impact of data breaches and information security incidents, while 24 (12.8%) strongly agreed. Meanwhile, 61 (32.3%) remained neutral. A smaller proportion of students, 8 (4.2%) and 5 (2.5%), disagreed and strongly disagreed, respectively, while 18 (9.7%) preferred not to respond.

The next set of findings focused on students' perceptions of the main causes of data breaches, whether due to technical failures (Q27) or human errors (Q28). In question 27, 52 (27.7%) and 65 (34.3%) of the students agreed and strongly agreed, respectively, that technical failings were the primary cause of data breaches, while 45 (23.9%) were neutral. Conversely, 9 (4.9%) and 2 (1.2%) disagreed and strongly disagreed, respectively, whereas 15 (8.0%) preferred not to express an opinion.

Regarding human errors as a contributing factor (Q28), 57 (30.3%) of the respondents neither agreed nor disagreed that weak student practices played a significant role in data breaches, while 55 (29.0%) agreed and 28 (14.8%) strongly agreed. Meanwhile, 29 (15.4%) disagreed, and a smaller proportion, 5 (2.5%), strongly disagreed. Additionally, 15 (8.0%) opted not to provide a response. Across these four questions, no significant differences were observed between universities in students' responses, as indicated by a p-value greater than 0.05 in the T-test analysis. Table 47 provides a detailed breakdown of frequencies and percentages for questions 25, 26, 27, and 28.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q25: To what extent do you agree with this statement 'I believe that the technical tools adopted by my organisation are appropriate to minimise data breaches'?	Strongly Agree	13(8.0)	32(19.7)	45(27.7)	0.255
	Agree.	15(9.3)	41(25.2)	56(34.3)	
	Neither Agree or Disagree	9(5.5)	30(18.4)	39(23.9)	
	Disagree	2(1.2)	6(3.6)	8(4.9)	
	Strongly Disagree.	0(0)	1(1.2)	1(1.2)	
	Prefer not to say	1(0.6)	12(7.4)	13(8.0)	
Q26: To what extent do you agree with this statement 'I think that the information systems and networks used in my university are managed to reduce the impact of data breaches and information security incidents'?	Strongly Agree	7(4.3)	14(8.5)	21(12.8)	0.133
	Agree.	19(11.6)	44(26.8)	63(38.5)	
	Neither Agree or Disagree	10(6.1)	43(26.3)	53(32.3)	
	Disagree	2(1.2)	5(3.0)	7(4.2)	
	Strongly Disagree.	0(0)	4(2.5)	4(2.5)	
	Prefer not to say	2(1.2)	14(8.5)	16(9.7)	
Q27: To what extent do you agree with the statement 'I think that technical failings are the main cause of data breaches'?	Strongly Agree	13(8)	32(19.7)	45(27.7)	0.255
	Agree.	15(9.3)	41(25.2)	56(34.3)	
	Neither Agree or Disagree	9(5.5)	30(18.4)	39(23.9)	
	Disagree	2(1.2)	6(3.6)	8(4.9)	
	Strongly Disagree.	0(0)	2(1.2)	2(1.2)	
	Prefer not to say	1(0.6)	12(7.4)	13(8)	
Q28: To what extent do you agree with the statement 'I think that weak student practices are the main cause of data breaches'?	Strongly Agree	7(4.4)	17(10.5)	24(14.8)	0.265
	Agree.	13(8)	34(21)	47(29.0)	
	Neither Agree or Disagree	13(8)	36(22.1)	49(30.3)	
	Disagree	6(3.7)	19(11.7)	25(15.4)	
	Strongly Disagree.	0(00	4(2.5)	4(2.5)	
	Prefer not to say	1(0.6)	12(7.4)	13(8)	

Table 47 Distribution of percentages and frequencies of students' survey in questions 25,26,27, and 28.

The following table shows the most common practices among students that may lead to technical risks and cause data breach incidents, as perceived by the students themselves (Q29).

118 (72%) of the students identified ‘clicking on unknown links’ as the most common practice, followed by ‘opening anonymous emails’ (105, 64%). This was followed by ‘choosing simple or outdated passwords’ and ‘sharing them with others’ (82, 50%).

Next, ‘browsing malicious websites within the university’s internal system’ was noted by 59 (36%), followed by ‘sharing the use of computers among students’ (58, 34.4%). ‘Using private computers for study purposes’ and ‘accessing university systems through them’ were identified by 35 (21.3%), while 17 (10.4%) preferred not to respond, and 3 (1.8%) mentioned other practices.

The results also indicated a relationship between the university and the sample response regarding ‘opening anonymous emails’ and ‘sharing the use of computers among students,’ where the p-value < 0.05. However, no relationship was found between the university and the sample response regarding the other practices, where the p-value > 0.05.

Variable name		**King Saud University (%)**	**Taibah university (%)**	**Total (%)**	**P-value**
Q29:The most common practices among students that may lead to technical risks, which may cause data breach incidents	Opening anonymous emails	35(21.3)	70(42.7)	105(64)	0.662
	Clicking up unknown links	30(18.3)	88(53.7)	118(72)	
	Choosing simple or not updated passwords and sharing them with others.	25(15.2)	57(34.8)	82(50)	
	Sharing the use of computers among students	24(14.6)	34(20.7)	58(34.4)	
	Using private computers for study purposes, and accessing university systems through them	12(7.3)	23(14)	35(21.3)	
	Browsing malicious websites within the internal system of university networks.	19(11.6)	40(24.4)	59(36)	
	Prefer not to say	0(0)	17(10.4)	17(10.4)	
	Others	0(0)	3(1.8)	3(1.8)	

Table 48 Distribution of percentages and frequencies of students’ survey in question 29.

The percentages in Table 48 reflect responses from participants who identified common practices that may lead to technical risks and data breach incidents. As participants were allowed to select multiple practices, the percentages naturally exceed 100%. This approach provides a comprehensive view of the frequency and prevalence of each practice among the participants. By allowing multiple responses, the table captures the multifaceted nature of behaviours contributing to data breach risks, which aligns with the study's objective to identify overlapping vulnerabilities in student practices.

Moreover, students were asked to describe the technical implications of data breaches in Question 30. A total of 43 responses were received, with 19 students explaining their inability to describe the technical impacts. Other responses mentioned these effects, including system downtime, data loss, viruses, and slow networks.

5-2-5 Students' Organisational Indicators of Data Breaches

Several questions in the student survey were categorised under the organisational axis, including questions 16, 17, 18, 19, 20, and 21.

For question 16, which examined students' awareness of how their personal data is collected and processed by their universities, Table 16 shows that 61 (31.8%) of the participants responded 'no', while 44 (22.7%) indicated that they 'don't know'. Meanwhile, 51 (26.7%) stated that they had partial knowledge of the process, whereas 28 (14.8%) claimed to be fully aware. Additionally, 8 (4.0%) preferred not to disclose their level of awareness.

Regarding question 17, which assessed students' familiarity with the data security policies implemented by their universities, responses revealed that 85 (44.5%) of students answered 'no', indicating a lack of awareness, while 32 (16.5%) expressed uncertainty. On the other hand, 25 (13.2%) of students reported being fully aware of these policies, while 36 (18.7%) had partial awareness. Additionally, 14 (7.1%) opted not to answer.

Question 18 aims to explore the students' awareness of making a data security complaint, 59(30.9%) of students had answered 'no', 21 (11%) answered 'do not know' how to make a complaint if they doubted that the personal data were leaked or disclosed to unauthorised individuals However, 47 (24.6%) were fully

aware, 42 (22%) were partly aware how to complain, and 22(11.5%) preferred not to say. Of interest here is the increase in the number of students who had not received data security training since they joined their universities approximately 117(61.3%), However, 15 (7.9%) of students had received training, 22 (11.5 %) had partly received training, 11(5.8%) answered 'don't know', and 26(13.5%) of them preferred not to say, which was the finding from in question 19.

It is important to note that in Questions 16, 17, 18, and 19, ‘No’ signifies a definite lack of knowledge, indicating that the student is certain they do not know the answer (‘I am sure I don't know’). In contrast, ‘I don’t know’ represents uncertainty, suggesting that the student is unsure whether they possess the knowledge (‘I am not sure if I know’). Meanwhile, ‘Yes, definitely’ indicates a high level of confidence and full awareness of the subject, while ‘Yes, to some extent or partly’ suggests partial knowledge, meaning the student is aware of some aspects but does not fully understand the topic in detail. (See the frequencies and percentage of students answering questions 16, 17, 18, and 19 in Table 49).

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q16: Do you know how your personal data is collected and processed by the university?	Yes, definitely	6(3.4)	20(11.4)	26(14.8)	0.818
	Yes, to some extent or partly	10(5.6)	37(21.1)	47(26.7)	
	No	15(8.6)	41(23.3)	56(31.8)	
	Don't know	9(5.1)	31(17.6)	40(22.7)	
	Prefer not to say	0	7(4.0)	7(4.0)	
Q17: Do you know the data security policies adopted by your university regarding data breaches?	Yes, definitely	6(3.3)	18(9.9)	24(13.2)	0.423
	Yes, to some extent or partly	8(4.4)	26(14.3)	34(18.7)	
	No	2(11)	61(33.5)	81(44.5)	
	Don't know	6(3.3)	24(13.2)	30(16.5)	
	Prefer not to say	2(1)	11(6.1)	13(7.1)	
Q18: Do you know how you can make a complaint if your personal data has been leaked or disclosed to unauthorised individuals by the university?	Yes, definitely	10(5.2)	37(19.4)	47(24.6)	0.346
	Yes, to some extent or partly	8(4.2)	34(17.8)	42(22)	
	No	16(8.4)	43(22.5)	59(30.9)	
	Don't know	7(3.7)	14(7.3)	21(11)	
	Prefer not to say	1(0.6)	21(10.9)	22(11.5)	
Q19: Have you received data security training since you joined the university?	Yes, definitely	5(2.6)	10(5.2)	15(7.9)	0.421
	Yes, to some extent or partly	6(3.1)	16(8.4)	22(11.5)	
	No	28(14.7)	89(46.6)	117(61.3)	
	Don't know	1(0.5)	10(5.2)	11(5.8)	
	Prefer not to say	2(1)	24(12.5)	26(13.5)	

Table 49 Distribution of percentages and frequencies from students' survey for questions 16,17,18, and 19.

.

The table shows the types of training received by students who reported being trained. According to Question 20, 33 (28.9%) of students received web-based training, followed by 23 (20.2%) who received mandatory formal training, 21 (18.4%) who received personal training, and 19 (16.7%) who received informal training.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q20: In case you received training on data security from your university, select the type of training.	Mandatory formal training .	4(3.5)	19(16.7)	23(20.2)	0.128
	Informal training .	5(4.4)	14(12.3)	19(16.7)	
	Web-based training .	9(7.9)	24(21.1)	33(28.9)	
	Personal training .	2(1.8)	19(16.7)	21(18.4)	
	Prefer not to say .	8(7)	28(24.6)	36(31.6)	

Table 50 Distribution of percentages and frequencies from students' survey for question 20.

The last question in the organisational axis focused on a statement given to students (Q21): 'I think that the data and information security awareness programmes provided by my university are sufficient.' This question aimed to explore their satisfaction with such programmes.

24.1% of the students neither agreed nor disagreed with the statement, while 22.5% disagreed and 9.4% strongly disagreed. In contrast, 16.8% of students agreed and 8.9% strongly agreed.

Sex and gender correlations with the axis.

It was found that there were no statistically significant differences between the gender and age variables and Questions 16, 17, 18, 19, and 20, where the p-value was greater than 0.05. However, the results showed that males responded more than females to Question 20, particularly in the areas of formal, informal, and web-based training.

This result may be influenced by a variety of factors, including cultural and social influences related to gender roles. Males were found to be more likely to engage with these types of training, which could be attributed to societal expectations that encourage males to develop technical skills and pursue fields

traditionally dominated by males, such as IT and engineering (Venkatesh et al., 2003). These gendered expectations can shape participation in training programs and the development of skills typically associated with male-dominated fields.

However, the relationship between gender and engagement in training is complex and may also be affected by other contextual factors, such as individual interest, access to training opportunities, and educational background, which could influence engagement levels in different types of training.

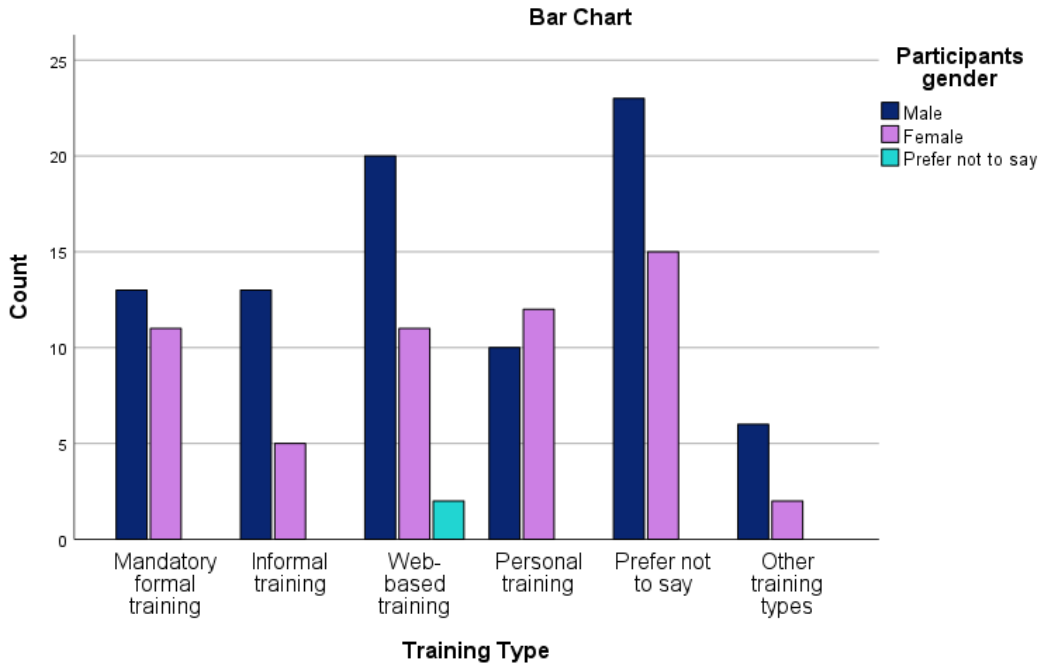

Figure 10 The correlation between question 20, the students' training types and the gender variable.

5-2-6 Students' Emotional Indicators of Data Breaches

This section provides insights into students' emotional responses. Questions 31, 32, 33, 34, 35, 36, 37, and 38 fall under this category. Question 31 measured students' fears regarding the potential leakage of their personal data to unauthorised individuals, which could expose them to fraud, extortion, or other harmful consequences. The findings indicate that 37.5% of students were strongly afraid, while 30.6% expressed fear. Additionally, 18.1% remained neutral. In contrast, 8.2% reported not being afraid, while 0.7% were strongly unafraid. Furthermore, 4.9% preferred not to express their emotions.

Question 32 explored students' privacy concerns regarding the data they provided to their universities. The results show that 29.4% of students were neutral about the statement, while 28.8% indicated that they had no privacy concerns, and 19.7% expressed strong confidence in their data security. Conversely, 11.0% had some concerns, and 6.8% had strong concerns. Additionally, 4.3% preferred not to disclose their feelings. Question 33 examined whether students perceived emotional responses such as anger, fear, and anxiety as negative consequences of data breaches. The responses revealed that 29.5% of students neither agreed nor disagreed, while 28.9% and 27.0% agreed and strongly agreed, respectively. Meanwhile, 6.7% and 2.5% disagreed and strongly disagreed, respectively, while 5.5% chose not to express their views. Question 34 assessed students' feelings regarding provocation in academia and its potential link to intentional or unintentional data leakage. The findings indicate that 28.7% and 28.1% of students agreed and strongly agreed with the statement, respectively. Meanwhile, 25.0% remained neutral. However, 12.5% disagreed, 1.2% strongly disagreed, and 4.4% preferred not to respond. For more details on the responses by the university, refer to Table 51, which presents the frequencies and percentages for each institution regarding questions 31, 32, 33, and 34.

Variable name		KSU (%)	TaibahU (%)	Total (%)	P-value
Q31: To what extent do you agree with the following statements 'I am afraid that my personal data may be leaked to unauthorised persons, which may expose me to fraud, extortion, or anything that offends me as a result of that leak'.	Strongly Agree	21(14.6)	52(36.2)	73(37.5)	0.006
	Agree.	16(11.2)	28(19.5)	44(30.6)	
	Neither Agree or Disagree	1(0.7)	25(17.4)	26(18.1)	
	Disagree	2(1.3)	10(6.9)	12(8.2)	
	Strongly Disagree.	0(0)	1(0.7)	1(0.7)	
	Prefer not to say	0(0)	7(4.9)	7(4.9)	
Q32: To what extent do you agree with the following statements 'I have no concerns about the privacy of my data and personal information that I have provided to my university'.	Strongly Agree	7(4.3)	25(15.3)	32(19.7)	0.181
	Agree.	13(8.0)	34(20.8)	47(28.8)	
	Neither Agree or Disagree	10(6.1)	38(23.3)	48(29.4)	
	Disagree	7(4.3)	11(6.8)	18(11)	
	Strongly Disagree.	3(1.9)	8(4.9)	11(6.8)	
	Prefer not to say	0(0)	7(4.3)	7(4.3)	
Q33: To what extent do you agree with the following statements 'I think the emotional responses (reactions) of individuals such as anger, fear, anxiety...etc., represent negative consequences of data breaches, which should be considered'.	Strongly Agree	16(9.9)	28(17.3)	44(27)	0.012
	Agree.	13(8.0)	34(20.9)	47(28.9)	
	Neither Agree or Disagree	9(5.5)	39(23.9)	48(29.5)	
	Disagree	1(0.6)	10(6.1)	11(6.7)	
	Strongly Disagree.	1(0.6)	3(1.9)	4(2.5)	
	Prefer not to say	0(0)	9(5.5)	9(5.5)	
Q34: I agree with this statement 'Too much provocation in the academia increases student anger and may result in intentional or unintentional data leakage	Strongly Agree	15(9.4)	30(18.7)	45(28.1)	0.069
	Agree.	11(6.9)	35(21.8)	46(28.7)	
	Neither Agree or Disagree	11(6.9)	29(18.1)	40(25)	
	Disagree	3(1.9)	17(10.6)	20(12.5)	
	Strongly Disagree.	0(0)	2(1.2)	2(1.2)	
	Prefer not to say	1(0.6)	6(3.7)	7(4.4)	

Table 51 Distribution of percentages and frequencies from students' survey for questions 31, 32, 33, and 34.

Question 35 explored the feeling of shock by examining whether individuals with sufficient security awareness would not be surprised by a data breach incident. The findings indicate that 25.8% of students agreed with this view, while 23.9% strongly agreed. Additionally, 28.8% remained neutral. In contrast, 12.9% disagreed, 4.3% strongly disagreed, and 4.3% chose not to express their opinion.

To evaluate students' confidence and comfort in their universities, question 36 assessed their experiences with disclosing personal data due to trust concerns. The results show that 37.2% of participants neither agreed nor disagreed, while 24.8% agreed and 18.6% strongly agreed. Conversely, 11.7% disagreed, 2.7% strongly disagreed, and 5.0% preferred not to respond.

Question 37 examined frustration and its potential impact on data security, investigating whether frustrated students could pose a threat by engaging in malicious activities. The findings reveal that 33.1% of students took a neutral stance, while 25.8% agreed and 17.2% strongly agreed. On the other hand, 15.9% disagreed, 2.5% strongly disagreed, and 5.5% opted not to share their opinion.

Regarding question 38, which explored students' curiosity about data breaches, the results show that 32.3% of participants neither agreed nor disagreed with tracking rumours about universities facing data security issues. Meanwhile, 17.7% agreed, and 12.8% strongly agreed. In contrast, 25.1% disagreed, 6.6% strongly disagreed, and 5.5% preferred not to answer.

For a detailed breakdown of responses by university, refer to Table 52, which presents the frequencies and percentages for each institution in relation to questions 35, 36, 37, and 38.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q35: I agree with this statement 'People who have enough security awareness would not be shocked if s/he experiences a data breach event'.	Strongly Agree	9(5.5)	30(18.4)	39(23.9)	0.389
	Agree.	10(6.1)	32(19.7)	42(25.8)	
	Neither Agree or Disagree	11(6.8)	36(22.0)	47(28.8)	
	Disagree	6(3.6)	15(9.3)	21(12.9)	
	Strongly Disagree.	3(1.9)	4(2.5)	7(4.3)	
	Prefer not to say	1(0.6)	6(3.6)	7(4.3)	
Q36: To what extent do you agree with this statement 'It is usually an unpleasant experience for me when I have to disclose my personal data to the university due to trust issues'.	Strongly Agree	9(5.6)	21(13)	30(18.6)	0.013
	Agree.	14(8.6)	26(16.1)	40(24.8)	
	Neither Agree or Disagree	7(4.4)	53(32.8)	60(37.2)	
	Disagree	8(5.0)	11(6.9)	19(11.7)	
	Strongly Disagree.	1(1.2)	4(2.5)	5(2.7)	
	Prefer not to say	1(0.6)	7(4.4)	8(5)	
Q37: I support this statement 'a frustrated student presents a potential threat to breach data security by performing malicious acts'.	Strongly Agree	9(5.5)	19(11.6)	28(17.2)	0.142
	Agree.	12(7.4)	30(18.4)	42(25.8)	
	Neither Agree or Disagree	10(6.1)	44(26.9)	54(33.1)	
	Disagree	8(4.9)	18(11.0)	26(15.9)	
	Strongly Disagree.	1(0.6)	3(1.9)	4(2.5)	
	Prefer not to say	0(0)	9(5.5)	9(5.5)	
Q38: To what extent do you agree with the following statement 'I am interested in tracking rumours that some universities are facing data security problems, especially tracking data breach incidents in universities'.	Strongly Agree	9(5.5)	12(7.3)	21(12.8)	0.061
	Agree.	7(4.3)	22(13.4)	29(17.7)	
	Neither Agree or Disagree	10(6.1)	43(26.2)	53(32.3)	
	Disagree	12(7.3)	29(17.7)	41(25.1)	
	Strongly Disagree.	2(1.2)	9(5.5)	11(6.6)	
	Prefer not to say	0(0)	9(5.5)	9(5.5)	

Table 52 Distribution of percentages and frequencies from students' survey for questions 35,36,37, and 38.

Sex and gender correlations with the axis.

The negative correlation between age and gender with Questions 31–38 indicates that there is no significant relationship between these variables and participants' responses to concerns about data breaches, privacy, emotional reactions, and trust issues regarding the disclosure of personal data.

In addition, the results indicate statistical differences between students at KSU and TaibahU in their responses to concerns about data leaks (Q31), emotional reactions to data breaches (Q33), and trust issues when disclosing personal data (Q36). These significant differences (with p-values less than 0.05) suggest that students at each university perceive and react to data security and privacy issues in distinct ways. These differences might reflect various factors, such as university-specific cultures, attitudes toward data privacy, or differences in training and awareness related to cybersecurity practices. For instance, students from one university might express greater concern or fear about their personal data being leaked, while students from the other university may be more confident about their data security.

However, the responses to Q32, Q34, Q35, Q37, and Q38, which have p-values greater than 0.05, do not exhibit statistically significant differences between students from KSU and TaibahU. This means that, for these particular questions, the university attended does not appear to have a significant impact on how students view or respond to data privacy concerns. Students at both universities likely share similar views or behaviours when it comes to these aspects.

5-2-7 Students' Needs and Wishes for Data Protection

It was necessary to investigate students' needs and wishes regarding the security and protection of their data. Figure 8 presents the statistics from Question 40, which identified students' needs from their universities for the development of personal data security measures.

94 (57.7%) of the participants found that organisational procedures were the most important aspect for improving the protection of personal data for the university to adopt. This was followed by technical protection tools (88, 54%) and personal aspects (51, 31.0%). Meanwhile, 26 (15.3%) of the participants

preferred not to respond, and 7 (4.3%) found that other aspects were important, such as developing ethical aspects (e.g., ensuring integrity and honesty).

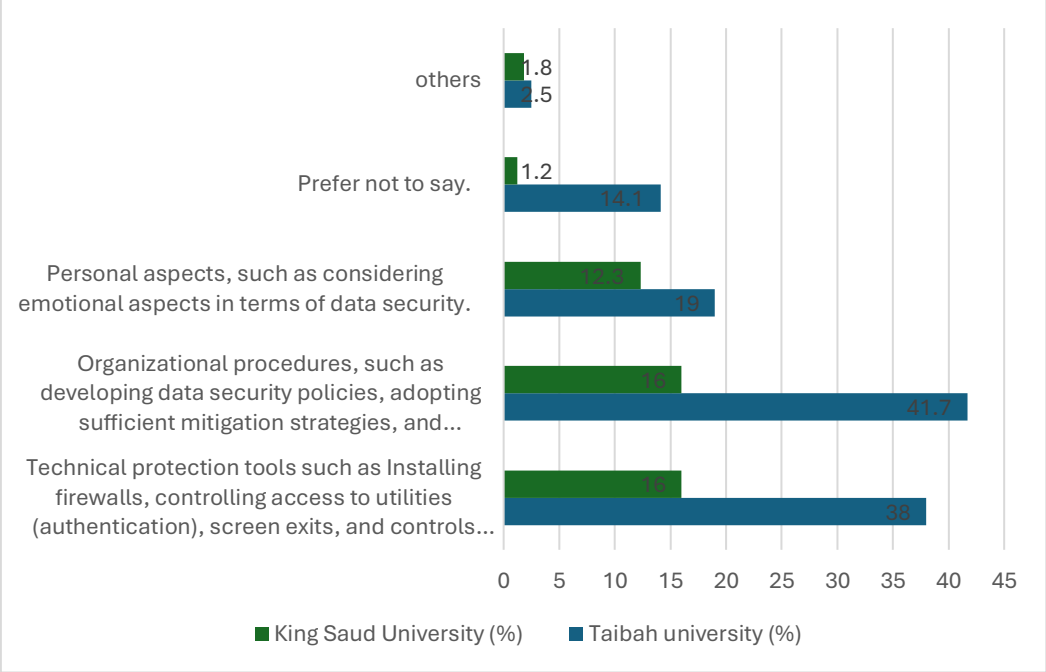

Figure 11 Sample response about the important aspects of developing data security.

According to the data from Question 39, students found that the most harmful aspect of data breaches was the technical part, followed by the organisational part (83 (52.2%)), and then the personal part (75 (47.2%)).

Question 41 was qualitatively designed to capture unlimited data on the changes that students want to improve the management of personal data. Fifty-seven responses were recorded. Students' responses focused on increasing awareness, such as adopting training programmes and holding workshops/conferences/exhibitions that engage students. One student stated, 'I would like to attend a course that will explain to me how to protect my data and my university data… I would also like to know which affordable anti-virus programmes to use.'

However, some other students' responses mentioned other changes, such as improving university security policies and systems and minimising personal data.

Additionally, data from Question 24 confirmed students' desire for the minimisation of personal data. Sixty-two participants (32.5%) think that personal data and information collected by the university should be reduced to some extent or partly, while 54 (28.3%) believe the university should definitely reduce the personal data collected on students. In contrast, 30 (15.7%) of them think that personal data and information collected by the university should not be reduced, while 12 (6.2%) were unsure whether they want the university to reduce the collection of personal data and information. Only 7 students (3.7%) preferred not to respond.

5-2-8 Students' Perceptions about Mitigating Data Breaches Impact

Two questions were addressed (Q22, Q23) in this section to understand students' perceptions of reducing the risk of data breaches or mitigating the consequences of data leaks.

Students were asked about the appropriateness of university strategies to mitigate the effects of data breaches in Q22. The findings indicate that 57 (33.8%) of the students were unsure whether the strategies used to mitigate the impact of data breaches were appropriate. Meanwhile, 41 (24.0%) and 27 (15.8%) of them found the strategies appropriate to some extent or definitely appropriate, respectively. However, 29 (17.0%) believed that the mitigation strategies were not appropriate, while 16 (9.4%) preferred not to say.

Students revered in Q23 which best way that they preferred to treat them for mitigating the impacts of breaches. 131(79.4%) students stated that compensation was the best way to deal with them to mitigate the beach's effects, followed by apology 75(45.5%), while 15(9.1%) of students preferred not to say.

It is important to note that in Q23, the total percentages exceed 100%. This is because the question allowed respondents to select more than one answer. As a result, the combined total of the percentages exceeds 100%.

Variable name		King Saud University (%)	Taibah University (%)	Total (%)	P-value
Q22: Do you think strategies to mitigate the impact of data breaches at the university are appropriate?	Yes, definitely	9(5.3)	18(10.5)	27(15.8)	0.239
	Yes, to some extent or partly	8(4.7)	33(19.3)	41(24.0)	
	No	7(4.1)	22(12.9)	29(17.0)	
	Don't know	16(9.4)	42(24.4)	58(33.8)	
	Prefer not to say	2(1.2)	14(8.2)	16(9.4)	
Q23: How would you prefer your university to treat you in case you are exposed to a data breach to mitigate the breach's effects?	Apology	27(16.4)	48(29.1)	75(45.5)	0.096
	Compensation.	35(21.2)	96(58.2)	131(79.4)	
	Prefer not to say	1(0.6)	14(8.5)	15(9.1)	

Table 53 Distribution of percentages and frequencies from students' survey for questions 22, and 23.

The analysis of the responses to Q22 and Q23 revealed that there are no statistically significant differences between the universities. For Q22, which asked whether students thought the strategies to mitigate the impact of data breaches were appropriate, the p-value was 0.239, which is greater than 0.05, indicating that the differences in responses between the two universities are not statistically significant. Similarly, for Q23, which asked students how they would prefer to be treated in case of a data breach, the p-value was 0.096, also greater than 0.05, suggesting that there are no significant differences between the universities in their preferences for mitigating the effects of a breach. Therefore, the results indicate that students at both universities share similar views on these issues.

Sex and gender correlations with the axis.

No statistical relationship was found between the variables of gender and age and the two questions related to mitigation strategies (Q22 and Q23). However, it was noted that students, whether male or female and of all ages, preferred the 'compensation' strategy to mitigate the effects of data breaches.

5-3 Survey Perspectives: A Comparative Lens and Discussion

The responses to the two questionnaires were diverse, including multiple age groups and various academic disciplines at the two universities. The male gender was predominant in the students' questionnaire, while the dominance of women was seen in the faculty members' questionnaire. The results reflected high support for the definition of data violation codified by the Personal Data Protection Regulation in the United Kingdom, with about 87.4% of the participants, 89.3% of faculty members, and students agreeing.

The results were quite positive in terms of incidents of data breaches, as a large number of data breaches were not detected in the Saudi environment, based on the opinions of the participants. A majority of students (89.8%) did not experience an incident of their personal data being violated within the framework of the university, and 71.7% outside the university. On the contrary, most of the faculty members (98.6%) preferred not to answer regarding exposure to a breach within the university context, which may be attributed to their loyalty toward the university. Meanwhile, 48.6% of staff denied exposure to a data breach outside the university context. Few students and faculty members consequently fully or partially managed a data breach (9.8% for students and 5.7% for staff).

In both surveys, participants affected by the data breach scored higher on both feelings of anger and anxiety. However, the statistical tests show special correlations between the female participants and feelings of fear as well as the male participants and feelings of anger. Further, the analysis revealed a decrease in the level of trust among those affected in the university after being exposed to a data breach.

