Co-design and modelling of security policy for cultural and behavioural aspects of security in organisations

Albesë Demjaha

A thesis submitted for the degree of

Doctor of Philosophy

at

UCL

2023
I, Albesë Demjaha confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.
Chi va piano va lontano.
Abstract

Organisations have historically applied a technology-oriented approach to information security. However, organisations are increasingly acknowledging the importance of human factors in managing secure workplaces. Having an effective security culture is seen as preferable to enforced compliance with policy. Yet, the study of security culture has not been addressed consistently, either in terms of its conceptual meaning or its practical implementation. Consequently, practitioners lack guidance on cultural elements of security provisioning and on engaging employees in identifying security solutions.

To address existing problems relating to security policy in respect of organisational culture, this thesis explores behavioural and cultural aspects of organisational security. We address gaps in human-centred research, focusing on the lack of work representing real-world environments and insufficient collaboration between researchers and practitioners in the study of security culture. We address these gaps through analytical work, a novel co-design methodology, and two user studies.

We demonstrate that current approaches to security interventions mirror rational-agent economics, even where behavioural economics is embodied in promoting security behaviours. We present two case studies exploring the dynamics between security provisioning and organisational culture in real-world environments, focusing on distinct groups of users — employees, security managers, and IT/security support — whose interactions are understudied.

Our co-design methodology surfaces the complex, interconnected nature of supporting workable security practices by engaging modellers and stakeholders in a collaborative process producing mutually understood and beneficial models. We find employees prefer local support and assurances of secure behaviour rather than guidance without local context. Trust-based relationships with support teams improve engagement. Policy is perceived through interactions with support staff and by observing everyday workplace security behaviours.

We find value in engaging with decision-makers and understanding their decision-making processes. We encourage researchers and practitioners to engage in a co-design process producing multi-stakeholder views of the complexities of security in organisations.
Impact Statement

As a result of the work conducted for this thesis, there are three academic publications, which are actively being disseminated — with reads and citations increasing over time.

The work presented in this thesis consistently considers the application of security in organisations and, as such, has the potential to impact both academia and industry. Additionally, because of the interdisciplinarity and domain-agnostic approach of this thesis, the work is expected to be applicable to more than one research field. The impact of this thesis can be attributed to both analytical, empirical and methodological contributions.

The behavioural economics thinking applied to security decision-making (Chapter 3) identifies a contradiction — which has not been identified thus far — relevant to current security provisioning and interventions in organisations. The contradiction is that current security interventions often mirror rational-agent economics, even where behavioural economics is embodied in the promotion of individual security behaviours. Identifying this contradiction can raise awareness for future interventions, which ought to consider employees as boundedly rational, especially when those interventions apply methods from behavioural economics. A consideration of bounded rationality can be useful in other fields in which behaviour-change methods are used to help non-expert employees with policy compliance.

The two user studies (Chapters 4 and 6) have been carefully designed having in mind the potential impact on the two organisations. Starting with the study objectives — the purpose was for the studies to be mutually beneficial both for the organisations and the researchers. The findings were reported back to each respective chief information security officer (CISO) and recommendations were produced based on the interactions with the stakeholders and the context of the organisations. Both organisations perceived this engagement as meaningful and useful for identifying unknowns, or for validating known unknowns.

Last, but not least, this thesis contributes a novel co-design methodology for security modelling (Chapter 5) with the ability to produce multi-stakeholder views of the complexities of security management in organisations.
This methodology has value for security research, not only from the methodological standpoint, but also due to the findings that surface as a result. The co-design methodology can be applied by researchers and practitioners looking to explore cultural and behavioural aspects of security in organisations. In addition, modellers of other fields can use the methodology to engage with relevant stakeholders in their modelling process.
Acknowledgements

First and foremost, I would like to thank my supervisors David Pym and Simon Parkin for their continuous support and patience during this long journey. David showed confidence in me from the very beginning and provided me with the opportunity to apply for the PhD programme and continue my journey at UCL. His interdisciplinary knowledge, academic experience, meticulousness and empathy have been invaluable to my completion and for that I will always be grateful. I want to thank Simon for always being available and continuing to supervise me even when it was no longer his obligation and thus providing me with a sense of stability until the end. His experience in human factors of security and knowledge of user studies has been an anchor for my work. Last but not least, I want to thank my previous supervisor Angela Sasse who even though moved to Germany during my PhD, provided me with enormous inspiration to work in human-centred security, and that inspiration always remains.

I am very grateful to Madeline Carr for examining my upgrade viva and giving me the feedback and motivation to move forward with my research. I am also thankful for the useful feedback from my examiners, Christos Ioanidis and Jason Nurse. I would also like to thank my co-authors and dear colleagues from UCL: Tristan Caulfield, Ingolf Becker, and Jonathan Spring.

Next, I would wholeheartedly like to thank The Alan Turing Institute, not only for fully funding my PhD, but for always showing care towards their students and facilitating such a welcoming and safe environment. In particular, I would like to thank Ben Murton and Samantha Selvarajah for their understanding and support, and for lifting me up when I needed it the most. Moreover, thank you is not enough to express my gratitude towards Debbie Dixon who kept me sane during all these years, guarded my self-confidence and gave me peace in moments of uncertainty.

I am immensely grateful to Company A and the university for generously donating their employees’ time to this research. In addition, the continuous support of Paul Jennings and Michael Sofowora has been beyond valuable. I am proud to have known them, both as amazing individuals, but also as
industry mentors who always helped me bridge the gap between research and industry.

I also want to thank my current employer, KPMG Norway, for always supporting my PhD as well as providing me with the time and mental space to finish it. I want to especially thank my manager Maren Magnus Voll and my director Nils Harald Børve for this invaluable opportunity.

As for my dearest friends, I owe a big thank you to Lina, who has been my PhD buddy from day one, as well as my family in lonely London. Moreover I want to thank my friend Guxim who has also become family, for always believing in me and being there every step of the way. I want to extend my gratitude to two beautiful souls, Zafu and Talia, for always showering me with positivity and motivation. In addition, I want to thank my friend Isuf for our daily office conversations (both personal and professional) and his valuable advice.

Words are insufficient to express my appreciation to my family. First and foremost, my parents, Agon and Teuta, who have always sacrificed anything necessary to help and support me, both in an academic, emotional, and nurturing aspect. My progress and growth would not have been possible without them. In addition, I want to thank my brother Dritëro for his unconditional faith in my abilities, and for always sparking my intellectual creativity. And, I want to thank my grandparents, Mika and Adani, for always supporting my academic goals and tirelessly showing me the importance of knowledge and hard work.

Last but certainly not least, I am eternally grateful to my husband Ardit for being my rock and biggest supporter in life. His continuous patience, encouragement, love, wit, and calming presence have been indispensable in completing this challenging journey. Thank you for being my eternal source of inspiration, hope, and strength — të kom çdo xho!
Contents

Dedication iii
Abstract v
Impact Statement vii
Acknowledgements ix
Contents xi
List of Figures xvii
List of Tables xix

1 Introduction 1
  1.1 Research questions ........................................ 4
  1.2 Thesis contributions .................................... 5
    1.2.1 Empirical and analytical contributions ............... 6
    1.2.2 Methodological contributions ....................... 7
  1.3 Published work ......................................... 7
  1.4 Our concept of security culture ....................... 10
  1.5 Thesis structure .................................... 11

2 Background: Organisational Culture and Co-design Foundations 13
  2.1 Organisational culture ............................... 14
  2.2 Security culture .................................... 17
    2.2.1 What is security culture? .......................... 17
    2.2.2 Security culture and organisational culture ..... 19
    2.2.3 Measuring security culture ...................... 20
    2.2.4 Transforming security culture ................... 22
  2.3 Modelling security culture ........................... 23
  2.4 Reflections from literature review ................... 24
## Contents

2.4.1 Addressing the gaps ........................................... 26
2.5 Co-design for security modelling ................................. 26
  2.5.1 What is co-design? ........................................ 26
  2.5.2 Co-design and modelling ................................... 27
  2.5.3 Co-design and security .................................... 28
2.6 Our co-design methodology ...................................... 29
2.7 Summary ......................................................... 31

3 Security Economics for Behaviour Intervention ................. 35
  3.1 Introduction ................................................... 35
  3.2 Terminology ................................................... 38
  3.3 Towards a consistent strategy ................................ 39
    3.3.1 Why we are here, with too few choices ................. 41
  3.4 Applying economics principles to organisational security .. 43
    3.4.1 Rational vs. bounded decision-making ................. 43
    3.4.2 Group decisions, herding, and culture ................. 45
  3.5 A framework for security choices ............................ 47
    3.5.1 Bounded security decision-making ..................... 47
    3.5.2 Framework implementation ............................ 55
  3.6 Worked example ................................................ 59
    3.6.1 Process .................................................. 60
    3.6.2 Available policy choices ............................. 63
    3.6.3 Decision-maker choices ............................... 64
  3.7 Related work .................................................. 64
  3.8 Summary ....................................................... 66

4 A Case Study of Post-Breach Security Changes .................. 69
  4.1 Introduction ................................................... 69
  4.2 Reactions to security breaches ............................... 70
  4.3 Case study .................................................... 72
    4.3.1 About the organisation ................................ 72
    4.3.2 Methodology ........................................... 73
  4.4 Results ........................................................ 77
    4.4.1 Post-shock security .................................... 78
    4.4.2 Security theatre undermines policy .................... 80
    4.4.3 Security is like detention ............................ 82
    4.4.4 Security is a blocker .................................. 83
    4.4.5 Lack of effective communication ....................... 84
4.4.6 Zero risk appetite ........................................ 85
4.4.7 Sensible security is likely to work .................. 87
4.4.8 Behaviour change is required ....................... 88
4.5 Summary .................................................. 90

5 Co-design for Security Modelling ......................... 91
  5.1 Introduction ............................................. 91
  5.2 Modelling for security ................................. 94
    5.2.1 Challenges of modelling ......................... 95
  5.3 Modelling behavioural and cultural aspects of security 97
    5.3.1 Challenges of modelling behavioural and cultural aspects 97
  5.4 Co-design for security modelling .................... 99
    5.4.1 What is co-design? ............................... 99
    5.4.2 Co-design and modelling ....................... 99
    5.4.3 Co-design and security ....................... 100
  5.5 Our methodology ..................................... 101
  5.6 Case study: Reflections .............................. 105
    5.6.1 The organisation ............................... 105
    5.6.2 Methodology ..................................... 106
    5.6.3 Main findings .................................. 108
    5.6.4 Reflections ..................................... 108
  5.7 Candidate model .................................... 112
  5.8 Summary .............................................. 114

6 A Case Study Examining the Role of Security Practices in Organisational Culture 115
  6.1 Introduction ......................................... 115
  6.2 Background and related work ....................... 117
    6.2.1 Organisational security ....................... 117
    6.2.2 Holistic views of organisational security .......... 119
    6.2.3 Co-design of organisational security solutions .......... 119
  6.3 Methodology ......................................... 121
    6.3.1 Co-design modelling process .................. 121
    6.3.2 Co-design modelling components ............... 122
    6.3.3 Supporting security management decision-making .......... 125
    6.3.4 Interview study (substantiating the model) ......... 127
    6.3.5 Qualitative data collection and the modelling framework 130
  6.4 Results ............................................... 132
6.4.1 Administrative employees ........................................ 133
6.4.2 IT and security support ........................................... 140
6.4.3 Reflection by policy decision-makers ............................ 144

6.5 Discussion ............................................................ 145
6.5.1 Limitations .......................................................... 147
6.5.2 Recommendations .................................................. 148

6.6 Summary ............................................................... 149

7 Discussion .................................................................. 151
7.1 Introduction ............................................................. 151
7.2 Summary of work ....................................................... 151
7.3 How to understand people in organisations: crossing boundaries at security trading zones ............................................. 152
7.4 Bringing it all together ................................................. 155
7.5 What are the success factors for co-design? ...................... 156
7.6 Reflecting on the findings and their value for future security research ................................................................. 160
7.6.1 Users ‘vs.’ managers ................................................. 160
7.6.2 Communication ...................................................... 160
7.6.3 Centralised vs. decentralised ..................................... 163
7.6.4 Security (of) culture ............................................... 164

8 Conclusions ................................................................. 167
8.1 Overview of findings ................................................... 168
8.2 Summary of contributions ............................................ 169
8.2.1 Empirical and analytical contributions ......................... 169
8.2.2 Methodological contributions .................................... 170
8.3 Recommendations ..................................................... 171
8.3.1 Recommendations for researchers ............................ 171
8.3.2 Recommendations for practitioners .......................... 172
8.4 Limitations .............................................................. 173
8.5 Future work ............................................................. 174
8.5.1 A security diet ....................................................... 174
8.5.2 Co-design with stakeholders .................................... 175
8.5.3 Security modelling and investment forecasting .............. 175

Bibliography ................................................................. 177

A Glossary: Economics Terminology .................................. 197
# List of Figures

2.1 The classical mathematical modelling cycle. (see, e.g., McColl 1995). 30
2.2 Co-design in the translation zone (adapted from Caulfield, Ilau and Pym 2022b). 31
2.3 Modelling cycle, translation zone, and co-design. 32
3.1 An illustration of bounded rationality. 38
3.2 A decision point in a decision-maker’s process of bounded security decision-making (elements adapted from Caulfield and Pym 2015a). 48
3.3 A zoomed-in view of the available policy choices and decision-maker choices. 53
3.4 Implementation steps of the bounded security decision-making framework. 56
4.1 The classical mathematical modelling cycle (see, e.g., McColl 1995). 93
4.2 Modelling cycle, translation zone, and co-design. 102
4.3 The mapping of the case study components to the co-design modelling cycle. 112
4.4 The candidate conceptual model in the form of an entity-relationship (ER) model representing the interview themes from Company A. 113
5.1 The co-design process applied in this study (adapted from Demjaha, Pym and Caulfield 2021; Caulfield, Ilau and Pym 2022b). 123
5.2 Exchangeable artefacts between modellers and stakeholders in the translation zone. 126
5.3 Co-design in the translation zone (adapted from Caulfield, Ilau and Pym 2022b; McColl 1995). 131
5.4 The conceptual model in the form of an entity-relationship (ER) model representing the interview themes. 133
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Definitions of organisational culture.</td>
<td>15</td>
</tr>
<tr>
<td>2.2</td>
<td>Schein’s three levels of culture (adapted from Schein 2010).</td>
<td>16</td>
</tr>
<tr>
<td>3.1</td>
<td>Examples of ‘contradictory’ and ‘better’ approaches to supporting secure behaviours in organisations (derived from experiences reported in real-world settings, and relevant studies).</td>
<td>42</td>
</tr>
<tr>
<td>3.2</td>
<td>Rationality vs. bounded rationality in decision-making.</td>
<td>44</td>
</tr>
<tr>
<td>4.1</td>
<td>Produced themes from thematic analysis.</td>
<td>79</td>
</tr>
<tr>
<td>5.1</td>
<td>Themes from thematic analysis.</td>
<td>109</td>
</tr>
<tr>
<td>6.1</td>
<td>Themes identified during thematic analysis.</td>
<td>134</td>
</tr>
<tr>
<td>A.1</td>
<td>Traditional and behavioural economics terminology — part 1.</td>
<td>197</td>
</tr>
<tr>
<td>A.2</td>
<td>Traditional and behavioural economics terminology — part 2.</td>
<td>198</td>
</tr>
</tbody>
</table>
Individuals as well as organisations have become dependent on technology in their everyday lives. As a result, information flow has rapidly increased and has drastically changed the way we view the Internet. Once a convenient commodity, the Internet has now additionally become a key source of cyber attacks. In the United Kingdom, the overwhelming majority of organisations rely on some type of digital service, and are hence highly subjected to cyber security risks (Ell and Gallucci 2022). The latest Cyber Security Breaches Survey shows that 39% of organisations in the UK have identified a cyber security breach or attack in the last year, and 62% of higher education institutions reported experiencing attacks or breaches at least weekly (Ell and Gallucci 2022). This situation makes information security a priority for businesses. However, prioritisation unfortunately does not guarantee usable and effective information security. Although the need for information security has significantly increased, it is difficult for an organisation to be secure without the input of its employees who — in addition to their primary tasks — have to make security decisions on a daily basis.

The human-centred approach existed in the very roots of information security. Even when security was purely a mechanism used by the military, Kerckhoffs clearly stated that such mechanisms should not require a long list of rules and must be easy to remember, easy to use, and stress-free for people (1883). Unfortunately, these principles have been widely ignored in security as the field has predominantly applied a technology-oriented approach. By assigning blame to users rather than tailoring security to their capabilities and goals (Sasse, Brostoff and Weirich 2001), security compliance in organisations remains insufficient (Beautement, Sasse and
1: Introduction

Wonham (2009). However, recent initiatives increasingly encourage a serious focus on human-centred security, after all — ‘security that doesn’t work for people, doesn’t work’.

Security policy compliance in organisations can be problematic if the fit to employee needs and expectations is not considered. Employees in organisations have primary work tasks to complete — an employee may base decisions about compliance and non-compliance on whether the controls mandated by policy are perceived to be aligned with completion of these tasks. People have limitations which arise from their inherent capacities to manage information and cognitive workload (Benson et al. 2015) — the intention should not be to overcome these capacities, but rather to accommodate them. Finding solutions in a way that is both efficient for the policy-maker and inclusive of end-user needs is increasingly seen as necessary for a sustainable security programme.

As an attempt to shift from forceful compliance, organisations nowadays are keen to create and nourish a healthy security culture (Pfleeger, Sasse and Furnham 2014). However, security culture is not being used unanimously, both in terms of its definition as well as its practical implementation and evaluation. There is no universal definition for security culture or an accepted way of measuring it (Malcolmson 2009). There is also no set of accepted dimensions and concepts describing security culture (Nasir et al. 2019). Although many authors began to recognise the importance of having a security culture in an organisation (Sizer and Clark 1989; Schwarzwalder 1999; Breidenbach 2000; Solms 2000; Andress and Fonseca 2000; Clark-Dickson 2001; Beynon 2001), no definitive consensus has been reached over the meaning of security culture or its relationship to organisational culture (Uchendu et al. 2021). Additionally, there is a lack of practical guidance for practitioners on how to approach security culture in organisations (Nasir et al. 2019), which makes the work of security managers all the more challenging.

We acknowledge that managing organisational security involves a level of uncertainty and complexity that impacts both the security managers and the employees. Because of a lack of rigorous methods in human-centred security, there is no clear approach for organisations to explore and understand what is going on in their own environments, and to engage their employees in more workable security solutions. In order to address — and further understand — the identified problems in relation to security policy vis-à-vis organisational culture, this thesis takes an interdisciplinary approach in exploring the behavioural and cultural aspects of security in organisations. The proposed methodology aims to improve our understanding of the

---

1https://www.ncsc.gov.uk/information/people-strongest-link
dynamics between security provisioning and organisational culture in a real-world environment, by focusing on capturing the different perspectives of stakeholders, as well as utilising their areas of expertise. In aiming to bridge the gap between researchers and practitioners, we propose a model co-design methodology for security. The methodology brings together researchers/modellers and stakeholders in a collaborative process with the purpose of producing a model which deepens — but also represents — the understanding of all stakeholders involved.

While the proposed methodology draws on established methodologies such as co-design, and other participatory approaches, it should not be confused with participatory modelling (PM) due to several reasons. From the perspective of participatory modelling, the fact that stakeholders may lack (modelling) expertise is considered a challenge when applying the methodology. The approach proposed in this thesis emphasises instead the expertise of stakeholders in their respective domain as a strength, and as a necessity for meaningful modelling. While the model co-design methodology embraces the participatory approach of PM, it focuses more heavily on co-design, rather than potential participation.

It is important to distinguish that the purpose is not for a group of people to translate something for another group of people, but to create a shared understanding. It is the translation of all of the stakeholders’ understanding into a shared representation. Behavioural economics provides a language for articulating that shared understanding. Its role is that it provides the conceptual and potentially more technical language for instantiating the use of a co-design methodology. In the use of behavioural economics as a conceptual language for articulating what goes on in the translation process between the stakeholders and the researchers, co-design complements this process in application.

As such, this methodology enables better opportunities for capturing the behavioural and cultural aspects influencing security in organisations. Through better understanding of the system, the co-design methodology can help improve security decision-making. Simultaneously, the thesis shows how modelling security culture through a co-design approach can help facilitate the required system and context knowledge to represent culture more accurately. Through co-design, stakeholders are able to identify opportunities for capturing observations of aspects which influence security policy. Constructs from both traditional and behavioural economics are used to represent which shared artefacts are pertinent in a complex ecosystem. By deconstructing the idea that employees are rational decision-makers, as per traditional economics, we highlight the elements in the bounded decision-making process that stakeholders should account for in policy-making.

In summary, the thesis proposes a co-design approach which aims to tackle the
challenges of problem definition, data availability, and data collection associated with modelling behavioural and cultural aspects of security. This process of modelling co-design is a proposed solution to these challenges, in particular for models aiming to incorporate organisational security culture. The co-design methodology is applied in the setting of a financial company (Company A), and a large university. This involves iterative rounds of interviews connected by the co-design methodology: 15 security managers managing a security team of 100 employees; 14 employees working with high-value data with specific security needs; 7 support staff across both local, central IT and IT-security support teams; and two senior security decision-makers in the organisation. The iterative co-design approach brings together the viewpoints of a range of stakeholders that capture key influences driving secure working practices. We provide recommendations for improvements to workplace security, including to shift the focus towards how policy is communicated to employees.

1.1 Research questions

This thesis focuses on the behavioural and cultural aspects of security by taking an exploratory approach and addressing the following, open-ended, research questions:

*How does the role of security align with organisational culture, and how can we enhance our understanding and mapping of this relationship in a manner that is practical for practitioners and decision-makers? How can we establish a connection between security and other areas of the organisation, effectively bridging the gap and promoting an aligned and integrated approach?*

The thesis chapters address the research questions in the following way:

- **Chapter 2 — Background: Organisational Culture and Co-design Foundations:** By reviewing and analysing relevant literature, this chapter explores the relationship between security culture and organisational culture and discusses the need for a better, and more practical representation of this relationship for decision-makers and practitioners. It also points to gaps in current literature on security culture, highlighting the motivation for a methodology which can help bridge the gap between security and organisational culture.
- **Chapter 3 — Security Economics for Behaviour Intervention:** This chapter portrays non-security employees as boundedly rational and explores their bounded decision-making process when faced with security choices. The conceptual framework in this chapter highlights the need to understand how security
considerations align with other organisational factors and emphasises the importance of aligning security practices with other areas of the organisation, as well as ensuring an integrated approach to security decision-making.

• Chapter 4 — A Case Study of Post-Breach Security Changes: Through a unique case study showing a company’s culture after experiencing a breach, this chapter notes the importance of effective communication in security management. The case study provides an example of misalignment between the role of security and the organisational objectives and the value of identifying and managing this misalignment for security practitioners and decision-makers. The culture of the company portrayed in this case study indicates that financial and human resources are not necessarily sufficient for aligning security with the company culture. The need for promoting an aligned approach and communication across the organisation is further emphasised.

• Chapter 5 — Co-design for Security Modelling: This chapter addresses the research questions directly as it proposes a novel methodology for co-design which aims to more accurately capture the behavioural and cultural aspects of security in organisations. The methodology aims to bridge the gap between research and practice by engaging stakeholders in a process of mutual learning, co-creating the objectives of the model and incorporating the insights and perspectives of all stakeholders involved.

• Chapter 6 — A Case Study Examining the Role of Security Practices in Organisational Culture: This chapter demonstrates, through a case study of a university, the role of security in organisational culture represented in a conceptual model of the organisation. The co-design methodology is applied at the university through interviews with administrative staff, support staff from local and central IT and IT-security teams, as well as senior security decision-makers. The co-design methodology reveals the significance of bridging any existing gaps in security support and aiming for alignment between stakeholders by fostering effective communication, trust, and relationships between security providers and employees.

1.2 Thesis contributions

The work presented in this thesis makes several research and methodological contributions towards understanding the role of organisational culture in security behaviours and compliance with security policy, as well as the importance of co-design and stakeholder involvement when studying human-centred security. The main contributions of the thesis are summarised in the following way:
1 Introduction

1.2.1 Empirical and analytical contributions

- Current approaches to security interventions reflect expectations from traditional economics, even when methods from behavioural economics, such as nudging, are applied to encourage secure behaviours. Such approaches assume that employees are rational — as opposed to boundedly rational — and do not support non-expert employees in finding and adopting appropriate security behaviours. We identify and address this contradiction by constructing a framework that accommodates a set of security behaviours, as a continuous programme of choices which must be provisioned for to adequately support ‘good enough’ security decisions. By applying knowledge from both traditional and behavioural economics, we map out the necessary moving parts for making meaningful user-facing policies.

- The first case study — with Company A — provides an example of how an exaggerated or inadequate policy design can impact, not only the security culture, but the entire culture of the organisation. The consequences that a breach may have on an organisation’s security investments and overall strategy are rarely studied, making the point of view provided in this case study a unique one. In addition, the study highlights that a lack of financial and human resources — often seen as the main barrier to achieving security in organisations — is not always the solution to every single security problem. Although Company A was able to invest significantly in security, the lack of effective communication was a source of friction in the organisation.

- We surface the complex and interconnected nature of supporting workable security practices of employees by analysing security use and support in the same organisation according to the proposed co-design approach, evidenced through direct qualitative engagement. Within the partner organisation studied here, we find that employees appreciated explicit assurance that they were following guidance correctly; they also valued the qualities of local support in understanding their contextual needs, but also in accommodating employees not being sure and asking questions (as the non-experts that organisation security assumes them to be). This highlights new, informal dimensions to technical support (Poole et al. 2009) and support networks (Kocksch et al. 2018); specifically, translating these processes to the setting of a workplace. The findings of this thesis surface the role of care in IT security (Kocksch et al. 2018), including the moralities around how to engage constructively with employees who are not sure how to exactly ‘do the right thing’ for security (Kirlappos, Beaumé and Sasse 2013).
1.2.2 Methodological contributions

- In this thesis, significant modelling challenges are identified in the various stages of the modelling process; the initial phases of modelling, when the purpose and specification of the model are identified, during the construction of the model, and also during the eventual use of the model. Furthermore, the thesis identifies concrete obstacles when trying to represent and model security-related behavioural and cultural factors.

- Through the identification of challenges with modelling in general, and with modelling behavioural and cultural aspects of security in particular, the thesis contributes a new methodology for modelling co-design. We introduce co-design into the classical modelling cycle and develop a methodology for security modelling that addresses the identified challenges. Rather than keeping the stakeholders out of the loop, this co-design process aims to facilitate collaboration and mutual learning between modellers and stakeholders towards achieving a mutually beneficial goal. We structure engagement through a novel co-design approach — applied in a second case study at a large university — and executed with senior security managers at the centre, framed around their decision-making concerns and options (such as policy communications, and usability characteristics of provisioned security technologies). This serves to directly link the study of employees and support staff to security managers, to produce a multi-stakeholder view of the complexities of provisioned security in an organisation (Parkin, Van Moorsel et al. 2010).