In terms of organisational aspects, nearly half of the student participants stated they did not know how the university collected and processed their data, and more than a quarter of the employees also agreed with the same opinion. More than half of the participants, whether students or faculty members, did not know the data security policies used in their universities, but they did know how to report a security complaint. Also, 61.3% of the students, and 67.1% of the employees, did not receive security training.

Both students and employees require awareness programmes for data security, as 31.9% of the students and 37.1% of the employees believe that the university's programmes are insufficient. Opinions differed on whether the mitigation strategies used by the universities included in the study were appropriate, but they all agreed that ‘compensation’ is very appropriate to mitigate the effects of data breaches, with a percentage ranging from 79.4% of the students to 48.4% of the faculty members participating in the survey.

Surprisingly, a majority of respondents, both students and faculty, knew how to file a complaint. Although a significant number of participants did not receive training, they knew how to report a breach. This is a strong point in favour of universities, especially in the context of the major transformations they are undertaking in terms of data protection.

However, it is possible that universities collect a lot of personal data, as the results showed the aspirations of the participants regarding minimising their personal data (60.8% of students and 65.7% of faculty members). This may be due to a lack of education and clarity as to why the data is needed or a need to better reflect on what is collected.

Regarding the technical aspect, 52.9% of the students and 47.1% of the employees agreed that data breaches are mainly caused by technical failings, while 45.6% of the employees and 37.2% of the students believe that human errors are the main cause. Likewise, opening anonymous emails and clicking on unknown links were identified as common practices from the perspectives of both students and employees.

The next section of the survey focused on the investigation of emotional aspects. The analysis revealed participants' negative concerns and feelings regarding the security of their personal data, such as fear of data leakage (77.1% for employees, 51.2% for students), and privacy concerns (48.5% for both employees and students). Nearly half of the employee participants and a quarter of the students consider anger, fear, and anxiety as negative consequences of data breaches. Furthermore, half of the respondents believe that an employee's anger may represent a vulnerability that threatens the data security system.

Opinions differed as to whether people with high awareness are not shocked when exposed to a data breach incident, with differing views in both surveys. The analysis also revealed a significant result for the university: both faculty members (52.8%) and students (36.7%) believe that a frustrated individual may represent a vulnerability that threatens cybersecurity in the university. Internal actors within an organisation clearly have the potential to breach systems.

In the final part of the survey, respondents were asked what aspects they would like to improve in terms of managing the security of their data. Respondents in both surveys mentioned the need to develop the organisational aspects of data security management. This is a natural result, given that the organisational side recorded negative trends, such as the lack of awareness among university stakeholders of how their data is processed, and the failure to receive the necessary training.

In conclusion, the study found no statistically significant differences between the two universities overall. Most student responses at KSU and TaibahU were closely aligned, with twenty-five questions showing substantial statistical agreement. However, differences were noted in six questions: 8, 9, 31, 33, 36, and 40, which may reflect unique institutional experiences or specific concerns at each university. Similarly, while no significant differences emerged in twenty-seven employee survey questions, four questions—9, 16, 26, and 27—did show variation, suggesting different perspectives or responses to these issues. Despite these differences, the overall trend indicates a high level of similarity between the two universities' responses.

A point of particular note was the number of participants who skipped or omitted answers to questions relating to directly criticising the universities. This evidences that it was correct to make these questions optional and that it was valuable to have this covered for these two sets of stakeholder participants through the survey approach. This gave people the opportunity to answer anonymously if they so chose. It removed any expectations or pressures to respond. Students might have felt more pressured to answer had they been interviewed by the researcher, who might have been deemed to be in a position of power. Conversely, managers who were interviewed were potentially

expected to be able to better answer this and to be less threatened by the position of the researcher. These considerations and reflections on the data collection instruments and their appropriateness are important findings within the delivery of this research into a sensitive area, which others may build upon.

The next chapter pulls together the findings from the quantitative and qualitative data, drawing in the perspectives from the three stakeholder data sets. It further considers the findings in the context of the broader literature review.

Chapter 6: Results Integration and Discussion

Introduction

In this chapter, research results were outlined and compared to understand the intricate landscape of data breaches in Saudi Arabian universities, aiming to uncover the multidimensional impacts, challenges, and needs for safeguarding data integrity within these two esteemed and established universities. The focus was on presenting and interconnecting fundamental quantitative statistics with pertinent qualitative information directly correlated with the research questions while drawing in differing stakeholder perspectives. This chapter sets out these overarching research results, shedding light on the multidimensional impacts of data breaches, the diverse awareness levels among stakeholders regarding their personal data security, and the challenges and needs for protecting personal data that bridge the knowledge gap. By exploring these dimensions, I sought to advance the understanding of the evolving landscape of data breaches in Saudi Arabian universities and contribute to the development of information security strategies and policies within this important sector — and potentially beyond

6-1 Convergent Mixed Methods Design

The application of a convergent mixed methods design in this study offered a range of significant benefits. Firstly, it provided a more comprehensive and holistic understanding of the research questions by combining the strengths of both quantitative and qualitative data collection and analysis methods (Brannen, 2016). This design facilitated the integration of diverse data types, enabling the researcher to address complex, multi-dimensional phenomena and examine the issue from multiple perspectives. The flexibility of a convergent design allowed the researcher to tailor data collection methods to suit the needs of different stakeholder groups. For instance, engaging students through surveys was deemed more appropriate than conducting direct interviews, particularly given the sensitive nature of the research topic. This approach ensured access to different stakeholders while respecting institutional power dynamics.

Moreover, the integration of quantitative and qualitative data promoted methodological rigour by balancing the weaknesses and biases of each method, thereby mitigating their limitations (Creswell & Creswell, 2018). By merging datasets, the researcher could assess the extent of convergence or divergence between various facets of the issue under investigation. Ultimately, this design enhanced the validity, reliability, and richness of the research outcomes, contributing to a nuanced and comprehensive understanding of the researched phenomenon.

Triangulation and Its Application to the Study

Triangulation is a methodological approach used to enhance the credibility and validity of research findings by integrating multiple data sources, methods, or perspectives (Cohen et al., 2002). It minimises biases and fosters a more comprehensive understanding of the phenomenon under investigation. There are four primary types of triangulation: data triangulation, investigator triangulation, theoretical triangulation, and methodological triangulation (Denzin, 2017). In this study, a triangulation strategy was employed to comprehensively explore the ramifications of data breaches within higher education (HE) institutions in Saudi Arabia. Specifically, methodological triangulation was utilised by integrating quantitative data from surveys with qualitative insights from semi-structured interviews. The quantitative and qualitative datasets were initially analysed separately to maintain their integrity, before being combined in the final phase to enable triangulation and ensure a holistic understanding of the research problem.

A side-by-side comparison of the datasets was conducted to identify areas of convergence, divergence, and complementarity (Creswell &Plano Clark, 2006). Quantitative data provided measurable insights into risk perceptions, such as technical failures and weak practices, while qualitative data contextualised these findings, shedding light on underlying factors like organisational gaps and technical skill deficiencies. For instance, participants in interviews emphasised issues such as hardware failures or inadequate system updates as contributors to data breaches. By employing triangulation, the study reduced single-method bias and enhanced the validity and depth of its findings. This systematic

approach aligned with the study's objective to examine data management practices and explore the broader implications of data breaches within HE institutions in Saudi Arabia.

6-2 Mix Results and Findings

This research undertakes five questions to provide a deep lens of data protection in HEIs in Saudi Arabia.

6-2-1 Q1: What are the causes of the data protection breach in SA HEIs?

The researcher investigated this question through the formulation of distinct thematic categories, namely data breach experiences, and data breach risks.

6-2-1-1 Data Breach Experience

Regarding experiences of data breaches, managers in both universities did not report incidents of data breaches but reported some attempts that had been successfully prevented and thwarted. Various forms of security breach attempts were documented within the contexts of the two universities. At TaibahU, instances of compromise included email phishing and external attacks. Conversely, KSU reported intrusions in the form of command and control (C&C) attacks, malware, and Denial-of-Service (DDoS) attacks. The analyses conducted in the study did not definitively identify any overt reference to a breach incident resulting in substantial damage. Instead, the managers acknowledged the occurrence of attempted breaches or vulnerabilities, asserting that these issues were actively being mitigated and resolved. The KSU manager mentioned that ***'We are constantly exposed to attempts to hack into our data systems***', while the TaibahU manager indicated that' ***We have security attempts to penetrate that are monitored, and we have vulnerabilities that are closed'***.

When faculty members were asked about their experience with data breach incidents within the university setting in the survey, 98.6% of them (100% of KSU staff & 96.6 of TaibahU staff) preferred not to answer. It would have been possible for them to indicate if they had not experienced any breaches. However, the choice not to respond stood out as unexpected, implying a

potential hesitancy or reluctance among faculty members to divulge their experiences of data breaches in the university context. Notably, 88% of students (71.4 KSU students & 92.6 TaibahU students) responded that they had not personally experienced any data breach incidents within their respective universities. This aligned with the information provided by managers, providing a degree of consistency and confirmation regarding the prevalence of data breach incidents as perceived by these two groups. A similar pattern of results was obtained in Al-Sulaimi's (2022) study regarding experiences of breaches.

Faculty members who had encountered data breaches were tasked with identifying the type of breach by selecting from a drop-down list provided in the survey, comprising eight pre-approved breach types recognised by experts and pertinent to the academic community (Collins et al., 2011; Hammouchi et al.,2019). The highest number of votes in both universities was attributed to the category labelled ‘unknown’.

However, discernible variations were observed in the responses from KSU, where ‘payment card fraud’ secured the second-highest number of votes. The third place was shared equally between ‘hacking or malware’ and ‘data stolen’. Conversely, the least reported breach types at KSU included ‘insider attack’, ‘physical loss of data’, and ‘unintended disclosure’. In contrast, at TaibahU, the second-highest votes were allocated to both ‘unintended disclosure’ and ‘hacking or malware’. The third-place positions were evenly distributed among ‘payment card fraud’, ‘insider attack’, ‘physical loss of data’, ‘data stolen’, and ‘device loss’, with equal percentages.

In addition, a limited number of students reported instances of data breaches, providing details regarding the type of breach they experienced. Consistent with the responses from employees, these affected students concurred in designating the category 'unknown' as the predominant choice, indicating the highest percentage for the type of breach. This agreement among affected students and employees in selecting a breach type of 'unknown' could be attributed to the affected individuals' challenges in proficiently identifying the breach or the delay in promptly notifying the occurrence of the breach. These factors hinder the university's investigative procedures. Moreover, differences

in percentage distributions emerged when comparing the types of data breaches experienced by students in the two universities. At KSU, the combined categories of unintended disclosure and hacking or malware secured the second-place position, while payment card fraud, data theft, and loss of devices jointly occupied the third-place position. Conversely, at TaibahU, data stolen claimed the second-highest rank, followed by unintended disclosure and hacking or malware. Equal percentages were observed for payment card fraud and device loss, succeeded by insider attacks and physical data loss. Table 54 illustrates a comprehensive synthesis of both qualitative and quantitative data on this theme.

Data Breach Experiences		KSU	TaibahU
Managers' Perspective	A breach experience was notified	Attempts were deterred	Attempts were deterred
	A breach type was reported	C&C attacks	Email phishing
		Malware	External attacks
		DDoS attacks.	
Employees' Perspective	A breach experience was notified	Employees opted not to disclose their experiences of a data breach incident within the university context, with over half of them reporting exposure to incidents outside the university context.	Employees opted not to disclose their experiences of a data breach incident within the university context, and over a quarter of them reported exposure to incidents outside the university context.
	A breach type was reported	Unknown	Unknown
		Payment card fraud	unintended disclosure + hacking or malware'
		Hacking or malware + data stolen.	Payment card fraud+ insider attack+ physical loss of data+ data stolen+ device loss.
		Insider attack + physical loss of data + unintended disclosure.	
Students' Perspective	A breach experience was notified	A small number of students (1.1%) experienced data breaches within the university context, and (5,2%) outside the university.	A small number of students (2.1%) experienced data breaches within the university context, and (14,7%) outside the university.
		Unknown	Unknown
		Unintended disclosure and hacking or malware	Data stolen

	A breach type was reported	Payment card fraud+ data theft+ loss of devices.	Unintended disclosure and hacking or malware
			payment card fraud+ device loss+ insider attack+ physical data loss.

Table 54 Converging qualitative and quantitative findings within the theme of the data breach experience.

6-2-1-2 Data Breach Risks

Within the context of data breach risk assessment and personal data security management, managers, faculty members, and students' perspectives diverged. Interview analysis illuminated some risks, categorising them across three distinct levels: technical, organisational, and personal. A slight convergence and divergence in perspectives emerged among managers at the two universities. Consensus emerged regarding the recognition of non-compliance with security policies as an organisational threat, while human errors in technology usage were identified as a technical threat. KSU managers revealed some organisational risks including a dearth of skilled professionals and budgetary limitations. Conversely, managers at TaibahU highlighted other technical risks, including software and systems updates, external attacks, and budget considerations for licence renewal.

Furthermore, managers at both universities extended their discourse beyond organisational and technical scopes, speaking about personal risks. KSU managers addressed the risk of over-trust and excessive empathy as cultural characteristics in SA, while counterparts at TaibahU referred to personal factors such as exploitation, bullying, defamation, and blackmail. Al-Qahtani (2021) who studied some factors associated with cybercrime in the Saudi context, as perceived by faculty members at Princess Noura University, unveiled a multitude of culturally influential factors. These included limited awareness among internet users concerning their legal obligations and the role of the residential environment in fostering isolation and individuality among family members. However, in line with Al-Qahtani's findings, it can be concluded from

the findings that personal risks such as over-trust and extortion play a major role in Saudi society as data security threats.

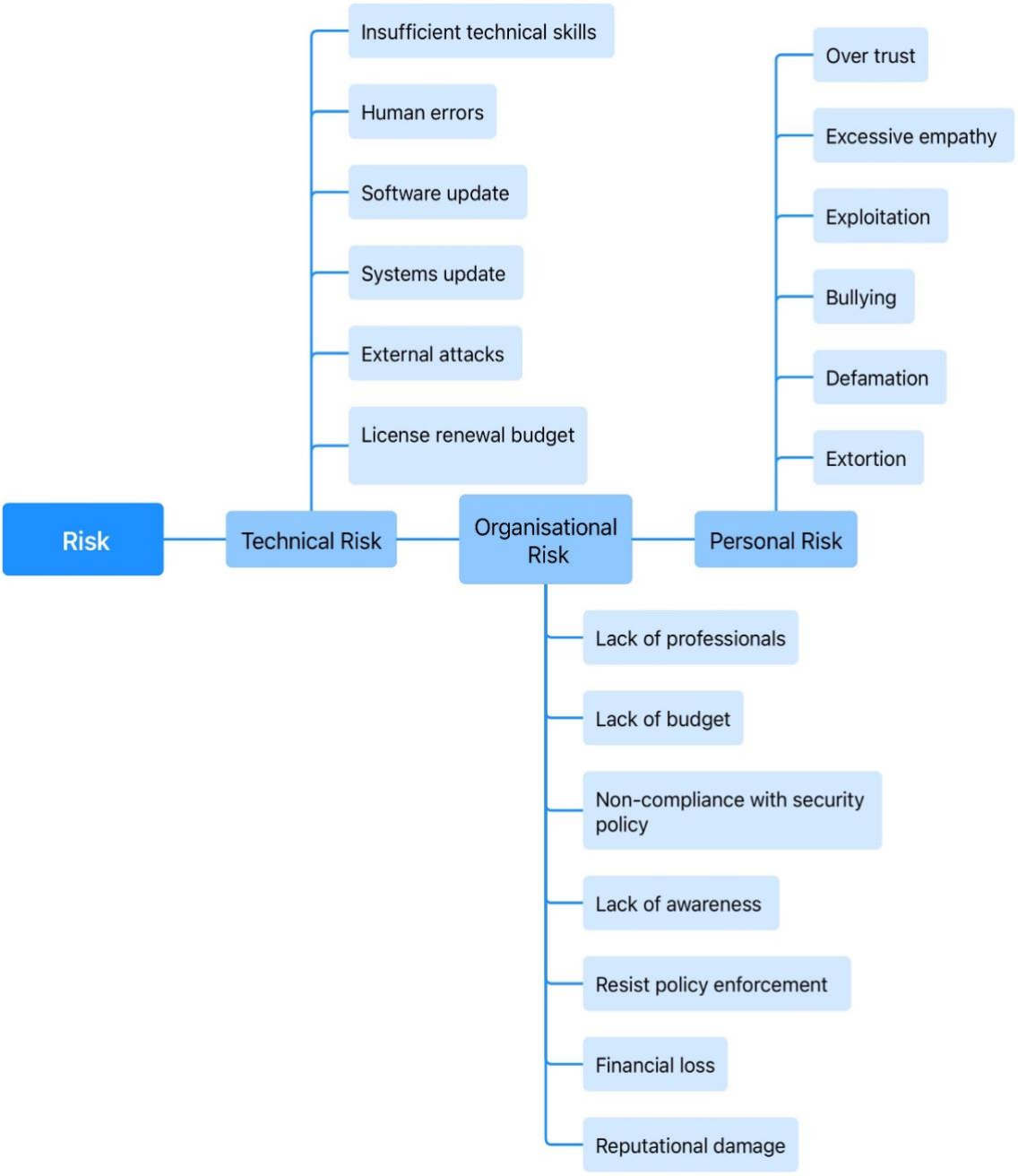

Figure 12 Classification of codes highlighting data breach risks.

Surveys analysis provided insights into specific risk perceptions, with ‘technical failures’ being acknowledged by 47.1% of employees (36.6% KSU’s employees & 62% of TaibahU’s employees- rates were calculated in each university separately) and 52.9% of students, along with ‘weak technical practices’ identified by 45.1% of employees (43.9% KSU’s employees & 48.3% of TaibahU’s employees- rates were calculated separately for each university) and 37.2% of students (10,5% KSU’s students & 26.7% of TaibahU’s students- rates were calculated in total). Notably, faculty members were more inclined to attribute data breaches to technical failures than their own or organisational failings. The imperative to acknowledge and address the risk posed by technical threats whether they are through malfunctions organisational gaps, or individual practices is critical.

Managers recognised this broader significance. A manager at TaibahU stated that ***'Some weak practices may create vulnerabilities'***, and another manager at KSU mentioned that' ***In my opinion, technical risks related to users are caused by a lack of technical skills'***. Meanwhile, another manager added, '***The technical risks are varied, such as hardware failure and problems with system updates from Microsoft'***. This finding aligns with the findings of Al-Sheety (2014); nevertheless, it is essential to note that Al-Sheety's study primarily concentrated on two specific vulnerabilities within the context of King Saud hospitals, namely the sharing of passwords and computers among employees. (See Table 55, which classifies poor practices from both staff and student perspectives).

	Practices	%		Practices	%
Faculty members	Opening anonymous emails	20.8	**Students**	Clicking up unknown links	72
	Clicking up unknown links	20.8		Opening anonymous emails	64
	Choosing simple or not updated passwords and sharing them with others	17		Choosing simple or not updated passwords and sharing them with others	50
	Sharing the use of computers among employees	14.2		Sharing the use of computers among employees	34.4
	Using private computers for work purposes, and accessing university systems through them	10.4		Browsing malicious websites within the internal system of university networks	36
	Browsing malicious websites within the internal system of university networks	13.2		Using private computers for work purposes, and accessing university systems through them	21.3

Table 55 Poor practices from both staff and student perspectives.

Furthermore, the analysis of survey responses highlights frustration as a significant perceived threat to data security. When combining the responses of "strongly agreed" and "agreed," 52.8% of employees and 43% of students identified frustration as a critical risk factor. This finding reinforces the notion that psychological states, particularly frustration, can contribute to vulnerabilities in data protection. Additionally, the interview analysis introduced the concept of 'over-trust' as a unique dimension of personal risk

6-2-2 Q2: How do SA HEIs tackle personal data risks, including personal data policies and processes?

Subsequent to an exploration of the inherent risks in data security management within HEIs, the second research question shifted towards the examination of administrative procedures adopted by universities to govern and manage these risks. The mixed-method research framework employed in this study facilitated the acquisition of data necessary for discerning the potential convergence or divergence among the perspectives of managers, academic faculty, and students. Specifically, managers were asked about their insights into security

procedures, policies, and institutional regulations, while faculty members and students were surveyed to gauge their awareness of these institutional protocols. This methodological approach served the dual purpose of pinpointing areas of congruence among these perspectives and evaluating the effectiveness of existing security policies.

6-2-2-1 Adopting Data Security Policies

Interview analyses affirmed that each university adheres to its unique set of data security policies while concurrently embracing the security standards and guidelines stipulated by the National Cybersecurity Authority (NCA). This aligns with the vision elucidated by SA, which is explicated within a framework of data management and governance overseen by the Data Management Office. This framework grants organisations autonomy in crafting their security policies, with the requirement that such policies conform to the overarching legislative framework of the state. (Refer to Chapter 1 for more information about the framework).

Within the cohort of managers interviewed, KSU managers highlighted security policies related to access, email use, and network access, whereas TaibahU managers emphasised a focus on policies focused on managing identities, access, and powers, and safe use of information assets. The KSU manager described these policies, stating, '***We have multiple straightforward policies***', while the TaibahU manager characterised these policies as '***compatible with the latest developments in the field of cybersecurity'***.

When the interviewed managers were questioned about their comprehension of procedures concerning the implementation of policies relating to data breaches, particularly in terms of responsibilities and accountability, a notable degree of understanding was evident. However, this finding presents a notable deviation from the findings of a prior study conducted by Asel and Al-Aifan (2014), which focused on the state of information security at King Abdulaziz University (KAU), a prominent HE institution in SA. The study by Asel and Al Aifan (2014) unveiled a series of constraints influencing the authority vested in the Deanship of Information Technology, which formulates and oversees

policies related to the imposition of sanctions and the execution of security protocols. The observed disparity between these outcomes perhaps could be attributed to the recent establishment of the personal data and information protection system, which was enacted in 2022 and has advanced the data governance landscape. In contrast, Asel and Al-Aifan's study was published in 2014, thus, this study result reflects the development in aspects of responsibility and accountability related to data breaches and personal data protection in the Kingdom of SA.

6-2-2-2 Awareness of Data Security Policies

A noteworthy convergence emerges when assessing the viewpoints of managers, faculty members, and students concerning the level of awareness regarding security policies. Managers underscored the significant challenge posed by policy compliance and awareness as a high-risk issue.

Survey results reveal that 44.5% of students and 44.3% of faculty members acknowledged a lack of awareness regarding their institutions' data security policies, indicating that nearly half of the university population remains uninformed about the frameworks designed to safeguard sensitive information

This observation aligns with the findings presented by Alghathar and Alsubaih (2012), who underscore the substantial risk linked to non-compliance with information security standards among employees in Saudi organisations. This insight highlights a critical area of concern regarding the potential consequences of inadequate policy understanding and adherence within the educational context. The following table illustrates an increase in percentages in the 'no' box, indicating that participants denied knowledge of the security policies at the two universities, whether students or faculty members.

Variable name		KSU Staff (%)	TaibahU Staff (%)	Total (%)	KSU Student (%)	TaibahU Student (%)	Total (%)
Do you know the data security policies adopted by your university regarding data breaches?	Yes, definitely	2.9	2.9	5.7%	3.3	9.9	13.2
	Yes, to some extent or partly	10	7.1	17.1%	4.4	14.3	18.7
	No	**24.3**	**20**	**44.3%**	**11**	**33.5**	**44.5**
	Don't know	10%	5.7	15.8%	3.3	13.2	16.5
	Prefer not to say	11.4%	5.7	17.1%	1	6.1	7.1

Table 56 Distribution of percentages related to the theme of data security policy awareness.

While managers reported the existence of training and awareness initiatives implemented by their respective universities, a substantial percentage of faculty members (67.2%) and students (61.3%) in both universities stated that they had not received any form of data security training since their employment or enrolment in the university.

This contradiction highlights the need for universities to prioritise training programmes and the dissemination of data security policies. This requirement was recommended by Al-Omran (2011) when he investigated the awareness of information security among faculty members at Majmaah University. Additionally, a significant proportion of both employees (38.6%) and students (31.8%) affirmed their lack of awareness regarding the collection and processing of personal data undertaken by their respective universities.

An essential finding that emerged from the analysis of interview data underscores a notable disparity in perception. Specifically, managers expressed the viewpoint that individuals' skills in data security awareness are insufficient. A manager at KSU stated, ***'Some people don't have sufficient awareness of dealing with technology***', and another manager discussed technical obstacles, ***'such as the employees' lack of awareness of technology'***. At TaibahU, a manager emphasised the need for improvement, stating, ***'Increasing individuals' awareness of data security programmes to reduce weak practices that may create gaps in the university's systems and programmes'***.

Meanwhile, a considerable number of students and employees argued that the data security programmes at their respective universities were inadequate. (See the misleading percentages in red in the table, which indicate participants' dissatisfaction—whether students or faculty members—with the information security awareness programmes at their universities).

Satisfaction with data security awareness programmes		KSU Staff (%)	TaibahU Staff (%)	KSU Student (%)	TaibahU Student (%)
I think that the data and information security awareness programmes provided by my university are sufficient.	Strongly Agree	2.4	0	15	8
	Agree.	12.2	13.8	12.5	19.7
	Neither Agree or Disagree	31.7	31	30	24.8
	Disagree	**22.0**	**34.5**	**30**	**24.1**
	Strongly Disagree.	12.2	6.9	5	12.4
	Prefer not to say	19.5	13.8	7.5	10.9

Table 57 Distribution of percentages related to the theme of satisfaction with data security awareness programmes.

It is worth noting that the universities under investigation do offer information security awareness programmes, with a quarter of the participants, including both students and employees who have undergone training, acknowledging the receipt of formal training. Consequently, the findings underscore the imperative for managers to enhance their training projects and develop models for augmenting data security awareness, in alignment with the recommendations outlined in Alsahafiy (2019) and Al-Sadhan (2020) research.

In terms of the appropriateness of technical resources, managers conveyed their satisfaction with the Information Technology (IT) infrastructure within their respective universities, which includes anti-virus protection programmes, firewalls, intrusion detection and prevention systems, and robust information systems. This result contradicts Alshanbari (1998), who indicated that there was a lack of information systems infrastructure in Saudi HE, suggesting that IT infrastructure has since been developed.

Similarly, survey analysis also revealed a consensus in the perceptions of employees and students, with a mean agreement score of 27.1 for employees and 36.1 for students, affirming the suitability of the technical tools employed

within their universities. This finding may imply a comparative strength in the technical dimension, as opposed to the organisational or administrative dimension.

Furthermore, incidents of data breaches are documented through the dedicated E-platform ‘Haseen’, which, during interviews conducted by the researcher, exhibited a recurring pattern in the nomenclature of security programmes and platforms within the Saudi context. It became evident that security platforms and initiatives in this context bear unique Arabic names designed to convey specific and distinct meanings to capture public attention and engagement.

6-2-3 Q3: What are the multidimensional impacts of data breaches on stakeholders technically, organisationally, and personally?

This research question sought to comprehensively examine the multidimensional impacts resulting from data breaches, with a particular emphasis on elucidating their tripartite dimensions, encompassing the technical, organisational, and personal domains.

6-2-3-1 Technical Implications

Managers identified several technical implications associated with data breaches, including elements such as the 'loss of data or digital data assets', 'disruption of university networks,' and 'disruption of systems'. Faculty members and students perceived these consequences as potentially involving device damage and disruptions to university systems.

Managers also reported instances of hacking attacks, including Denial-of-Service (DDoS) attacks, malicious viruses, Command and Control (C&C) attacks, and email phishing scams. A manager at KSU described the risk of these attacks, saying, ***'Some attacks are sophisticated and new, and the server sometimes cannot detect new vulnerabilities'***. Another at TaibahU stated, ***'One of our students received a threatening message from a hacker on his account’***.

Based on the research findings, it is conceivable that certain types of technical breaches may be particularly relevant to educational institutions. Within these contexts, it is notable that universities have traditionally been open

environments, eager to consume new knowledge from outside the organisational boundaries. As such, they may be more vulnerable to certain attacks. For example, email phishing events were also encountered by the University of Virginia in the US (2016) and the University of Nottingham in the UK (University of Nottingham, 2023). Additionally, as evidenced by Varshini (2019), DDoS attacks can often originate from students or staff, introducing additional internal threats.

Assessing the technical consequences is of paramount importance in gauging the extent of damages. A director from KSU emphasised the necessity of correlating the determination of sanctions and accountability with the assessment of the technical consequences of the event. The director articulated that **'After determining the technical implications ..., the choice of setting and implementing the penalty is left to the University Board of Directors**'. This perspective underscores the recognition of the essential role played by technical implications in informing subsequent actions related to consequences and accountability within the institutional context, both at the top level of management and across the university more broadly.

6-2-3-2 Organisational Implications

The research findings unveiled various organisational consequences arising from data breaches. These implications can be categorised as follows:

- ✓ **Reputational damage:**

Managers assert that data breaches have an adverse influence on the reputation of universities. A KSU manager argued, '***The effects on the institution may harm its reputation***', and the TaibahU manager supported this idea by stating, '***Data breaches affect the reputation of universities'***. When faculty members and students were presented with a statement assessing their inclination to monitor rumours or erroneous information concerning data breach incidents at universities, both groups demonstrated commendable awareness. Notably, both faculty and students exhibited a balanced stance, showing a mix of disinterest and neutrality regarding their eagerness to track rumours associated with data breach incidents in the university context.

Reputational damage		KSU		TaibahU	
Variable name		**Staff (%)**	**Student (%)**	**Staff (%)**	**Student (%)**
I am interested in tracking rumours that some universities are facing data security problems, especially tracking data breach incidents in universities.	Strongly Agree	4.9	18.4	10.3	11.6
	Agree.	7.3	15.9	3.4	17.8
	Neither Agree or Disagree	**26.8**	**31.5**	**38.1**	**32.5**
	Disagree	**36.6**	**28.9**	**24.1**	**22.5**
	Strongly Disagree.	2.4	5.3	3.4	7.8
	Prefer not to say	22	0	20.7	7.8

Table 58 Distribution of percentages related to the theme of reputational damage. Percentages were calculated separately for each category.

- ✓ **Financial impacts:**

Managers have contributed valuable insights concerning the financial ramifications associated with data breaches. They emphasised that data breaches entail significant financial implications for the university, encompassing budget depletion and wastage, in addition to the university incurring substantial costs in the process of recovering from the repercussions of such breaches. A manager highlighted this effect, stating: '***Restoring and recovering systems may be even more expensive than building data and information systems'.***

Conversely, survey participants were not specifically queried about the financial aspects of data breaches, as it was believed that these respondents might not provide accurate or comprehensive information regarding the monetary losses incurred. However, some faculty members did touch upon the financial impact when discussing the occurrence of data breaches, particularly noting the costs associated with the theft and subsequent sale of personal data to advertising companies.

- ✓ **Low quality of university's services:**

Interview participants elaborated on various organisational impacts attributed to data breaches, delineating how these impacts adversely affected the quality of services rendered by the university. These impacts included disruptions to university network services, a tangible effect on university performance, and instances of service crashes. At KSU, a manager stated, ***'Data breaches hinder access to networks and greatly affect university performance'***, while another at TaibahU mentioned, '***We have to find workarounds to resume running these services or systems'***.

In parallel, survey participants were presented with a statement designed to gauge their opinions concerning the efficacy of information systems and networks in their respective universities in mitigating and minimising the consequences of data breaches and data security incidents. Notably, a substantial proportion of faculty members (37.1%) and students (51.3%) 'strongly agreed' and 'agreed' with the statement, indicating a positive assessment of the quality and effectiveness of the university systems in managing data breach impacts.

In the assessment of disparities between the two universities, clear distinctions surfaced in the preferences of both students and faculty members. Specifically, TaibahU garnered higher percentages in terms of the perceived effectiveness of information systems and networks from the students' perspective, whereas KSU received a higher percentage from the faculty members' perspective. This disparity highlights the significant dynamics in the evaluations of information technology infrastructures, emphasising the importance of considering diverse stakeholder viewpoints in gauging institutional performance.

University's services/networks quality				
To what extent do you agree with this statement 'I think that the information systems and networks used in my university are managed to reduce the impact of data breaches and information security incidents'?		**KSU (%)**	**TaibahU (%)**	**Total (%)**
Staff's perspectives	Strongly Agree	7.1	2.9	10
	Agree.	17.1	10	27.1
	Neither Agree or Disagree	14.3	21.4	35.7
	Disagree	1.4	1.4	2.9
	Strongly Disagree.	5.7	0	5.7
	Prefer not to say	12.9	5.7	18.6
		KSU (%)	**TaibahU (%)**	**Total (%)**
Student's perspectives	Strongly Agree	4.3	8.5	12.8
	Agree.	11.6	26.8	38.5
	Neither Agree or Disagree	6.1	26.3	32.3
	Disagree	1.2	3.0	4.2
	Strongly Disagree.	0	2.5	2.5
	Prefer not to say	1.2	8.5	9.7

Table 59 Distribution of percentages related to the theme of the university's services & network quality.

6-2-3-3 Personal Implications

The present study investigated the personal impacts of data breaches, with a particular focus on the emotional responses they elicit. The examination of these impacts is significant, as emotional aspects have historically been underrepresented in the Saudi HE context (Sinan, 2003; Alhubaishy & Aljuhani, 2021). The findings of the present study revealed a common recognition among managers, faculty members, and students regarding the presence of emotional responses, involving anger, fear, anxiety, shock, and sadness, as negative outcomes associated with data breaches. However, interview analyses revealed additional impacts, including alienation, depression, destruction, disappointment, discomfort, lack of confidence, embarrassment, guilt, isolation, panic, trauma, and uncontrolled anger. The imbalance in emphasis between quantitative and qualitative findings arises from the inherent nature of the

qualitative approach, which allows for greater depth and flexibility compared to the quantitative approach. Consequently, the qualitative method has unveiled a broader spectrum of emotional effects associated with data breaches.

✓ Anger response

According to the research findings, anger emerged as the predominant negative emotional response to data breaches. 25.8% of faculty members and a substantial 52.7% of students, who had experienced data breaches, reported anger as their prevailing emotional response to these incidents. Furthermore, a significant portion of the survey participants in both universities, including 41% of employees and 56% of students (the total of Strongly Agree and Agree responses from each group), endorsed the notion that heightened provocation within the university environment could engender anger and potentially result in data leakage, whether intentional or inadvertent. It can be noted that this study critically examined anger from different lenses: one as an immediate emotional response to data breaches, and the other as a potential consequence of university-induced anger that could lead to data breaches.

I agree with this statement 'Too much provocation in the academia increases student anger and may result in intentional or unintentional data leakage.		**KSU (%)**	**TaibahU (%)**	**Total (%)**
Staff's perspectives	Strongly Agree	7.1	5.7	12.8
	Agree.	11.4	17.1	28.6
	Neither Agree or Disagree	12.9	5.7	18.6
	Disagree	10	5.7	15.7
	Strongly Disagree.	4.3	0	4.3
	Prefer not to say	12.9	7.1	20
		KSU (%)	**TaibahU(%)**	**Total (%)**
Student's perspectives	Strongly Agree	9.4	8.7	28.1
	Agree.	6.9	21.8	28.7
	Neither Agree or Disagree	6.9	18.1	25
	Disagree	1.9	10.6	12.5
	Strongly Disagree.	0	1.2	1.2
	Prefer not to say	0.6)	3.7	4.4

Table 59 Distribution of percentages related to the theme of anger response.

During the interviews, managers consistently identified anger as an adverse response to data breaches, offering multiple contextual interpretations for this emotion. These contexts can be synthesised into three overarching concepts. First, individuals might experience anger because they have been diligently adhering to stringent security measures yet still fall victim to a breach.

Second, there was a perspective suggesting that anger, as a reaction to data breaches, could potentially lead to severe health complications, including the risk of heart attacks. Lastly, it was mentioned that anger may result from the extension of preexisting emotional reactions, compounded by the inability to identify suitable solutions. One manager said, '***When the affected person does not find a solution, his fear turns into anger'.*** Another describes the issue: ***'With the feeling of anger, the problem worsens and grows, and they get stuck until they give up'***.

- ✓ **Fear response**

Fear emerged as the second most prevalent emotional response to data breaches, as evidenced by survey results, with percentages standing at 16.9% among faculty members and a significant 49% among students. In contrast, the qualitative analysis revealed a greater emphasis placed by the interviewed managers on the role of fear as an influential factor in data breaches, surpassing anger in significance. This was reflected not only in the interview analysis, which indicated a higher frequency of the term 'fear' compared to 'anger,' but also in the implicit focus on describing fear as more significant than anger. For instance, a manager underscored, '***The victim's first reaction is fear.*** *Another said,* ***'The feeling of fear can spoil the beauty of life'***.

Moreover, the survey analysis further illuminated that a total of 72.9% of faculty members and 68.1 of students who 'strongly agreed' or 'agreed', expressed fear regarding potential data leakage, as well as apprehensions of being susceptible to fraud or blackmail. Managers acknowledged this fear, particularly in the context of the exploitation of personal data for these nefarious purposes.

Additionally, the study's results indicated varying degrees of privacy concerns between faculty members and students, with 50% of faculty members expressing apprehensions about the privacy of their data, while 48.5% of students reported having no such concerns. This discrepancy can be attributed to distinct levels of awareness among faculty members and students regarding the risks associated with data breaches.

To what extent do you agree with the following statements 'I am afraid that my personal data may be leaked to unauthorised persons, which may expose me to fraud, extortion, or anything that offends me as a result of that leak'.		**KSU (%)**	**TaibahU(%)**	**Total (%)**
Staff's perspectives	Strongly Agree	20	20	40
	Agree.	21.4	11.4	32.9
	Neither Agree or Disagree	4.3	1.4	5.7
	Disagree	0	1.4	1.4
	Strongly Disagree.	0	1.4	1.4
	Prefer not to say	12.9	5.7	18.6
		KSU (%)	**TaibahU(%)**	**Total (%)**
Student's perspectives	Strongly Agree	14.6	36.2	37.5
	Agree.	11.2	19.5	30.6
	Neither Agree or Disagree	0.7	17.4	18.1
	Disagree	1.3	6.9	8.2
	Strongly Disagree.	0	0.7	0.7
	Prefer not to say	0	4.9	4.9

Table 60 Distribution of percentages related to the theme of fear response.

- ✓ **Anxiety reaction**

Anxiety emerged as the third significant impact of data breaches, garnering responses from 25% of faculty members and 48% of students. In addition, insights from KSU managers underscored anxiety as a prominent emotional reaction that typically ensues following a data breach, which may manifest at different levels. A manager stated, ***'You know that anxiety and depression are different levels'***. In contrast, managers at TaibahU casually alluded to the prevalence of feelings of depression as another significant emotional response experienced in the aftermath of breaches, a manager said, ' ***The effects are fear and anxiety that the data will be exploited destructively for the person, and then the effect will be stronger'***. This outcome aligns with the

findings of Sinan (2003), which affirmed the presence of elevated levels of anxiety among Internet users.

- ✓ **Shock response**

Shock was categorised as the fourth adverse consequence of data breaches, with 12.1% of faculty members and 28% of students indicating that they experienced shock or surprise following a data breach incident. Interviews with managers revealed a recognition of the potential variety of emotional responses triggered by data breaches, spanning from surprise to shock. One KSU manager expressed, '***This shock often gives rise to numerous negative emotional responses, such as disappointment, and feelings of disloyalty***', while another at TaibahU stated, '***Some experience shock'***.

Moreover, it became apparent that these emotional reactions can vary among individuals based on various factors, such as education level and age (for an in-depth exploration of these factors, refer to the relevant chapter on qualitative data analysis). The research sought to investigate whether these negative emotions correlated with other factors, including, but not limited to, awareness levels.

While 30% of faculty members (who 'disagreed' or 'strongly disagreed') rejected the notion that individuals with sufficient security awareness would be less shocked if they encountered a data breach, a notable 49.7% of students (who 'strongly agreed' or 'agreed') supported this idea. This suggests that faculty members generally perceive shock as a negative emotional response stemming from data breaches, irrespective of the individual's level of awareness.

I agree with this statement' People who have enough security awareness would not be shocked if s/he experiences a data breach event'.		KSU (%)	TaibahU (%)	Total (%)
Staff's perspectives	Strongly Agree	4.3	4.3	8.6
	Agree.	7.1	10.0	17.1
	Neither Agree or Disagree	15.7	8.6	24.3
	Disagree	17.1	11.4	28.6
	Strongly Disagree.	1.4	0	1.4
	Prefer not to say	12.9	7.1	20
		KSU (%)	**TaibahU(%)**	**Total (%)**
Student's perspectives	Strongly Agree	5.5	18.4	23.9
	Agree.	6.1	19.7	25.8
	Neither Agree or Disagree	6.8	22.0	28.8
	Disagree	3.6	9.3	12.9
	Strongly Disagree.	1.9	2.5	4.3
	Prefer not to say	0.6	3.6	4.3

Table 61 Distribution of percentages related to the theme of shock response.

In summary, the findings of this study underscore the adverse emotional impacts associated with data breaches. Nevertheless, the extent of these effects varies considerably among stakeholders, contingent upon a range of interconnected factors. Interview analysis illuminated certain determinants, notably disparities in awareness, education, and personal experience. Meanwhile, survey analysis unveiled correlations with a distinct set of variables, specifically gender, age, and occupational level.

The outcomes of this survey investigation revealed a noteworthy gender-based discrepancy, with a more pronounced fear response observable among females and a prevalence of anger reactions among males. This divergence in emotional responses may be attributed to the unique sociocultural context of the study's participants.

Furthermore, it is worth noting that participants falling within the age brackets of 25-34 and 35-44 exhibited heightened emotional susceptibility, potentially linked to hormonal fluctuations characteristic of these age groups (Fontani et al., 2004). This observation underscores the intricate interplay between biological and psychosocial factors in shaping individuals' emotional responses

to data breaches, shedding light on a nuanced aspect of this intricate phenomenon.

6-2-4 Q4: Why do stakeholders think their personal data should be protected? How would they like things to change within data management in terms of technical, organisational, and personal aspects?

Two focal themes were discussed to answer this question: participants' ‘awareness’ and ‘wishes’ to bridge the gap between their knowledge and needs.

6-2-4-1 Data Breach Awareness

In the context of data breach awareness, the qualitative insights obtained from interview participants, specifically managers, at both universities predominantly emphasised a singular facet in their definitions of the concept of a data breach, which was characterised by unauthorised access to university data and systems. Nevertheless, these interview analyses revealed the presence of additional nuanced dimensions to the concept. In the case of KSU, the qualitative examination identified a lexicon comprising terms such as ‘altering’, ‘damaging’, ‘destroying’, ‘possession’, ‘ownership’, ‘theft’, ‘exploitation of data’, ‘individual privacy’, and ‘private rights’.

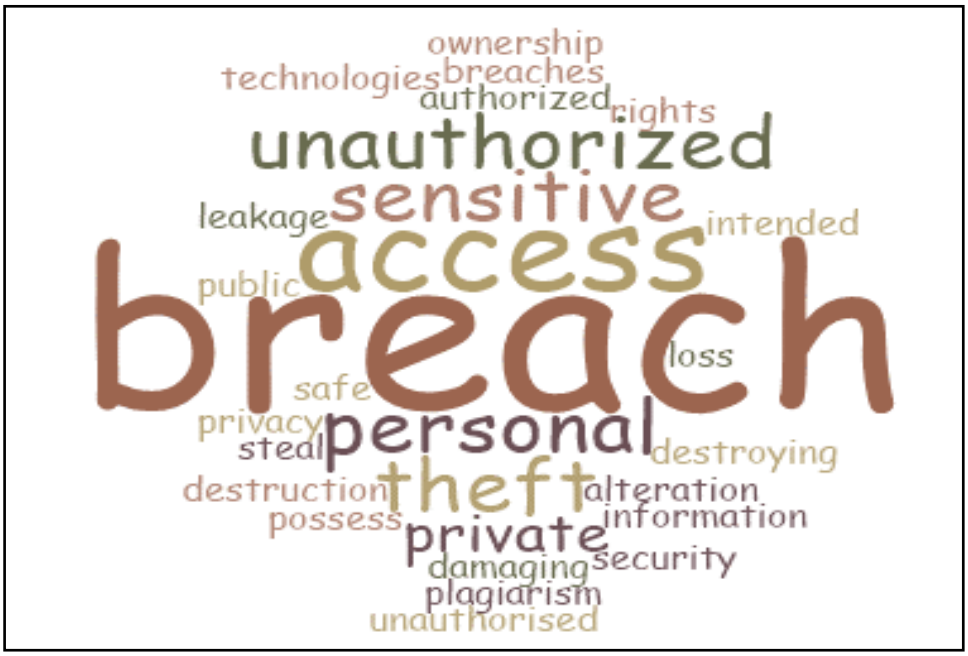

Figure 13 Word frequency of the definition of data breaches at KSU.

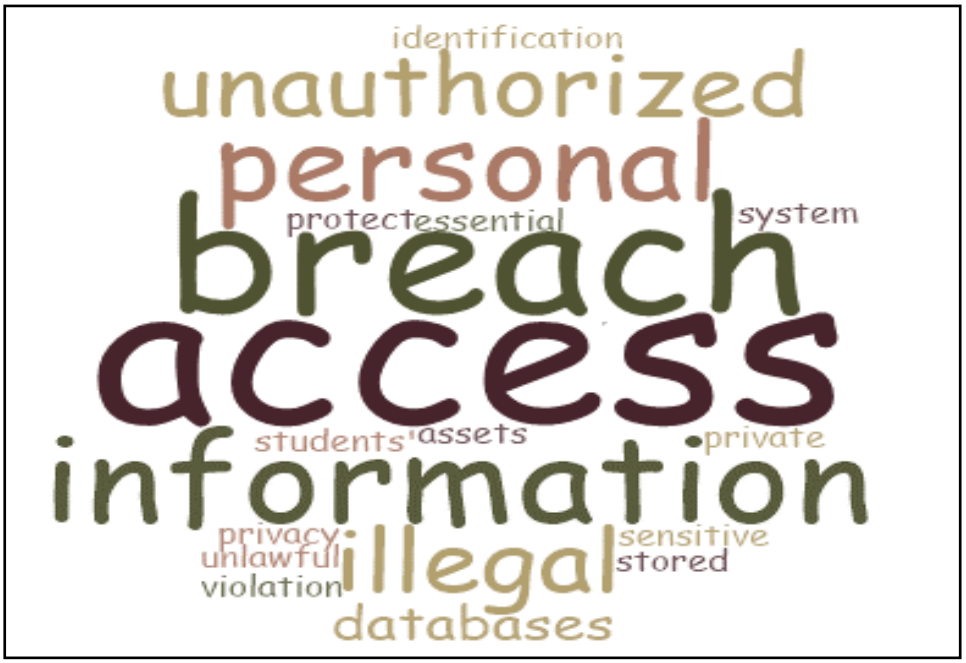

Figure 14 Word frequency of the definition of data breaches at TaibahU.

Conversely, the perspectives expressed by participants from TaibahU encompassed terms such as ‘unlawful access’, ‘unauthorised access’, ‘violation of privacy’, ‘private data’, and ‘university property’. Notably, this interview analysis demonstrated a convergence of viewpoints among faculty members and managers regarding the core tenet of unauthorised access as it pertains to the concept of data breach. However, the interpretation of data breaches among students focused on concepts such as ‘theft’, ‘modification’, and ‘espionage’, reflecting variations likely attributed to differing levels of education within these distinct categories. Complementing these interview findings, survey analysis revealed substantial agreement with the definition of data breaches, as stipulated by the UK General Data Protection Regulation (GDPR, 2021) among faculty members (87%) and students (89%).

6-2-4-2 Data Management Needs

Before explicating the participants' requirements for a data security management system to protect personal data, it is imperative to elucidate the developmental challenges prevalent in the country. Diverging perspectives regarding the development of personal data security emerged among the study's participants. Managers expressed satisfaction with the presence of the NCA, contending that the authority represents a pivotal step in enhancing the management and regulation of data security in SA. A statement from a manager at KSU underscores the essential role of the authority, asserting, ***'The most significant changes in the field of data security and protection in Saudi Arabia include the presence of the National Cybersecurity Authority (NCA)***'. Meanwhile, a manager from TaibahU highlighted the transformative developments in SA, emphasising, ***'SA has witnessed great advancements, commencing with the great roles played by the NCA’***. Managers described several collaborative initiatives between their universities and the NCA, notably including cybersecurity projects and digital transformation efforts aligned with the goals of Saudi Vision 2030. Managers also cited instances of successful digital ventures within the domain of data protection and security, such as the ‘***Haseen***’ platform introduced by the authority. Nevertheless, they underscored the need for various improvements, which spanned several key areas, including:

- Distribution of powers.
- Financial support.
- Recruitment of qualified personnel.
- Enhancement of permissions control.
- Raising awareness.
- Advancements in software development.
- Regular systems maintenance.
- Comprehensive training initiatives.
- Implementation of workshops.

At KSU there were additional needs, such as problem-solving skills, reporting data breaches, and software maintenance. Meanwhile, at TaibahU there were specific needs, including converting systems that operate on outdated technologies and ensuring copies of the data are securely stored.

Furthermore, faculty members and students were asked to prioritise the aspects they considered important for improving personal data protection. They first emphasised organisational procedures, such as developing data security policies, adopting sufficient mitigation strategies, and intensifying data security awareness programmes among employees and students. Next, they highlighted the importance of technical protection tools, including installing firewalls, controlling access to utilities (authentication), implementing screen exit controls, hiding IP addresses, intrusion detection systems, and data encryption. Finally, they acknowledged personal considerations, such as incorporating emotional aspects into data security measures.

Which of the following aspects do you think are important for developing the process of protecting your personal data that you would like your university to adopt?		KSU (%)	TaibahU (%)	Total (%)
Staff's perspectives	Technical protection tools	33.3	36.5	69.8
	Organisational procedures	34.9	40.4	75.3
	Personal aspects	25.4	19.2	44.6
	Prefer not to say	3.2	3.8	7
	Other	3.2	0	3.2
		KSU (%)	**TaibahU(%)**	**Total (%)**
Student's perspectives	Technical protection tools	16	38	54
	Organisational procedures	16	41.7	57.7
	Personal aspects	12.3	19	31.3
	Prefer not to say	14.1	1.2	15.3
	Other			

Table 62 Distribution of percentages related to the theme of the need for a data protection system. The percentage may exceed 100% because respondents could select more than one answer to the question.

6-2-5 Q5; How do SA HE mitigation strategies help to manage and recover from security breaches?

This research question explored the post-breach recovery efforts and assessed the alignment of perspectives among university managers, employees, and students in the institutions under examination. The study aimed to comprehend the strategies devised and actions undertaken by universities to recuperate from data breaches, offering insight into the extent to which these strategies with the perceptions of the respective stakeholders.

Managers from both universities disclosed the existence of comprehensive plans for managing data breaches and mitigating their repercussions. Comments extracted from the KSU dataset, such as ***'We have plans in place to address any potential breaches***,' ***'We have plans to assist victims of cybercrime***,' and ***'I have a treatment plan in case we receive a scenario involving a cyber-attack, data leakage, exploitation, fraud, etc***.,' underscore the institution's preparedness and response strategies in mitigating the challenges posed by cybersecurity threats.

Conversely, statements gleaned from the TaibahU dataset, such as '***We have business continuity plans to pre-emptively mitigate potential disruptions in the event of a data breach***,' and ***'Strategic plans facilitate a comprehensive approach over a one to three-year horizon in addressing***

identified gaps,' emphasise the importance of strategic foresight and systematic planning in cybersecurity risk management.

However, a line of inquiry focused on ascertaining stakeholders' perceptions, particularly those of faculty members and students, regarding the efficacy and adequacy of these remedial strategies in containing the impact of data breaches within their academic institutions. Remarkably, a notable proportion—54.2% of employees and 52.1% of students—responded in the negative, opting for either ‘No’ or ‘I don't know.’

This divergence in viewpoints might indicate a knowledge gap among stakeholders concerning institutional procedures and mitigation protocols, highlighting a potential area for improvement in awareness and communication within the university community.

Furthermore, the investigation extended to exploring suitable methods for mitigating the impacts of data breaches, analysed from a comprehensive, three-pronged perspective. University managers involved in the study perceived various mitigation strategies, including containment of the breach, issuing apologies, taking responsibility for the violation, notifying affected individuals, offering compensation, and extending support to those impacted.

One of the responses from managers at KSU regarding the mitigation of emotional impacts asserted, **‘We acknowledge the breach and act within a structured plan.’** In contrast, a manager from TaibahU outlined a different approach, stating, **‘We assume responsibility, guide beneficiaries appropriately, and provide the necessary support and follow-up.’**

These responses underscore the deliberate strategies employed by the respective institutions in addressing the emotional consequences that arise in the aftermath of security breaches.

How would you prefer your university to treat you in case you are exposed to a data breach to mitigate the breach's effects?		KSU (%)	TaibahU(%)	Total (%)
Staff's perspectives	Apology	35.4	30.2	65.6
	Compensation	45.8	51.2	97
	Prefer not to say	6.3	9.3	15.6
	Other	12.5	9.3	21.8
		KSU (%)	TaibahU(%)	Total (%)
Student's perspectives	Apology	16.4	29.1	45.5
	Compensation	21.2	58.2	79.4
	Prefer not to say	0.6	8.5	9.1

Table 63 Distribution of percentages related to the theme of data breach mitigation.

The above table presents the perspectives of faculty members and students at both universities regarding their preferences for an effective strategy to mitigate data breaches. The total percentage exceeds 100% because respondents could select more than one answer to the question. Since each selection is counted independently, the total percentage represents the cumulative frequency of all choices rather than a proportion of unique respondents. Among mitigation strategies, the 'compensation' approach emerged as the most favoured, receiving significant support from 97% of faculty members and 79.4% of students. It was closely followed by the 'apology' strategy, with 65.6% of faculty members and 45.5% of students indicating their preference.

The study further identified a statistically significant relationship between the variable 'job level' and the preferred mitigation strategy, attributed to the direct correlation between job levels and income. Interestingly, the analysis also revealed a gender-based disparity in strategy preferences, with females showing a predilection for the 'compensation' method and males displaying a preference for the 'apology' strategy. However, there was no statistically significant association between gender and the preferred mitigation method.

These findings have not been identified in other research literature related to the Saudi HE institution sector. Compensation and institutional responses are important aspects of this landscape and warrant further attention moving forward.

6-3 Discussion

The interview analysis revealed that persistent and ongoing attempts to infiltrate university data systems continue to occur, with these efforts frequently being thwarted by the robust deterrence systems implemented by the universities under investigation. Interestingly, a stark contrast in reported experiences of data breaches emerged, with only a minority of students acknowledging such incidents, while a significant proportion of faculty members remained neutral in their responses regarding data breach experiences. This study identified eight distinct types of data breaches, drawing from previous sources, including unintentional disclosures, hacking or malware attacks, payment card fraud, insider breaches, physical data losses, data theft incidents, hardware losses, and unknown violations. Notably, the 'unknown' violation type received the highest number of responses, potentially reflecting challenges related to breach management, investigatory inefficiency, or inadequate awareness among participants. Crucially, the statistical data underscored that all eight types of data breaches are prevalent within the Saudi HE sector.

Comparatively, previous research exploring these eight breach types within HEIs in the United States found that seven of these were evident in the university community (Garrison & Ncube, 2011; Holtfreter & Harrington, 2015; Hammouchi et al., 2019; Al-Mulhim et al., 2020), with the exception being 'payment card fraud' (Collins et al., 2011). In contrast, this study suggests Saudi universities may be susceptible to all these breach types, including 'payment card fraud', as substantiated by the current study sample and reinforced by illustrative cases in the literature review (Parr, 2013). This divergence highlights the critical need for comprehensive data security measures and enhanced awareness within the Saudi educational context to effectively combat a wide range of data breaches. It underscores the urgency of developing proactive strategies to mitigate these risks and uphold the integrity of sensitive data within academic institutions.

The findings of this study align with prior research that has explored the landscape of data security risks. This study highlights significant organisational risks and challenges in the domain of personal data security management,

including resistance to or non-compliance with data security policies, budgetary constraints, limited awareness, and a lack of professional expertise.

Notably, the study's most significant revelations pertain to the participants' lack of familiarity with their university's data security policies, the inadequacy of the training programmes available to them, and the insufficiency of effective awareness-building mechanisms for addressing data breaches. While this insight represents a novel contribution, the broader challenges related to information security, cybersecurity awareness, and training have been recurrent topics of discussion (Marks & Rezgui, 2009; Albarrak, 2011; Badie & Lashkari 2012; Chan & Mubarak, 2012; Metalidou et al., 2014; Nadim 2014; Alzahrani & Alomar, 2016; Arutyunov, 2017; Areishi & Aldossary 2018; Yerby & Floyd, 2018; Al-Qahtani, 2019). However, this study found that in the KSU context, there were issues with over-trust, which may be a global phenomenon but could hold particular significance within Saudi Arabian cultures. Equally, it is important to acknowledge this response as overseas students travel internationally, necessitating the design of university systems that account for the cultural complexities of all student populations.

What further sets this study apart is not only its specific focus on ‘personal data breaches’ but also the unique diversity of its sample, drawn from multiple universities and stakeholders. It has attempted to map a far broader landscape than most previous studies. As such, the significance of the study lies in its completion of a crucial link in the chain of prior research efforts, integrating technological, organisational, and personal impacts, including emotional effects. In terms of outreach, it draws on and underscores the vital importance of bolstering awareness and training programmes within Saudi institutions (Albarrak, 2011; Asel & Al-Aifan, 2014; Nadim, 2014; Alzahrani & Alomar, 2016; Arutyunov, 2017; Areishi & Al-Dossary, 2018). In addition, it offers some novel suggestions as to how this could be implemented, advocating for more open approaches to training and workshop-based change.

Technical data security risks present a formidable challenge within today's highly interconnected digital landscape. The intricate integration of IT infrastructure, systems, and networks underpinning educational institutions

exposes them to a wide range of vulnerabilities. The realm of cyber threats, encompassing hacking, malware incursions, and system susceptibilities, jeopardises the sanctity, integrity, and accessibility of sensitive data. While the current analysis identified several technical risks in Saudi universities that could compromise data security—including inadequacies in technical competencies, hindrances in system and software modernisation, constraints in budgets for licence renewals, and the threat of external attacks such as viruses—it simultaneously illuminated a notable maturation in the technical domain when contrasted with findings from previous studies (Al-Shanbari, 1998; Alsadhan, 2015; Alkhudary et al., 2020). This evolution underscores the growing recognition among universities of the pivotal role played by technical infrastructure and their deepening engagement with information technology systems. It also highlights university officials' awareness of the complexities of technical risks and their efforts to fortify the safeguards surrounding digital data assets.

This study was primarily structured to provide a comprehensive exploration of data breaches, focusing on three key dimensions: the technical, organisational, and personal aspects. The interview analysis conducted during this research enabled the identification of two crucial personal risks, previously overlooked in the Saudi academic landscape, which pose threats to the personal data security framework: ‘over-trust’ and ‘excessive empathy,’ both prevalent within Saudi Arabian (SA) society. In addition, it recognised the significance of family-related impacts, which are highly influential in SA but not necessarily as significant in other societal contexts. It is essential to recognise that discussions about data and information security should be contextualised within the societal framework. Whilst previous studies have explored various factors, such as extortion (Alghadyan, 2018; Al-Qahtani, 2021), the study findings highlighted the importance of understanding these nuanced cultural elements in shaping the data security landscape.

University data breaches have far-reaching repercussions that permeate various facets of academic life. A robust security environment is imperative to ensure the confidentiality, integrity, and accessibility of sensitive data, which are foundational for academic and administrative functions. Data breaches not only

compromise data integrity but also trigger a cascade of adverse effects. The present study has revealed a range of multidimensional consequences resulting from data breaches within universities under scrutiny. These institutions have reported a spectrum of regulatory consequences encompassing reputational damage, financial losses, and disruption of university services and networks. The significance of reputation as a fundamental metric for gauging the quality of university services, as perceived by students, was affirmed in this study. Notably, research participants demonstrated an awareness of the need to discern credible information from rumours and misleading narratives surrounding data breaches.

However, a security breach within the academic context can prove catastrophic, engendering financial losses, service disruptions, individual and organisational impacts, and long-term reputational damage. Although prior investigations into data breaches that addressed financial implications in SA were inaccessible—potentially due to the recent implementation of data protection laws within the country—the findings from this study revealed a pronounced financial strain on institutions. Participants cited the substantial cost incurred in mitigating the aftermath of data breaches, aligning with the literature, which indicates that a single data breach in the Middle East may reach a staggering cost of £5.36 million (IBM Security, 2020).

Beyond the immediate consequences, data breaches have a far-reaching impact, eroding the trust of affected individuals, fostering scepticism, and diminishing trustworthiness. These findings echo those from the international context (Ayereby, 2018), emphasising that data breaches adversely affect trust in institutions, subsequently influencing academic quality, institutional reputation, and the well-being of the community. The ramifications of university data breaches are intricate and pervasive, underscoring the critical importance of robust security measures in safeguarding the integrity and reputation of academic institutions.

The study's findings extend beyond the confines of the technical domain, exploring the organisational and personal dimensions, particularly emotional responses. The research sample reported various technical consequences,

including data loss, network and system disruptions, device damage, hacking, denial-of-service (DDoS) attacks, malware attacks, command and control (C&C) attacks, and email scams. While these technical impacts have been documented on both local and global scales (Garrison & Ncube, 2011; McClurg, 2015; Beaudin, 2017), the present study provides unique insights into their prevalence in the Saudi educational context.

Furthermore, the review underscores a significant gap in the exploration of the psychological impact of data breaches within HEIs, both in SA and worldwide (Muhammed, 2000; Mollick, 2006; Taddicken, 2014; Tanantaputra et al., 2017; Alghadyan, 2018; Padyab & Ståhlbröst, 2018; Bada & Nurse, 2020; Holmes, 2015). The study introduces original data concerning the psychological impacts, capturing five primary emotional responses—anger, fear, anxiety, shock, and sadness—resulting from data breaches.

McClurg's (2015) investigation of the issue helped the researcher to posit a random conjecture of the existence of varying impacts that could be associated with each type of data breach; a conjecture that had not been subjected to empirical scrutiny. The study's outcomes, however, partially support this but reveal the nuanced and divergent consequences of data breaches. In essence, determining the extent of the impacts of these consequences was associated with several factors, including the nature of the breach, the extent of awareness and educational preparedness, the degree of familial openness, and the sensitivity and confidentiality of the compromised data.