- The university study enabled engagement with distinct stakeholder groups within a large organisation, namely employees and support teams, within an approach that also involved regular engagement with security managers. Support teams especially have been rarely considered in research up to now, despite their role in resolving problems (such as with passwords, access cards, etc.) and ensuring access to provisioned IT. By linking the experiences of different groups within the same organisation through security management decisions, we detail a richer picture of the story of organisational security provisioning and identify connections through an iterative co-design approach.

1.3 Published work

All research presented in this thesis has been conducted in collaboration with fellow researchers. Several chapters make use of manuscripts that have been produced both by the thesis author and other co-authors. While the thesis author is the first
author and main contributor of all the publications included in this thesis, it is likely that parts of manuscripts that were not entirely phrased by the thesis author have been reused. Each chapter indicates which original publication the work is based on.

The publications which underpin chapters of this thesis, as well as the thesis author’s personal contributions, are listed below:

Chapter 3: Security Economics for Behaviour Intervention


**Summary.** The paper presents a model for ‘bounded security decision-making’, which attempts to integrate various insights from behavioural economics, psychology, human factors, and complex systems into a unified framework of how security decisions are made.

**Author’s contributions.**
1. Reviewed the concepts of rationality, including the original concept of rationality stemming from traditional economics, as well as the concept of bounded rationality from behavioural economics;
2. Applied the concept of bounded rationality to security decision-making, considering both individual and group decision-making;
3. Presented a framework for security choices which demonstrates a decision-maker’s process of bounded security decision-making, taking into account decision-maker preferences, information asymmetries, moral hazard, and available policy and decision-maker choices;
4. Designed the framework implementation steps to be applied in organisations;
5. Wrote, reviewed, and presented the paper at STAST 2019;
6. Extended the original paper with consideration of culture and team dynamics for the journal version.

Chapter 4: A Case Study of Post-breach Security Changes

**Paper.** 2 Fast 2 Secure: A Case Study of Post-Breach Security Changes by Albesë Demjaha, Tristan Caulfield, M. Angela Sasse and David Pym, IEEE

**Summary.** The paper presents a qualitative case study where 15 semi-structured interviews are conducted with security managers in an organisation which navigates post-breach security changes.

**Author’s contributions.**
1. Facilitated research opportunity and goals with organisation stakeholders;
2. Was embedded in the organisation, where author worked in the security department and engaged with employees and stakeholders during a period of 6 months;
3. Designed case study methodology;
4. Conducted all 15 face-to-face interviews with security managers;
5. Transcribed all interviews;
6. Analysed all interview transcripts using Thematic Analysis;

**Chapter 5: Co-design for Security Modelling**


**Summary.** The paper proposes a co-design methodology for security modelling by integrating the concept of co-design into the classical modelling cycle. The work focuses on the engagement between modellers and stakeholders in the process of objective identification and model specification, design, and construction.

**Author’s contributions.**
1. Identified the challenges of modelling in general, and those of modelling behavioural and cultural aspects of security in particular;
2. Reviewed existing work in the field of co-design and modelling applied in the security domain;
3. Integrated the concept of co-design into the classical modelling cycle by providing a ‘human factors’ perspective;
4. Extracted methodological reflections from a case study;
5. Demonstrated co-design in a real-world context;
6. Mapped case study reflections to our co-design process;
7. Wrote and presented the paper at STAST 2021.

Chapter 6: A Case Study Examining the Role of Security Practices in Organisational Culture

Paper. The trivial tickets build the trust: A co-design approach to understanding security support interactions in a large university by Albesē Demjaha, David Pym, Tristan Caulfield and Simon Parkin (working draft — to be submitted).

Summary. The paper applies a co-design methodology to address the alignment between centrally-mandated and locally-managed security initiatives in the setting of a large university and presents a conceptual model of these interactions. This involves iterative rounds of interviews connected by the co-design methodology: 14 employees working with high-value data with specific security needs; 7 support staff across both local and central IT and IT-security support teams; and two senior security decision-makers in the organisation.

Author’s contributions.
1. Designed the study methodology;
2. Applied a co-design approach by continuously engaging with university stakeholders;
3. Conducted all 21 interviews via MS Teams;
4. Transcribed all interviews;
5. Analysed all interview transcripts using Thematic Analysis;
6. Designed conceptual model;
7. Provided recommendations to stakeholders;
8. Wrote and revised the majority of the paper.

1.4 Our concept of security culture

It is important to clarify in advance what we mean by frequent terminology used in this thesis, in this case — (information) security and security culture.

We define security in the following way:

Security is about ensuring that just the right agents have access to just the right resources at just the right times.

We also note that in this thesis, ‘security’ and ‘information/cyber security’ are used interchangeably. We do not assume a big difference between security more
generally and information security in particular. Referring to the definition above, an instance of information security is when the resources to be accessed are information resources, but on the other hand, the security problem of information resources may well depend on the security problem of other resources as well. For example, if a piece of information is stored in a safe which can only be accessed by a key, the security of that information then depends on keeping the key safe. We therefore make a choice to not decouple security and information security for the purposes of this thesis.

The definition of security culture must relate to the definition of security in the first place. The concept of security and the concept of security culture are related by policy and behaviours — and other factors or components in culture which have some sort of mapping to the definition of security. For the purposes of this thesis, we keep the following broad definition of security culture:

‘Security culture can be characterised as how we do security around here.’
(adapted from Deal and Kennedy 1982; Schein 2010)

The definition above is helpful yet not limiting and additional components can be attributed to the definition, as those components may differ from context to context. For example, from the studies in this thesis, relevant components relating to security culture are communication, policy (and lack thereof), behaviours, involvement of employees, relationships, context, and organisational structure.

1.5 Thesis structure

The thesis consists of eight chapters, including the current introductory chapter. The role of Chapter 2 is two-fold. Primarily, it serves as a literature review which explores the moving parts of organisational and security culture and how these can be captured in a real-world setting. Additionally, the chapter focuses on the role of co-design in modelling behavioural and cultural aspects of security and the overarching co-design methodology that is revisited throughout the thesis.

Chapter 3 explores how behaviour interventions in organisations can benefit from both traditional and behavioural economics. The chapter presents a framework for accommodating bounded security decision-making — within an ongoing programme of behaviours which must be provisioned for and supported.

Chapter 4 presents an in-depth case study of a single company, reflecting the impact of post-breach security changes on the company culture. The use of participatory methods in the case study marks the beginning of co-design thinking in the thesis.
Chapter 5 introduces a methodology that engages modellers and system stakeholders through a modelling co-design process. The co-design approach aims to tackle the challenges of problem definition, data availability, and data collection associated with modelling behavioural and cultural aspects of security. The chapter also reflects on the case study presented in Chapter 4, and the methodological insights that largely shaped the eventual co-design methodology presented in Chapter 5.

Chapter 6 presents a final case study conducted at a large university. The case study explores individual security behaviours and how these are shaped by policy, but also by local team and individual responses to security situations. The work in this chapter aims to identify the dynamics between security provisioning and the organisational culture, inform the conversation around security culture, and its relationship with skills and expectations associated with other non-security behaviours in the workplace.

The discussion in Chapter 7 brings together the findings from previous chapters and discusses them in light of existing research. Chapter 7 also reflects on the interdisciplinarity of this thesis and discusses the methodological aspects of the thesis.

Finally, Chapter 8 summarises the conclusions and directions for future work. It also proposes a number of recommendations for practitioners and researchers working in the field of security.
Background: Organisational Culture and Co-design Foundations

‘Tell me and I forget, teach me and I may remember, involve me and I learn.’

(Xunzi 312-230 BC)

This chapter provides motivational background for the remainder of the thesis. Here, we provide a detailed account of current literature in security culture — by focusing on defining, understanding, measuring and transforming security culture. The chapter reflects on whether security culture should be defined in a silo, or as part of organisational culture. We summarise the identified gaps in current security culture literature and motivate the need for the rigorous modelling of security culture through a co-design methodology. As noted in the Introduction (Section 1.1), this chapter addresses the research questions by analysing relevant literature, and exploring the relationship between security culture and organisational culture as well as the need for a better, and more practical representation of this relationship for decision-makers and practitioners.

Sections 2.5 and 2.6 are an edited version of the following publication:

2: Background: Organisational Culture and Co-design Foundations

2.1 Organisational culture

Organisational culture was first introduced by Jacques in 1951 (Hatch 2018). Although the theory did not gain much attention at first, it soon amounted to a considerable body of research (Hatch 2018). A commonly used phrase in association with organisational culture is — ‘how we do things around here’ (Deal and Kennedy 1982). However, there are several authors that have provided their own definitions of organisational culture, as summarised in Table 2.1. Although the definitions seem quite different from each other at a first glance, they actually comprise of very similar terminology. The most common word used in the majority of the definitions is members, which suggests that organisational culture relates to a set of members. Other patterns are visible in the terminology used to describe organisational culture. For example:

- Way of thinking and doing of things; way in which members relate; way things get done; way to perceive, think, and feel;
- Behaviours required to fit in; appropriate behaviours; how people behave;
- Collectively accepted meanings; common understandings; shared emotionally charged belief systems; system of shared values.

It is evident that organisational culture is contingent upon a community and that particular community’s behaviours, and common understandings. All the authors referenced in Table 2.1 portray this in one way or another. However, culture is not developed by every single collection of people (Schein 2010). When using the word community, especially as part of organisational culture definitions, that word entails a sufficient amount of shared history between that community to even be able to develop a culture. Thus, instead of using ‘a collection of people’ to define organisational culture, the words community, group, or team are better suited to indicate some level of culture formulation (Schein 2010).

Looking at the very first definition (Hatch 2018), organisational culture is almost described as a process that must be learned when joining an organisation in order to fit in. However, it is also pointed out that the culture is only shared between all of the organisation’s members ‘to a greater or lesser degree’. This implies that there will be members in the organisation whose views may differ from the majority’s views or who simply have not had sufficient experience with the rest of the community and therefore lack shared assumptions. Schein explains that shared assumptions often lead to the creation of subcultures within the organisation (Schein 2010). Members of subcultures often have something in common; this could be a similar experience, educational background, or even a shared task. Such ‘silos’ or ‘stove pipes’ can
<table>
<thead>
<tr>
<th>Author</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliot Jacques (1952)</td>
<td>‘The culture of the factory is its customary and traditional way of thinking and doing of things, which is shared to a greater or lesser degree by all its members, and which new members must learn, and at least partially accept, in order to be accepted into service in the firm.’</td>
</tr>
<tr>
<td>Andrew Pettigrew (1979)</td>
<td>‘Culture is a system of publicly and collectively accepted meanings operating for a given group at a given time. This system of terms, forms, categories, and images interprets a people’s own situation to themselves.’</td>
</tr>
<tr>
<td>Geert Hofstede (1980)</td>
<td>‘Organisational culture is defined as the way in which members of an organisation relate to each other, their work and the outside world in comparison to other organisations.’</td>
</tr>
<tr>
<td>Deal and Kennedy (1982)</td>
<td>‘Organisational culture refers to the way things get done around here in the organisation.’</td>
</tr>
<tr>
<td>Meryl Reis Louis (1983)</td>
<td>‘Organisations are culture-bearing milieux, that is, they are distinctive social units possessed of a set of common understandings for organising action and languages and other symbolic vehicles for expressing common understandings.’</td>
</tr>
<tr>
<td>Edgar Schein (1985)</td>
<td>‘The pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to these problems.’</td>
</tr>
<tr>
<td>Robert A. Cooke (1987)</td>
<td>‘Culture refers to the behaviours that members believe are required to fit in and meet expectations within their organisation.’</td>
</tr>
<tr>
<td>John Van Maanen (1988)</td>
<td>‘Culture refers to the knowledge members of a given group are thought to more or less share; knowledge of the sort that is said to inform, embed, shape, and account for the routine and not-so-routine activities of the members of the culture...A culture is expressed (or constituted) only through the actions and words of its members and must be interpreted by, not given to, a fieldworker...Culture is not itself visible, but is made visible only through its representation.’</td>
</tr>
<tr>
<td>Harrison Trice and Janice Beyer (1993)</td>
<td>‘Cultures are collective phenomena that embody people’s responses to the uncertainties and chaos that are inevitable in human experience. These responses fall into two major categories. The first is the substance of a culture - shared, emotionally charged belief systems that we call ideologies. The second is cultural forms - observable entities, including actions, through which members of a culture express, affirm, and communicate the substance of their culture to one another.’</td>
</tr>
<tr>
<td>Stephen McGuire (2003)</td>
<td>‘Organisational culture is a system of shared values, beliefs and norms of members of an organisation, including valuing creativity and tolerance of creative people, believing that innovating and seizing market opportunities are appropriate behaviours to deal with problems of survival and prosperity, environmental uncertainty, and competitors’ threats, and expecting organisational members to behave accordingly.’</td>
</tr>
<tr>
<td>Eric Flamholtz (2001; 2011)</td>
<td>‘In a very real sense, corporate culture can be thought of as a company’s “personality.” Every organisation regardless of size has a culture that influences how people behave, in a variety of areas, such as treatment of customers, standards of performance, innovation, etc.’</td>
</tr>
</tbody>
</table>

Table 2.1: Definitions of organisational culture.
sometimes create communication barriers in the organisation. In order to maintain the effectiveness of an organisational culture, such barriers must be overcome and a goal alignment must be reached between the various subcultures (Schein 2010).

In order to extend the meaning of organisational culture beyond its various definitions, we use Schein’s model of organisational culture (Schein 2010). This model has been widely accepted in the research community of organisational culture and is the model on which most security culture frameworks are based on (Schlienger and Teufel 2002; Kraemer and Carayon 2005; Van Niekerk and Von Solms 2005; Furnell and Thomson 2009). In fact, security culture is often automatically linked to Schein’s model, treating said model as the default for organisational culture (Da Veiga and Eloff 2010).

Schein views organisational culture as an individual’s set of assumptions within a group. These assumptions are divided into three levels, each level of assumptions being more difficult to articulate and change (Schein 2010). Table 2.2 describes the three levels of assumptions in more detail.

<table>
<thead>
<tr>
<th>Table 2.2: Schein’s three levels of culture (adapted from Schein 2010).</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Artefacts</td>
</tr>
<tr>
<td>Visible and feelable structures and processes</td>
</tr>
<tr>
<td>Observed behaviour</td>
</tr>
<tr>
<td>(Difficult to decipher)</td>
</tr>
<tr>
<td>2. Espoused Beliefs and Values</td>
</tr>
<tr>
<td>Ideals, goals, values, aspirations</td>
</tr>
<tr>
<td>Ideologies</td>
</tr>
<tr>
<td>Rationalisations</td>
</tr>
<tr>
<td>(May or may not be congruent with behaviour and other artefacts)</td>
</tr>
<tr>
<td>3. Basic Underlying Assumptions</td>
</tr>
<tr>
<td>Unconscious, taken-for-granted beliefs and values</td>
</tr>
<tr>
<td>(Determine behaviour, perception, thought, and feeling)</td>
</tr>
</tbody>
</table>

Due to the complexity of each of these assumption levels, achieving cultural change in an organisation is a challenging process. As a basis for cultural change, Schein recommends talking to as large number of employees as possible to get a detailed account of their underlying backgrounds (Schein 2010). Changing the organisational culture is a transformation process which first requires the unlearning of behaviours in order to move on to new ones (Schein 2010). Cultural interventions should occur when differences are identified between the current and the desired culture. According to Schein, such a transformation process primarily relies on influential people in the organisation which are often part of senior management or even the board (Schein 2010). A full description of Schein’s model of organisational
culture can be found in his book which specifically addresses the above issues (Schein 2010).

2.2 Security culture

As information security has transformed into an asymmetrical race between organisations and cyber criminals, technology-oriented measures are not sufficient to keep an organisation secure. Given that the majority of breaches are attributed to user behaviour (Sasse, Brostoff and Weirich 2001), organisations should increasingly focus on employee behaviour. Many authors have advocated that developing a security culture is necessary within organisations in order to improve their overall security (Martins and Elofe 2002; Schlienger and Teufel 2002). In fact, there is empirical evidence that a strong security culture drives policy compliance (D’Arcy and Greene 2014) and that cultivating a security culture decreases the risk to information assets (Da Veiga and Eloff 2010).

Although security culture is often treated as a ‘panacea’ to all security challenges — a solution to insecure behaviours and non-compliance — it is actually a very complex concept to understand, define, as well as implement. Maynard, Ruighaver and Chia acknowledge the fact that the larger part of authors who advocate for security culture do not have a clear definition of what it is, or an understanding of how to develop it (2002). Security culture literature has been expanding rapidly, but unfortunately not many solutions have been provided for the fundamental problems which have been identified in the field, and many works tend to oversimplify security culture (Reid, Van Niekerk and Renaud 2014). Below is a review of the contributions that have been made so far in the security culture literature as well as the gaps that remain.

2.2.1 What is security culture?

The academic community working on security culture has acknowledged the importance of having a clear and standardised definition of security culture (Schlienger and Teufel 2002; Maynard, Ruighaver and Chia 2002; Malcolmson 2009).

Ruhwanya and Ophoff categorised security culture definitions into four types; shared values view, action-based view, mental model view and problem-solving view (2020). While each understanding of security culture contributes to research (Ruhwanya and Ophoff 2020), different definitions still circle around, with new researchers joining the community not knowing which one to refer to. Many of these definitions are adapted from organisational culture (Schein 2010), while others have been
created by the authors themselves. Despite the parallels between definitions for organisational culture and security culture, there is no universally agreed upon description (Uchendu et al. 2021). The following are some examples of definitions created by the security community:

- ‘Information security culture has three focus areas namely artefacts and creations; collective values, norms and knowledge; and basic assumptions and beliefs.’ (Schlienger and Teufel 2003b)
- ‘An information security culture emerges from the assumption about what characteristics and behaviour are encouraged to be acceptable, and it results in the manner people behave with regard to information security in the organisation.’ (Martins and Elofe 2002)
- ‘Security culture is a descriptive term about how members perceive security within the organisation.’ (Woodhouse 2007)
- ‘Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact.’ (Malcolmson 2009)
- ‘The attitudes, assumptions, beliefs, values and knowledge that employees and stakeholders use to interact with the organisation’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time.’ (Da Veiga and Eloff 2010)

One observation that came out of this literature search is that many authors discuss the necessity of defining security culture prior to continuing to anything more specific, however, only a few of them actually provide such a definition. There were not many more definitions available other than the ones included above. At this stage, it cannot be concluded whether any of the above definitions are adequate enough to be used for further work or to qualify as an accepted definition of security culture. However, Da Veiga carefully assessed some more frequently used definitions of security culture (such as that of Schlienger and Teufel 2003b, Martins and Elofe 2002 and one by the Information Security Forum2) – to create a definition of her own:

2: Information security culture refers to the shared values (‘what is important’) and beliefs (about ‘how things work’) that people in the organisation have about information security. It interacts with the organisation’s systems and procedures to influence behaviour (‘the way we do things around here’) Forum 2000.
2.2: Security culture

‘An information security culture is defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in an organisation to protect its information assets. This information security culture changes over time.’ (Da Veiga et al. 2008)

Although Da Veiga’s definition of security culture remains one among others, she at the very least used a method to evaluate other definitions and compose a better one for the purpose of her own research. Such practice should be encouraged and implemented by others – especially when publishing a piece on security culture. Furthermore, organisations that intend to focus on security culture for the purpose of improving their overall security, should also define what they mean by the term.

Similarly to definitions of security culture, Nasir et al. did not find a set of accepted concepts and dimensions describing security culture (2019). There are however certain dimensions that are more commonly found when measuring security culture. Based on the number of occurrences, dimensions such as change management, security policy, leadership and governance, and trust are used more frequently (Nasir et al. 2019). The frequency of these dimensions is also reiterated by Uchendu et al. who identify top management, responsibility and trust, as well as change management as recurring dimensions for security culture (2021). However, the dimensions are not always consistently defined either (Nasir et al. 2019; Uchendu et al. 2021; Malcolmson 2009) — as for example with trust — which has been defined as the level of trust between managers and employees (Martins and Elofe 2002; Da Veiga, Martins and Eloff 2007), but also as the trust users have in the communications of the organisation (Da Veiga and Martins 2015; Martins and Da Veiga 2014).

2.2.2 Security culture and organisational culture

The concept of security culture stems from that of organisational culture. But, there is little research exploring the relationship between the two. The conceptualisation of information security culture is mostly based on concepts of organisational culture (Nasir et al. 2019), which is also in line with the findings of Reid, Van Niekerk and Renaud (2014), and Schlienger and Teufel (2002) who consider information security culture a subculture of organisational culture. According to Uchendu et al., there is a clear relationship between definitions used to describe security culture
and organisational culture (2021). Lim et al. identify three types of relationships between organisational and security culture (2009):

1. Security culture is separated from organisational culture;
2. Security culture is a subculture of organisational culture;
3. Security culture is embedded into organisational culture.

While these relationship types focus on the extent to which security is an integral part of organisational culture, they should perhaps instead convey how security culture should be treated as a concept. Should it be a separate entity within an organisation, or simply a subculture that exists within the organisational culture? Such a categorisation is crucial in the process of defining what security culture means to organisations. Without making such a decision, it is difficult to go any further into the process of evaluating the culture.

Some authors state that security should be embedded within organisational culture (Connolly 2000; Lim et al. 2010) and focus on factors such as people, training, processes and communications (Martins and Elofe 2002). Nosworthy argues that an organisation’s security is influenced by the organisational culture in such a way that it may hinder change depending on the critical business processes of the company (2000). On the other hand, Lim et al. say that many authors advocate for the creation of an information security culture exactly because the impact of the organisational culture on employees is significant (Lim et al. 2009). According to Woodhouse, in order to secure a company’s information assets, security and risk mitigation should be submerged into organisational culture (2007). By doing so, it would be easier to ensure that all employees are mindful of security when conducting their work tasks.

2.2.3 Measuring security culture

A number of authors have pointed out the importance of being able to measure an organisation’s current security culture before attempting any intervention (Martins and Elofe 2002; Maynard, Ruighaver and Chia 2002; Schlienger and Teufel 2003a; Da Veiga and Elhoff 2010). This has either been done through large-scale surveys or through in-depth interviews. Martins and Elofe developed a questionnaire for measuring security culture in an organisation (2002). They view the organisation in three levels; the organisational, the group, and the individual level. Each of these levels has its own controls – organisational level (policy and procedures, risk analysis, benchmarking, budget), group level (management, trust), individual level (awareness, ethical conduct), and finally, change, which relates to all levels. They developed 45 statements for the questionnaire based on these nine controls.
to evaluate the perceptions and attitudes of employees towards security culture. Likert-type scales were used to determine participants’ responses.

Martins and Elofe’s questionnaire (2002) was later re-evaluated in a different paper (Da Veiga, Martins and Eloff 2007). As a result of this evaluation, the questionnaire was improved and republished (Da Veiga and Eloff 2010). The new ‘assessment instrument’ — as it is referred to in the updated version (Da Veiga and Eloff 2010) — is based on seven information security dimensions (similar to the previous questionnaire) and consists of 85 statements which were also discussed with industry experts. Once again, the assessment instrument uses Likert-type scales.

Schlienger and Teufel use a mixed approach when evaluating security culture — they conduct a questionnaire and interviews (2003a). Their questionnaire targets the company’s employees and focuses on three parts; individual attitude, perception of company’s attitude, and best solution (Schlienger and Teufel 2003a). The interviews, on the other hand, are conducted with the Chief Information Security Officer of the company as well as a security technician. They are unstructured interviews and focus on the company’s security policy, corporate culture, and the analysis of the questionnaire results. In a following paper, Schlienger and Teufel state that a questionnaire is best suited for an assessment (2005). Similarly to Martins and Elofe, their updated questionnaire divides organisational behaviour into three layers; organisation, group, and individual (2002). The questions are based on twenty areas borrowed from Robbins’ organisational behaviour model (Robbins 2001). The questionnaire consists of 42 questions answered on a five point Likert scale (Schlienger and Teufel 2005).

Maynard, Ruighaver and Chia develop a research model for assessing security culture within an organisation (2002). Their model is based on Detert, Schroeder and Mauriel’s framework which is linked to a set of values and beliefs that influence successful Total Quality Management (2000). The research model consists of several dimensions, including orientation to work, tasks, co-workers, and isolation versus collaboration/cooperation. The authors conducted in-depth interviews with three employees of an organisation. The questions were based on a careful evaluation of information security areas identified from security literature as well as on the model dimensions. The goal of the interviews was to determine participants’ security awareness, their personal security habits, and most importantly, the security culture in the company (Maynard, Ruighaver and Chia 2002).

Although measuring security culture through surveys is the most common practice, this method does not always lead to the accurate measurement of day-to-day security behaviours (Uchendu et al. 2021). Conducting case studies, as well as maintaining a close interaction with practitioners can lead to better knowledge of
real-world environments and employees’ day-to-day roles and activities (Uchendu et al. 2021). First and foremost, tools and methods used for measuring security culture should avoid a one-size-fits-all approach and instead adapt to the characteristics of an organisation (Sas et al. 2021).

2.2.4 Transforming security culture

Transforming people’s behaviour is difficult, and requires detailed attention (Lacey 2010). In order to change an organisation’s security culture, the employees’ values, norms, and beliefs must also be changed (Thomson, Solms and Louw 2006). However, an unlearning of such beliefs could result in a strong resistance to change as well as anxiety in employees (Thomson, Solms and Louw 2006). It is therefore important to have a detailed change process when attempting to transform an organisation’s security culture. Some authors have contributed such processes for cultural change (Schlienger and Teufel 2002; Van Niekerk and Von Solms 2005; Thomson, Solms and Louw 2006).

Schlienger and Teufel define a model for information security culture implementation and change based on a pre-evaluation survey conducted at a company and on the theory of internal marketing (2003b). The five main phases of the model are: pre-evaluation, strategic planning, operative planning, implementation and post-evaluation (Schlienger and Teufel 2003b). The implementation phase is further separated into four stages (management commitment, internal communication, know-how transfer and employee commitment) which are supported by the four marketing Ps – product, price, place and promotion (Schlienger and Teufel 2003b).