To enhance personal data management in Saudi universities, the consensus among participants is to prioritise the development of technical, organisational, and personal aspects, respectively. Survey perspectives advocate the need for organisational enhancements, encompassing the formulation of data security policies, implementation of robust mitigation strategies, and the intensification of data security awareness programmes among faculty members and students, with a notable indication of the participants' inclination to minimise personal data. Despite extensive literature highlighting the awareness deficit in the Saudi context (Albarrak, 2011; Nadim, 2014; Alzahrani & Alomar, 2016; Areishi & Al-Dossary, 2018), perceptible changes remain sluggish. Interview participants

also emphasise the necessity of presenting training and awareness programmes,

In conclusion, the study participants articulated a set of imperatives and requirements for mitigating the consequences of data breaches. These imperatives included the necessity for (1) the establishment of comprehensive contingency plans to effectively address data breaches, (2) acknowledging and assuming responsibility for data breach incidents, (3) ensuring the prompt and transparent reporting of breach events and their attendant consequences, (4) the provision of adequate compensation for those adversely affected by such incidents, (5) the implementation of robust data protection management practices, (6) the dedicated commitment to the safeguarding of personal data, (7) the implementation of strategies for apologies and compensating victims, and (8) the better understanding and planning for dealing with the emotional and cultural factors in the breach landscape.

These prescriptive insights not only underscore the landscape of data breaches but also emphasise the critical role of proactive planning and ethical responsibility in the field of data security. In addition, the research has evidenced some novel findings in the Saudi Arabian (SA) context, particularly in highlighting the need for further research in such a complex landscape. This study has shed light on the necessity for more research—both in terms of holistic studies that build on this work in different contexts and in-depth investigations that further develop understanding within each of the complex components of this domain. Moving forward, research must delve deeper into technological, organisational, and personal domains, as well as explore the granular aspects within each area. As we transition into a world increasingly reliant on data—with the potential to improve and transform life, education, and work—we simultaneously face growing risks related to cyber warfare, cybercrime, technical failures, and human errors.

Chapter 7: Research Conclusion

Introduction

The chapter represents the culmination of a research effort exploring the landscape of data breaches within university settings. This exploration has revealed a gold chain of thoughts and perspectives regarding personal data management and data breaches through the lens of technological, organisational and personal impacts. Through a convergent mixed-methods approach, this investigation has critically examined the risks and impacts of data breaches on individuals and organisations. The study has been ambitious in its scope, seeking to consider these holistically. To achieve its objectives, it has engaged a diverse group of participants, including managers, faculty members, and students, providing a comprehensive panorama of perspectives. The inclusion of these varied stakeholders offers a deeper understanding of the complexities involved in managing personal data security, addressing data breaches, and overcoming the challenges of post-breach recovery.

This chapter begins by outlining the significant contributions of this research and then, in greater detail, highlights the research results. By navigating through the findings, insights into distinct challenges and potential opportunities are gained in protecting sensitive information within the unique context of higher education (HE) in Saudi Arabia (SA). The culmination of this process leads to the development of robust recommendations tailored to address the identified challenges and harness the available opportunities in data security management. These recommendations have the potential to be actively implemented within Saudi universities, contributing to the effective management of cyber threats and aligning with the nation's aspirations for secure and transformative technological advancements in higher education institutions (HEIs). Finally, this chapter provides valuable direction for future initiatives in strengthening cybersecurity frameworks within the Saudi higher education sector, as well as for future research. Through this comprehensive mixed-methods exploration, the research lays the groundwork for a more resilient and secure future for Saudi universities in an increasingly digital age. Moreover, its insights can inform HEIs more broadly.

7-1 Research Contributions

The research landscape on data breaches in Saudi universities, along with strategies for protecting data and mitigating their effects, has made significant contributions, shedding light on an increasingly pressing issue in higher education (HE) and beyond. This research topic is of critical importance as universities in Saudi Arabia (SA) and the broader Middle East grapple with the challenges of digital transformation while facing a growing threat from cyberattacks. In this research contribution, I highlight the key insights made in this area and their broader implications.

Advancing Knowledge of Data Breach Effects: One of the primary contributions of this research is the enhancement of understanding regarding the effects of data breaches in Saudi universities. This work has expanded knowledge on the various dimensions of this issue. By investigating the technical, organisational, and personal impacts of data breaches, the researcher has provided a more holistic perspective on the challenges faced by universities and the repercussions of security incidents. This knowledge is instrumental in guiding institutional preparedness, as well as shaping prevention and response strategies to enhance data security frameworks.

Tailoring Strategies to the Saudi Context: Research in this domain has recognised the unique challenges and opportunities present in the Saudi context. The Saudi Data Protection Law, which came into effect in 2024, has established a regulatory framework for data security. The researcher has identified key stakeholder needs related to managing personal data, enabling universities to better align their strategies with these requirements. Consequently, implementing the new data protection law and ensuring that it is effectively communicated to stakeholders will be more seamless if institutions take this study into account. Compliance is not only critical for legal adherence and avoiding fines and penalties, but it also enhances institutional credibility by minimising reputational risks and ensuring secure, efficient, and trustworthy data management practices.

Enhancing Data Protection Measures: Research in this field has contributed to strengthening data protection measures in Saudi universities. The researcher has highlighted the importance of comprehensive policies, robust access controls, and advanced cybersecurity technologies in safeguarding sensitive information. As a result, universities are increasingly implementing these recommendations to bolster their defences against data breaches.

Strengthening Cybersecurity Awareness: This research has underscored the crucial role of cybersecurity awareness and training programmes for faculty, staff, and students. These initiatives have become instrumental in fostering a security-conscious culture within universities, where individuals are not only aware of the risks but also actively engaged in preventing data breaches. Additionally, this study has identified specific cultural factors that should be considered in cybersecurity training. Notably, Saudi individuals often exhibit strong trust in their organisations and systems, which can, at times, result in over-reliance on institutional security measures. Therefore, cybersecurity training should also focus on empowering users to recognise their individual responsibilities in safeguarding data. Raising awareness of how cyberattacks can be facilitated through human interactions is essential, ensuring that faculty, staff, and students play an active role in detecting and reporting suspicious activities.

Crisis Preparedness and Communication: Scholarly work has emphasised the importance of having well-structured incident response plans and crisis communication strategies in place. This contribution helps university managers mitigate the damage caused by data breaches and swiftly restore stakeholders' trust by addressing students' and faculty members' expectations for transparent communication. The study provided evidence that apologising and informing individuals in the event of a data breach is valuable and should be the first step in managing the situation and making reparations. In certain circumstances, compensation may also be warranted.

Collaboration with National Initiatives and Related Universities: The researcher has highlighted the value of collaboration with government initiatives, such as the NCA. These partnerships enable universities to leverage

national resources and expertise to strengthen their data security measures. In addition, the study identified differences between the two universities under investigation, suggesting that university networks in SA could engage in mutually beneficial knowledge-sharing to enhance their cybersecurity strategies.

Psychological Impacts: This study has developed a framework that demonstrates the psychological impacts of data breaches on faculty members and students. Understanding how breaches affect stakeholders emotionally is a crucial contribution, as it enables universities to offer more effective responses, support systems, and counselling services. In the SA context, it is particularly important to consider the broader family networks, which were identified as a significant factor influencing emotional responses to breaches. Additionally, the study explored the psychological impact on those responsible for managing breaches, highlighting their need for support and resilience-building strategies. The research identified innovative approaches to enhancing resilience among managers, including targeted workshops and creative coping mechanisms to better equip them for crisis management.

Supporting Saudi Vision 2030: This research has demonstrated how data breaches can impede the goals of Saudi Vision 2030, particularly in the areas of digital transformation and the knowledge economy. By highlighting this connection, the study contributes to the alignment of data security efforts with the broader national development agenda, emphasising the need for robust cybersecurity frameworks to support Saudi Arabia's technological advancements and economic diversification.

Inspiring Future Research: One of the most notable contributions of this study is its potential to inspire further research on data breaches and security in universities. This research not only adopts a holistic perspective but also encourages future studies to explore more focused and granular aspects of cybersecurity challenges. The dynamic nature of cyber threats and the ever-evolving digital landscape necessitate ongoing inquiry to ensure resilience against emerging security risks.

The research methodology used in this study offers a valuable reference for researchers and practitioners interested in developing a robust framework for cybersecurity research. The researcher's pragmatic approach allowed for adaptability, providing the flexibility to select appropriate research methods based on the research questions and resource availability. This flexibility led to the development of a mixed-methods approach, employing a comparative design that combined quantitative data (including open-ended questions) from faculty members and students with qualitative insights gathered through interviews with university managers. This convergent data collection and analysis generated nuanced insights that would have been difficult to achieve using only quantitative or qualitative methods. Triangulating results from these two datasets enhanced the reliability and validity of the research findings.

The methodologies employed throughout this research—including convergent data collection, data triangulation, and integration of multiple perspectives—offer valuable guidance for researchers who seek to apply diverse methodological approaches in their work. The study was carefully designed to address power dynamics and the sensitivity of the subject matter under investigation. The survey tool ensured a balanced and inclusive approach by allowing for optional questions and anonymous responses, thus minimising potential biases. Meanwhile, interviews with participants in positions of authority facilitated in-depth discussions, enabling a richer exploration of cybersecurity issues with informed stakeholders.

Translating Across Cultures: This study also provides valuable insights for researchers working across linguistic and cultural boundaries. The findings highlight the advantages of conducting research in native languages, allowing for more precise and culturally relevant data collection. However, the study also acknowledges the challenges posed by translation, particularly the risk of semantic shifts and loss of meaning when converting concepts between languages. As a result, the research underscores the importance of transparency in translation processes and calls for greater clarity when presenting translated research findings. By recognising the nuances of language and cross-cultural communication, this study contributes to

enhancing the accuracy and reliability of research conducted in multilingual and multicultural contexts.

Overarching Impacts: In conclusion, this research on the effects of data breaches in Saudi universities, along with strategies for data protection and mitigation, has made substantial contributions. These contributions not only strengthen the security and resilience of SA universities but also have wider implications for the nation's knowledge-based transformation within its broader national agenda. Furthermore, the findings offer valuable insights for global higher education institutions, fostering cross-institutional learning while highlighting the distinct perspectives and value of Arabic conceptualisations of data security and privacy.

7-2 Highlight Research Results

This study examined various dimensions of data security in universities, focusing on technical, organisational, and personal aspects of data breaches. The research identified several key findings that provide a comprehensive understanding of cybersecurity challenges in higher education. These findings include:

Understanding of a Data Breach Concept: Interview participants from both universities identified data breaches as unauthorised access to university data and systems, signifying a shared foundational understanding of the concept. Expanding on this primary definition, participants demonstrated a more nuanced grasp, incorporating terms such as altering, damaging, possession, theft, and exploitation of data. This broader conceptualisation reflects their recognition of the various ways in which data breaches can occur and impact institutions.

Moreover, survey analysis reinforced this shared understanding, revealing substantial alignment with the General Data Protection Regulation (GDPR) definition of data breaches, with 87% of faculty members and 89% of students recognising this widely accepted interpretation. This high level of consensus underscores a strong awareness among participants regarding the nature and implications of data breaches.

Data Breach Experience and Management: In the investigation of data breach occurrences within a university setting, responses exhibited confusion when responding to inquiries about encounters with security breach events. Both students and managers shared similar perspectives on the perceived rarity of data breaches in the educational context of both university settings. However, the results from students showed statistically significant variances in the rate of experiencing data breach incidents, indicating a probability disparity between the two universities. Notably, faculty members demonstrated a potential hesitancy to disclose their experiences, with many opting not to respond when questioned about data breaches in both universities. While managers involved with managing the security reported diverse attempts to compromise university data systems, including email phishing, external attacks, and command-and-control attacks, there was no explicit confirmation of significant damage. Intriguingly, a considerable number of affected faculty staff and students categorised the type of breach as ‘unknown’, indicating real challenges in effectively addressing, managing, or reporting such incidents.

However, there were other types significantly recorded besides the type ‘unknown’. Perspectives revealed that the most frequently encountered breaches involved ‘unintended disclosure’ and ‘data theft’ among students, while employees encountered challenges related to ‘malware’ and ‘payment card fraud’. Given the risks faced by employees and students, it seems necessary to allocate substantial resources to universities to ensure security management, particularly since their internal computer networks are highly vulnerable to malware attacks. To address human factor-related activities like fraud, data theft, or unintentional disclosure, proactive measures such as regular information security training for employees and students, as well as the use of physical locks on computer equipment to deter theft, are an important part of the defence mechanism. The number of participants who claimed to have managed a data breach exceeded those who reported experiencing a breach within their university, suggesting a likelihood of individuals turning to their universities for assistance in handling data breaches, whether occurring within or outside the academic context.

Technical Implications: Perspectives on data breach risks and impacts were diverse among managers, faculty, and students regarding the technical side. The study's results pointed out the danger of the technical side, with interview participants elucidating this risk by providing different information about attack types and their impact. These technical impacts were external attacks, email phishing, malicious viruses, DDoS attacks, and C&C attacks. The technical risks included insufficient technical skills, human errors, software/systems updates, and license renewal budgets. Survey participants marked technical risk as the most harmful aspect of data breaches, without a statistical differencing detected between the two universities, except for the staff results which indicated differences between universities in the appropriacy of technical tools adopted by the universities, and that might signalise the possible differences in technical tools that each university owns.

Organisational Implications: Interview participants acknowledged the significance of organisational risks, such as non-compliance with policies and insufficient budgets. Data breaches were also acknowledged to negatively impact university reputations, with financial implications, including budget depletion and recovery costs. Disruptions to university network services and crashes were noted to affect the quality of services. Although respected universities had data security policies, stakeholders (employees/students) conceded their lack of awareness of those policies, with participants knowing where to report breaches within universities for survey participants or within the state for interview participants. The survey's responders marked the organisational side as the second most harmful aspect of data breaches. Most of those responders acknowledged not receiving data security training, considering awareness programmes insufficient, and expressing unfamiliarity with personal data processing. Interview participants refuted this, highlighting the need for awareness security programmes.

Statistically, the findings regarding organisational risk reflected consistent perspectives and views across both universities, except for the discrepancy observed in the students' results regarding the reduction/minimisation of personal data, which varied between the universities. This suggests a potential disparity in the volume of personal data collected by each university from

people for processing. However, these variations in the volume of collecting personal data are significant, particularly considering the country's implementation of a personal data protection law, slated to take effect in 2024 (Baig, 2023). This legislation acknowledges data minimisation as a fundamental principle.

Personal Implications: Participants in the study underscored the significance of personal aspects, particularly emotional responses, as an actual risk and consequence of data breaches. Interview analysis revealed a multitude of emotional reactions, including fear, anger, anxiety, shock, sadness, guilt, alienation, frustration… etc, identified by participants as negative outcomes. However, there was variability among managers regarding the perceived importance of each emotional response. In contrast, survey analysis highlighted that anger emerged as the predominant emotion among participants, followed by fear and anxiety. Surprisingly, the study unveiled notable gender-based differences in emotional reactions to data breaches. The quantitative data from surveys indicated an increase in fear among females, while anger exhibited an upward trend among males. Certainly, gaining a deeper comprehension of the emotional distinctions between genders is crucial for the development of targeted and effective mitigation strategies tailored to each specific emotional response. Recognising the gender-specific nuances in emotional reactions to data breaches allows for a more nuanced approach to addressing the psychological impact on individuals. Strategies can be devised to provide targeted support, coping mechanisms, and communication methods that are suitable for the predominant emotional responses within each gender.

The research discerned distinct patterns of emotional sensitivity to data breaches based on age. Specifically, survey participants in the 25-34 and 35-44 age groups demonstrated heightened emotional susceptibility. This finding suggests that individuals within these age brackets may experience and perceive the emotional impact of data breaches more acutely compared to other age groups. The recognition of age-specific emotional patterns contributes to a nuanced understanding of the diverse ways in which individuals across different demographics respond to the emotional impact of data breaches.

Cultural Factors: The research highlighted the unique characteristics of the Saudi security environment, which is largely shaped by cultural acceptance. Campaigns such as 'Kollona Amn' demonstrate the use of culturally resonant names for security initiatives to enhance community engagement and promote protection. Phrases such as ‘Alhamdulillah’ and ‘Mashallah’ carry significant cultural and emotional weight, making their inclusion essential for understanding the security context and assessing participants’ levels of satisfaction or concern.

The findings underscored the substantial impact of cultural factors on perceptions of data security and emotional responses within the Saudi context. The qualitative study revealed that data breaches affect traditional families more profoundly than moderate families. Traditional families, deeply rooted in cultural norms and societal expectations, experience heightened distress from privacy violations, particularly when they involve the exposure of personal photos, especially of women. In contrast, moderate families may feel less societal pressure, making breaches particularly distressing for those who adhere to stricter cultural values. Furthermore, the quantitative study revealed that females reported higher levels of fear compared to males, further emphasising the influence of cultural context on emotional reactions to data breaches.

Data Protection Needs: The examination of participants' perspectives on personal data management needs revealed several key insights. Interview participants expressed satisfaction with the NCA in SA, indicating a positive perception of the existing cybersecurity governance framework. The study highlighted a proactive approach, with collaborative initiatives between universities and the NCA, suggesting a collective effort to strengthen personal data security measures. Managers identified several areas for improvement, which are essential for enhancing cybersecurity frameworks. These areas include the distribution of authority, financial support, recruitment of qualified personnel, permissions control, awareness campaigns, software development, systems maintenance, and comprehensive training initiatives and workshops.

Survey analysis indicated alignment among faculty members and students regarding their prioritisation of key elements in the development of data security processes. Many participants placed the highest priority on organisational procedures, recognising their fundamental role in ensuring effective data governance. Following this, a substantial proportion of respondents acknowledged the critical importance of technical protection tools in enhancing data security, reflecting a shared understanding of the necessity of advanced technological safeguards. Finally, participants recognised the significance of personal aspects, including individual responsibility and awareness. This quantitative ranking of priorities underscores the holistic approach advocated by participants, emphasising the need to integrate technical, organisational, and personal dimensions into comprehensive data security strategies within university settings.

Data Breaches Mitigation: The research's results disclosed that managers at both universities had articulated comprehensive plans for managing data breaches. Mitigation efforts included containment measures, issuing apologies, taking responsibility, notifying affected individuals, and providing support. Notably, among these mitigation strategies, 'compensation' emerged as the preferred choice for faculty members (97%) and students (79.4%), indicating a strong preference toward financial remediation. This preference for compensation was statistically significant, revealing a correlation between job levels and the chosen mitigation method. Additionally, a gender-based disparity was observed, with females favouring 'compensation' and males leaning towards the 'apology' strategy. However, this gender-based preference did not establish a statistically significant association. These findings highlighted the complexity of recovery strategies, showcasing the need for nuanced approaches that consider job level, gender difference, and diverse perspectives among stakeholders in the aftermath of data breaches.

Overall, one of the most prominent findings of this study is the strong correlation between the effects of data breaches and the surrounding environment and culture. This is evident in the perspectives of various stakeholders, as discussed in Chapters 4, 5, and 6, where the severity of a breach’s impact is

influenced by societal norms, institutional values, and cultural perceptions of privacy and security.

However, among these findings, two are particularly influential and relevant for universities, as they have a direct impact on cybersecurity practices and contribute to the development of a safer and more resilient university environment. Their adoption can lead to meaningful improvements in policies, awareness, and overall institutional security. These are:

1. Lack of Awareness and Compliance with Data Security Policies
2. Emotional and Psychological Impacts of Data Breaches

These findings highlight that managing personal data security in universities is not solely a technical matter but also a broader organisational and behavioural challenge. The lack of awareness reveals a difficulty in communicating policies effectively, ensuring compliance, and engaging stakeholders, which may lead to inconsistent security practices and an increased risk of breaches. At the same time, the emotional and psychological effects of data breaches point to an important aspect often overlooked in cybersecurity strategies—where technical measures are prioritised, while the human impact on trust, confidence, and well-being receives less attention. Recognising and addressing these challenges can help universities strengthen their security culture, enhance engagement with data protection measures, and create a more supportive and secure academic environment.

7-3 Research Recommendations

This dissertation aims to provide a comprehensive exploration of data breaches within the context of HEIs in SA. Drawing upon extensive literature reviews, and stakeholder perspectives, through mixed-methods findings, the research recommendations outlined aim to guide future inquiries and contribute valuable insights to the evolving landscape of data security. HE institutions, following the example of KSU/ TaibahU, should prioritise the alignment of their technological infrastructure with national and international cybersecurity standards. This involves periodic evaluations, updates, and adherence to regulations set forth by entities like the National Cyber Security Authority (NCS) and ISO. A

commitment to maintaining a secure and compliant technological foundation is pivotal in the face of ever-changing cybersecurity landscapes.

This study's findings underscored the importance of establishing strong organisational measures in both universities to face and manage the organisational risks and potential impacts in the event of a data breach. It was acknowledged that in the current threat landscape, all risks cannot be negated. Therefore, universities should focus on the development and implementation of comprehensive policies and procedures and bridge the gap between their written regulations and implementing these regulations. Universities should create a culture that prioritises and integrates these measures into everyday practices ensuring they are well understood. A crucial requirement expressed by stakeholders was to minimise the collection of their personal data to that data which is really needed. Therefore, universities must decrease the amount of personal data collected and establish a policy for safeguarding personal data, ensuring that key principles such as data minimisation are clearly outlined and the rationale for processing data is well understood. From the results, it can be recognised that human risk factors are a substantial risk in data protection, and there should be a concerted effort to enhance awareness and ensure there is a better understanding of the threat landscape.

Considering the study's findings, it is strongly recommended that both universities institute comprehensive and intensive training programmes focused on data security for their stakeholders. Data security training plays an essential role within the university setting, serving as a foundational element to equip faculty, staff, and students with the necessary knowledge and skills essential for protecting sensitive data/information and mitigating potential cybersecurity risks, particularly in the context of data breaches (Arutyunov, 2017). Given the escalating reliance of educational institutions on digital platforms and information systems (Asadullah et al., 2018; Gorshenin, 2018; Habib et al., 2021), there is an imperative to underscore the significance of fostering a culture of cybersecurity awareness.

Data security training programmes contribute to raising awareness about the evolving landscape of cyber threats, and educating individuals on best practices

for handling, transmitting, and storing data securely. By instilling a strong awareness of the potential consequences of data breaches and the role each individual plays in maintaining a secure environment, data security training enhances the overall resilience of universities against cyber threats and fosters collective responsibility for protecting sensitive and personal data. However, the emotional learnings from this study evidence that there is a need to carefully consider how this is done and to implement it in a manner which does not exacerbate individual fears, i.e. individuals need to be informed and enabled positively.

Observing variations in perceptions between KSU and TaibahU, it is recommended that both institutions engage in a comprehensive review and dialogue with stakeholders. Requesting detailed feedback and initiating collaborative efforts can contribute to refining information systems and personal data management, fostering transparency, collaboration, and communication. It was noted in KSU that there was potentially too much-infounded trust in systems. Under the umbrella of NCA, collaborative efforts between the universities could be initiated to share best practices and insights related to data security management. This exchange of knowledge might aid each university in refining its respective systems to align more closely with the expectations and requirements of its distinct user groups and promote positive competition across universities.

Furthermore, all perspectives expressed the emotional impacts of data breaches, although individuals may exhibit varying emotional reactions. The research revealed that data breaches elicit a range of emotional responses, e.g., anger, fear, anxiety, and shock. This overlooked aspect warrants significant attention from universities. They must prioritise the emotional well-being of both staff and students, demonstrating their commitment to supporting those affected by information security incidents. This can be achieved by establishing specialised support channels, such as counselling services or helplines, where employees/students can seek emotional support and guidance following such incidents. Apologies and compensation need to be planned so that they can be used in an appropriate way as needed. The study recommendations can be summarised below. Students are discussed first as it

is important to centre those with potentially the least overall power in the processes.

7-3-1 Recommendations for Students

Participation in Training Programmes: Actively engage in comprehensive data security training programmes offered by the university. This includes learning about technical aspects, data management, organisational systems, and understanding personal impacts. It is important to stress these are both university and life skills for personal future protection and use in future work scenarios.

Conscientious Use of Technology: Students should ensure careful use of hardware and software, staying aware of risks to both them and the university. they should show appreciation for university investments in modern IT infrastructure, including servers, devices, systems, and data.

Adherence to Institutional Guidelines: Students should follow institutional guidelines regarding permissible devices, software, and usage, especially in terms of sharing.

Maintaining Security Measures: Through Installing up-to-date antivirus and firewall programmes to protect against potential security threats. Regularly updating passwords and avoid sharing them with others. Utilising secure USB storage media for data storage purposes.

Safe Use of Email: It's essential for students to use their university-provided email accounts and familiarise themselves with the email usage policy. Students should be careful when opening emails or clicking on unknown links, as these actions could introduce malware into university systems. Additionally, students should keep their email passwords private and update them regularly to prevent potential security breaches.

Seeking Technical Support: Students should promptly seek assistance from designated technical support channels or other responsible entities within the university when encountering technical, organisational, and personal issues. They must understand when to report situations and be made to feel empowered to do so even if something has gone wrong through their own error.

Addressing Emotional Impacts: Students should raise awareness about the emotional impacts of data breaches and seek support if experiencing feelings of anger, fear, anxiety, depression, mistrust, or other emotions. they should use university resources such as counselling services to address any emotional distress caused by data breaches. They must recognise the emotional dimensions and risks associated with data breaches and avoid ignoring negative feelings that could potentially lead to long-term health concerns.

Self-Learning and Awareness: Engage in self-learning to stay informed about recent developments in data breach protection and understand the risks associated whether technical, organisational, or personal with data breaches. It is important to see this as a process of continual evolution which is part of their life skillset.

7-3-2 Recommendations for Faculty Members

Responsible Use of Technology: Faculty members should prioritise responsible use of technology to uphold the integrity of university systems. This involves adhering to usage conditions for both hardware and software and regularly installing and updating antivirus and firewall programmes to protect against emerging threats. Frequent password updates and stringent practices against sharing passwords are essential to prevent unauthorised access. By following these practices, faculty members play a crucial role in safeguarding university systems from potential security breaches.

Proper Use of Email : Faculty members should avoid opening unsolicited emails or clicking on suspicious links that could potentially introduce malware or facilitate hacking. Given their role in handling student personal data for academic purposes, it is essential for faculty to use official university email systems and networks for any data transfers or processing to ensure security.

Secure Classroom Practices: In classrooms equipped with shared computers, faculty members should diligently log out from the university system after each use to prevent inadvertent data leakage. This simple yet critical practice helps protect sensitive information from unauthorised access and ensures that subsequent users cannot view or alter personal data. By maintaining strict adherence to this protocol, faculty contribute significantly to

the overall security of the university's data management system and protecting the privacy of all users.

Participate in Training and Share Knowledge :Faculty members should actively engage in the university’s training programmes and advocate for their expansion to enhance information security awareness. Training faculty on data security is crucial, as they play a pivotal role in influencing students to adopt effective security practices. By sharing their own experiences and best practices with students, faculty members significantly contribute to creating a more informed and secure academic community.

Compliance and Data Protection: Adherence to data protection policies and regulations set by the university is essential for safeguarding personal data. Faculty members must ensure that personal data is collected and stored securely, in line with established guidelines, to protect student privacy. Additionally, compliance with university regulations concerning data creation, collection and data storage is vital, especially when handling large volumes of students' personal data and more sensitive personal data. This commitment to data protection supports the overall integrity of the university’s data management practices.

Seek Emotional Support When Needed :Faculty members should feel comfortable addressing and mitigating emotional impacts when observed, without hesitation or embarrassment. It is important for them to be open about their emotional responses and seek psychological or social counselling through the university's communication channels as needed. By sharing their concerns about privacy and emotional well-being, faculty can alleviate stress and manage their emotions more effectively, which can positively impact their teaching roles.

7-3-3 Recommendations for Managers Involved in Security Management

Validate Software Licenses and Effectiveness: Regularly validate the licenses and contracts of antivirus protection programmes to ensure their

legality and effectiveness. This process helps maintain software reliability and robust protection against security threats.

Generate Utilisation Reports: Produce regular reports detailing the usage trends of hardware and software within the institution. These reports provide insights into technological needs, usage patterns, and areas for improvement, aiding decisions on technology management and upgrades.

Provide Antivirus Recommendations: Create and maintain a comprehensive list of suitable antivirus software for use by both students and faculty. Ensure this list is easily accessible and prominently displayed within the user interface.

Monitor Compliance and Identify Vulnerabilities: Continuously monitor adherence to information security policies and identify potential vulnerabilities. This vigilance helps maintain a secure environment and address weaknesses proactively.

Develop and Implement Data Management Policies: Focus on developing and implementing comprehensive data management policies with an emphasis on data security. Ensure these policies are clearly communicated to all stakeholders.

Communicate Security Vulnerabilities: Inform users, including faculty and students, about identified security vulnerabilities. Prioritising and addressing these vulnerabilities enhance security measures and fosters improved collaboration.

Facilitate Comprehensive Training Programmes: Oversee the implementation of thorough data security training programmes for faculty, staff, and students. Equip the university community with the knowledge and skills needed to protect sensitive information effectively.

Encourage Collaboration Between Universities: Promote collaboration with other universities to share best practices and insights related to data security management. Such collaborative efforts can enhance data security across institutions.

Address Emotional Aspects of Data Breaches: Establish policies to consider the emotional impact of data breaches. Outline support mechanisms and resources for those affected by breaches.

Prioritise Emotional Well-being: Provide access to counselling services and support resources for students, faculty, and staff affected by data breaches. Implement training programmes to raise awareness about emotional impacts and coping strategies.

Foster Transparency and Communication: Create a culture of transparency and open communication within the university community and processes that enable better engagement which addresses the emotional concerns related to data breaches promptly and effectively.

7-3-4 Recommendations for Universities- Leadership, Governance Structures, Funding, and Audit

Establish a Specialised Cybersecurity Team: Forming a dedicated team responsible for monitoring, managing, and responding to cybersecurity threats. This team should comprise qualified employees with expertise in various aspects of data security—technical, organisational, and emotional—to effectively address the repercussions of data security breaches.

Develop Comprehensive Cybersecurity Policies: Create and implement clear policies that define data protection and incident response procedures, covering all technical, organisational, and personal aspects. Ensure these policies align with the new data protection law, which emphasises data minimisation—a priority confirmed by study participants, including students and faculty members. Regularly review and update these policies and communicate them effectively to all stakeholders. Additionally, develop policies to mitigate the effects of data breaches, such as providing financial compensation or other forms of support to affected individuals.

Improve Incident Response Plans: Develop detailed incident response plans that include containment measures, communication strategies, and recovery protocols. These plans should address the repercussions of data breaches

across technical, organisational, and personal dimensions. Regularly test these plans through simulations and drills to ensure their effectiveness.

Promote a Security-Aware Culture: Implement regular awareness and training programmes on data security and breach response for managers, faculty, staff, and students. Emphasise the importance of individual responsibility in protecting data and recognising potential threats. Given the risks in Saudi society, such as overconfidence and empathy, it is crucial to educate individuals about the importance of protecting sensitive data. Ensure that individuals are aware of access to counselling services and support programmes to help them deal with the psychological and emotional consequences of data breaches, which are as important as the technical and organisational aspects.