Van Niekerk and Von Solms present a framework for fostering an information security sub-culture within an organisation (2005). The framework borrows elements from behavioural science theories such as organisational learning theory, transformative change management, and outcomes based education (Van Niekerk and Von Solms 2005). The steps of the framework are the following (Van Niekerk and Von Solms 2005):

1. Attain top management commitment;
2. For each business problem, define the culture change in the context of the specific business problem;
3. Educate the employees;
4. Define culture change metrics;
5. Provide feedback to the employees;
6. Review and refine the culture change process.
Another model for culture change is one named MISSTEV (Model for Information Security Shared Tacit Espoused Values) by Thomson, Solms and Louw (2006). The authors use the term ‘information security obedience’ to describe the combination of corporate culture, information security, and corporate governance (Thomson, Solms and Louw 2006). Thus, the purpose of the MISSTEV model is to achieve information security obedience. The model contains two key components; the Conscious Competence Learning Model and Nonaka’s Modes of Knowledge Creation – the two are merged and create the MISSTEV model (Thomson, Solms and Louw 2006). The first component focuses on the process of learning a new skill or behaviour whereas the second component identifies existing knowledge and converts it into new knowledge. Through the interaction of these two components, the model details the progression from the creation of a corporate information security policy to the achievement of obedience (Thomson, Solms and Louw 2006).

2.3 Modelling security culture

A lot of the works included in this literature review consist of conceptual models and frameworks (for example, Maynard, Ruighaver and Chia 2002, and Van Niekerk and Von Solms 2005). These models and frameworks are predominantly used to show generalised accounts of what security culture is, how it can be measured, and cultivated. Such conceptual models are also useful for providing an in-depth overview of the factors pertaining to security culture and a detailed account of an organisation’s security culture. Other types of models can also be applied to complement the representation of security culture in an organisation. Models are often built and used to assist organisations and people in increasing their effectiveness at work (Pidd 1997). The purpose of these models is not to substitute intelligence or humanity (Pidd 1997), but to rather serve as tools which can help organisations better understand certain concepts and behaviours.

Traditionally, models tend to be created out of data that is collected for a certain research purpose. However, ‘for modelling purposes, data are best ordered à la carte rather than table d’hôte’ (p.97). Simply building a model from any exploratory data may be a mistake (Pidd 1997), and it may negatively affect the usefulness and accuracy of that model. According to Pidd, ‘modelling should drive any data collection and not the other way around’ (p.95). The approach of building models from any given available data should be switched to a model-driven data approach instead. Before attempting any large-scale data collection, it is crucial to already have a relatively clear idea of what type of model might be needed (Pidd 1997).
The type of data to collect can only be determined after developing an idea of the model and its parameters (Pidd 1997).

Security economics is one field in which modelling has shown to benefit information security. For example, the compliance budget (Beautement, Sasse and Wonham 2009) — a conceptual and an economics model — represents how individuals perceive the costs and benefits of security compliance in their organisation. An alternative example of real-world data being matched with a representative model of a system can be seen in the work of Caulfield and Pym, in which the risks of carrying data on USB sticks are mathematically modelled (2015a). Hartmann, Jaeger and Eckhardt, on the other hand, examine how social relations affect information security policy through the use of relational models theory (2018). Simulation modelling has been used to model password policy and its impact (Shay, Bhargav-Spantzel and Bertino 2007), and describe the extent to which the policies of security managers deliver their security objectives (Caulfield and Pym 2015b).

Cultural and behavioural aspects of security are not usually considered when modelling security policy, despite evidence which suggests that security culture drives policy compliance (D’Arcy and Greene 2014). The representation of security culture is often too complex, or oversimplified (Reid, Van Niekerk and Renaud 2014) to be modelled in a useful manner. Behavioural economics provides useful insights about people’s decision-making and interaction with a system, which can in turn aid the modelling of that behaviour (Caulfield, Baddeley and Pym 2016). Modelling of security culture may particularly benefit security managers and other system owners who manage security behaviours in dynamic environments. Conceptual models of organisations can depict the security relationships and interactions in the organisational culture. As a result, security managers can gain a better understanding of the moving components and cultural aspects which are relevant to consider when making security decisions and designing security policies.

2.4 Reflections from literature review

Security culture did not gain the attention of researchers until the beginning of this century (Ruighaver, Maynard and Chang 2007). Only then did they start to recognise the importance of a security culture in maintaining the security of information systems in organisations (Ruighaver, Maynard and Chang 2007). Unfortunately, the majority of this research is still limited in scope and it predominantly focuses on employee compliance with security policies rather than actual behaviour change.

While the security research community has now established that developing a positive security culture can improve security behaviours in organisations, there is
still a lack of practical guidance about how security culture should be approached by managers (Nasir et al. 2019). What does security culture represent for the organisation, which aspects are relevant, how it can be evaluated in this context — these are all difficult questions that managers are left with. Practitioners face the challenge of identifying the adequate aspects of security culture for their organisation (Nasir et al. 2019). While practitioners may carry more knowledge about the real-world environment at the organisation (Uchendu et al. 2021), researchers carry a wider understanding of security culture and its components (Da Veiga et al. 2020). It is challenging to take a ‘one-size-fits-all’ approach when it comes to security culture due to significant differences between organisations — both in their environment and their needs. Tools and methods used should be adaptable to the organisation, and a collaboration between researchers and practitioners is required to create strong and practical-based approaches (Sas et al. 2021). For example, Schlienger and Teufel conduct unstructured interviews with the CISO of an organisation (2003a), and the International Atomic Energy Agency recommends a semi-structured approach which engages staff from the entire organisation (2017).

It is certainly not uncommon to find gaps and limitations within a field of research. However, these limitations become more pertinent when they are consistent throughout the literature in that research community. Malcolmson identified some of these key research gaps more than ten years ago (2009). While contributions made in security culture research so far are clearly valuable, the field remains somewhat fragmented and disintegrated. The following key gaps still remain:

- There is no accepted, standardised way of defining security culture and different meaning is attributed to the same terms by different researchers (Sub-section 2.2.1);
- There is no consensus on the relationship between organisational and security culture or sufficient understanding of how this relationship impacts security behaviours in practice (Section 2.1 and sub-section 2.2.2);
- There is insufficient work representing real-world security environments and cultures when measuring security culture (Sub-section 2.2.3);
- There is a lack of collaboration and shared methodology between researchers and practitioners when studying security culture and consequently insufficient practical guidance for organisations related to security culture (Sub-section 2.2.4 and Section 2.3).
2.4.1 Addressing the gaps

To address the identified gaps in the literature, we propose a novel co-design methodology for security modelling. The methodology aims to facilitate an active relationship with stakeholders, and explore the cultural and behavioural factors of security in organisations. Security managers are often unaware of how their security policies may impact the ability of users to comply with security (Parkin, Moorsel et al. 2010). An effective policy in theory may not necessarily translate into secure behaviour in practice if there is a misalignment between the policy, the employees, and the organisational processes (Beautement et al. 2016). It is important for security managers to become aware of the interdependencies between security mechanisms, the capabilities of employees, and the business processes of the organisation (Parkin, Moorsel et al. 2010). The effectiveness of security solutions and policies are dependent on how employees behave and implement these policies (Coles et al. 2008). A deeper understanding of human behaviour can help determine whether a security policy is cost-effective for the organisation and the employees (Coles et al. 2008). Rather than implementing interventions where employees are expected to already have the required knowledge (Parkin, Arnell and Ward 2021), our approach focuses instead on capturing the different perspectives of stakeholders in the organisation, as well as utilising their areas of expertise.

The next section summarises the co-design foundations which have motivated our work and provides a snapshot of our methodology which is revisited in more detail throughout the thesis.

2.5 Co-design for security modelling

2.5.1 What is co-design?

The term co-design is commonly affiliated with participatory design — established in the 1970s — and user-centred design (David, Sabiescu and Cantoni 2013). As it is predominantly influenced by participatory design, co-design is often treated as an updated term for participatory design (David, Sabiescu and Cantoni 2013). The core principle of co-design is that it facilitates collaboration between all stakeholders in the design process. The established understanding of co-design shifts the expert role from the researcher or designer onto the user or stakeholder (Mironcika et al. 2020), and thus enables the participation of various stakeholders in the design process from the early stages. Kleinsmann and Valkenburg provide a useful definition for co-design which captures the process thoroughly (Kleinsmann and Valkenburg 2008, p.2–3):
‘Co-design is the process in which actors from different disciplines share their knowledge about both the design process and the design content. They do that in order to create shared understanding on both aspects, to be able to integrate and explore their knowledge and to achieve the larger common objective: the new product to be designed.’

David, Sabiescu and Cantoni similarly argue that co-design is based on shared goals and a collective understanding between all stakeholders, while still accounting for the difference in their perspectives and expectations (2013). In order for co-design artefacts to be effective, they should relate to — and reflect the views of the group intended to benefit from it (David, Sabiescu and Cantoni 2013). Co-design has been associated with benefits such as improved creativity and idea generation as well as better knowledge and cooperation between stakeholders (Steen, Manschot and De Koning 2011). According to Steen, co-design can be viewed as a process of abduction (2013). A similar perspective is provided by Dorst, who argues that abduction is fundamental to design thinking (2011). When co-design is done through abduction, problems and potential solutions are explored in an iterative process whereby problem and solution co-evolve (Steen 2013, p.18).

The application of participatory methods in security was not always considered a step in the right direction (Faily et al. 2013). Users were, for a very long time, treated as the problem rather than a part of the solution (Nhinda and Shava 2021). Applying participatory methods such as co-design and co-creation are necessary to reflect the perspective of users and stakeholders, and to derive secure practices collectively (Nhinda and Shava 2021). In addition, co-design ensures the consideration of contextual and cultural factors when designing security solutions (Bada, Sasse and Nurse 2019).

2.5.2 Co-design and modelling

Participatory modelling (PM) is the closest representation of co-design in modelling. It can be defined as ‘a purposeful learning process for action that engages the implicit and explicit knowledge of stakeholders to create formalised and shared representations of reality’ (Voinov et al. 2018, p.1). PM addresses the realisation that stakeholders are more likely to comply with policies if they are engaged in the process of developing those policies and that they can contribute useful knowledge, experience, and skills to the process (Voinov et al. 2016).

The terms participatory modelling, collaborative modelling, and co-modelling are often used interchangeably, as no clear distinctions have been identified between them (Basco-Carrera et al. 2017). Basco-Carrera et al. attempt to make a distinction
by associating collaborative modelling more strongly with co-design as it is better suited for contexts with high cooperation (2017). PM, on the other hand, involves a lower level of cooperation in comparison.

Methods such as participatory and collaborative modelling have emerged because of an increased focus on stakeholder involvement in fields such as water resources management. In fact, most work in participatory modelling has been done in research areas such as environment and planning, water resources management, and resource and environmental modelling (Landström et al. 2011; Basco-Carrera et al. 2017; Voinov et al. 2016; Voinov et al. 2018).

Ideally, stakeholder involvement would occur in most (if not all) stages of participatory modelling (Voinov et al. 2016). Given that complete participation is not always a possibility, there are ‘ladders’ of stakeholder participation which differentiate between different levels of involvement (Basco-Carrera et al. 2017). Co-design is better suited for our methodological approach due to its increased focus on high stakeholder participation.

### 2.5.3 Co-design and security

To the best of our knowledge, there is a scarcity of work in security research that applies participatory modelling or co-design. Ionita et al. implement the principles of participatory modelling to evaluate whether such a collaborative approach would improve the quality of final models (2015). They apply their approach in the context of a risk assessment and find favourable results from implementing participatory modelling (Ionita et al. 2015). Coventry et al. utilise the concept of co-creation in the development of their behaviour change framework (2014).

Beautement et al. emphasise the importance of capturing data in a real-world environment by proposing a methodology which consists of passive and active data collection cycles — meant to collect accurate data about security behaviours and attitudes in organisations (2016). Heath, Hall and Coles-Kemp intersect aspects of co-design and participatory physical modelling when designing the security of a home banking system (2018). Their methodology engages participants in a process of creative interaction in which they address different security scenarios by using LEGO kits and deliver useful insights by doing so (Heath, Hall and Coles-Kemp 2018).

The above-mentioned examples demonstrate co-design thinking and principles (Beautement et al. 2016), and attempt to facilitate an interaction between co-design and modelling (Heath, Hall and Coles-Kemp 2018). However, no comprehensive methodology has been proposed for co-designing security modelling, at least not
one that reflects our understanding of co-design. Our approach aims to facilitate stakeholder involvement on a deeper level, by agreeing on the objectives in the beginning, and ensuring continued participation — and co-creation — throughout the entire co-design process.

2.6 Our co-design methodology

This section introduces new, original thesis work which is then presented in Chapter 5 in greater detail. A synopsis of the co-design methodology is presented in this section in order to provide context to the reader about the importance of the methodology early on in the thesis.

The task of managing organisational security is often accompanied by a level of uncertainty and complexity. This uncertainty impacts both the security managers who are responsible for achieving the organisation’s security objectives, and the employees who are faced with taking security decisions on a daily basis. Modellers are also faced with uncertainties about what security problems should be modelled, and which data is available and should be collected. The security culture literature shows that organisational culture is a complex phenomenon and often an important factor for policy decisions and security behaviours. The knowledge of security stakeholders is necessary for understanding and representing such a complex phenomenon accurately. The identified gaps in the literature emphasise the need to better understand security culture in real-world environments and bridge the gap between researchers/modellers and practitioners.

For the purpose of helping modellers and stakeholders overcome some of these challenges, we propose a model co-design methodology for security. We use the term modellers to refer to a collection of stakeholders who collaborate and contribute to the construction of the model. This may include researchers and academics who use a range of different modelling tools in their work. In this instance, the modellers are a team consisting of experts in human-centred security as well as experienced security modellers. A co-design modelling process will bring both modellers and stakeholders together in a cooperative process to produce a model that deepens the understanding of all stakeholders involved. We define our co-design methodology in the following way:

*Model co-design is a process that engages modellers and system stakeholders cooperatively in the acts of objective identification and model specification, design, and construction with the aims of aligning model objectives with the needs of the stakeholders; and designing a model that...*
is feasible given the limits of data availability, which are discovered as part of the process.

This definition captures something that is quite different from participatory modelling. Because our methodology facilitates the construction of a shared understanding, there is built in from the beginning, not only the interpretation of the domain by the modellers, but the interpretation of the model by the domain experts. Participatory modelling, on the other hand, is driven by the modellers and appropriate advice is taken from various stakeholders at various points. Here we posit a stronger requirement — the model that is agreed upon has to be understood — and properly reflect the understanding of the stakeholders, not merely the modellers’ understanding of the understanding of the stakeholders.

Figure 2.1: The classical mathematical modelling cycle. (see, e.g., McColl 1995)

We can describe our co-design modelling process as a modification of the classic modelling cycle, which is shown in Figure 2.1. The perspective of the classic modelling cycle is very modelling- and modeller-centric and it assumes that the objectives of the model have already been specified.

We then show Figure 2.2 as an updating of the basic classical cycle to incorporate a translation zone between the domain and model side (Caulfield, Ilau and Pym 2022b). Later — in Figure 2.3 — we go into a lot more detail on how to understand the incorporation of the translation zone. The main contribution of the later representation comes at the level of application, and how the cycle can be implemented in practice. In our conception of co-design, modellers and stakeholders work together to determine the objectives of the model, which are refined based on observations of the system, the data required to produce a model, and the limits of data availability. Figure 2.3 presents our co-design cycle.

Our methodology enables better opportunities for capturing the behavioural and cultural aspects influencing security in organisations. By aiding a better understand-
2.7 Summary

Figure 2.2: Co-design in the translation zone (adapted from Caulfield, Ilau and Pym 2022b).

...ing of the system, co-design can help improve security decision-making. Modelling, whether conceptual or otherwise, can be used as a tool for managing uncertainty associated with security decisions (Fielder et al. 2016). Modelling security culture through a co-design approach can help facilitate the required system and context knowledge to represent culture more accurately. By engaging stakeholders from an early stage, any knowledge that they may possess can be integrated into the process in its very foundational stages. Co-creating the questions (or problem) with the stakeholders is just as important as co-creating the model. Better questions allow for a better understanding of what a model needs to do, and what data is needed for it. In addition, stakeholders can help identify opportunities to capture observations of the cultural and behavioural aspects influencing security policy. Constructs from traditional and behavioural economics can then be used to characterise those observations in ways that are better suited for modelling by considering theories such as bounded rationality and herd behaviour (Caulfield, Baddeley and Pym 2016).

2.7 Summary

This chapter aimed to (1) provide the motivation for the co-design methodology by reviewing current literature in security culture and identifying relevant gaps, and (2) give a general overview of our methodology and its co-design foundations. Our
<table>
<thead>
<tr>
<th>Modelling Cycle</th>
<th>Description</th>
<th>Stakeholders</th>
<th>Modellers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td>The cycle starts when a stakeholder, such as a system manager, has questions about a system. Observations about the architecture and behaviour of the system. Observations about the availability of data. Data collection. Induction of candidate model via techniques such as abduction and dialogue between stakeholders and modellers. Interpretation against observations. This is the translation zone.</td>
<td>Stakeholders may have questions about the design or behaviour of the system.</td>
<td>Modellers accept that there is a prima facie case for the applicability of their techniques.</td>
</tr>
<tr>
<td>Observation &amp; Candidate Model Data Availability</td>
<td>Design of a candidate model subject to observations and available data. Deduction from properties of the candidate model alone. A collection of properties of the candidate model that can be interpreted back in the domain. Interpretation of candidate model properties as domain properties. A collection of properties of the domain implied by properties of the candidate model. Validation of the implied properties of the domain against observed properties of the domain. Candidate model meets objectives, passes validation, and therefore becomes the model.</td>
<td>- Share their knowledge of the system and the questions they have about it. - Express their desired outcomes from the modelling process. - Share insights about available data and its limitations. - Support the translation of observations into candidate model structure and parameters.</td>
<td>- Interpret the requirements from the stakeholders. - Learn about the system from stakeholders. - Share capabilities and constraints of the modelling tools and process. - Design the candidate model.</td>
</tr>
<tr>
<td>Interpretation</td>
<td>Model Consequences</td>
<td>Observe what properties of the model are derived.</td>
<td>Extrapolate preliminary consequences from the candidate model.</td>
</tr>
<tr>
<td>Induction</td>
<td>Domain Consequences</td>
<td>Collaboratively establish a method for translating properties of the model to properties of the domain. Express properties of the domain that are implied by properties of the model.</td>
<td></td>
</tr>
<tr>
<td>Deduction</td>
<td></td>
<td>Compare the properties of the domain that are implied by the model with the observed properties of the domain. Understand the model sufficiently and can use it in the domain.</td>
<td></td>
</tr>
<tr>
<td>Finish</td>
<td></td>
<td>Observe the validation because they need to understand its result for the next step of the iteration of the candidate model. Evaluate the model in reference to the objectives.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2.3: Modelling cycle, translation zone, and co-design.
methodology is described in greater depth in Chapter 5, and is further explored in Chapter 6. The next chapter presents analytical work in security decision-making, based on constructs from traditional and behavioural economics.
Security Economics for Behaviour Intervention

‘The behaviour of individuals is the tool with which the organisation achieves its targets.’

(Herbert A. Simon 1947)

3.1 Introduction

Information security in larger organisations is often managed by an information security manager and/or a security team — the (information) security function of the organisation. The security function is recognised as having the expertise to identify and manage the security technologies and processes necessary to protect the organisation from threats to its assets. Outwardly, this is embodied in controls and procedures, often detailed in the organisation’s security policy (or policies).

Policy may dictate specific security-related behaviours, which employees are expected to adopt. There are myriad ways to promote adoption of a behaviour (Carabán et al. 2019), with challenges in guaranteeing successful change (Renaud and Zimmermann 2018). Declaring a behaviour in a security policy is not an assurance that the behaviour will happen. This reality has drawn increasing attention to the need to manage behaviour change effectively. Consideration of behaviour change theory and behavioural economics (Briggs, Jeske and Coventry 2017) is one such approach.

Both research and practice have shown that behaviours defined in policy may not be adopted in organisations. Employees may not see how policy applies to them, find it difficult to follow, or regard policy expectations as unrealistic (Kirlappos, Beaumont and Sasse 2013) (where they may well be (Information Security Forum...
Rather than abandoning security, employees may create their own alternative behaviours (Blythe, Koppel and Smith 2013), in an effort to approximate secure working (Kirlappos, Parkin and Sasse 2014). Organisational support can be critical to whether secure practices persist (Dourish et al. 2004) or whether security-related issues begin to be delegated to others.

To compound these challenges, security policies in organisations may not fit the security needs and ways of working of different employee groups; this extends to how they perceive and address security risks (Beautement et al. 2016; Blythe, Coventry and Little 2015). General advice may be relevant but not actionable, and specific advice only applicable in very particular circumstances (Reeder, Ion and Consolvo 2017). It is then in the security function’s interest to address the distinct security needs of (official or informal) groups of users. For these reasons, the sense of how to work securely can also come from colleagues (Kirlappos and Sasse 2015) or managers (Kirlappos, Beautement and Sasse 2013). If solutions are more specific to a discernible group, the more immediately usable they are for that group, albeit with a need to tailor those solutions upfront. There are, however, benefits to understanding group-specific needs, as with phishing guidance (Steves, Greene and Theofanos 2019), where distinct business functions have their own challenges (e.g., a finance team discerning a genuine invoice email from a fake one, where other functions would simply not expect to receive invoices).

The security function must have a strategy for how to provision for security, provide workable policy, and support user needs. Rational security micro-economics has proved to be useful for explaining the interaction between organisational security policies and behaviours (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016), where security ecosystems are otherwise too complicated to study directly in this way. We revisit principles of information economics and behavioural economics in tandem, identifying contradictions which point to gaps in support.

This chapter addresses the research questions (as highlighted in the Introduction (Section 1.1), through the portrayal of non-security employees as boundedly rational and an exploration of their bounded decision-making process when faced with security choices. The conceptual framework in this chapter highlights the need to understand how security considerations align with other organisational factors and emphasises the importance of aligning security practices with other areas of the organisation, as well as ensuring an integrated approach to security decision-making. The rest of the chapter is structured as follows:

- In Section 3.2, we provide the foundational terminology and definitions that
underpin bounded rationality for security in organisations;

- We review the capacity for various economics principles to explain a range of security-related behaviours (Section 3.3);
- We then demonstrate how current approaches to infrastructure and provisioning of security mirror unbounded, rational-agent economics, even when techniques more familiar to bounded-agent behavioural economics are applied to promote individual behaviours (Section 3.4). We show through examples how these contradictions align with regularly cited causes of security non-compliance from the literature, and point to more appropriate solutions;
- We present a framework (Section 3.5), based on consolidated economics principles, with the following goal:

  Better support for ‘good enough’ security-related decisions, by individuals and groups within an organisation, that best approximate secure behaviours under constraints, such as limited time or knowledge.

This requires identifying the factors affecting security behaviours that should be considered by the organisation in order to inform policy design, support the identification of provisioning requirements, and describe expectations of users. The framework is intended to underpin provisioning to reach this goal.

In considering the factors affecting security behaviours, a clearer consideration can be conducted for establishing assumptions about target groups within an organisation. At present, security controls are generally applied to all users, and interventions are targeted at all users — such assumptions are less likely to be reliable as organisations become larger and more complex;

- We then apply the framework to one of the most widely promoted security behaviours (Section 3.6), the maintenance of up-to-date device software, demonstrating through comparison with independent user studies where the consolidated economics approach — bounded security decision-making — can anticipate organisational support requirements;
- We provide a review of related work (Section 3.7) and conclude with a summary (Section 3.8);
- A supporting glossary of economics terminology is detailed in Appendix A.

The content of this chapter is an edited version of the following publication:

3.2 Terminology

Before we present our conceptual framework, we must make a choice of terminology and definitions. It is important to define explicitly the central concept in this chapter, that of *bounded rationality*. We turn to the definition of Herbert Simon, who introduced the concept of bounded rationality with the following motivation:

‘Broadly stated, the task is to replace the global rationality of economic man with the kind of rational behaviour that is compatible with the access to information and the computational capacities that are actually possessed by organisms, including man, in the kinds of environments in which such organisms exist.’ (Simon 1955, p.99)

We define bounded rationality as the idea that humans have certain constraints — cognitive, time, and information/knowledge — that limit their decision-making processes; as such, bounded rational agents turn to ‘satisficing’ rather than ‘optimising’ (Simon 1955, 1956; Simon 1997; Baddeley 2017). The components of our definition are illustrated in Figure 3.1.

*Cognitive constraints* may include limits on memory or numerical processing, as well as limited skills or knowledge. Having *time constraints* means that a bounded rational agent does not have unlimited time to make a decision — and may therefore be required to sometimes rush a decision. *Incomplete information* suggests that in the real world, complete information is unattainable and the bounded rational agent must take decisions without necessarily knowing everything relevant about that decision. *Satisficing* — in contrast to optimising — is a decision-making strategy which accounts for the above limitations and accepts a ‘good enough’ choice rather

![Figure 3.1: An illustration of bounded rationality.](image-url)
Towards a consistent strategy

Existing research has identified that organisational security approaches may ask too much of staff (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016), or leave staff to adapt advice to their local context (Kirlappos, Beautement and Sasse 2013). Organisations often have a recognised security function, as an individual or team. We assume for simplicity that this function is also responsible for influencing the behaviour of employees toward it being more secure. This involves defining rules which employees must follow. Employees are typically assumed to be able to apply that advice as it is, and that it both addresses their security needs and does not impact any other, non-security needs that the decision-maker has (Beautement, Sasse and Wonham 2009). That is, that the decision is natural, easy to make, and carries no unexpected consequences. We show that this is not a robust set of assumptions, through the following dilemmas. Where such dilemmas emerge, it creates a situation where an employee has a decision to make which draws further on their resources rather than being natural and free of effort.

Respect me and my time, or we are off to a bad start. Security behaviour provisions tend to imply that the decision-maker has resources available to complete training and policies, but in an organisation the decision-maker is busy with their paid job. To avoid ‘decision fatigue’ and the ‘hassle factor’ (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016) of complying with security, we must acknowledge that for the busy decision-maker, moving resources to security can require a loss to something else. This requires an institutional view to helping the decision-maker to negotiate where that cost will be borne from. The notion of a
‘compliance budget’ (Beaumont, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016) suggests to reduce the demands of security expectations, where here we note the need for an upper bound on expectations. This then leads to a design principle, that any additional time needed to identify and apply a security related behaviour must be negotiated for employees, not by employees.

**If this is guidance, be the guide.** The security function must assume that employees are (security) novices. They then will need to be told the cost of security and exactly what the steps are. Otherwise, the novice must guess the duration of an unfamiliar behaviour, and exactly what constitutes the behaviour in its entirety (e.g., knowing where to find personal firewall settings (Raja et al. 2010)). An employee is also likely to base their security behaviours on their interaction with colleagues or managers (Pahnila, Siponen and Mahmood 2007) and follow their behaviours instead of the policy advocated ones. Unchecked, this leads to satisficing (see Section 3.2). Current approaches appeal to the skilful user, or assume ‘non-divisible’ target behaviours (Ashenden and Lawrence 2013) with only one, clear way to do what is being asked (that establishing what must be done is not itself a draw on resources). Another design principle is then to move toward providing a clear way to apply a security-related behaviour, that will match known work-related situations or group dynamics and social influences on policy compliance — or otherwise that help is available to find an alternative.