Establish Clear Reporting Channels: Create accessible and well-publicised channels for reporting data breaches and suspicious activities. Ensure all stakeholders know how to report incidents and the steps that will be taken in response.

Allocate Sufficient Budget for Cybersecurity: Ensure adequate financial resources are allocated to cybersecurity initiatives, including acquiring advanced security technologies, software updates and licenses, hiring qualified personnel, and ongoing training programmes. Allocate a budget for recovering from data breaches, considering all technical, organisational, and personal risks. Additionally, allocate funds to cover financial or moral compensation for those affected by data breaches.

7-4 Future Research

Given the identified perceptions regarding the technical implications of data breaches, there is a need for further empirical investigation to better identify the specific mechanisms and mitigation strategies associated with each identified aspect, namely the loss of data or digital assets, disruptions in university networks, and disturbances in system functionality. This knowledge exists in sectors but is protected and not made explicit thus preventing others from putting in place clear prevention strategies. It is more known in some regulatory environments but needs to develop in the HEI sector globally. Within this

context, exploring the alignment between managerial perspectives and the actual technical vulnerabilities within university settings could offer valuable insights. Future research could involve a comprehensive analysis of recent data breach incidents for enhancing data security measures in academic institutions.

Whilst this study's findings indicated a low reported frequency of data breaches according to participants' perceptions in the included universities, they also highlighted the need for greater transparency in reporting such incidents. Therefore, undertaking a longitudinal study to trace the evolution of data breach trends, including near misses, in Saudi HE institutions over an extended period would be valuable. This would enable a better understanding of the changing nature of threats, vulnerabilities, and the effectiveness of countermeasures implemented by institutions. Additionally, it would provide insights into emerging risks and inform proactive strategies for future preparedness.

Future work could explore several organisational aspects, particularly investigating factors that influence individual practices contributing to data breaches, such as password sharing. As part of this, examining the relationship between security awareness, training programmes, and the adoption of secure practices among people would be valuable. It would be important to identify strategies to enhance individuals' awareness and adherence to security policies.

In addition, the study's findings underscore the profound implications of data breaches on the reputation and trustworthiness of educational institutions. Data is fundamental to the functioning of universities, and their reputation is of paramount importance in enhancing their standing in both local and international university rankings. Whilst this study provides initial insights into the influence of reputation and trust, future research could conduct a more in-depth exploration, such as investigating how incidents of data breaches influence public perception, institutional credibility, and stakeholder trust. Such research would offer valuable guidance for reputation management strategies.

The data management landscape in SA is formally governed by the regulations set forth by the Saudi Data Security Governance and Management Organisation, operating within the framework of the national organisation for

data management. Within this regulatory context, significant provisions have been established to oversee data security processes. It is recommended that further empirical research be undertaken to assess the extent of adherence by HE institutions to this established framework. The present study, involving field visits to the headquarters of two universities, revealed the existence of data management offices within these institutions. A subsequent research study could explore more profoundly evaluating the specific roles and tasks undertaken by these data management offices, shedding light on their effectiveness and contribution to data management practices within the HE sector.

Although this dissertation does not specifically explore the legal risks and impacts of data breaches in depth (although this was touched upon), it recommends a comprehensive study to assess the real-world impact of the Personal Data Protection Law PDPL in SA. Exploring how HE institutions are adapting to the PDPL, the challenges they face, and the overall effectiveness of the PDPL in protecting personal data. This includes an evaluation of Privacy Impact Assessment (PIA) practices by investigating the methodologies employed by universities in conducting PIAs, as mandated by the PDPL. It would also be beneficial to evaluate the effectiveness of PIAs in identifying and mitigating potential privacy risks associated with the launch of services based on user's personal data. In addition, further research could examine the awareness levels and perceptions of users regarding data privacy in SA. This could include an investigation into how well users understand their rights, such as consent withdrawal and access to personal data, and an assessment of their satisfaction with the measures taken by HE institutions to protect their privacy.

Other research could evaluate the effectiveness of penalties outlined in the PDPL and the enforcement mechanisms in place. It could assess whether the prescribed penalties serve as adequate deterrents for non-compliance and whether regulatory authorities have been effective in ensuring adherence to the law.

Additionally, building on the emotional impacts identified in the study, future research should investigate the specific mechanisms influencing individuals'

emotional responses to data breaches. Exploring gender-based and age-related variations in emotional reactions can provide a more comprehensive understanding of the emotional dimensions surrounding data breaches. A deeper examination of gender-related variables, such as societal expectations, cultural norms, and individual coping mechanisms, could elucidate the complex interplay between gender, culture and emotional responses in the context of data breaches. Furthermore, the heightened emotional susceptibility observed in specific age groups, particularly those aged 25–34 and 35–44, prompts further investigation into the intersectionality of age, hormonal changes, and psychosocial factors. Longitudinal studies tracking emotional responses over time and correlating these with hormonal fluctuations could provide valuable insights into the evolving nature of individuals' reactions to data breaches across different life stages.

Future research could undertake an independent or comparative exploration of emotional reactions. The study's qualitative findings from interviews underscore the need for a deeper exploration into individual emotional reactions following data breaches, given the diverse set of emotions elicited by such incidents. The survey results indicate that anger received the highest endorsement, closely followed by fear as the predominant emotional impact. To enhance understanding, further research should independently investigate each emotional reaction. Future studies should examine contributing risk factors, variations across individuals, and effective strategies to manage or control these emotional responses. Notably, preliminary findings highlight disparities in the duration of anger and fear reactions among affected individuals, suggesting nuanced differences between those two emotional responses (Chatterjee et al., 2019). Consequently, a research recommendation is proposed for comparative studies that specifically examine distinct emotional reactions, such as anger versus fear or shock versus anxiety. This comparative analysis should include factors influencing their emergence, development, and mitigation strategies, with a specific focus on demographic comparisons to elucidate key variations in emotional responses.

Future studies may benefit from focusing specifically on one category within the HE to thoroughly explore the effects of data breaches within that contextual

group with very specific data types. Focusing specifically on one category, e.g., students within a particular discipline context will enable a more in-depth analysis of the effects of data breaches on key variables. The study's outcomes reveal noticeable variations in perceptions of data breaches among distinct groups and universities. The results suggest that cultural and social intricacies play a crucial role in shaping the data breach landscape. The observed disparities in perspectives underscore the importance of a nuanced understanding of the socio-cultural context, as these factors significantly influence the interpretation of and response to data breach incidents

This research insight also confirms the need for future investigations to explore more deeply the complex interplay between cultural and social factors. Given the diverse international contexts examined in the literature, there is an opportunity to investigate the cross-cultural implications of data breaches in HE institutions. An international comparative analysis of emotional and organisational impacts across different cultural settings could provide valuable insights into how responses and coping mechanisms vary. Additionally, research should consider how crossing language barriers influences these responses. Lastly, considering the rapid growth of technology and its increasing impact on HE institutions, ongoing research is needed to stay abreast of emerging trends and potential shifts in the multidimensional risks and implications of data breaches.

7-5 Conclusion

A synthesis of the primary findings, recommendations, and contributions highlights the importance of exploring data breaches in Saudi university settings. The results emphasise the complexity of the issue, with managers, faculty, and students offering varied perspectives. By identifying technical, organisational, and personal (emotional) risks and impacts, the study has provided a comprehensive analysis of the intricacies of data breaches within the Saudi higher education (HE) context.

Building upon these findings, the recommendations presented in this chapter offer actionable insights tailored to address data breaches. From prioritising the alignment of technological infrastructure with cybersecurity standards to

advocating for comprehensive training programmes, collaborative initiatives, and emotional support services, these recommendations serve as a roadmap for Saudi universities in fortifying their data security measures.

Beyond the actionable recommendations, this chapter underscores the broader contributions of the research. By advancing knowledge on the effects of data breaches, tailoring strategies to the Saudi context, enhancing data protection measures, and strengthening cybersecurity awareness, this study contributes to the development of data security within HE. Its support for Saudi Vision 2030, collaboration with national initiatives, and exploration of psychological impacts showcase the research's alignment with broader national goals and societal well-being.

This synthesis of contributions, findings, and recommendations lays the foundation for more secure HE landscapes, fostering a culture of data security and strengthening institutions against ever-evolving threats. It is anticipated that the researcher will return to Saudi Arabia to educate others and implement change in practice, given her enhanced expertise, equipping her university employer with the knowledge and strategies necessary to thrive in the digital age while preserving the integrity and security of their data.

References

Abraham, R., Schneider, J., vom Brocke, J., 2019. Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Abu Musa, A., 2004. The importance of the risks of electronic accounting information systems, an applied study on Saudi establishments. Trade and Finance Journal 1–54.

Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., Aldehim, G., 2018. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. International Journal of Cyber Warfare and Terrorism (IJCWT) 8, 46–59.

Acquisti, A., Friedman, A., Telang, R., 2006. Is There a Cost to Privacy Breaches? An Event Study 19.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D., 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4. https://doi.org/10.1093/cybsec/tyy006

Ahmad, A., Ruighaver, A.B., Teo, W.T., 2005. An information-centric approach to data security in organizations, in: TENCON 2005 - 2005 IEEE Region 10 Conference. Presented at the TENCON 2005 - 2005 IEEE Region 10 Conference, pp. 1–5. https://doi.org/10.1109/TENCON.2005.301322

Akan, M.F., Karim, M.R., Chowdhury, A.M.K., 2019. An analysis of Arabic-English translation: Problems and prospects. Advances in Language and Literary Studies 10, 58–65.
Al Amro, S., 2017. Cybercrime in Saudi Arabia: fact or fiction? International journal of computer science issues 14, 36–42. https://doi.org/10.20943/01201702.3642
Al Omran, H., 2011. Awareness of information security among faculty members in universities: a case study for Majmaah University. Arab Federation for Libraries and Information 10–44.
Al Shelash, A., 2020. The reality of the competitive advantages of universities and professional colleges in the Kingdom of Saudi Arabia An analytical study using the SWAT analysis and ways to improve them in the light of the two approaches to comprehensive quality and strategic planning. The Scientific Journal of the Faculty of Education - Assiut University 36.
Alabdulatif, A., 2018. Cybercrime and Analysis of Laws in Kingdome of Saudi Arabia. ProQuest Dissertations Publishing.
Alaqla, A., 2010. Requirements for applying e-learning environments in Saudi universities. Journal of Specific Education Research 2010, 53–68. https://doi.org/10.21608/mbse.2010.143730
AlAtiwi, S., 2010. Studying the relationship between information technology, constructivist theory, university environment and globalization: A proposed model for developing human capital in the era of globalization. The Arab Journal for Security Studies and Training (Saudi Arabia). URL http://yarab.yabesh.ir/yarab/handle/yad/328352 (accessed 9.17.21).
Al-Attar, M.M., 2017. The role of the family and kindergartens in developing the value of childhood among pre-school children in the Kingdom of Saudi Arabia. Al Baha University Journal for Human Sciences. 2.
AlAwdah, A., 2021. Obstacles to managing e-learning in Al-Ahsa in the Kingdom of Saudi Arabia in light of the Corona pandemic. The Scientific Journal of the Faculty of Education - Assiut University 37, 474–506. https://doi.org/10.21608/mfes.2021.173805
Albarrak, A.I., 2011. Evaluation of users information security practices at King Saud University Hospitals. Global business and management research 3, 1-.
Albreathin, R.A. bin H., 2020. A proposed vision for developing digital citizenship values among university students in light of the Kingdom's Vision 2030. Culture Association for Development 20, 61–92.
Albrechtsen, E., Hovden, J., 2009. The information security digital divide between information security managers and users. Computers & Security 28, 476–490. https://doi.org/10.1016/j.cose.2009.01.003
Al-Dunaibat, M., Shawabkeh, A., Al-Baqour, K., 2020. The role of human resource management processes in achieving information security: an applied study on Saudi public universities. Management & Economics Research Journal 2, 1–23.
Alexander, V.D., Thomas, H., Cronin, A., Fielding, J., Moran-Ellis, J., 2008. Mixed methods. Researching social life 3, 125–144.
Alghadyan, S.A.R., 2018. Forms of Crimes of Cyber blackmailing and their Motives and their Psychological Implications from the Point of View of Teachers, Members of the Committee and Psychological Counselors. Journal of Security Research 27, 157–226.
Al-Ghathar, K., Al-Subaih, A., 2012. The state of information security in the Kingdom of Saudi Arabia. Journal of Information Studies. 189–205.

Al-Habadan, T., 2021. The role of strategic planning in developing the performance of academic leaders in Saudi universities. Journal of the Faculty of Education (Assiut) 37, 71–103. https://doi.org/10.21608/mfes.2021.210168
Alhubaishy, A., Aljuhani, A., 2021. The challenges of instructors' and students' attitudes in digital transformation: A case study of Saudi Universities. Educ Inf Technol. https://doi.org/10.1007/s10639-021-10491-6
Alison Jane Pickard, 2017. Research Methods in Information. Facet Publishing, London, UNKNOWN.
Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., Janicke, H., 2020. A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied sciences 10, 3660-. https://doi.org/10.3390/app10103660
Al-Kaysi, M.I., 2015. Morals and manners in Islam: A guide to Islamic Adab. Kube Publishing Ltd.
Alkhudary, J., Salami, H., Klebi, N., 2020. Cyber security and artificial intelligence in Saudi universities. Journal of University performance Development (JUPD) 12, 217–233. https://doi.org/10.21608/jpud.2020.170391
Al-Maliki, N.S.J., 2023. The Saudi citizen between leading change 2030 and promoting the concept of responsible citizenship. URL https://scpmagazine.com/single-article.php?path=catagories/ar/%D8%A7%D9%84%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA%20%D8%A7%D9%84%D8%A5%D8%B1%D8%B4%D8%A7%D8%AF%D9%8A%D8%A9/%D8%A7%D9%84%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AA%D8%B1%D8%A8%D9%88%D9%8A%D8%A9/article54461/ (accessed 12.6.23).
Al-Mukhaita, M.Y., 2021. Social factors of youth becoming victims of cybercrimes: A field study in the city of Hofuf. Social Service Journal 70, 265–288.
Al-Mulhim, R.A., Al-Zamil, L.A., Al-Dossary, F.M., 2020. Cyber-attacks on Saudi Arabia Environment. International Journal of Computer Networks and Communications Security 8, 26–31. https://doi.org/10.47277/IJCNCS/8(3)1
Al-Mutawa, A.S.S., 2020. How Aware are Students of the Faculty of Education In Shakra of Anti-Cybercrime and How to Enhance that Educationally? Journal of Educational Sciences 290–373.
Almutrajiy, A., 2021. The impact of individual values on social behavior: honesty and modesty. Mafahim Journal for Philosophical and Humanistic Studies 4, 59–75.
ALOtaibi, S., AlMufeez, K., 2021. The Digital Transformation Governance in Educational Administrations in the Kingdom of Saudi Arabia in the light of International Practices. 1 66, 192–216. https://doi.org/10.33193/JALHSS.66.2021.462
Al-Otaibi, W.S., Al-Shammari, M.M., Ata, A.I., Ibrahim, T.A., Malkawi, H.F., Alkhuzaim, K.M., 2021. The Role of Saudi Universities in Enhancing Students' Digital Citizenship: University of Hail as a Model. Turkish Online Journal of Qualitative Inquiry 12.
Al-Qahtani, A.M., 2010. The social values and customs of domestic workers and the values and customs of the Saudi family (Thesis). Naif Arab University for Security Sciences, College of Social Sciences, Department of Sociology, 2010.
Al-Qahtani, Manal.M., 2021. The Contributions of Social Work to Reducing the Risks of Cybercrime Is a Study Applied to Members of the Educational Staff of the College of Social Work at Princess Nourah Bint Abdulrahman University. ournal of Educational Sciences and Human Studies 54–82.
Al-Qahtani, N., 2019. Awareness of cybersecurity among Saudi university students from a social perspective: a field study. Social Society in Sharjah 36, 85–120.

Alqurashi, R.K., 2020. Cyber Attacks and Impacts: A Case Study in Saudi Arabia. IJATCSE 9, 217–224. https://doi.org/10.30534/ijatcse/2020/33912020
Al-Rodiman, A., 2013. The application of Shari'ah and international human rights law in Saudi Arabia.
Alsadhan, A., 2015. Difficulties facing the application of e-learning system at Shaqra University from the prespective of specialists. Faculty of Education Journal-Mansoura University 40, 356–390.
Al-Sadhan, M., 2020. Requirements to achieve cyber security for management information systems at King Saud University. Faculty of Education Journal-Mansoura University 1–29.
Alsahafiy, M.A.H., 2019. A proposed model to raise awareness of cybersecurity among computer teachers in general education: an analytical study on the education administration in Jeddah Governorate. Journal of Scientific Research in Education 20, 493–534.
Alshammari, A., 2017. The university administration challenges in emerging Saudi universities and ways of confrontation it. Faculty of Education Journal- Ain Shams University 41, 61–117.
Al-Shanbari, H.A., 1998. The scientific and technical information system in Saudi higher education: a systems approach. ProQuest Dissertations Publishing.
Al-Sheety, E., 2014. Evaluation of information security and privacy policies in educational institutions in the Kingdom of Saudi Arabia: an empirical study on Qassim University. Journal of the Egyptian Association for Information Systems and Computer Technology 14, 11–24. https://doi.org/10.21608/jstc.2014.119253
AlSulaimi, A.M., 2022. Saudi Citizens' Awareness of Cyber Protection Methods. p193-236.
Alzahrani, A., Alomar, K., 2016. Information Security Issues and Threats in Saudi Arabia: A Research Survey. International journal of computer science issues 13, 129–135. https://doi.org/10.20943/01201606.129135
Alzahrani, A.Y., 2020. Cyber security strategies in light of modern technologies and challenges: a comparative study. URL http://repository.nauss.edu.sa//handle/123456789/66656 (accessed 9.1.21).
Alzamil, Z.A., 2018. Information security practice in Saudi Arabia: case study on Saudi organizations. Information & Computer Security 26, 568–583. https://doi.org/10.1108/ICS-01-2018-0006
Alzuhair, N.F., Alkhuzaim, K.M., Almutairi, D.T., 2022. A Proposal to Include the Image of the Saudi Personality in Middle School English Books in Light of Saudi Arabia's Vision 2030. Journal of Higher Education Theory & Practice 22.
Amani Qalyobi, 2022. The role of faculty members in promoting digital citizenship for their students: Umm Al-Qura University as a model. Journal of Umm Al-Qura University for Educational and Psychological Sciences 14, 263–290. https://doi.org/10.54940/ep95298808
Andress, J., 2019. Foundations of Information Security: A Straightforward Introduction. No Starch Press.
Angelis, J.N., Miller, J.C., 2020. An Empirical Investigation of the Effects of Individuality on Responses to Data Theft Crimes. IEEE transactions on engineering management 1–14. https://doi.org/10.1109/TEM.2020.2974742
Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Areishi, G., Al-Dossary, S., 2018. The role of higher education institutions in promoting a culture of information security in society. King Fahd National Library 24, 302–373.
Arutyunov, V.V., 2017. On the training of highly qualified scientific staff in the field of information security. Scientific and technical information processing 44, 64–68. https://doi.org/10.3103/S0147688217010075
ARWU, 2021. World University Rankings - 2020 | Saudi Arabia Universities in Top 1000 universities | Academic Ranking of World Universities - 2020 | Shanghai Ranking - 2020. URL http://www.shanghairanking.com/World-University-Rankings-2020/Saudi-Arabia.html (accessed 5.24.21).
Asadullah, A., Faik, I., Kankanhalli, A., 2018. Digital Platforms: A Review and Future Directions. PACIS 248.
Asel, G., Al-Aifan, A., 2014. Information Security in Saudi Universities: A Study of King Abdulaziz University. King Fahd National Library 20, 250–289.
Atim, Z.A.H., 2020. Evidence In The Saudi Electronic Transaction System, A Comparative Study With The Uncitral Model Laws. J. Legal Ethical & Regul. Isses 23, 1.
Atrews, R.A., 2020. Cybenvarfare: Threats, Security, Attacks, and Impact. Journal of Information Warfare 19, 17–28.
Ayereby, M.P.-M., 2018. Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems. ProQuest Dissertations Publishing.
Bada, M., Nurse, J.R.C., 2020. Chapter 4 - The social and psychological impact of cyberattacks, in: Benson, V., Mcalaney, J. (Eds.), Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp. 73–92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6
Badie, N., Lashkari, A.H., 2012. A new evaluation criteria for effective security awareness in computer risk management based on AHP. Journal of Basic and Applied Scientific Research 2, 9331–9347.
Baig, A., 2023. Understanding Saudi Arabia's Personal Data Protection Law (PDPL) - Securiti. URL https://securiti.ai/saudi-arabia-personal-data-protection-law/ (accessed 12.5.23).
BBC, 2021. Afghanistan: MoD shared more than 250 Afghan interpreters' details on email. BBC News.
BBC, 2020. Blackbaud Hack: Universities lose data to ransomware attack. BBC News.
Beaudin, K., 2017. The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches. New Directions for Institutional Research 2016, 37–48. https://doi.org/10.1002/ir.20202
Beaudin, K., 2015. College and university data breaches: regulating higher education cybersecurity under state and federal law. Journal of college and university law 41, 657-.
Bell, E., Bryman, A., Harley, B., 2022. Business research methods. Oxford university press.
Bentley, J.M., Ma, L., 2020. Testing perceptions of organizational apologies after a data breach crisis. Public relations review 46. https://doi.org/10.1016/j.pubrev.2020.101975
Bhargav-Spantzel, A., Squicciarini, A.C., Modi, S., Young, M., Bertino, E., Elliott, S.J., 2007. Privacy preserving multi-factor authentication with biometrics. Journal of computer security 15, 529–560. https://doi.org/10.3233/JCS-2007-15503
Bilgic, A., Hoogensen Gjørv, G., Wilcock, C., 2019. Trust, Distrust, and Security: An Untrustworthy Immigrant in a Trusting Community. Political psychology 40, 1283–1296. https://doi.org/10.1111/pops.12613

Bisogni, F., Asghari, H., 2020. An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws. Journal of information policy (University Park, Pa.) 10, 45–82. https://doi.org/10.5325/jinfopoli.10.2020.0045
Bisson, D., 2020. 7 Data Breaches Caused by Human Error | Venafi. URL https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role (accessed 4.14.21).
Blaikie, N., Priest, J., 2019. Designing Social Research: The Logic of Anticipation. Polity Press, Newark.
Bland, C.J., Schmitz, C.C., 1986. Characteristics of the successful researcher and implications for faculty development. Academic medicine 61, 22–31. https://doi.org/10.1097/00001888-198601000-00003
Bongiovanni, I., 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & security 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003
Borgman, C.L., 2018. Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier. Berkeley Technology Law Journal 33, 365–412. https://doi.org/10.15779/Z38B56D489
Brannen, J., 2016. Mixing Methods: Qualitative and Quantitative Research / edited by Julia Brannen (Thomas Coram Research Unit, Institute of Education)., First edition. ed. Routledge, London.
Bryman, A., 2016. Social Research Methods. Oxford university press.
Caminal, R., Di Paolo, A., 2019. YOUR LANGUAGE OR MINE? THE NONCOMMUNICATIVE BENEFITS OF LANGUAGE SKILLS. Economic inquiry 57, 726–750. https://doi.org/10.1111/ecin.12542
Carlton, M., Levy, Y., 2015. Expert assessment of the top platform independent cybersecurity skills for non-IT professionals, in: SoutheastCon 2015. Presented at the SoutheastCon 2015, pp. 1–6. https://doi.org/10.1109/SECON.2015.7132932
Chan, H., Mubarak, S., 2012. Significance of information security awareness in the higher education sector. International Journal of Computer Applications 60.
Chapman, D.J., 2019. How safe is your data? Cyber-security in higher education. Oxford : Higher Education Policy Institute: 2019 6.
Chatterjee, S., Gao, X., Sarkar, S., Uzmanoglu, C., 2019. Reacting to the scope of a data breach: The differential role of fear and anger. Journal of business research 101, 183–193. https://doi.org/10.1016/j.jbusres.2019.04.024
Chua, H.N., Wong, S.F., Low, Y.C., Chang, Y., 2018. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and informatics 35, 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005
Church-Morel, A., Bartel-Radic, A., 2016. Skills, Identity, and Power: The Multifaceted Concept of Language Diversity. Management international (Montréal) 21, 12–24. https://doi.org/10.7202/1052494ar
Clark, S., 2019. Oregon State University reports IT security incident. Life at OSU. URL https://today.oregonstate.edu/news/oregon-state-university-reports-it-security-incident (accessed 4.14.21).
Clark, V.L.P., Ivankova, N.V., 2016. Mixed Methods Research: A Guide to the Field. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320. https://doi.org/10.4135/9781483398341
Clarke, M., 2012. Integrity and Commitment in the Anthropology of Islam, in: Articulating Islam: Anthropological Approaches to Muslim Worlds. Springer, pp. 209–227.

Cohen, J., 2019. UConn Health email breach compromises data from 326,000 patients. Modern Healthcare. URL https://www.modernhealthcare.com/article/20190226/NEWS/190229939/uconn-health-email-breach-compromises-data-from-326-000-patients (accessed 4.14.21).
Cohen, L., Manion, L., Morrison, K., 2002. Research methods in education. routledge.
Collins, J., Vincenzo A Sainato, David N Khey, 2011. Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. International journal of cyber criminology 5, 794-.
Coombs, W.T., Holladay, S.J., Claeys, A.-S., 2016. Debunking the myth of denial's effectiveness in crisis communication: context matters. Journal of Communication Management 20, 381–395. https://doi.org/10.1108/JCOM-06-2016-0042
Creswell, J., Creswell, D., 2018. Research design: qualitative, quantitative, and mixed methods approaches / John W. Creswell and J. David Creswell., 5th edition, International student edition. ed. Los Angeles ; Sage.
Creswell, J.W., Creswell, D., 2018. Research design: qualitative, quantitative, and mixed methods approaches / John W. Creswell and J. David Creswell., 5th edition, International student edition. ed. Los Angeles ; Sage.
Creswell, J.W., Plano Clark, V.L., 2006. Designing and Conducting Mixed Methods Research. SAGE Publications Inc. URL https://us.sagepub.com/en-us/nam/designing-and-conducting-mixed-methods-research/book241842 (accessed 10.25.23).
Croasmun, J.T., Ostrom, L., 2011a. Using Likert-Type Scales in the Social Sciences. Journal of Adult Education 40, 19–22.
Croasmun, J.T., Ostrom, L., 2011b. Using likert-type scales in the social sciences. Journal of adult education 40, 19–22.
CSRC, C.C., 2021. Cyber Attack - Glossary | CSRC. URL https://csrc.nist.gov/glossary/term/cyber_attack (accessed 11.14.21).
CST, 2023. Maintaining the Privacy of Personal Data. URL https://www.cst.gov.sa/en/RulesandSystems/privacy/Pages/default.aspx (accessed 12.5.23).
Curtis, J., 2018. University of Greenwich fined £120,000 for breach of sensitive data. IT PRO. URL https://www.itpro.co.uk/data-breaches/31170/university-of-greenwich-fined-120000-for-breach-of-sensitive-data (accessed 5.12.21).
Curtis, S.R., Carre, J.R., Jones, D.N., 2018. Consumer security behaviors and trust following a data breach. Managerial auditing journal 33, 425–435. https://doi.org/10.1108/MAJ-11-2017-1692
Dai, F., 2017. The SAGE Encyclopedia of Communication Research Methods. SAGE Publications, Inc. https://doi.org/10.4135/9781483381411
Daines, R., 2023. LibGuides: Statistics Resources: Independent Samples T-test. URL https://resources.nu.edu/statsresources/IndependentSamples (accessed 9.28.23).
Das, S., 2020. A Risk-reduction-based Incentivization Model for Human-centered Multi-factor Authentication. ProQuest Dissertations Publishing.
Data, S., Authority, A.I., 2021. Data Management and Personal Data Protection Standards (2021).
Davidoff, S., 2019. Data Breaches: Crisis and Opportunity / Davidoff, Sherri., 1st edition. ed. Addison-Wesley Professional.

Dempsey, L., Dowling, M., Larkin, P., Murphy, K., 2016. Sensitive Interviewing in Qualitative Research. Research in Nursing & Health 39, 480–490. https://doi.org/10.1002/nur.21743
Denning, D.E.R., 1999. Information warfare and security / Dorothy E. Denning. Addison-Wesley, Reading, Ma. ; Harlow.
Denscombe, M., 2008. Communities of Practice: A Research Paradigm for the Mixed Methods Approach. Journal of mixed methods research 2, 270–283. https://doi.org/10.1177/1558689808316807
Densham, B., 2015. Three cyber-security strategies to mitigate the impact of a data breach. Network security 2015, 5–8. https://doi.org/10.1016/S1353-4858(15)70007-3
Denzin, N.K., 2017. The Research Act: A Theoretical Introduction to Sociological Methods. Routledge, New York. https://doi.org/10.4324/9781315134543
Detlor, B., 2010. Information management. International journal of information management 30, 103–108. https://doi.org/10.1016/j.ijinfomgt.2009.12.001
Dillon, R.L., Paté-Cornell, M.E., 2005. Including technical and security risks in the management of information systems: A programmatic risk management model. Systems engineering 8, 15–28. https://doi.org/10.1002/sys.20016
Doherty, N.F., Anastasakis, L., Fulford, H., 2009. The information security policy unpacked: A critical study of the content of university policies. International journal of information management 29, 449–457. https://doi.org/10.1016/j.ijinfomgt.2009.05.003
Dowell, D., Morrison, M., Heffernan, T., 2015. The changing importance of affective trust and cognitive trust across the relationship lifecycle: A study of business-to-business relationships. Industrial marketing management 44, 119–130. https://doi.org/10.1016/j.indmarman.2014.10.016
Eberlin, R.J., Tatum, B.C., 2008. Making just decisions: organizational justice, decision making, and leadership. Management Decision 46, 310–329. https://doi.org/10.1108/00251740810854177
Edwards, B., Hofmeyr, S., Forrest, S., 2016. Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity 2, 3–14. https://doi.org/10.1093/cybsec/tyw003
Elhai, J.D., Hall, B.J., 2016. Anxiety about internet hacking: Results from a community sample. Computers in human behavior 54, 180–185. https://doi.org/10.1016/j.chb.2015.07.057
Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. Industrial management + data systems 106, 345–361. https://doi.org/10.1108/02635570610653498
Essential Guide to Higher Education Data Breaches, 2021. URL https://www.collegeconsensus.com/resources/university-data-breaches/ (accessed 9.5.21).
Evans, M., He, Y., Maglaras, L., Janicke, H., 2019a. HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & Security 80, 74–89. https://doi.org/10.1016/j.cose.2018.09.002
Evans, M., He, Y., Maglaras, L., Yevseyeva, I., Janicke, H., 2019b. Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics 127, 109–119. https://doi.org/10.1016/j.ijmedinf.2019.04.019
Experts Bureau, 2023a. Bureau History. URL https://www.boe.gov.sa/en/About/Pages/default.aspx (accessed 12.5.23).