**Frame a decision to make, not a decision made.** Advice is given assuming that what is advised is the best choice, and there is no other choice to be articulated. The advocated choice is rarely, if ever, presented alongside other choices (such as previous sanctioned behaviours, or ad-hoc, ‘shadow security’ behaviours that were not sanctioned but have been used in the past). A choice is often perceived, meaning there can be a ‘gulf of evaluation’ (Renaud and Goucher 2014) between perception and reality, which must be navigated. An example is when users form incomplete/incorrect understanding of how provisioned two-factor authentication technology options work in reality (Dutson et al. 2019). A principle here is to reduce the need for the decision-maker to invest resources in establishing which perceived choice is appropriate, so that one advisable, workable behaviour becomes apparent, preferred, and approachable, and hence more likely to be adopted. Such framing is one means to de-emphasise harmful behaviours in the environment (Clear 2018). This also requires understanding what appeals in non-advocated behaviours and accounting for it in the advocated behaviour, so that there is a workable choice available (Kirlappos, Parkin and Sasse 2015).
3.3: Towards a consistent strategy

**Edit out the old, edit in the new.** Providing more security advice is often presumed to be better for security, but is not (Herley 2013), and can instead create confusion. Stale advice can persist unless it is curated (Hielscher et al. 2021) — an employee may do the wrong thing which is insecure, or the wrong thing which was secure but now is not. When policies and technologies change, the decision-maker is often left to do the choice-editing. An example is when old and new security policies are accessible but without time-stamps. The principle here is twofold — if the security function is committed to defining security behaviours, they should also commit to managing the communication of secure behaviours, rather than leaving it to employees to identify the right behaviour to follow. This includes explicitly communicating behaviours which are no longer advocated choices. It is unrealistic to expect employees to go direct to the source every time, where they may instead ask managers or peers how to address dilemmas (Kirlappos, Parkin and Sasse 2014).

3.3.1 Why we are here, with too few choices

To explore how employee security behaviours relate to security provisioning in organisations, we consider traditional economics and behavioural economics in the context of supporting effective behaviour change. We derive the ‘pillars’ of behaviour change from the COM-B model (Michie, Van Stralen and West 2011): **Capability**, **Opportunity**, and **Motivation**, which are all required to support a change to a particular **Behaviour**. We discuss how each pillar is represented in organisations according to the two economic approaches.

**Traditional economics.** The move from centralised to decentralised computing (Pallas 2009) has resulted in an imposed information asymmetry of having a recognised security function distinct from everyone else in the organisation. An asymmetry may occur between the organisation and the employee if the security function declares formal rules and informal rules (training, behaviours) (Pallas 2009), assuming that the decision-maker (individual employee) has the same knowledge that they do.

Conversely, the security function does not know about expectations placed on the decision-maker by other functions, assuming they have the capacity to approximate the same knowledge; Capability to enact a behaviour then cannot be assumed. Motivation comes from formal policies, and architectural means which force certain behaviours (Pallas 2009). However, if Motivation to follow security rules is not
Table 3.1: Examples of ‘contradictory’ and ‘better’ approaches to supporting secure behaviours in organisations (derived from experiences reported in real-world settings, and relevant studies).

<table>
<thead>
<tr>
<th>Behaviour</th>
<th>Contradictory Approach</th>
<th>Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy compliance</td>
<td>Publishing policy without communicating location to staff (Kirlappos, Parkin and Sasse 2014)</td>
<td>Assumes knowledge of policy and time to find it</td>
</tr>
<tr>
<td>Secure passwords</td>
<td>Not communicating the rules for a secure password (Parkin et al. 2015)</td>
<td>Assumes expert knowledge about passwords</td>
</tr>
<tr>
<td>Authentication choice</td>
<td>Integrating a suite of options into login without explaining the options (Dutson et al. 2019)</td>
<td>Lacking support for making reasoned decision</td>
</tr>
<tr>
<td>Do secure work</td>
<td>Advocating generic security practices (Kirlappos, Beautement and Sasse 2013)</td>
<td>Staff must relate practices to work</td>
</tr>
<tr>
<td>Trained-for security</td>
<td>Provide training but no time to do it (Beautement, Sasse and Wonham 2006; Anderson, McCusker and Pym 2016)</td>
<td>Staff must negotiate the time themselves</td>
</tr>
<tr>
<td>Top-down training</td>
<td>Provide training which suspects colleagues (e.g., screen-locking)</td>
<td>Staff must reconcile training with local/team culture</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behaviour</th>
<th>Better Approach</th>
<th>Successes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy compliance</td>
<td>Ensure that the environment naturally supports policy-compliant behaviour (Kirlappos, Parkin and Sasse 2014) / relay policy directives to managers</td>
<td>Does not assume any extra effort from staff / managers can relay policy to their team</td>
</tr>
<tr>
<td>Secure passwords</td>
<td>Examples of ‘strong’ passwords (CyberAware UK)</td>
<td>Assumes little-to-no prior knowledge</td>
</tr>
<tr>
<td>Authentication choice</td>
<td>Communicating the different options in a suite of options at the point of configuration</td>
<td>Puts choices side-by-side</td>
</tr>
<tr>
<td>Do secure work</td>
<td>Visible board-level support (Demjaha et al. 2013), sector-specific tailoring (e.g., differentiated NCSC Guidance for Small Biz. and Small Charities)</td>
<td>Supports interpretation of a perceived choice to business conditions</td>
</tr>
<tr>
<td>Trained-for security</td>
<td>Agree a fixed window of paid time to complete training</td>
<td>Cost to (pri. and sec.) tasks negotiated for staff</td>
</tr>
<tr>
<td>Top-down training</td>
<td>Provide training which respects trust and culture between colleagues (Kirlappos and Sasse 2015)</td>
<td>Staff do not have to feel awkward applying training</td>
</tr>
</tbody>
</table>

sufficiently related to the assets which the decision-maker cares about, it will not support the recognition of risks which require the behaviour (Beris, Beautement and Sasse 2015) (also impacting Opportunity).

**Behavioural economics.** In organisations, capabilities must be supported, but this is often approached in a ‘one-size-fits-all’ way, such that the decision-maker is forced, through the Motivation of enforced formal rules, to seek out the knowledge to develop the Capabilities they need. However, they may not know if they have the complete and correct knowledge unless someone with that knowledge checks (and acts to reduce the information asymmetry). An Opportunity for a new behaviour may be created, through training or shaping of the environment, and assumed to be the provision of behaviour beneficial to the decision-maker (Renaud and Zimmermann 2018). If a choice of a particular behaviour is beneficial to a decision-maker, they may be assumed to gravitate toward it, even when that choice is offered alongside existing behaviours. If a behaviour is only assumed to be beneficial by the
entity creating it, but not guaranteed to also be beneficial according to the decision-maker’s view and needs — Motivation is then not guaranteed. If the provisioned choices (the assumed Capability) are not perceived as beneficial they may instead adopt ‘shadow security’ behaviours (Kirlappos, Parkin and Sasse 2014) which better match their available resources.

Examples of ‘contradictory’ and ‘better’ approaches to supporting secure behaviours in organisations are illustrated through real-world examples in Table 3.1.

3.4 Applying economics principles to organisational security

We demonstrate how a strategic approach is lacking in how to manage the relatively high marginal costs of realising the informal rules awareness and culture (Pallas 2009), which are intended to support formal rules in an organisation. Although enforcement costs are low for informal rules (Pallas 2009), there is a reliance on ‘tacit consent’ to govern appropriate behaviour. For example, an employee may have freedom to access the Internet as they see fit while working, but it would be assumed that they will not visit dubious websites. This then raises the issue that the centrally defined security policy may not be the only set of rules that informs employee behaviour. Cues as to how to address security may come from colleagues, be discussed or agreed implicitly within groups or indeed by non-work cultural aspects. Critically, culturally-derived behaviours cannot be managed hierarchically, but instead through ‘informal control’, with every employee influencing to some extent how others around them behave. These aspects of organisation behaviour indicate that it is not always obvious how to follow appropriate, doable security behaviours.

3.4.1 Rational vs. bounded decision-making

In traditional economics, a decision-making structure assumes a rational agent (Simon 1956; Simon 1997). The rational decision-maker is equipped with the capabilities and resources to make the decision which will be most beneficial for them. The decision-maker knows all possible choices, and is assumed to have complete information when evaluating those choices, as well as a detailed analysis of probability, costs, gains, and losses (Simon 1997). The decision-maker is then capable of making an informed decision that is simultaneously the optimal decision for them.

Behavioural economics, on the other hand, challenges the assumption that decision-makers take fully rational decisions. Instead, the field refers to the concept of
Table 3.2: Rationality vs. bounded rationality in decision-making.

<table>
<thead>
<tr>
<th>Traditional economics</th>
<th>Behavioural economics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RATIONAL DECISION-MAKER</strong></td>
<td><strong>BOUNDED DECISION-MAKER</strong></td>
</tr>
<tr>
<td>- detailed evaluation of costs, gains, and losses</td>
<td>- brief consideration of perceived costs, gains, and losses</td>
</tr>
<tr>
<td>- complete information</td>
<td>- incomplete information</td>
</tr>
<tr>
<td>- careful calculation of potential investment</td>
<td>- cognitive and time constraints</td>
</tr>
<tr>
<td>↓</td>
<td>- quick evaluation of risks driven by loss aversion</td>
</tr>
<tr>
<td>chosen outcome</td>
<td>↓ decision fatigue</td>
</tr>
<tr>
<td>↓</td>
<td>↓ satisficing</td>
</tr>
<tr>
<td>optimal decision</td>
<td></td>
</tr>
</tbody>
</table>

*bounded rationality*, which explains that a decision-maker’s rationality is bounded because of cognitive limitations, resource constraints and time restrictions. These considerations also challenge the plausibility of complete information, which is practically unrealistic for a bounded decision-maker. According to these restrictions, the bounded decision-maker turns instead to ‘rules of thumb’ and makes ad-hoc decisions based on a quick evaluation of *perceived* probability, costs, gains, and losses (Johnson et al. 2012; Simon 1956). It is this quick evaluation that must be supported.

Table 3.2 outlines the differences between the decision-making process of a rational decision-maker and that of a bounded one. The neoclassical assumption of rationality (Simon 1997) is quite unachievable outside of its theoretical nature. From the standpoint of traditional rationality, the decision-maker is assumed to have an objective and completely true view of the world and everything in it. Because of this objective view, and the unlimited computational capabilities of the decision-maker, it is expected that the decision they take will be the one that provides maximal utility. However, in reality — decisions can be bounded, imperfect, and prone to unknown implications. Such implications include *externalities*, which are situations imposed on others and can be both positive or negative (Baddeley 2013).

It is a common misconception that behavioural economics postulates irrationality in people. The difference in viewpoint arises from how rationality was originally defined, rather than from the assumption that people are rational beings. It is agreed upon that people have reasons, motivations, and goals when deciding to do something — whether they do it well or badly, they do engage in thinking and reasoning when making a decision (Simon 1997). However, it is important to denote in a more realistic manner how this decision-making process looks like for a bounded agent. It is by considering these principles that we explore a more constructive
approach to decision-support by employees in organisations.

While an objective view of the world always leads to the optimal decision (Table 3.2), a bounded agent often settles for a satisfactory decision. Simon (1997) argues that people tend to make decisions by *satisficing* (Johnson et al. 2012) rather than optimising. They use basic decision criteria that lead to a combination of a satisfying and sufficient decision, which, from their perspective, is ‘good enough’ considering the different constraints. Furthermore, when faced with too many competing decisions, a person’s resources become strained and *decision fatigue* (Vohs et al. 2014) often contributes to poor choices. In organisation security behaviours, it has been shown that this fatigue can lead to decisions being circumvented or delayed (Beautement, Sasse and Wonham 2009).

### 3.4.2 Group decisions, herding, and culture

The recent consideration of socio-psychological factors in economics helps deconstruct the expectation of rationality being a dichotomous concept. While traditionally there may be an expectation to categorise behaviours such as herding in a binary manner and label it as either rational or irrational (Baddeley 2010), the concept of bounded rationality (Simon 1956) provides perspective and context into the complexity of individual and group decision-making. Generally there has been greater focus on modelling individual decision-making (Kocher and Sutter 2005), although many important daily decisions are often taken by *groups*. Decision-making in groups is also likely to occur when faced with uncertainty and people start equating their beliefs with those of others. (Baddeley 2013).

Engaging in herding and replicating others’ decisions is a way of social learning (Baddeley 2010), and a part of the heuristics and ‘rules of thumb’ applied by bounded decision-makers (Baddeley 2013). *Herding* occurs when people do not act completely independently but rather follow others and copy their behaviours (Baddeley 2010). Groups or individuals may think that herd behaviour is a rational choice because they believe that others are better informed than they are. However, herd behaviour may sometimes be perceived as irrational if only engaged in for conformity, rather than an actual belief that the right behaviour is being followed (Shiller 1995).

Herding is often used interchangeably with the term *information cascade*, but they are in fact significantly different — an information cascade happens when people follow the behaviours of others with zero regard to their private information (Çelen and Kariv 2004). Another difference between the two is that while engaging in herding, individuals can still receive and consider private information.
or a signal that may lead to a different behaviour than that of the herd (Baddeley and Parkinson 2012). Thus, herding still allows a process of social learning, which, by comparison, ceases during an information cascade because of the uninformative nature of the process (Çelen and Kariv 2004). Information cascading may then lead to negative externalities if the copied behaviour is wrong and no individual or group questions it — regardless of their private signals (Baddeley and Parkinson 2012).