Experts Bureau, 2023b. The Basic Law of Governance in Saudi Arabia. URL https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1 (accessed 12.7.23).
Fetters, M.D., Curry, L.A., Creswell, J.W., 2013. Achieving Integration in Mixed Methods Designs—Principles and Practices. Health Services Research 48, 2134–2156. https://doi.org/10.1111/1475-6773.12117
Fidel, R., 2008. Are we there yet?: Mixed methods research in library and information science. Library & information science research 30, 265–272. https://doi.org/10.1016/j.lisr.2008.04.001
Fontani, G., Lodi, L., Felici, A., Corradeschi, F., Lupo, C., 2004. Attentional, emotional and hormonal data in subjects of different ages. Eur J Appl Physiol 92, 452–461. https://doi.org/10.1007/s00421-004-1108-3
Fowler, K., 2016. Data Breach Preparation and Response / Fowler, Kevvie., 1st edition. ed. Syngress.
Franke, T.M., Ho, T., Christie, C.A., 2012. The Chi-Square Test: Often Used and More Often Misinterpreted. The American journal of evaluation 33, 448–458. https://doi.org/10.1177/1098214011426594
Fugard, A., 2020. Thematic analysis / by Andi Fugard & Henry W. W. Potts ; edited by Paul Atkinson, Sara Delamont, Alexandru Cernat, Joseph W. Sakshaug & Richard A. Williams. SAGE Publications Ltd., London.
Fulford, H., Doherty, N.F., 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. Information management & computer security 11, 106–114. https://doi.org/10.1108/09685220310480381
Galletta, A., Cross, W., 2013. Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication / Anne Galletta., Qualitative Studies in Psychology. New York University Press, New York, NY.
Garba, S.B., 2004. Managing urban growth and development in the Riyadh metropolitan area, Saudi Arabia. Habitat international 28, 593–608. https://doi.org/10.1016/j.habitatint.2003.10.008
Garrison, C., 2010. Lessons Learned from University Data Breaches. Palmetto Business and Economic Review 13, 27–37.
Garrison, C., Ncube, M., 2011. A longitudinal analysis of data breaches. Information management & computer security 19, 216–230. https://doi.org/10.1108/09685221111173049
GASTAT, 2019. Introduction. General Authority for Statistics. URL https://www.stats.gov.sa/en/258 (accessed 5.22.21).
GDPR, 2021. Art. 4 GDPR – Definitions. General Data Protection Regulation (GDPR). URL https://gdpr-info.eu/art-4-gdpr/ (accessed 11.14.21).
Gentles, S., Charles, C., Ploeg, J., McKibbon, K.A., 2015. Sampling in Qualitative Research: Insights from an Overview of the Methods Literature. Qualitative report 20, 1772-. https://doi.org/10.46743/2160-3715/2015.2373
Gill, P., Stewart, K., Treasure, E., Chadwick, B., 2008. Methods of data collection in qualitative research: interviews and focus groups. British Dental Journal 204, 291–295. https://doi.org/10.1038/bdj.2008.192
Given, L.M., 2008. The Sage encyclopedia of qualitative research methods Lisa M. Given, editor. SAGE, Los Angeles, [Calif.] ; London.
Goddard, R.D., Villanova, P., 2006. Designing surveys and questionnaires for research. The psychology research handbook: A guide for graduate students and research assistants 114–125.
Gorshenin, A., 2018. Toward modern educational IT-ecosystems: from learning management systems to digital platforms, in: 2018 10th International Congress

on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, pp. 1–5.
Graham, R.W., 2005. Illustrating triangulation in mixed-methods nursing research. Nurse researcher 12.
Grix, J., 2010. The foundations of research / Jonathan Grix., 2nd ed. ed, Palgrave study skills. Palgrave Macmillan, Basingstoke.
Guellouh, L., 2023. The value of honesty in islam and its effects on development. Al-Hikma Journal for Islamic Studies 10, 136–155.
Guha, E.A., Indurkar, S.K., 2020. A Study on Cyber Crime and Data Breach Management. Research Journal of Engineering and Technology 11, 113–117. https://doi.org/10.5958/2321-581X.2020.00020.3
Guilford, J.P., 1954. Psychometric methods.
Habib, M.N., Jamal, W., Khalil, U., Khan, Z., 2021. Transforming universities in interactive digital platform: case of city university of science and information technology. Education and Information Technologies 26, 517–541.
Haleblian, J.J., Pfarrer, M.D., Kiley, J.T., 2017. High-Reputation Firms and Their Differential Acquisition Behaviors. Strategic management journal 38, 2237–2254. https://doi.org/10.1002/smj.2645
Hamby, S., Blount, Z., Smith, A., Jones, L., Mitchell, K., Taylor, E., 2018. Digital poly-victimization: The increasing importance of online crime and harassment to the burden of victimization. Journal of trauma & dissociation 19, 382–398. https://doi.org/10.1080/15299732.2018.1441357
Hamim, H., Rosyidah, R.U., 2023. The language of gratitude: "Alhamdulillah" as an expression of appreciation to improve well-being. Presented at the Conference Psychology and Flourishing Humanity (PFH 2023), Atlantis Press, pp. 225–234. https://doi.org/10.2991/978-2-38476-188-3_23
Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., Koutbi, M.E., 2019. Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. Procedia computer science 151, 1004–1009. https://doi.org/10.1016/j.procs.2019.04.141
Hands, A.S., 2022. Integrating quantitative and qualitative data in mixed methods research: An illustration. Canadian journal of information and library science 45, 1–20. https://doi.org/10.5206/cjilsrcsib.v45i1.10645
Hassanzadeh, Z., Marsen, S., Biddle, R., 2019. We're Here to Help: Company Image Repair and User Perception of Data Breaches.
Heffernan, T., Wilkins, S., Butt, M.M., 2018. Transnational higher education: The importance of institutional reputation, trust and student-university identification in international partnerships. International journal of educational management 32, 227–240. https://doi.org/10.1108/IJEM-05-2017-0122
Hewitt, R., Natzler, M., Higher Education Policy Institute (HEPI) (United Kingdom), 2019. Students or Data Subjects? What Students Think about University Data Security. HEPI Report 122 (No. 978-1-908240-56–9), Higher Education Policy Institute. Higher Education Policy Institute.
Holmes, M., 2015. Researching Emotional Reflexivity. Emotion Review 7, 61–66. https://doi.org/10.1177/1754073914544478
Holtfreter, R.E., Harrington, A., 2015. Data breach trends in the United States. Journal of financial crime 22, 242–260. https://doi.org/10.1108/JFC-09-2013-0055
Hughes-Lartey, K., Li, M., Botchey, F.E., Qin, Z., 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon 7, e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Hunt, G., 2021. Data Breaches - Universities a Growing Target for Data Theft. TitanHQ. URL https://www.titanhq.com/blog/universities-and-the-risk-from-cyber-crime/ (accessed 4.14.21).
IBM Security, 2020. Cost of a Data Breach Report 2020 82.
Irfandhi, K., Indrawati, A., Alexandra, D., Wanandi, K., Harisky, Y., Liawatimena, S., 2016. Implementation of Information Technology Service Management at Data And Information System Center of XYZ University. ComTech (Jakarta) 7, 41–52. https://doi.org/10.21512/comtech.v7i1.2220
Ishii, K., Komukai, T., 2016. A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K., in: Kreps, D., Fletcher, G., Griffiths, M. (Eds.), Technology and Intimacy: Choice or Coercion, IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, pp. 86–105. https://doi.org/10.1007/978-3-319-44805-3_8
ITProPortal, S.F., 2020. Half of UK universities suffered a data breach last year. ITProPortal. URL https://www.itproportal.com/news/half-of-uk-unversities-suffered-a-data-breach-last-year/ (accessed 4.14.21).
Jackson, K., 2019. Qualitative data analysis with NVivo / Kristi Jackson & Pat Bazeley., 3rd edition. ed. Sage Publications, London.
Jaeger, J., 2013. Human error, not hackers, cause most data breaches. Compliance week 10, 56-.
Jenkins, P., Potter, S., 2007. No more "personal notes"? Data protection policy and practice in Higher Education counselling services in the UK. British journal of guidance & counselling 35, 131–146. https://doi.org/10.1080/03069880701219849
Jeong, C.Y., Lee, S.-Y.T., Lim, J.-H., 2019. Information security breaches and IT security investments: Impacts on competitors. Information & Management 56, 681–695. https://doi.org/10.1016/j.im.2018.11.003
Jin, Y., Liu, B.F., Anagondahalli, D., Austin, L., 2014. Scale development for measuring publics' emotions in organizational crises. Public relations review 40, 509–518. https://doi.org/10.1016/j.pubrev.2014.04.007
Jin, Y., Pang, A., 2010. Future Directions of Crisis Communication Research: Emotions in Crisis - The Next Frontier. https://doi.org/10.1002/9781444314885.ch33
John W Coffey, 2019. Difficulties in Determining Data Breach Impacts. Journal of systemics, cybernetics and informatics 17, 9–13.
Johnson, R.B., Onwuegbuzie, A.J., 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. Educational researcher 33, 14–26. https://doi.org/10.3102/0013189X033007014
Joshi, C., Singh, U.K., 2017a. Information security risks management framework – A step towards mitigating security risks in university network. Journal of information security and applications 35, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006
Joshi, C., Singh, U.K., 2017b. Information security risks management framework – A step towards mitigating security risks in university network. Journal of information security and applications 35, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006
Jourdan, S.Z., 2010. An investigation of organizational information security risk analysis. ProQuest Dissertations Publishing.
Juma'h, A.H., Alnsour, Y., 2020. The effect of data breaches on company performance. International journal of accounting and information management 28, 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

Kacha, L., Zitouni, A., 2017. An Overview on Data Security in Cloud Computing, in: Cybernetics Approaches in Intelligent Systems, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 250–261. https://doi.org/10.1007/978-3-319-67618-0_23

Kaiser, G., Presmeg, N., 2019. Compendium for early career researchers in mathematics education. Springer Nature.

Karanja, E., 2017. The role of the chief information security officer in the management of IT security. Information and Computer Security 25, 300–329. https://doi.org/10.1108/ICS-02-2016-0013

Kashgary, A.D., 2011. The paradox of translating the untranslatable: Equivalence vs. non-equivalence in translating from Arabic into English. Journal of King Saud University - Languages and Translation 23, 47–57. https://doi.org/10.1016/j.jksult.2010.03.001

Khalaila, R., 2013. Translation of Questionnaires Into Arabic in Cross-Cultural Research: Techniques and Equivalence Issues. J Transcult Nurs 24, 363–370. https://doi.org/10.1177/1043659613493440

Khandkar, S.H., 2009. Open coding. University of Calgary 23, 2009.

Kim, H.J., Cameron, G.T., 2011. Emotions Matter in Crisis: The Role of Anger and Sadness in the Publics' Response to Crisis News Framing and Corporate Crisis Response. Communication research 38, 826–855. https://doi.org/10.1177/0093650210385813

Kim, J., 2017. Cyber-security in government: reducing the risk. Computer Fraud & Security 2017, 8–11. https://doi.org/10.1016/S1361-3723(17)30059-3

Kinzig, A.P., Ehrlich, P.R., Alston, L.J., Arrow, K., Barrett, S., Buchman, T.G., Daily, G.C., Levin, B., Levin, S., Oppenheimer, M., 2013. Social norms and global environmental challenges: the complex interaction of behaviors, values, and policy. BioScience 63, 164–175.

KSU, 2021a. King Saud University. URL https://ksu.edu.sa/en/about-ksu (accessed 5.23.21).

KSU, 2021b. King Saud University- colleges. URL https://ksu.edu.sa/en/colleges (accessed 5.23.21).

Kude, T., Hoehle, H., Sykes, T.A., 2017. Big data breaches and customer compensation strategies. International journal of operations & production management 37, 56–74. https://doi.org/10.1108/IJOPM-03-2015-0156

Labrecque, L.I., Markos, E., Swani, K., Peña, P., 2021. When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. Journal of business research 135, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

Larini, M., Barthes, A., 2018. Quantitative and statistical data in education: from data collection to data processing / Michel Larini, Angela Barthes., Science, society and new technologies series. Education set ; v. 2. ISTE Ltd, London, UK.

Leavy, P., 2017. Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches, 1st ed. Guilford Publications, New York.

Leavy, P., Hesse-Biber, S.N., 2006. Emergent Methods in Social Research. SAGE Publications Inc. US, Thousand Oaks. https://doi.org/10.4135/9781412984034

Likert, R., 1932. A technique for the measurement of attitudes. Archives of Psychology 22 140, 55–55.

Linda Bloomberg, Marie Volpe, 2008. Presenting Methodology and Research Approach. https://doi.org/10.4135/9781452226613.n3

Liu, C.-W., Huang, P., Lucas, H.C., 2020. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. Journal of management information systems 37, 758–787. https://doi.org/10.1080/07421222.2020.1790190

Louise, B., While, A., 1994. Collecting data using a semi-structured interview: a discussion paper. Journal of advanced nursing 19, 328–335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Maarouf, H., 2019. Pragmatism as a supportive paradigm for the mixed research approach: Conceptualizing the ontological, epistemological, and axiological stances of pragmatism. International Business Research 12, 1–12.

Maher, C., Hadfield, M., Hutchings, M., de Eyto, A., 2018. Ensuring Rigor in Qualitative Data Analysis: A Design Research Approach to Coding Combining NVivo With Traditional Material Methods. International journal of qualitative methods 17, 160940691878636-. https://doi.org/10.1177/1609406918786362

Malavet, J.N., 2017. Cyber Security in Higher Education: Accuracy of Resources Utilized by Information Technology Departments to Prevent Data Breaches. ProQuest Dissertations Publishing.

Marks, A., Rezgui, Y., 2009. A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing, in: 2009 International Conference on Management and Service Science. Presented at the 2009 International Conference on Management and Service Science, pp. 1–7. https://doi.org/10.1109/ICMSS.2009.5302667

Marshall, B., Cardon, P., Poddar, A., Fontenot, R., 2013. Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. Journal of Computer Information Systems 54, 11–22. https://doi.org/10.1080/08874417.2013.11645667

Mason, M., 2010. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. Forum : Qualitative Social Research 11, n/a.

McClurg, J., 2015. Cybersecurity in Higher Education: Oversight and Due Diligence. ProQuest Dissertations Publishing.

MCIT, 2013. 2.6 billion cybercrime costs in Saudi Arabia. Ministry of Communications and Information Technology. URL https://www.mcit.gov.sa/en/media-center/news/93609 (accessed 4.16.21).

McKim, C.A., 2017. The Value of Mixed Methods Research: A Mixed Methods Study. Journal of mixed methods research 11, 202–222. https://doi.org/10.1177/1558689815607096

Meenagh, B., Tucker, L., 2023. Saudi Arabia's data protection law enters into force.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., Skourlas, C., 2014. Human factor and information security in higher education. Journal of systems and information technology 16, 210–221. https://doi.org/10.1108/JSIT-01-2014-0007

Miller, C., 2017. Count Me In: Quantitative Research in Asia-Pacific Affairs, in: Muddy Boots and Smart Suits. ISEAS–Yusof Ishak Institute Singapore, Singapore, pp. 73–92. https://doi.org/10.1355/9789814459792-007

Ministry of education, 2021. The Emergence of the Ministry. Ministry of education. URL https://www.moe.gov.sa/en/aboutus/aboutministry/Pages/About.aspx (accessed 5.22.21).

Mohsin, M., Main, C., 2024. Mashallah Meaning: When to Say It, Translation, & More. wikiHow. URL https://www.wikihow.com/Mashallah-Meaning (accessed 7.17.24).

Mollick, J.S., 2006. Do Concerns about Error in Data and Access to Data Affect Students' Feeling of Alienation? Journal of information privacy & security 2, 29–45. https://doi.org/10.1080/15536548.2006.10855785
Morgan, R.M., Hunt, S.D., 1994. The Commitment-Trust Theory of Relationship Marketing. Journal of Marketing 58, 20-. https://doi.org/10.2307/1252308
Morse, J.M., 2000. Determining Sample Size. Qualitative health research 10, 3–5. https://doi.org/10.1177/104973200129118183
Muhammed, R., 2000. Psychological alienation and its relationship to creativity among university students. Alarabi Lel Maaref Bookstore.
Mukthar, A., Sultan, M., 2017. Big Data Analytics for Higher Education in Saudi Arabia 15, 22.
Nadim, A., 2014. Security and privacy of data and information of faculty members in Saudi universities on social media sites on the Internet: a field study. King Fahd National Library 20, 208–249.
Nazaha, 2023. URL https://nazaha.gov.sa/ (accessed 11.20.23).
NCA, 2023. National Cybersecurity Authority. URL https://nca.gov.sa/en/about (accessed 12.5.23).
NCSC, 2018. Implementing the Cloud Security Principles. NCSC. URL https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles (accessed 4.16.21).
NDMO, 2023. National Data Management Office. URL https://sdaia.gov.sa/ar/Sectors/Ndmo/Pages/default.aspx (accessed 11.28.23).
Newcomer, K.E., Hatry, H.P., Wholey, J.S., 2015. Handbook of Practical Program Evaluation, Essential texts for nonprofit and public leadership and management. John Wiley & Sons, Incorporated, Hoboken.
O'Cathain, A., Murphy, E., Nicholl, J., 2007. Why, and how, mixed methods research is undertaken in health services research in England: a mixed methods study. BMC health services research 7, 85–85. https://doi.org/10.1186/1472-6963-7-85
Onwuegbuzie, A.J., Leech, N.L., 2005. On Becoming a Pragmatic Researcher: The Importance of Combining Quantitative and Qualitative Research Methodologies. International journal of social research methodology 8, 375–387. https://doi.org/10.1080/13645570500402447
Paat, Y.-F., Markham, C., 2021. Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Social work in mental health 19, 18–40. https://doi.org/10.1080/15332985.2020.1845281
Padayachee, K., 2013. A conceptual opportunity-based framework to mitigate the insider threat. IEEE, pp. 1–8. https://doi.org/10.1109/ISSA.2013.6641060
Padyab, A., Ståhlbröst, A., 2018. Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. Info (Cambridge, England) 20, 528–544. https://doi.org/10.1108/DPRG-05-2018-0023
Parr, C., 2013. 5 examples of fraud that universities can learn from. Times Higher Education (THE). URL https://www.timeshighereducation.com/features/5-examples-of-fraud-that-universities-can-learn-from/2008457.article (accessed 10.4.21).
Parvaiz, G., Mufti, O., Wahab, M., 2016. Pragmatism for Mixed Method Research at Higher Education Level. Business & Economic Review 8, 67–78. https://doi.org/10.22547/BER/8.2.5
Patel, S.K., Rathod, V.R., Prajapati, J.B., 2013. Comparative analysis of web security in open source content management system, in: 2013 International Conference on Intelligent Systems and Signal Processing (ISSP). Presented at the 2013

International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 344–349. https://doi.org/10.1109/ISSP.2013.6526932
Penberthy, W.J., 2020. Remediation Approaches for the Recovery of Trust after a Privacy Breach at an Educational Institution: An Exploratory Case Study. ProQuest Dissertations Publishing.
Perrow, C., 2011. Software Failures, Security, and Cyberattacks. TATuP 20, 41–46. https://doi.org/10.14512/tatup.20.3.41
Pickard, A., 2013. Research methods in information / Alison Jane Pickard ; with contributions from Sue Childs, Elizabeth Lomas, Julie McLeod and Andrew K. Shenton. Facet Publishing, London.
Pickard, A.J., 2013. Research methods in information / Alison Jane Pickard ; with contributions from Sue Childs, Elizabeth Lomas, Julie McLeod and Andrew K. Shenton., Second edition. ed. Facet, London.
Pilotti, M.A., Abdulhadi, E.J., Algouhi, T.A., Salameh, M.H., 2021. The new and the old: Responses to change in the Kingdom of Saudi Arabia. Journal of International Women's Studies 22, 341–358.
Pirim, T., James, T., Boswell, K., Reithel, B., Barkhi, R., 2008. An Empirical Investigation of an Individual's Perceived Need for Privacy and Security. International journal of information security and privacy 2, 42–53. https://doi.org/10.4018/jisp.2008010103
Plano Clark, V.L., 2019. Meaningful integration within mixed methods studies: Identifying why, what, when, and how. Contemporary educational psychology 57, 106–111. https://doi.org/10.1016/j.cedpsych.2019.01.007
Pranggono, B., Arabo, A., 2021. COVID-19 pandemic cybersecurity issues. Internet technology letters 4, n/a. https://doi.org/10.1002/itl2.247
PRC, 2021. Data Breaches | Privacy Rights Clearinghouse. URL https://privacyrights.org/data-breaches (accessed 5.12.21).
Rajab, M., Eydgahi, A., 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Computers & security 80, 211–223. https://doi.org/10.1016/j.cose.2018.09.016
Redscan Research: Over half of UK universities reported a data breach to the ICO in 2019/20, 2020. . Respiratory Therapeutics Week.
Routsis, V., 2020. Informational Privacy and Self-Disclosure Online: A Critical Mixed-Methods Approach to Social Media. UCL University College London.
Saeid, O.D.M., 2019. Community awareness of information crimes among university students: A study from the perspective of community organization in social service. Social service magazine 61, 335–375.
Saheb, M.H., 2013. University information security policy: case study. Cybrarians journal.
Saleh, R.H., 2020. The Role of Social Media in Providing New Opportunities in Work and Life: A Qualitative Study of Professional Saudi Arabian Women. Université d'Ottawa/University of Ottawa.
Sandelowski, M., 2000. Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies. Research in nursing & health 23, 246–255. https://doi.org/10.1002/1098-240X(200006)23:3<246::AID-NUR9>3.0.CO;2-H
Santos, N., Koblitz, B., 2008. Security in distributed metadata catalogues. Concurrency and Computation: Practice and Experience 20, 1995–2007.

Sarkar, M.K., Kumar, S., 2016. A framework to ensure data storage security in cloud computing, in: 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, pp. 1–4.
Saudi Press Agency, 2023. Saudi Arabia Participates in Celebrations of World Human Rights Day. URL https://spa.gov.sa/ (accessed 12.7.23).
SDAIA, 2023a. Saudi Authority for Data and Artificial Intelligence. Laws and Regulations. Saudi Authority for Data and Artificial Intelligence. URL https://sdaia.gov.sa:443/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx (accessed 12.5.23).
SDAIA, 2023b. Data Quality Guide | Open data portal. URL https://od.data.gov.sa/ar/guidelines/data-quality (accessed 11.28.23).
Sen, R., Borle, S., 2015. Estimating the Contextual Risk of Data Breach: An Empirical Approach. Journal of Management Information Systems 32, 314–341. https://doi.org/10.1080/07421222.2015.1063315
Shaikh, R., Sasikumar, M., 2015. Data classification for achieving security in cloud computing. Procedia computer science 45, 493–498.
Shankaranarayanan, G., Cai, Y., 2006. Supporting data quality management in decision-making. Decision support systems 42, 302–317.
Sheikha, A., 2015. Local development is a condition for the success of emerging universities. Economic news. URL https://www.aleqt.com/2015/04/25/article_952466.html (accessed 9.17.21).
Silverman, D.L., 2007. Data security breaches: the state of notification laws. Intellectual property & technology law journal 19, 5-.
Sinan, S.M.A., 2003. Psychological alienation and general anxiety among a sample of female students at Umm Al-Qura University in Mecca, both users and non-users of the Internet: a comparative study. Makkah.
Singh, A.N., Gupta, M.P., Ojha, A., 2014. Identifying factors of 'organizational information security management.' Journal of enterprise information management 27, 644–667. https://doi.org/10.1108/JEIM-07-2013-0052
Slusky, L., Partow-Navid, P., 2012. Students Information Security Practices and Awareness. Journal of Information Privacy and Security 8, 3–26. https://doi.org/10.1080/15536548.2012.10845664
Smith, L., Abouammoh, A., 2013a. Higher Education in Saudi Arabia: Reforms, Challenges and Priorities, in: Smith, L., Abouammoh, A. (Eds.), Higher Education in Saudi Arabia, Higher Education Dynamics. Springer Netherlands, Dordrecht, pp. 1–12. https://doi.org/10.1007/978-94-007-6321-0_1
Smith, L., Abouammoh, A., 2013b. Higher Education in Saudi Arabia: Achievements, Challenges and Opportunities / edited by Larry Smith, Abdulrahman Abouammoh., Higher Education Dynamics, 40. Springer, Dordrecht ; London.
Sohrabi Safa, N., Von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Computers & security 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006
Sokulski, C.C., Barros, M.V., Salvador, R., Broday, E.E., de Francisco, A.C., 2022. Trends in renewable electricity generation in the G20 countries: An analysis of the 1990–2020 period. Sustainability 14, 2084.
Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: A systematic review of quantitative studies. Information management & computer security 22, 42–75. https://doi.org/10.1108/IMCS-08-2012-0045
South & City College Birmingham, 2021. Cyber-Security Breach: How We're Responding. South & City College Birmingham. URL

https://www.sccb.ac.uk/latest-news/item/801-cyber-security-breach-how-we-re-responding (accessed 9.5.21).
Staff, R., 2013. Saudi Arabia says hackers sabotage government websites. Reuters.
Stokes, M., 2015. The utility of incident response plans for data breaches in higher education. ProQuest Dissertations Publishing.
Straub, D.W., Welke, R.J., 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS quarterly 22, 441–469. https://doi.org/10.2307/249551
Student news - Beware of email scams - University of Nottingham, 2023. . University of Nottingham. URL https://www.nottingham.ac.uk/currentstudents/news/beware-of-email-scams-1 (accessed 10.17.23).
Subedi, B.P., 2016. Using Likert Type Data in Social Science Research: Confusion, Issues and Challenges 3.
Syed, R., Dhillon, G., 2015. Dynamics of Data Breaches in Online SocialNetworks: Understanding Threats toOrganizational Information SecurityReputation. Thirty Sixth International Conference on Information System 1–17.
Taddicken, M., 2014. The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. Journal of computer-mediated communication 19, 248–273. https://doi.org/10.1111/jcc4.12052
Taibah University, 2021. Taibah University | About . URL https://www.taibahu.edu.sa/Pages/en/CustomPage.aspx?ID=47 (accessed 5.24.21).
Tanantaputra, J., Chong, C.W., Rahman, M.S., 2017. Influence of individual factors on concern for information privacy (CFIP), a perspective from Malaysian higher educational students. Library review (Glasgow) 66, 182–200. https://doi.org/10.1108/LR-05-2016-0043
Teddlie, C., Tashakkori, A., 2009. Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences. Sage.
Tuli, F., 2010. The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives. Ethiopian Journal of Education and Sciences 6.
Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Atanda, A., Ukwandu, E., 2021. Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene. https://doi.org/10.48550/arXiv.2103.06621
Ulven, J.B., Wangen, G., 2021a. A Systematic Review of Cybersecurity Risks in Higher Education. Future internet 13, 39-. https://doi.org/10.3390/fi13020039
Ulven, J.B., Wangen, G., 2021b. A Systematic Review of Cybersecurity Risks in Higher Education. Future internet 13, 39-. https://doi.org/10.3390/fi13020039
University of Maine, 2015. Media Report on Theft of Laptop Containing Student Roster Data. UMaine News. URL https://umaine.edu/news/blog/2015/02/19/media-report-on-theft-of-laptop-containing-student-roster-data/ (accessed 9.13.21).
U.S.News, 2021. The Best Universities in Saudi Arabia, Ranked . URL https://www.usnews.com/education/best-global-universities/saudi-arabia (accessed 5.24.21).
Varshini, R., 2019. Who and Why Make DDoS Attacks on The Site of Colleges and Universities ? GBHackers on Security | #1 Globally Trusted Cyber Security News Platform. URL https://staging.gbhackers.com/ddos-attack-colleges-universities/ (accessed 10.17.23).

Veltsos, J.R., 2012. An Analysis of Data Breach Notifications as Negative News. Business Communication Quarterly 75, 192–207. https://doi.org/10.1177/1080569912443081
Violet, Cropper, K., Panis, A., Davis, K., 2019. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. Emotion 19, 1353–1365. https://doi.org/10.1037/emo0000508
VISION 2030, 2022. A Sustainable Saudi Vision - Vision 2030. URL https://www.vision2030.gov.sa/v2030/a-sustainable-saudi-vision/ (accessed 6.3.22).
Vollstedt, M., Rezat, S., 2019. An introduction to grounded theory with a special focus on axial coding and the coding paradigm. Compendium for early career researchers in mathematics education 13, 81–100.
Wang, P., Johnson, C., 2018. Cybersecurity incident handling: a case study of the Equifax data breach. Issues in Information Systems 19.
Waqar, A., Raza, A., Abbas, H., Khurram Khan, M., 2013. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. Journal of Network and Computer Applications 36, 235–248. https://doi.org/10.1016/j.jnca.2012.09.001
Wilson, T., Maimon, D., Sobesto, B., Cukier, M., 2015. The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. Journal of Research in Crime and Delinquency 52, 829–855. https://doi.org/10.1177/0022427815587761
Yerby, J., Floyd, K., 2018a. Faculty and Staff Information Security Awareness and Behaviors. Journal of The Colloquium for Information Systems Security Education 6, 23–23.
Yerby, J., Floyd, K., 2018b. Faculty and Staff Information Security Awareness and Behaviors. Journal of The Colloquium for Information Systems Security Education 6, 23–23.
Yin, R.K., 2012. Case study methods, in: APA Handbook of Research Methods in Psychology, Vol 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological, APA Handbooks in Psychology®. American Psychological Association, Washington, DC, US, pp. 141–155. https://doi.org/10.1037/13620-009
Yusuf, S., 2021. Digital Technology and Inequality: The Impact on Arab Countries. Economic Research Forum (ERF).
Yvonne Feilzer, M., 2010. Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm. Journal of mixed methods research 4, 6–16. https://doi.org/10.1177/1558689809349691
Zhang, R., Gong, J., Ma, S., Firdaus, A., Xu, J., 2023. Automatic Coding Mechanisms for Open-Ended Questions in Journalism Surveys: An Application Guide. Digital Journalism 11, 321–342. https://doi.org/10.1080/21670811.2022.2037006
Zhang, Z., Gupta, B.B., 2018. Social media security and trustworthiness: Overview and new direction. Future generation computer systems 86, 914–925. https://doi.org/10.1016/j.future.2016.10.007
Zhe, D., Qinghong, W., Naizheng, S., Yuhan, Z., 2017. Study on Data Security Policy Based on Cloud Storage. Presented at the 2017 Ieee 3rd international conference on Big Data Security on cloud (BigDataSecurity), pp. 145–149. https://doi.org/10.1109/BigDataSecurity.2017.12
Zubcoff, J.J., Vaquer, L., Mazón, J.-N., Maciá, F., Garrigós, I., Fuster, A., Carcel, J.V., 2016. The university as an open data ecosystem. International journal of design &

nature and ecodynamics 11, 250–257. https://doi.org/10.2495/DNE-V11-N3-250-257

APPENDICES

Appendix A: Permission letter

Dear Dean of Scientific Research,

My name is Haifa Almugamisi, and I am a doctoral candidate, from the College of Faculty of Arts and Humanities at University College London's Department of Information Studies as well as a lecturer at Taibah University. My PhD study is sponsored by the Government of the Kingdom of Saudi Arabia to study in the UK.

I am writing to ask for your permission to carry out a research study at the university of King Saud. Please note that I am in addition approaching other universities. However, I am particularly keen that King Saud University engages in this work as a leading university. I hope that the work I will undertake will be of some benefit to your university.

My research aims to examine the general landscape of data breaches in Saudi universities, the strategies of data management, and the universities background in mitigating data breach incidents. It also investigates the multidimensional effects of data breaches on university's stakeholders. The research will use two methods for data collection, which will be (in-person or online) interviews with IT managers, and online surveys distributed to students and academic staff in three Saudi universities, namely King Saud University, King Abdelaziz University, and Taibah University. The intention of the research is to identify best practice in Saudi universities and areas for information security enhancements as information security challenges rise. As well as complying with Saudi research requirements, the research is subject to the UK Data Protection Act and UK ethical compliance requirements. Every effort will be made to protect the identities of those who take part.

The findings of the research will be used for the PhD and in addition will be published in academic articles and presentations. In addition, I would share the findings with you and hope that this will be of benefit to you.

I would greatly appreciate receiving your permission. If you require any additional information, please contact me at [redacted].

Note: A copy of the survey's questions (some changes might be made to the survey questions after they are tested), a supervisor letter, a scholarship letter, and a student statement are attached to this letter.

Thank you for your consideration of this request.

Kind regards,

Haifa Almugamisi

Information Studies/PhD Student

University College London

سعادة عميد البحث العلمي..... حفظكم الله

السلام عليكم ورحمة الله وبركاته.

ارجو من سعادتكم الموافقة ومنحي الاذن لأجراء دراسة بحثية في جامعتكم المحترمة، حيث انني طالبة دكتوراه في قسم دراسات المعلومات بكلية لندن الجامعية (UCL) في المملكة المتحدة، وعضو هيئة تدريس (محاضر) في جامعة طيبة في المملكة العربية السعودية، مبتعثه من قبل وزارة التعليم.

يهدف بحثي إلى دراسة المشهد العام لخروقات البيانات في الجامعات السعودية، واستراتيجيات إدارة البيانات، والتعرف على خلفية وخبرة الجامعات السعودية في التخفيف من حوادث انتهاكات البيانات. كما يبحث في الآثار متعددة الأبعاد لانتهاكات البيانات على المنتسبين للجامعة. سيستخدم البحث طريقتين لجمع البيانات، وهما المقابلات (الشخصية أو عبر الإنترنت) مع مديري تكنولوجيا المعلومات في جامعتكم المحترمة، ومسح عبر الانترنت سيوزع على الطلاب وأعضاء هيئة التدريس.

يستهدف البحث ثلاث جامعات سعودية وهم جامعة الملك سعود، وجامعة الملك عبد العزيز، وجامعة طيبة. ولكن نحن مهتمين بشكل خاص على أن جامعة الملك سعود تشارك في هذا العمل كجامعة رائدة ونظرا لمكانتها المرموقة بين الجامعات السعودية، لكي نتمكن من تحديد أفضل الممارسات في الجامعات السعودية ومجالات تحسين أمن المعلومات مع تزايد تحديات أمن المعلومات. يخضع البحث لقانون حماية البيانات ومتطلبات الامتثال الأخلاقي في المملكة المتحدة بالإضافة إلى انه سيتم الامتثال لمتطلبات البحث السعودي كذلك. سيتم بذل كل جهد لحماية هويات المشاركين. سوف تستخدم نتائج البحث للحصول على درجة الدكتوراه بالإضافة إلى نشرها في المقالات الأكاديمية والعروض التقديمية. كما أيضا سيتم مشاركة نتائج البحث معكم على أمل ان تكون مفيدة لكم.

سأكون ممتنا للغاية لمساعدتكم بالموافقة على المشاركة في البحث، إذا كنت بحاجة إلى أي معلومات إضافية، يرجى الاتصال بي على [redacted]

ملاحظة: يتم إرفاق نسخة من أسئلة الاستبيان (قد يتم اجراء تغييرات طفيفة على أسئلة الاستبيان بعد اختبارها). أيضا في المرفقات نسخة من خطاب المشرف، واثبات المنحة للباحث والحالة الدراسية.

شكرا جزيلا على اهتمامكم.

هيفاء المغامسي

دراسات المعلومات / طالب دكتوراه

كلية لندن الجامعية UCL

Appendix B: Interview Invitation Form

Interview Invitation Form

استمارة دعوة المقابلة

سيدي العزيز / سيدتي

يُطلب منك المشاركة في دراسة بحثية أجرتها الآنسة هيفاء المغامسي، طالبة دكتوراه، من كلية الآداب والعلوم الإنسانية في قسم دراسات المعلومات بكلية لندن الجامعيةUCL . البحث جزء من دراسة دكتوراة.

يهدف البحث إلى دراسة المشهد العام لخروقات البيانات في الجامعات السعودية، والتعلم من استراتيجياتها في إدارة البيانات، وخلفيتها في التخفيف من حوادث خرق البيانات الجامعية، والتحقيق في الآثار المتعددة الأبعاد لخرق البيانات على أصحاب المصلحة من الطلاب وأعضاء هيئة التدريس.

تم اختيارك كمشارك محتمل في هذه الدراسة بسبب مسؤولياتك الإدارية والإشرافية بشأن تكنولوجيا المعلومات وأمن البيانات في جامعتك الموقرة. لديك ضماننا الشخصي والمهني بأن خصوصيتك وسريتك سيتم احترامهما أثناء معالجة البيانات.

يتم توفير ورقة معلومات ونموذج الموافقة المصاحب. آمل أن تقوم بمراجعة هذه الأمور والتفكير في المشاركة في هذا البحث. أتطلع إلى الاستماع منك والإجابة على أي أسئلة أخرى قد تكون لديك. أتمنى أن تكون على استعداد لإجراء مقابلة.

تفضلوا بقبول فائق الاحترام،

الباحث

Dear Sir/ Madam,

You are asked to participate in a research study conducted by Miss. Haifa Almugamisi, doctoral candidate, from the College of Faculty of Arts and Humanities at the UCL Department of Information Studies.

The research is part of a PhD study. It aims to examine the general landscape of data breaches in Saudi universities, learn from their strategies in data management, and their background in mitigating university data breach incidents and investigate the multidimensional effects of data breaches on student and faculty stakeholders.

You were selected as a possible participant in this study due to your administrative and supervisory responsibilities on information technology and data security at your esteemed university.

You have our personal and professional assurance that your privacy and confidentiality will be respected during processing data. An information sheet and accompanying consent form is provided. I hope that you will review these and consider participating in this research. I look forward to hearing from you and answering any further questions you may have. I very much hope you will be willing to undertake an interview.

Yours Sincerely,

Researcher

Lecturer

Department of Information and Learning Resources

Taibah University, Saudi Arabia

PhD student

Department of Information Studies

University College London, United Kingdom

محاضر

قسم المعلومات ومصادر التعلم

جامعة طيبة، المملكة العربية السعودية

طالب دكتوراه

قسم دراسات المعلومات

جامعة كلية لندن، المملكة المتحدة

Appendix C: Participant Information Sheet for Managers

Participant Information Sheet for Managers

UCL Research Ethics Committee Approval ID Number: 21595/001

Title of Study: Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia.

Department: Information Studies

Name and Contact Details of the Researcher(s): Haifa Almugamisi

Telephone: [redacted] **Email:** [redacted]

Name and Contact Details of the Principal Researcher: Elizabeth Lomas

Telephone: [redacted] **Email**: [redacted]

We are pleased to invite you to participate in this research project. Please take the time to read the following information about your participation in the research should you choose to proceed with participation. If you need more information, please ask us on the contact details available on the form. We are very keen to ensure that everything is clear. You may organise a meeting to discuss this further without any pressure to formally take part in this project.

Overview

This research is being undertaken for a PhD from University College London in the United Kingdom. The results of the research may be published in journals and presented at conferences.

What is the project's purpose?

The research aims to examine the general landscape of data breaches in Saudi Universities, in order to explore current strategies in data management, and their effectiveness in mitigating University data breach incidents. It will investigate the multidimensional effects of data breaches on student and faculty stakeholders. The research hopes to contribute to understandings of data management by shedding light on the reality of data and information security management in one of the Middle East countries. The study will be undertaken through multiple case studies at Saudi Universities, namely, King Saud University, Taibah University, and King Abdelaziz University, with the aim of representing Saudi higher education institutions. The research relies on the use of surveys and semi-structured interviews as data collection tools. The period for taking part in interviews will be approximately three months, starting from January to March 2022. The interviews are being conducted with data security managers, IT managers, and others with information and data knowledge, in order to learn about their mitigation strategies, their experiences in managing personal data, and their beliefs about data breaches impacts. You have been approached for this interview because we believe you have this knowledge. However, if you are unsure about your suitability to participate then please do discuss this further.

Do I have to take part?

Taking part in this project is entirely voluntary. However, we believe that you can make a very important contribution to work which we hope will improve data and information security in Saudi Arabia. Your responses will be very valuable in enriching the research and as such we encourage you to participate. However, you have the right to decide whether to contribute or not. If you do choose to take part in the study, you will need to sign a consent form. You can withdraw without consequences of any kind, and you will be asked what you prefer to happen to the data you have provided up to that point. However, having taken part in your interview, if one month has elapsed since the interview then we can no longer withdraw you entirely from the work. This is because your responses will have been aggregated into the writing up.

What will happen to me if I take part?

Once you agree to participate, the researcher will contact you to determine your interview preferences. The interview will last approximately one hour, and you will have the freedom to choose the appropriate time between January and March 2022. *[Text for female participants in red and male participants in blue]* The interview will be held in the manner that suits you, either in person or remotely. Where it is held in person then we will follow all Covid-19 protocols that are in place at the time of the interview. A risk assessment will be conducted ahead of the interview so we can make sure that all safety precautions have been followed. Where it is conducted online then this will be via UCL Microsoft Teams unless there is another platform you prefer which is also secure.

The interview will be held in remotely via UCL Microsoft Teams unless there is another platform you prefer which is also secure.

Will I be recorded and how will the recorded media be used?

It will make the work of the researcher easier if the interview is recorded so that she can listen properly to what you are saying. However, the interview will only be recorded after your full consent. Alternatively, you may choose to be interviewed but not recorded in which case interview notes will be made.

If you agree then your interview will be recorded using UCL's Microsoft Teams Software. All recordings will be used for analysis only. No one outside the project will be allowed access to the original recordings. A transcript

What will be the format of the interview?

Since the interview will be semi-structured, you will be given a copy of the interview questions in advance, but you are likely to be asked other questions that flow from our discussions. All questions are optional. These will include optional demographic data questions such as age, gender and job title. These will be aggregated and used anonymously and all the data you provide will be used for purely scientific purposes. The interview will take approximately one hour.

How will my data be used?

We will analyse and code your data to obtain a picture of how all participants approach data breaches and views on security and impacts. Sample quotes may be used from your interview. However, every care will be taken to ensure that you remain anonymous in any outputs from the work. All data will be retained securely in line with UCL's retention policies and destroyed securely. Any recordings of interviews will be destroyed as soon transcriptions are finalised. All transcriptions will be kept until 1 year

after the completion of the PhD. The interview consent forms will be kept until 5 years after the completion of the PhD.

Will my taking part in this project be kept confidential?

Your personal data will be kept strictly confidential. A unique identifier will be assigned to link your contribution in the research to your interview responses in the way make your identity anonymised. Your audio files and transcripts will store on the reliable storage tools within UCL's systems, as the researcher only can access them. All data will be kept according to UCL's retention policies and in accordance with the UK Data Protection Act 2018. Further information on the management of research data at UCL is at the Privacy Notice here https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

Limits to confidentiality

Your confidentiality will be respected subject to legal constraints and professional guidelines in the UK and the SA.

What are the possible disadvantages and risks of taking part?

The potential risk is considered minimal. Data will be collected from you and your university officially within the permissions provided. You have a promise that the facts will be described in an accurate and fair manner and used for research purposes as set out. Every effort will be made to maintain your confidentiality.

Please note that very occasionally particular research projects are audited to ensure that all processes are being conducted legally and ethically. In such instance the audit team respect all the confidentiality parameters of the research. This is a safeguarding measure to ensure that research is appropriately conducted.

What are the possible benefits of taking part?

It's anticipated that by examining the current state of data breaches, mitigation strategies, and implications, the research will provide beneficial information that can be used to improve the management of data breaches locally and globally. This research will provide valuable information that will add to the body of knowledge in the field of data security, information technology, and education. It will also help provide an honourable image of the universities work environment and its development in the Middle East. You will be offered the opportunity to receive a copy of the completed thesis.

What if something goes wrong?

If you wish to raise a complaint, please contact the Principal Researcher Dr Elizabeth Lomas([redacted]). We will deal with your complaint as soon as possible.

If you still are not satisfied with the handling of your complaint, you can contact the Chair of the UCL Research Ethics Committee (ethics@ucl.ac.uk).

What will happen to the results of the research project?

A copy of the research thesis will be deposited with UCL and the British Library. It is likely that the work outputs will be published in one of the scientific journals and presented at national or international conferences.

Local Data Protection Privacy Notice

University College London (UCL) is the controller of this project, providing data protection responsibility, and can be contacted at (data-protection@ucl.ac.uk). For further information on the privacy notice, please click on the following link https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

Contact for further information

Researcher: Haifa Almugamisi: [redacted]

Project Supervisor: Dr Elizabeth Lomas: [redacted]

Please keep a copy of this information sheet in case you needed anything later.

Thank you for reading and considering contributing to this project.

ورقة معلومات المشاركين خاصة بالمدراء

رقم معرف لجنة الأخلاقيات: 21595/001

عنوان الدراسة: وجهات نظر متعددة لخروقات البيانات في مؤسسات التعليم العالي، دراسة حالة الجامعات في السعودية

القسم: دراسات المعلومات

اسم الباحث وتفاصيل الاتصال: هيفاء المغامسي

تليفون: [redacted]

اسم المشرف الرئيسي وتفاصيل الاتصال: اليزابيث لوماس

تليفون: [redacted] **ايميل:** [redacted]

يسعدنا دعوتكم للمشاركة في هذا المشروع البحثي. يرجى أخذ الوقت الكافي لقراءة المعلومات التالية حول مشاركتك في البحث إذا اخترت متابعة المشاركة. إذا كنت بحاجة إلى مزيد من المعلومات، فيرجى التواصل معنا من خلال تفاصيل الاتصال المتوفرة في النموذج. نحن حريصون جدًا على التأكد من أن كل شيء واضح. يمكنك تنظيم اجتماع لمناقشة هذا الأمر بشكل أكبر دون أي ضغط للمشاركة رسميًا في هذا المشروع.

نظرة عامة

يتم إجراء هذا البحث للحصول على درجة الدكتوراه من جامعة كوليدج لندن في المملكة المتحدة. يمكن نشر نتائج البحث في المجلات وعرضها في المؤتمرات.

ما هو الغرض من المشروع؟

يهدف البحث إلى دراسة المشهد العام لخروقات البيانات في الجامعات السعودية، لاستكشاف الاستراتيجيات المطبقة حاليا في إدارة البيانات، ومدى فاعليتها في التخفيف من حوادث خرق البيانات الجامعية. تحقق الدراسة أيضا في الآثار متعددة الأبعاد لانتهاكات البيانات على أصحاب المصلحة من الطلاب وأعضاء هيئة التدريس. حيث ان البحث يأمل في المساهمة في فهم إدارة البيانات من خلال تسليط الضوء على واقع إدارة أمن البيانات والمعلومات في إحدى دول الشرق الأوسط. لتمثيل مؤسسات التعليم العالي السعودية سيعتمد إجراء الدراسة على اسلوب دراسة حالات متعددة في الجامعات السعودية، وهي جامعة الملك سعود، وجامعة طيبة، وجامعة الملك عبد العزيز. من خلال استخدام الاستطلاعات المسحية والمقابلات شبة المنظمة كأدوات لجمع البيانات. ستكون فترة المشاركة في المقابلات حوالي ثلاثة أشهر، ابتداءً من يناير إلى مارس

2022. وستُجرى المقابلات مع مديري أمن البيانات ومديري تكنولوجيا المعلومات وغيرهم ممن لديهم خبرة ومعرفة بإدارة البيانات وذلك للتعرف على استراتيجيات التخفيف الخاصة بهم، والاستفادة من خبراتهم في إدارة البيانات الشخصية، والتعرف على وجهات نظرهم حول اثار انتهاكات البيانات المتعددة الابعاد.

لقد تم الاتصال بك لإجراء هذه المقابلة لأننا نعتقد أن لديك المعرفة المناسبة، ولكن إذا لم تكن متأكدًا من مدى ملاءمتك للمشاركة يرجى توضيح التفاصيل للباحث.

هل يجب على المشاركة؟

المشاركة في هذا المشروع تطوعية بالكامل. ولكن نعتقد ان مساهمتك مهمة للغاية في هذا البحث الذي يأمل ان يحسن من امن البيانات والمعلومات في المملكة العربية السعودية. لذا نشجعك على المشاركة حيث ان ردودك ستكون ذات قيمة كبيرة في إثراء البحث. علما انه لديك الحق الكامل فيما إذا كنت ترغب بالمساهمة من عدمها. ستحتاج إلى التوقيع على نموذج الموافقة المرفق في حالة اخترت المشاركة في الدراسة. مع ملاحظة انه يمكنك الانسحاب دون عواقب من أي نوع، وفي حالة انسحابك سيتم سؤالك ماذا تريد ان يحدث للبيانات التي قدمتها مسبقا. وسيتم قبول انسحابك قبل مضي شهر واحد من اجراء المقابلة، اما بعد ذلك فلا يمكننا سحبك بالكامل مع المشاركة خاصة إذا تم الانتهاء من جمع البيانات والتحضير لمرحلة التحليل والكتابة.

ماذا سيحدث لي إذا شاركت؟

بمجرد موافقتك على المشاركة، سيتصل بك الباحث لتحديد تفضيلات مقابلاتك. ستستغرق المقابلة حوالي ساعة واحدة، وسيكون لك الحرية في اختيار الوقت المناسب بين يناير ومارس عام 2022.

للمشاركات الاناث: ستُجرى المقابلة بالطريقة المناسبة لكي سواء حضورياً أو عن بُعد. عندما يتم إجراؤها حضورياً، فسوف يتم التقيد بجميع بروتوكولات Covid-19 المعمول بها في مقر العمل. سيتم إجراء تقييم للمخاطر قبل المقابلة حتى نتمكن من التأكد من اتباع جميع احتياطات السلامة. اما في حالة اختيارك اجراء المقابلة عبر الانترنت، فسيتم استخدام برنامج UCL Microsoft Teams ما لم يكن هناك نظام أساسي آخر تفضله يكون آمنًا أيضًا.

للمشاركين الذكور: سيتم اجراء المقابلة عن بعد من خلال برنامج UCL Microsoft Teams مالم يكون هناك نظام أساسي اخر تفضله ويكون امن

هل سيتم تسجيلي وكيف سيتم استخدام الوسائط المسجلة؟

تسجيل المقابلة سيسهل عمل الباحثة للاستماع بشكل صحيح إلى المعلومات المقدمة، ولكن لن يتم تسجيل المقابلة الا بعد موافقتك الكاملة. سنكون متفاهمين في حالة رفضك تسجيل المقابلة وسيتم الاعتماد على تدوين ملاحظات فقط. اما إذا وافقت، فسيتم تسجيل مقابلتك باستخدام برنامج Microsoft Teams الخاص بـ UCL. سيتم استخدام جميع التسجيلات للتحليل فقط. لن يُسمح لأي شخص خارج المشروع بالوصول إلى نسخة التسجيلات الأصلية.

كيف سيكون شكل المقابلة؟

نظرًا لأن المقابلة ستكون شبه منظمة، فسيتم إعطاؤك نسخة من أسئلة المقابلة مسبقًا، ولكن من المحتمل أن تُطرح عليك أسئلة أخرى تطرأ من مناقشاتنا. علما ان الإجابة على كل الأسئلة اختيارية. سيتضمن ذلك أسئلة البيانات الديموغرافية الاختيارية مثل العمر والجنس والمسمى الوظيفي. سيتم تجميعها واستخدامها بشكل مجهول وسيتم استخدام جميع البيانات .التي تقدمها لأغراض علمية بحتة. ستستغرق المقابلة حوالي ساعة.

كيف سيتم استخدام بياناتي؟

سنقوم بتحليل وترميز بياناتك للحصول على صورة لكيفية تعامل جميع المشاركين مع خروقات البيانات ووجهات النظر حول الأمان والتأثيرات. يمكن استخدام اقتباسات عينة من مقابلتك. ومع ذلك، سيتم اتخاذ كافة الإجراءات اللازمة لضمان عدم الكشف عن هويتك في أي مخرجات من العمل. سيتم الاحتفاظ بجميع البيانات بشكل آمن بما يتماشى مع سياسات الاحتفاظ الخاصة بشركة UCL ويتم إتلافها بشكل آمن .سيتم تدمير أي تسجيلات للمقابلات بمجرد الانتهاء من النسخ. سيتم الاحتفاظ بجميع النسخ حتى عام واحد بعد الانتهاء من الدكتوراه. سيتم الاحتفاظ باستمارات الموافقة على المقابلة حتى 5 سنوات بعد الانتهاء من الدكتوراه.

هل ستبقى مشاركتي في هذا المشروع سرية؟

سيتم الاحتفاظ ببياناتك الشخصية بسرية تامة. سيتم تعيين معرّف فريد لربط مساهمتك في البحث بإجابات المقابلة بالطريقة التي تجعل هويتك مجهولة. يمكن للباحث فقط الوصول إلى البيانات.

سيتم الاحتفاظ بجميع البيانات UCL سيتم تخزين ملفاتك الصوتية ونصوصك على أدوات التخزين الموثوقة داخل أنظمة ووفقًا لقانون حماية البيانات في المملكة المتحدة لعام 2018. يمكنك الاطلاع على UCL وفقًا لسياسات الاحتفاظ في وإشعار الخصوصية من خلال الرابط التالي UCL مزيد من المعلومات حول إدارة بيانات البحث في

https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

حدود السرية

سيتم احترام سريتك وفقًا للقيود القانونية والإرشادات المهنية في كلا من المملكة المتحدة والمملكة العربية السعودية.

ما هي العيوب والمخاطر المحتملة للمشاركة؟

تعتبر المخاطر المحتملة ضئيلة. سيتم جمع البيانات منك ومن جامعتك رسميًا ضمن الأذونات المقدمة. نوعدك بأنه سيتم وصف جميع بياناتك بطريقة دقيقة وعادلة واستخدامها لأغراض البحث. سيتم بذل اقصى الجهود للحفاظ على سريتك. يرجى ملاحظة أنه في بعض الأحيان يتم تدقيق مشاريع بحثية معينة لضمان إجراء جميع العمليات بشكل قانوني وأخلاقي. في مثل هذه الحالة، يحترم فريق التدقيق جميع معايير سرية البحث. علما ان هذا إجراء وقائي لضمان إجراء البحث بشكل مناسب.

ما هي فوائد ممكنة من المشاركة؟

من المتوقع أنه من خلال فحص الحالة الحالية لانتهاكات البيانات واستراتيجيات التخفيف والآثار المترتبة، سيوفر البحث معلومات مفيدة يمكن استخدامها لتحسين إدارة انتهاكات البيانات محليًا وعالميًا. سيوفر هذا البحث ايضا معلومات قيمة ستضيف إلى مجموعة المعرفة في مجال أمن البيانات وتكنولوجيا المعلومات والتعليم. كما سيساعد في تقديم صورة مشرفة عن بيئة عمل الجامعات وتطورها في الشرق الأوسط. ستتاح لك الفرصة للحصول على نسخة من الأطروحة المكتملة.

ماذا لو حدث خطأ ما؟

إذا كنت ترغب في تقديم شكوى، يرجى الاتصال بالباحثة الرئيسية الدكتورة إليزابيث لوماس (e.lomas@ucl.ac.uk). سنتعامل مع شكواك في أقرب وقت ممكن .إذا كنت لا تزال غير راضٍ عن التعامل مع شكواك، يمكنك الاتصال برئيس لجنة أخلاقيات البحث في جامعة لندن.(ethics@ucl.ac.uk)

ماذا سيحدث لنتائج مشروع البحث؟

سيتم إيداع نسخة من أطروحة البحث لدى UCL والمكتبة البريطانية. من المحتمل أن يتم نشر مخرجات العمل في إحدى المجلات العلمية وعرضها في المؤتمرات الوطنية أو الدولية.

إشعار خصوصية حماية البيانات المحلية

تعد كلية لندن الجامعية (UCL) المتحكم في هذا المشروع وتتحمل مسؤولية حماية البيانات، يمكنك التواصل مع إدارة البحث في الجامعة على الايميل التالي (data-protection@ucl.ac.uk). لمزيد من المعلومات حول إشعار الخصوصية يرجى النقر على الرابط التالي

https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

عناوين التواصل

الباحثة: هيفاء المغامسي [redacted] مشرفة المشروع: الدكتورة إليزابيث لوماس [redacted]

يرجى الاحتفاظ بنسخة من ورقة المعلومات هذه في حالة احتياجك لأي شيء لاحقًا.

شكرا جزيلا لك على قراءة المعلومات السابقة، مقدرين جدا تفكيرك في المساهمة بالمشروع

Appendix D: Consent Form for Managers

CONSENT FORM FOR MANAGERS

استمارة الموافقة للمديرين

Please complete this form after you have read the Information Sheet.

يرجى إكمال هذا النموذج بعد قراءة ورقة المعلومات

Title of Study: Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia

عنوان الدراسة: وجهات نظر متعددة لخروقات البيانات في مؤسسات التعليم العالي، دراسة حالة الجامعات في السعودية

Department: Information Studies

القسم: دراسات المعلومات

Name and Contact Details of the Researcher(s): Haifa Almugamisi

اسم الباحث وتفاصيل الاتصال: هيفاء المغامسي

h[redacted] : / ايميل Email : [redacted] /تليفون Telephone

Name and Contact Details of the Principal Researcher: Elizabeth Lomas

اسم الباحث الرئيسي وتفاصيل الاتصال: اليزابيث لوماس

[redacted] : / ايميل Email [redacted] : /تليفون Telephone

Name and Contact Details of the UCL Data Protection Officer:

اسم وتفاصيل الاتصال بمسؤول حماية البيانات فيUCL :

This study has been approved by the UCL Research Ethics Committee: Project ID number: 21595/001

تمت الموافقة على هذه الدراسة من قبل لجنة أخلاقيات البحث في UCL رقم معرف المشروع: 001/21595

Once you sign this consent form, you confirm your willingness to participate in this research, and you will be contacted to schedule an interview. You should read this consent form in conjunction with the information sheet provided. In addition, you should make sure you have asked any questions about the research to help inform your decision as to whether to participate. All information you provide will be used for research purposes. Your personal data will be collected in accordance with the UK Data Protection Laws (the General Data Protection Regulation and the UK Data Protection Act 2018. All operations related to the collection and processing of data in any form will follow the data protection policies of the University of UCL, because the university is the data controller. Every effort will be made to keep your data securely. Your contributions to this study will be anonymised, as the researcher will make every effort to conceal your identity, and to generate a unique identification code for you. All data will be retained in accordance with UCL's data policies and retention schedules. Further information is on the accompanying information sheet.

بمجرد التوقيع على نموذج الموافقة هذا، فإنك تؤكد رغبتك في المشاركة في هذا البحث، وسيتم الاتصال بك لتحديد موعد مقابلة. يجب عليك قراءة نموذج الموافقة هذا بالإضافة إلى ورقة المعلومات الملحقة معه. يجب عليك التأكد من أنك قد طرحت أي أسئلة حول البحث للمساعدة في اتخاذ قرارك بشأن المشاركة. سيتم استخدام جميع المعلومات التي تقدمها لأغراض البحث. سيتم جمع بياناتك الشخصية وفقًا لقوانين حماية البيانات في المملكة المتحدة (اللائحة العامة لحماية البيانات وقانون حماية البيانات في المملكة المتحدة لعام 2018. جميع العمليات المتعلقة بجمع البيانات ومعالجتها ستتبع سياسات حماية البيانات الخاصة بجامعةUCL، لكونها المتحكم في البيانات. سيتم بذل كل جهد للحفاظ على بياناتك بشكل آمن. ستكون مساهماتك في هذه الدراسة مجهولة المصدر، حيث سيبذل الباحث قصارى جهده لإخفاء هويتك، وإنشاء رمز تعريف فريد سيتم الاحتفاظ بجميع البيانات وفقًا لسياسات البيانات الخاصة بجامعة UCL وجداول الاحتفاظ بها. يرجى الاطلاع على ورقة المعلومات المرفقة للتعرف على مزيد من التفاصيل حول مشاركتك.

	Element **عناصر**	**Please tick the box** **يرجى وضع علامة في المربع**
1	I confirm that I have read and understood the Information Sheet for the above study. I have had an opportunity to consider the information and what will be expected of me. I have also had the opportunity to ask questions which have been answered to my satisfaction and I would like to take part in an individual interview.	
	أؤكد أنني قد قرأت وفهمت ورقة المعلومات الخاصة بالدراسة أعلاه. لقد أتيحت لي الفرصة للنظر في المعلومات وما هو متوقع مني. كما أتيحت لي الفرصة لطرح الأسئلة التي تم الرد عليها بشكل مرضي وأود المشاركة في مقابلة فردية.	
2	I understand that I will be able to withdraw my data up to a month after conducting the interview.	
	أدرك أنني سأتمكن من سحب بياناتي لمدة تصل إلى شهر بعد إجراء المقابلة.	
3	I understand that my personal information data will be used for the purposes explained to me which relate to the research as set out. I understand that according to data protection legislation, 'public task' will be the lawful basis for processing my data.	
	أفهم أنه سيتم استخدام بيانات معلوماتي الشخصية للأغراض الموضحة لي والمتعلقة بالبحث على النحو المبين. أفهم أنه وفقًا لتشريعات حماية البيانات، ستكون "المهمة العامة" هي الأساس القانوني لمعالجة بياناتي.	
4	I understand that I will remain anonymous in the research and be referred to with a unique identification code.	
	أفهم أنني سأظل مجهول الهوية في البحث وسيتم ربطي برمز تعريف فريد والاشارة إلى به.	
5	I understand that quotes may be used from my interview but nothing that would identify me will be used.	
	أفهم أنه يمكن استخدام الاقتباسات من مقابلتي، ولكن لن يتم استخدام أي شيء من شأنه تحديد هويتي.	
6	I understand that confidentiality will be respected subject to legal constraints and professional guidelines.	
	أفهم أنه سيتم احترام السرية وفقًا للقيود القانونية والمبادئ التوجيهية المهنية.	
7	I understand that my information may be subject to review by responsible individuals from the University for monitoring and audit purposes.	
	أفهم أن معلوماتي قد تخضع للمراجعة من قبل أفراد مسؤولين من الجامعة لأغراض المراقبة والتدقيق.	
8	I understand that I can withdraw within 1 month of the interview, and any personal data that I have provided will be deleted. I understand that my data will have been aggregated a month after conducting the interview.	
	أفهم أنه يمكنني الانسحاب في غضون شهر واحد من المقابلة، وسيتم حذف أي بيانات شخصية قدمتها. أفهم أنه سيتم تجميع بياناتي بعد شهر من إجراء المقابلة.	
9	I understand the potential benefits and risks of participating.	
	أنا أفهم الفوائد والمخاطر المحتملة للمشاركة.	
10	I understand that the data will not be made available to any commercial organisations but is solely the responsibility of the researcher undertaking this study.	
	أفهم أن البيانات لن تكون متاحة لأية منظمات تجارية وستكون فقط متاحة للباحث الذي يقوم بهذه الدراسة.	

11	I understand that I will not benefit financially from this study or from any possible outcome it may result in in the future.	
12	أفهم أنني لن أستفيد مالياً من هذه الدراسة أو من أي نتيجة محتملة قد تنتج عنها في المستقبل.	
13	I agree that my anonymised research data will not be archived for future use by other researchers.	
	أوافق على أن بياناتي البحثية مجهولة المصدر لن يتم أرشفتها لاستخدامها في المستقبل من قبل باحثين آخرين.	
14	I am aware of who I should contact if I wish to lodge a complaint.	
	أنا على علم بمن يجب أن أتصل به إذا كنت أرغب في تقديم شكوى.	
15	I voluntarily agree to take part in this study.	
	أوافق طواعية على المشاركة في هذه الدراسة.	
16	I understand my data will be retained in line with UCL's retention policies. Any recordings of interviews will be destroyed as soon transcriptions are finalised. All transcriptions will be kept until 1 year after the completion of the PhD. The interview consent forms will be kept until 5 years after the completion of the PhD.	
	أدرك أنه سيتم الاحتفاظ ببياناتي بما يتماشى مع سياسات الاحتفاظ في UCL. سيتم تدمير أي تسجيلات للمقابلات بمجرد الانتهاء من النسخ. سيتم الاحتفاظ بجميع النسخ حتى عام واحد بعد الانتهاء من الدكتوراه. سيتم الاحتفاظ باستمارات الموافقة على المقابلة حتى 5 سنوات بعد الانتهاء من الدكتوراه.	
17	I consent to my interview being audio/video recorded and understand that the recordings will be destroyed immediately following transcription. To note: If you do not want your participation recorded you can still take part in the study.	Yes/No
	أوافق على تسجيل مقابلتي بالصوت / الفيديو وأدرك أنه سيتم إتلاف التسجيلات فور نسخها. ملاحظة: إذا كنت لا تريد تسجيل مشاركتك، فلا يزال بإمكانك المشاركة في الدراسة	نعم / لا
18	I understand that the information I have submitted will be published as a thesis and I wish to receive a copy of it.	Yes/No
	أفهم أن المعلومات التي قدمتها سيتم نشرها كأطروحة بحث وأرغب في الحصول على نسخة منها.	نعم / لا

_____	_____	_____
Name of participant	Date	Signature
اسم المشارك	التاريخ	التوقيع
_____	_____	_____
Researcher	Date	Signature
اسم الباحث	التاريخ	التوقيع

- The UCL Data Protection Policy is available at the following link:

سياسة حماية بيانات جامعة UCL متاحة على الرابط التالي:

Policies | Legal Services - UCL – University College London

- The UCL Data Management Policy is available at:

سياسة إدارة بيانات جامعة UCL متاحة على:

Policies & funders' expectations | Library Services - UCL – University College London

- UCL's Privacy Notice can be viewed at:

يمكن الاطلاع على إشعار الخصوصية في جامعة UCL على:

https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

Appendix E: Participant Information Sheet for Survey Participants

Participant Information Sheet for Survey Participants

UCL Research Ethics Committee Approval ID Number: 21595/001

Title of Study: Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia.

Department: Information Studies

Name and Contact Details of the Researcher(s): Haifa Almugamisi

Telephone: [redacted]
Email: [redacted]

Name and Contact Details of the Principal Researcher: Elizabeth Lomas

Telephone: [redacted] **Email**: [redacted]

We are pleased to invite you to participate in this research project. Please take the time to read the following information about your participation in the research should you choose to proceed with participation. If you need more information, please ask us on the contact details available on the form. We are very keen to ensure that everything is clear. You may organise a meeting to discuss this further without any pressure to formally take part in this project.

Overview

This research is being undertaken for a PhD from University College London in the United Kingdom. The results of the research may be published in journals and presented at conferences.

What is the project's purpose?

The research aims to examine the general landscape of data breaches in Saudi Universities, in order to explore current strategies in data management, and their effectiveness in mitigating University data breach incidents. It will investigate the multidimensional effects of data breaches on student and faculty stakeholders. The research hopes to contribute to understandings of data management by shedding light on the reality of data and information security management in one of the Middle East countries. The study will be undertaken through multiple case studies at Saudi Universities, namely, King Saud University, Taibah University, and King Abdelaziz University, with the aim of representing Saudi higher education institutions. The research relies on the use of surveys and semi-structured interviews as data collection tools. You have been selected to participate in the questionnaire because we believe you have the knowledge. However, if you are unsure about your suitability to participate then please ignored the participation link.

Do I have to take part?

Taking part in this project is entirely voluntary. However, we believe that you can make a very important contribution to work which we hope will improve data and information security in Saudi Arabia. Your responses will be very valuable in enriching the research and as such we encourage you to participate. However, you have the right to decide whether to contribute or not. If you do choose to take part in the study, you will need to

sign a consent form. You can withdraw without consequences of any kind, and you will be asked what you prefer to happen to the data you have provided up to that point. However, having taken part in your survey, if one month has elapsed since you answered the survey then we can no longer withdraw you entirely from the work. This is because your responses will have been aggregated into the writing up.

What will be the format of the survey?

The survey includes open-ended questions and closed questions that will take approximately 20 minutes to complete. All questions are optional. These will include optional demographic data questions such as age, gender and job title. These will be aggregated and used anonymously and all the data you provide will be used for purely scientific purposes.

How will my data be used?

We will analyse and code your data to obtain a picture of how all participants approach data breaches and views on security and impacts. Sample quotes may be used from your questionnaire. However, every care will be taken to ensure that you remain anonymous in any outputs from the work. All data will be retained securely in line with UCL's retention policies and destroyed securely. All transcriptions will be kept until 1 year after the completion of the PhD. The survey consent forms will be kept until 5 years after the completion of the PhD.

Will my taking part in this project be kept confidential?

Your personal data will be kept strictly confidential. All data will be kept according to UCL's retention policies and in accordance with the UK Data Protection Act 2018. Further information on the management of research data at UCL is at the Privacy Notice here https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

Limits to confidentiality

Your confidentiality will be respected subject to legal constraints and professional guidelines in the UK and the SA.

What are the possible disadvantages and risks of taking part?

The potential risk is considered minimal. Data will be collected from you and your university officially within the permissions provided. You have a promise that the facts will be described in an accurate and fair manner and used for research purposes as set out. Every effort will be made to maintain your confidentiality.

Please note that very occasionally particular research projects are audited to ensure that all processes are being conducted legally and ethically. In such instance the audit team respect all the confidentiality parameters of the research. This is a safeguarding measure to ensure that research is appropriately conducted.

What are the possible benefits of taking part?

It's anticipated that by examining the current state of data breaches, mitigation strategies, and implications, the research will provide beneficial information that can be used to improve the management of data breaches locally and globally. This research will provide valuable information that will add to the body of knowledge in the field of data security, information technology, and education. It will also help provide an

honourable image of the universities work environment and its development in the Middle East. You will be offered the opportunity to receive a copy of the completed thesis.

What if something goes wrong?

If you wish to raise a complaint, please contact the Principal Researcher Dr Elizabeth Lomas([redacted]). We will deal with your complaint as soon as possible.

If you still are not satisfied with the handling of your complaint, you can contact the Chair of the UCL Research Ethics Committee (ethics@ucl.ac.uk).

What will happen to the results of the research project?

A copy of the research thesis will be deposited with UCL and the British Library. It is likely that the work outputs will be published in one of the scientific journals and presented at national or international conferences.

Local Data Protection Privacy Notice

University College London (UCL) is the controller of this project, providing data protection responsibility, and can be contacted at (data-protection@ucl.ac.uk). For further information on the privacy notice, please click on the following link https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

Contact for further information

Researcher: Haifa Almugamisi: [redacted]

Project Supervisor: Dr Elizabeth Lomas: [redacted]

Thank you for reading and considering contributing to this project.

ورقة معلومات المشاركين خاصة بالمشاركين بالاستطلاع

رقم معرف لجنة الأخلاقيات: 21595/001

عنوان الدراسة: وجهات نظر متعددة لخروقات البيانات في مؤسسات التعليم العالي، دراسة حالة الجامعات في السعودية

القسم: دراسات المعلومات

اسم الباحث وتفاصيل الاتصال: هيفاء المغامسي

[redacted]

اسم المشرف الرئيسي وتفاصيل الاتصال: اليزابيث لوماس

تليفون: [redacted] **ايميل:** [redacted]

يسعدنا دعوتكم للمشاركة في هذا المشروع البحثي. يرجى أخذ الوقت الكافي لقراءة المعلومات التالية حول مشاركتك في البحث إذا اخترت متابعة المشاركة. إذا كنت بحاجة إلى مزيد من المعلومات، فيرجى التواصل معنا من خلال تفاصيل الاتصال المتوفرة في النموذج. نحن حريصون جدًا على التأكد من أن كل شيء واضح. يمكنك تنظيم اجتماع لمناقشة هذا الأمر بشكل أكبر دون أي ضغط للمشاركة رسميًا في هذا المشروع.

نظرة عامة

يتم إجراء هذا البحث للحصول على درجة الدكتوراه من جامعة كوليدج لندن في المملكة المتحدة. يمكن نشر نتائج البحث في المجلات وعرضها في المؤتمرات.

ما هو الغرض من المشروع؟ يهدف البحث إلى دراسة المشهد العام لخروقات البيانات في الجامعات السعودية، لاستكشاف الاستراتيجيات المطبقة حاليا في إدارة البيانات، ومدى فاعليتها في التخفيف من حوادث خرق البيانات الجامعية. تحقق الدراسة أيضا في الآثار متعددة الأبعاد لانتهاكات البيانات على أصحاب المصلحة من الطلاب وأعضاء هيئة التدريس. حيث ان البحث يأمل في المساهمة في فهم إدارة البيانات من خلال تسليط الضوء على واقع إدارة أمن البيانات والمعلومات في إحدى دول الشرق الأوسط. لتمثيل مؤسسات التعليم العالي السعودية سيعتمد إجراء الدراسة على اسلوب دراسة حالات متعددة في الجامعات السعودية، وهي جامعة الملك سعود، وجامعة طيبة، وجامعة الملك عبد العزيز. من خلال استخدام الاستطلاعات المسحية والمقابلات شبة المنظمة كأدوات لجمع البيانات. لقد تم اختيارك للمشاركة بهذا البحث لأننا نعتقد أن لديك المعرفة المناسبة، ولكن إذا لم تكن متأكدًا من مدى ملاءمتك للمشاركة يرجى تجاهل رابط المشاركة.

هل يجب على المشاركة؟ المشاركة في هذا المشروع تطوعية بالكامل. ولكن نعتقد ان مساهمتك مهمة للغاية في هذا البحث الذي يأمل ان يحسن من امن البيانات والمعلومات في المملكة العربية السعودية. لذا نشجعك على المشاركة حيث ان ردودك ستكون ذات قيمة كبيرة في إثراء البحث. علما انه لديك الحق الكامل فيما إذا كنت ترغب بالمساهمة من عدمها. ستحتاج إلى التوقيع على نموذج الموافقة المرفق في حالة اخترت المشاركة في الدراسة. مع ملاحظة انه يمكنك الانسحاب دون عواقب من أي نوع، وفي حالة انسحابك سيتم سؤالك ماذا تريد ان يحدث للبيانات التي قدمتها مسبقا. وسيتم قبول انسحابك قبل مضي شهر واحد من الإجابة على الاستبيان، اما بعد ذلك فلا يمكننا سحبك بالكامل مع المشاركة خاصة إذا تم الانتهاء من جمع البيانات والتحضير لمرحلة التحليل والكتابة.

كيف سيكون شكل الاستبيان؟ يتضمن الاستطلاع أسئلة مفتوحة وأسئلة مغلقة تستغرق حوالي 20 دقيقة لإكمالها. كل الأسئلة اختيارية. يتضمن المسح أسئلة البيانات الديموغرافية الاختيارية مثل العمر والجنس والمسمى الوظيفي. سيتم تجميعها واستخدامها بشكل مجهول وسيتم استخدام جميع البيانات التي تقدمها لأغراض علمية بحتة.

كيف سيتم استخدام بياناتي؟ سنقوم بتحليل وترميز بياناتك للحصول على صورة لكيفية تعامل جميع المشاركين مع خروقات البيانات ووجهات النظر حول الأمان والتأثيرات. يمكن استخدام اقتباسات عينة من الاستبيان الخاص بك. ومع ذلك، سيتم اتخاذ كافة الإجراءات اللازمة لضمان عدم الكشف عن هويتك في أي مخرجات من العمل. سيتم الاحتفاظ سيتم الاحتفاظ .ويتم إتلافها بشكل آمن UCL بجميع البيانات بشكل آمن بما يتماشى مع سياسات الاحتفاظ الخاصة بشركة بجميع النسخ حتى عام واحد بعد الانتهاء من الدكتوراه. سيتم الاحتفاظ بنماذج الموافقة على المسح حتى 5 سنوات بعد الانتهاء من الدكتوراه.

هل ستبقى مشاركتي في هذا المشروع سرية؟ سيتم الاحتفاظ ببياناتك الشخصية بسرية تامة. سيتم تخزين بياناتك على UCL ووفقًا لقانون UCL سيتم الاحتفاظ بجميع البيانات وفقًا لسياسات الاحتفاظ فيUCL أدوات التخزين الموثوقة داخل أنظمة حماية البيانات في المملكة المتحدة لعام 2018. يمكنك الاطلاع على مزيد من المعلومات حول إدارة بيانات البحث في UCL وإشعار الخصوصية من خلال الرابط التالي https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

حدود السرية:

سيتم احترام سريتك وفقًا للقيود القانونية والإرشادات المهنية في كلا من المملكة المتحدة والمملكة العربية السعودية.

ما هي العيوب والمخاطر المحتملة للمشاركة؟ تعتبر المخاطر المحتملة ضئيلة. سيتم جمع البيانات منك ومن جامعتك رسميًا ضمن الأذونات المقدمة. نوعدك بأنه سيتم وصف جميع بياناتك بطريقة دقيقة وعادلة واستخدامها لأغراض البحث. سيتم بذل اقصى الجهود للحفاظ على سريتك. يرجى ملاحظة أنه في بعض الأحيان يتم تدقيق مشاريع بحثية معينة لضمان إجراء جميع العمليات بشكل قانوني وأخلاقي. في مثل هذه الحالة، يحترم فريق التدقيق جميع معايير سرية البحث. علما ان هذا إجراء وقائي لضمان إجراء البحث بشكل مناسب.

ما هي فوائد ممكنة من المشاركة؟ من المتوقع أنه من خلال فحص الحالة الحالية لانتهاكات البيانات واستراتيجيات التخفيف والآثار المترتبة، سيوفر البحث معلومات مفيدة يمكن استخدامها لتحسين إدارة انتهاكات البيانات محليًا وعالميًا. سيوفر هذا البحث ايضا معلومات قيمة ستضيف إلى مجموعة المعرفة في مجال أمن البيانات وتكنولوجيا المعلومات والتعليم. كما سيساعد في تقديم صورة مشرفة عن بيئة عمل الجامعات وتطورها في الشرق الأوسط. ستتاح لك الفرصة للحصول على نسخة من الأطروحة المكتملة.

ماذا لو حدث خطأ ما؟ إذا كنت ترغب في تقديم شكوى، يرجى الاتصال بالباحثة الرئيسية الدكتورة إليزابيث لوماس (e.lomas@ucl.ac.uk). إذا كنت لا تزال غير راضٍ عن التعامل مع .سنتعامل مع شكواك في أقرب وقت ممكن شكواك، يمكنك الاتصال برئيس لجنة أخلاقيات البحث في جامعة لندن (ethics@ucl.ac.uk).

ماذا سيحدث لنتائج مشروع البحث؟ سيتم إيداع نسخة من أطروحة البحث لدى UCL والمكتبة البريطانية. من المحتمل أن يتم نشر مخرجات العمل في إحدى المجلات العلمية وعرضها في المؤتمرات الوطنية أو الدولية.

إشعار خصوصية حماية البيانات المحلية: تعد كلية لندن الجامعية (UCL) المتحكم في هذا المشروع وتتحمل مسؤولية حماية البيانات، يمكنك التواصل مع إدارة البحث في الجامعة على الايميل التالي (data-protection@ucl.ac.uk). لمزيد من المعلومات حول إشعار الخصوصية يرجى النقر على الرابط التالي https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

عناوين التواصل

الباحثة: هيفاء المغامسي [redacted] مشرفة المشروع: الدكتورة إليزابيث لوماس [redacted]

شكرا جزيلا لك على قراءة المعلومات السابقة، مقدرين جدا تفكيرك في المساهمة بالمشروع

Appendix F: Survey Questions

Please complete this form before you have answered the survey's questions.

Title of Study: Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia- **MPhil/PhD**

Department: Information Studies

Name and Contact Details of the Researcher(s): Haifa Almugamisi

Email: [redacted]

Name and Contact Details of the Principal Researcher: Elizabeth Lomas

Email: [redacted]

This study has been approved by the UCL Research Ethics Committee: Project ID number: 21595/001

We are pleased to invite you to take part in this research which aims to explore the impacts of data breaches, data management and mitigation strategies in universities, and anticipated changes in data security management from the faculty member's perspectives. This work will contribute to providing an evidence base on the reality of personal data security management. It will provide a deeper understanding of the effects of data breaches in Saudi institutions of higher education and enhance the actions taken to ensure data breaches are minimised. The survey is only open to faculty members in Saudi specific universities namely, King Saud University, King Abdelaziz University. and Taibah University. You need not have any experience to take part in this survey. Any views you have will be appreciated.

Data collection

This survey is a part of a PhD research at UCL university. The research will also be written up in articles and used in research presentations. We hope that the insights that you and others provide will contribute to understanding and improving the management of personal data in Saudi universities. All of the information collected will be anonymous and we ask you not to record your name. No IP addresses are being collected. The data you provide will be aggregated with others. Occasionally we may quote from text provided but will endeavour to ensure that any quotations do not identify you. The information collected within the survey will be kept securely at UCL in accordance with the retention policies at the UCL university. At the end of the study, it will be securely deleted. The survey may take between 15 to 20 minutes for completing it depending upon how much you wish to write. All of the information collected will be anonymous and used for research purposes to enhance data and information security. The results of the study will be used for the completion of a PhD, articles and presentations. In addition, the high-level findings will be shared with the university. However, you will not be identified and all quotations will be carefully checked to ensure this.

The UCL Data Protection Policy is available at the following link:

Policies | Legal Services - UCL – University College London

The UCL Data Management Policy is available at:

Policies & funders' expectations | Library Services - UCL – University College London

UCL's Privacy Notice can be viewed at:

https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice

If you have any questions or concerns about the research, please feel free to contact with Haifa Almugamisi, [redacted] /The research supervisor is Dr Elizabeth Lomas,[redacted]

☐ I **have read and understood the purposes of this research and voluntarily agree to my data being used anonymously for the stated research.**

Proceed to survey

Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia

General information

1. Select your university. **(Please tick ☑).**
   - ☐ King Saud University.
   - ☐ Taibah University.
2. Select your gender**. (Please tick ☑).**
   - ☐ Male.
   - ☐ Female.
   - ☐ Prefer not to say.
3. Select your age. **(Please tick ☑).**
   - ☐ 18-24
   - ☐ 25-34
   - ☐ 35-44
   - ☐ 45-54
   - ☐ 55 and up.
   - ☐ Prefer not to say.

4. What is your current job level?
   - ☐ Professor
   - ☐ Co-professor
   - ☐ Assistant Professor
   - ☐ Lecturer or language teacher
   - ☐ Teaching Assistant
   - ☐ Demonstrator
   - ☐ Manager
   - ☐ Administrative
   - ☐ Technician
   - ☐ other, please type your level:
   - ☐
5. What do you understand about data breaches? Please move to the next question if you do not feel comfortable providing a definition.
   ..……

6. Can you explain how data breaches happen?

   ……

7. One definition of a data breach is that it is a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.” Please indicate the extent to which you agree with this definition of a security breach **(Please tick ☑).** If you do feel that it omits anything or is not a precise definition then please feel free to make a comment.

- □ Strongly Agree
- □ Agree.
- □ Neither Agree or Disagree.
- □ Disagree.
- □ Strongly Disagree.
- □ Optional comment: …….

8. Have you ever experienced a data breach incident within your university? **(Please tick ☑)**
   - □ Yes
   - □ No
   - □ Prefer not to say.

9. Have you ever experienced a data breach incident outside a university context? **(Please tick ☑)**
   - □ Yes
   - □ No
   - □ Prefer not to say.

10. If you have experienced a data breach, please could describe the incident in more details? What caused it and what steps could have been taken to avoid it?
    ……
    ……

11. Have you ever had responsibility for managing aspects of a personal data breach within your university? **(Please tick ☑).**
    - □ Yes, definitely I led on managing a data breach.
    - □ Yes, I was involved in assisting with dealing with a breach.
    - □ No.
    - □ Don't know.
    - □ Prefer not to say.

12. Did you manage a personal data breach within your university? **(Please tick ☑).**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don't know.
    - □ Prefer not to say.

13. If you have managed a data breach, then can you select what sort of data breach it was?
    - □ Unintended disclosure.
    - □ Hacking or malware.
    - □ Payment card fraud.
    - □ Insider attack.

- □ Physical loss of data.
- □ Data stolen.
- □ Devices loss.
- □ Unknown.
- □ Other, please mention it: ……..

14. Could you describe how the previous data breach was managed, and how a similar breach might be avoided in the future?
……

15. Can you identify which of the following emotional responses you have felt when your personal data had been breached? **(You can select more than one option by ticking ☑ in the appropriate options).**
    - □ Anger.
    - □ Sadness.
    - □ Fright.
    - □ Anxiety.
    - □ Surprise.
    - □ Other, please mention it: ……
    - □ Prefer not to say.

16. To what extent do you agree with this statement ' the level of my trust in the institution has changed after my personal data was breached' **(Please tick ☑).**
    - □ Strongly Agree
    - □ Agree.
    - □ Neither Agree or Disagree.
    - □ Disagree.
    - □ Strongly Disagree.

Organisational Information

17. Do you know how your personal data is collected and processed by the university? **(Please tick ☑).**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don’t know.
    - □ Prefer not to say.

18. Do you know the data security policies adopted by your university regarding data breaches? **(Please tick ☑).**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don’t know.
    - □ Prefer not to say.

19. Do you know how you can make a complaint if your personal data has been leaked or disclosed to unauthorized individuals by the university? **(Please tick ☑).**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don't know.
    - □ Prefer not to say.

20. Did you receive data security training when you were employed at the university? **(Please tick ☑).**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don't know.
    - □ Prefer not to say.

21. In case you received training on data security from your university, select the type of training. **(You can select more than one option by ticking ☑ the applied options**).
    - □ Mandatory formal training.
    - □ Informal training.
    - □ Web-based training.
    - □ Personal training.
    - □ Other ……..
    - □ Prefer not to say.

22. To what extent do you agree with the following statement 'I think that the data and information security awareness programs provided by my university are sufficient'. **(Please tick ☑).**

□ Strongly Agree
□ Agree.
□ Neither Agree or Disagree.
□ Disagree.
□ Strongly Disagree.

23. Do you think strategies to mitigate the impact of data breaches at the university are appropriate? **Please tick ☑, and do add any comments on this that you feel able to provide.**
    - □ Yes, definitely.
    - □ Yes, to some extent or partly.
    - □ No.
    - □ Don't know.
    - □ Prefer not to say.
    - □ (Optional comment) ……...

24. How would you prefer your university treating you in case you exposed to a data breach in order to mitigate the beach's effects? **(Please tick all that apply ☑).**
    - ☐ Apology.
    - ☐ Compensation
    - ☐ Other, please mention it ……
    - ☐ Prefer not to say.

Technical Information

25. To what extent do you agree with the following statements. **Please tick ☑. (No more than one answer can be chosen).**

25	I believe that the technical tools adopted by my organization are appropriate to minimize data breaches.			
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.
26	I think that the information systems and networks used in my work environment are managed to reduce the impact of data breaches and information security incidents			
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.
27	I think that technical failings are the main cause of data breaches.			
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.
28	I think that weak employee practices are the main cause of data breaches.			
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.

29-From your perspective, what are the following most common practices among employees that may lead to technical risks, which may cause data breach incidents. **(You can select more than one option by ticking ☑ the applied options**).
- ☐ Opening anonymous emails.
- ☐ Clicking up unknown links.
- ☐ Choosing simple or not updated passwords and sharing them with others
- ☐ Sharing the use of computers among employees
- ☐ Using private computers for work purposes, and accessing university systems through them.
- ☐ Browsing malicious websites within the internal system of university networks.
- ☐ Other …….
- ☐ Prefer not to say.

30-How would you describe the technical impacts of data breaches?

.....

Emotional Information

31-To what extent do you agree with the following statements. **Please tick ☑. (No more than one answer can be chosen).**

31	I am afraid that my personal data may be leaked to unauthorized persons, which may expose me to fraud, extortion, or anything that offends me as a result of that leak.				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
32	I have no concerns about the privacy of my data and personal information that I have provided to my university.				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
33	I think the emotional responses (reactions) of individuals such as anger, fear, anxiety...etc., represent negative consequences of data breaches, which should be considered.				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
34	I agree with this statement, "Too much provocation in the work environment increases employee anger and may result in intentional or unintentional data leakage."				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
35	I agree with this statement " people who have enough security awareness would not be shocked if s/he experiences a data breach event”.				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
36	It is usually an unpleasant experience for me when I have to disclose my personal data to the university due to trust issues.				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
37	I support this statement "a frustrated employee presents a potential threat to breach data security by performing malicious acts".				
☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.	
38	I am interested in tracking rumors that some universities are facing data security problems, especially tracking data breach incidents in universities.				

☐ Strongly Agree	☐ Agree.	☐ Neither Agree or Disagree.	☐ Disagree.	☐ Strongly Disagree.

39-From your perspective, what is the most harmful aspect of data breaches? **(Please tick ☑).**

- ☐ Technically.
- ☐ Personally.
- ☐ Organizationally.
- ☐ Other (please comment) ……...

40-Which of the following aspects do you think are important for developing the process of protecting your personal data that you would like your university to adopt? **(Please tick ☑).**

- ☐ Technical protection tools such as Installing firewalls, controlling access to utilities (authentication), screen exits, and controls via (hiding IP addresses), intrusion detection systems, and data encryption.
- ☐ Organizational procedures, such as developing data security policies, adopting sufficient mitigation strategies, and intensifying data security awareness programs among employees.
- ☐ Personal aspects, such as considering emotional aspects in terms of data security.
- ☐ Other, please mention it……..
- ☐ Prefer not to say.

41-What are the changes you wish to see to improve the process of data security, and your personal data protection?

……
……

42-Do you have any other comments that you would wish to make?

……
……

Thank you for your help.

Appendix G: Interview Questions List

Interview questions:

The interview questions include three main themes that will be subjected to each candidate. However, if the candidate is a specialist in technical aspects, s/he will be asked more deeply about the technical aspects. As I will expand on asking questions based on the candidate's background. I might require a copy of policies or brochures.

For technical participants:

The expected time for the interview is approximately an hour and thirty minutes.

5 minutes for greeting and introduction.

Introductory questions: Estimated response time is 15 minutes

1- What do you understand when I talk about a data breach? [Then you might want to give an explanation of what you mean]
2- Can you tell me about your own role and responsibilities in respect of university security?
3- What works well in terms of the data protection systems that are in place?
4- What could be done better? What would facilitate doing things better?
5- What are the barriers?
6- What are the critical risks for the universities?
7- Do experiences from other places that universities could learn?

Technical information questions:

Main questions: Estimated response time is 20 minutes.

1- What guarantees the best to boost data security Technically?
2- What are the technical risks?
3- What can be done to improve these obstacles?
4- How does a data breach influence technically institutions and individuals?

Sub-questions: The expected response time is 10 minutes.

1- Would you tell me about your university's IT infrastructure?
2- What are the pros and cons?
3- How could be developed?
4- Could you explain the technical methods to protect data in the university?
5- Any university in the world is likely to be exposed to a data breach event, has your respected university experienced such an event before?
6- What sort of data breach was?
7- What does need to improve in order to reduce the impacts of such a breach?
8- What can you tell me about your university plans for growth in the technical aspect to prevent breaches?

9- Do you want to add any information?

Organizational information questions:

Main questions: Estimated response time is 15 minutes.

1- Could you tell me the university regulations for data protection?
2- What can be done to support accessibility rights/ sides?
3- What can be done to manage the responsibility and accountability aspects effectively for protecting data?
4- Can you describe the organizational impacts of data breaches whether on the university or stakeholders?
5- What is needed to recover from data breaches?
6- What could be changed, and why we do need to undertake this change? How would that be helpful?

Sub-questions: The expected response time is 5 minutes.

1- What sorts of personal data that the university is processed about individuals?
2- Who can access the stakeholders' personal data?

Emotional information questions:

Main questions: Estimated response time is 15 minutes.

1- Could you tell me about the personal risks of data breaches?
2- What are their consequences and impacts?
3- Why do data breaches affect individuals emotionally?
4- What can be done to diminish the emotional impacts?
5- Do university policies cover the personal aspects?
6- What can be done better to deal with victims of data breaches to repair trust?

Sub-questions: The expected response time is 5 minutes.

1- Have you ever recognized any emotional reactions within previous data security investigations?
2- What type of emotion was it? How was it treated?
3- How could tackle the negative emotional responses effectively?
4- What are the hinders in terms of emotional aspects?

For non-technical participants

The expected time for the interview is approximately an hour and thirty minutes.

5 minutes for greeting and introduction.

Organizational information questions:

Main questions: Estimated response time is 15 minutes.

1- Could you tell me the university regulations for data protection?
2- What can be done to support accessibility rights/ sides?
3- What can be done to manage the responsibility and accountability aspects effectively for protecting data?
4- Can you describe the organizational impacts of data breaches whether on the university or stakeholders?
5- What is needed to recover from data breaches?
6- What could be changed, and why we do need to undertake this change? How would that be helpful?

Sub-questions: The expected response time is 20 minutes.

1- What sorts of personal data that the university is processed about individuals?
2- Who can access the university stakeholders' personal data?
3- What operates well in the regulations to avoid breaches?
4- Can you talk about the penalties or fines?
5- What are the strengths and weaknesses of data security policies?
6- From your administrative perspective, what do we need to develop personal data protection systems in Saudi Arabia? How your university will be involved in this change?
7- Do you have any further information or clarification you wish to include?

Technical information questions:

Main questions: Estimated response time is 10 minutes.

1- What guarantees the best to boost data security Technically?
2- What are the technical risks?
3- What can be done to improve these obstacles?
4- How does a data breach influence technically institutions and individuals?

Emotional information questions:

Main questions: Estimated response time is 20 minutes.

1- Could you tell me about the personal risks of data breaches?
2- What are their consequences and impacts?
3- Why do data breaches affect individuals emotionally?
4- What can be done to diminish the emotional impacts?
5- Do university policies cover the personal aspects?
6- What can be done better to deal with victims of data breaches to repair trust?

Sub-questions: The expected response time is 20 minutes.

1- How can universities consider the emotional aspects?
2- Have you ever recognized any emotional reactions within previous data security investigations?

3- What type of emotion was it? How was it treated?
4- How could tackle the negative emotional responses effectively?
5- What are the hinders in terms of emotional aspects?
6- What are the current goals that the university is focused on to handle the emotional parts of the security crisis, and how does the university support hitting those goals?
7- Do you have any further information or clarification?

Appendix H: Interview Coding by NVivo