The role of culture has been generally noted as important for understanding complex socio-technical systems and identifying causes of problems involving people and processes (Davis et al. 2014). Organisational culture is commonly described as ‘the way we do things around here’ (Deal, Kennedy et al. 1983) — to reflect employees’ common behaviours in an organisational setting. An individual’s or a group’s propensity for engaging in herding or information cascades may be impacted by the culture of the organisation. The culture consolidates people’s responses to chaos and uncertainty through shared belief systems and actions (Vasu, Stewart and Garson 2017) — with herd behaviour being one such response to uncertainty (Baddeley 2010).

Decision-making in a security context is also influenced by factors such as uncertainty and limitations, often leading to sub-optimal decisions (Parsons et al. 2015). Parsons et al. found a positive relationship between security culture and security decision-making, suggesting that an improvement in culture would lead to an improvement in security behaviours (2015). The value of security culture is increasingly highlighted when there is a tendency for herd behaviour in the organisation. Shao, Siponen and Liu found that when security managers face uncertainty about their reputation, and making security investments, they are more likely to ignore their own information and follow others’ decisions instead (2020). Furthermore, a study by Yazdanmehr, Wang and Yang found that social influence between co-workers can significantly impact compliance with security policy (2020).

Such findings align with our goal to better support ‘good enough’ decisions that best approximate secure behaviours under various constraints. Ideas from both traditional and behavioural economics can be used as ‘rules of thumb’ when characterising various constraints and social phenomenon that impact security behaviours and compliance with security policy in organisations (Caulfield, Baddeley and Pym 2016). Findings about group decision-making and the influence of culture on behaviours shed light on our understanding of constraints imposed upon bounded decision-making. The culture and group dynamics within an organisation may affect whether herding or information cascades might supplant some of the criteria in bounded decision-making.
3.5 A framework for security choices

Current approaches to security provisioning in organisations appear as if to support the rational decision-maker, as per traditional economics. Such an approach does not support non-expert employees in finding and following appropriate security behaviours. We outline how to address the contradictions that currently exist in how traditional and behavioural economics have up to now been selectively represented, as follows below.

3.5.1 Bounded security decision-making

Security research increasingly focuses on organisational security and the interaction between managers, policies, and employees. Principles from economics have been deemed useful in security (Camp and Lewis 2006), and concepts from behavioural economics further support understanding of security behaviours in an organisational context (Briggs, Jeske and Coventry 2017). For security policies to be effective, they must align with employees’ limited capacity and resources for policy compliance (Caulfield and Pym 2015a). Furthermore, policy-makers should be aware of other recurring security behaviours in the organisation that are not aligned with policy to understand why such behaviours persist (Kirlappos, Parkin and Sasse 2014).

We use the term *bounded security decision-making* to move away from any ambiguity that arises when merging concepts from traditional and behavioural economics. This distances the work from the tendency to apply behavioural intervention concepts to security while assuming the intervention targets to be rational decision-makers. This is in itself a contradiction because a rational decision-maker would by default recognise and make the optimal choice, and would not require any behavioural aid or intervention (as explored in Section 3.3). Similarly, employees cannot possibly dedicate sufficient time or resources for every single task or policy to account for this (Caulfield and Pym 2015a). This is a consideration that must be acknowledged at the point of security policy design.

To represent these concepts within an information security strategy model, we adapt the security investment model developed by Caulfield and Pym (2015a), which is constructed within the modelling framework described in the work of Collinson, Monahan and Pym and Caulfield, Pym and Williams (2012; 2014). This model explicitly considers the decision-point for an employee (the decision-maker), and incorporates elements of the decision-making process (where we reconcile elements of behavioural economics), and available choices provided by the policy-
Security Economics for Behaviour Intervention

Figure 3.2: A decision point in a decision-maker’s process of bounded security decision-making (elements adapted from Caulfield and Pym 2015a).

3.5.1.1 Process

On the left-hand side we consolidate factors in decision-making from behavioural economics into the decision-making process that informs a decision (the arrow on the left-hand side). We outline the restrictive factors (limited skills, knowledge, time, and incomplete information) that characterise a bounded decision-maker. We acknowledge that the decision-maker is bounded in several ways, from individual
skills and knowledge to temporal restrictions set by the organisation. Our bounded
decision-maker has incomplete information about the world and others, and must
manage with information available within their abilities; they can only consider the
perceived costs, gains and losses and prioritise subjective interests when faced with
a choice.

When evaluating the risks that come with a choice — ‘losses loom larger than
gains’ (Kahneman and Tversky 2013, p. 279), and the decision-maker tries harder
to avoid losses rather than to encounter gains. This then puts the expectations of
the influencer at a loss, as the decision-maker may be more concerned with the loss
of productivity than with a potential security gain, where the latter may be all that
the influencer — the overseer and expert of security — can see.

**Decision-maker preferences.** The restrictive factors on the left hand side of Fig-
ures 3.1 and 3.2 influence the decision-maker’s preferences. Using these factors as a
reference point, the DM may have preferences over complying with one behaviour
over another. Advocated security behaviours compete with other behaviours (e.g.,
compliance with HR policies or work deadlines) for the DM’s choice of preference,
where that preference impacts their final decision. If compliance with, for example,
an HR policy requires less technical engagement (and time investment), this will
factor into the preferences. To consider the social element, costs may include any
loss of trust from colleagues if following policy (Kirlappos and Sasse 2015); for ex-
ample, a screen-locking policy in an office shared with trusted colleagues. There are
also social costs associated with asking for help — such as admitting incompetence
and dependence to others, which may provoke a feeling of powerlessness (Lee 1997).
Another is how difficulty in completing a task may be perceived, where seeking help
on an easy task may incur higher social costs; for example, embarrassment of failure
in front of peers and business partners/customers (Beautement, Sasse and Wonham
2009; Anderson, McCusker and Pym 2016), while asking for help on more difficult
tasks would be less embarrassing (DePaulo and Fisher 1980).

**Choices and decision.** The two boxes above the Decision circle represent the type
of choices available to the decision-maker. Available policy choices consist of the
rules listed in the security policy by the influencer, but also any included advice
on what to do and solutions provided. In organisations with security policies, the
influencer usually assumes that the only choices available to the decision-maker are
the ones noted by the policy itself. However, as literature shows, a choice may be to
circumvent the policy (Blythe, Koppel and Smith 2013; Koppel et al. 2015), or to
attempt to work in a way that best approximates compliance with secure working
policies, in the best way the decision-maker knows how to (Kirlappos, Parkin and Sasse 2014). Though workarounds and circumventions of policy predominantly go unnoticed in organisations, this does not eliminate them from the set of choices available to the decision-maker. Behaviours regarded as choices by the decision-maker — but which are hidden to the influencer — are another information asymmetry (one that introduces risks for the organisation (Kirlappos, Parkin and Sasse 2014)). By assuming that the only available choices come from the security policy, the influencer indirectly undermines policy by having less predictable control over policy compliance decisions in the organisation.

**Information asymmetry.** Information asymmetry regularly occurs between the influencer and the decision-maker. Such asymmetry can negatively impact the influencer, decision-maker, as well as the organisation. Although many asymmetries in security occur because of the influencer’s lack of awareness about the decision-maker’s restrictive factors (limited skills, knowledge, time, and incomplete information), there are additional reasons for their existence. The security function is often unaware of the security decisions outside of policy that are taken by the decision-maker — as well as the sources of information and influence upon such decisions. An expected source of influence on security behaviours and decisions is social interaction with others in the organisation (Pahnila, Siponen and Mahmood 2007). In the context of security policies and policy compliance, the following are examples of information asymmetry:

- The recognised differentiation of the influencer being more knowledgeable and capable in security than the decision-maker (as security is arguably the influencer’s primary task);
- The influencer’s lack of knowledge about the decision-maker’s context, and pressures that factor into their choice-making process (resulting in the influencer seeming to perceive the decision-maker as a rational decision-maker with motivation and resources dedicated to security);
- The influencer’s lack of awareness about competing company policies with which the decision-maker must also comply;
- The decision-maker’s lack of information about why security restrictions matter to the organisation (overly demanding policies may cause decision-makers to lose sight of why the policies exist in the first place);
- The influencer’s lack of awareness about the impact of social learning and group decision-making on security policy compliance;
- The influencer’s insufficient understanding of other non-policy behaviours (shadow security behaviours), which may or may not be secure.
Such discrepancies in knowledge and information between the influencer and the decision-maker cause friction and create a power imbalance. Asymmetries can be identified and understood, toward reducing the gap between influencer and decision-maker perceptions (which is engineered by having a distinct, designated security function).

**Moral hazard.** When a number of information asymmetries exist in the organisation, a moral hazard is likely occurring. A common example of a moral hazard is that of the principal-agent problem, when one person has the ability to make decisions on behalf of another. Here, the person making the decisions (the agent) is the decision-maker, and decisions are being made on behalf of the influencer (the principal) who represents the organisation’s security function. However, problems between the agent and the principal arise when there are conflicting goals and information asymmetry.

If we go back to the decision-maker’s perceived risks, we can argue that these are not synonymous with the risks that the influencer knows of or is concerned with. Hence, when the decision-maker enacts behaviours, they do so by prioritising their interests and aiming to reduce their perceived risks. Because of the information asymmetry that persists between the decision-maker and the influencer, as well as the decision-maker’s hidden choices driven by personal benefit, the influencer cannot always ensure that decisions are being made in their best interest. The moral hazard here is that the decision-maker can take more (security) risks because the cost of those risks will fall on the organisation rather than on the decision-maker themselves.

Information asymmetries also impact any decisions to allow for moral hazard in the workplace; for example, if forming an infrastructure where employees should keep their own work machine secure (for instance to keep software up-to-date), and at the same time be held personally responsible if it is not secure. The influencer decides that the employee has to take action (i.e., accept and manage the risk), but the action requires more commitment and expertise than the employee is assumed to have in making this decision. It is part of the contradiction of an organisation having an engineered information asymmetry, where the expert is there to support the non-expert. In comparison, having a ‘weak’ email filter creates an externality of more effort to detect phishing emails that have arrived in an Inbox; having a stronger filter creates a positive externality unless it removes legitimate emails. A moral hazard here would be to move the risk to the individual as if spotting a phishing email is easier than it actually is (so the risk is high but the ‘right’ behaviour is very difficult to sustain). This becomes a career-related moral hazard if security performance is linked to the terms by which a decision-maker is judged if things go
wrong, and what ‘doing it right’ looks like.

Moral hazards in organisations are likely to occur unconsciously — the influencer does not consciously make the decision to delegate the risk to the decision-maker, because they assume and expect the decision-maker to be (traditionally) rational. On the basis of that assumption, a rational decision-maker would know how to enact the given security behaviour without error, leaving no risk in the end. Thus, the way in which an influencer is to become aware of such a potential moral hazard, is by accepting employees as bounded decision-makers. Realising the possibility of a moral hazard would be the first step — the second step would be to safeguard against it so that the risk does not fall on the non-expert. Given the current way security non-compliance is commonly handled in organisations, the risk would very likely fall on the non-expert decision-maker.

**Choice architecture.** The circle in Figure 3.2 signifies the decision made by the decision-maker. In our framework, we refer to the circle by using the term ‘decision’ rather than ‘choice architecture’ for the following reasons: (1) while unusable advocated security behaviours persist, the set of choices is a composite of choices created by both the influencer and the decision-maker, which does not correspond to the accepted nature of a curated choice architecture, and; (2) referring to a choice architecture implies an intention to nudge decision-makers towards a particular choice, which also implies that there exists one optimal choice. As mentioned previously, a single optimal choice cannot exist for bounded decision-makers because they have perceived costs, gains, and losses individually; a more helpful approach would be to accommodate a range of choices rather than strictly advocate for one choice that is not being followed.

**Policy and decision-maker choices.** Figure 3.3 provides a zoomed in view of the available policy and decision-maker choices previously shown at a glance in Figure 3.2. The purpose of outlining these choices in a more detailed way is to really emphasise the variety of behaviours that may go unnoticed in an organisation — as well as the sources and influences of those behaviours. The discussion of the outlined behaviours reflects the concepts introduced in Section 3.4.2.

The circle on the left outlines the available policy choices that the influencer provides for the decision-maker, often being under the impression that the formal security policy is the only available choice in the organisation. The circle on the right outlines potential security behaviours that the decision-maker engages in — not necessarily aligned with the security policy. Lastly, in the middle of the figure there is an intersection between the available policy choices and the decision-maker
3.5: A framework for security choices

choices, which are labelled as *perceived policy choices* because although they are not confirmed as being viable security policy choices, the decision-maker could perceive them as such, because of the source of these choices.

![Diagram of security choices](image)

**Figure 3.3:** A zoomed-in view of the *available policy choices* and *decision-maker choices*.

The decision-maker choices outlined in Figure 3.3 differ in the following way:

- **Shadow security behaviour.** This type of behaviour refers to security practices outside the authority of the organisation, developed by employees who do not intend to neglect security (Kirlappos, Parkin and Sasse 2014). Shadow security behaviours emerge because of security-incurred costs such as cognitive load, disruption, and time (Kirlappos, Parkin and Sasse 2015), which are in line with the restricted factors of a bounded decision-maker outlined in Figure 3.2. The decision-maker choosing to enact a shadow security behaviour may be conscious of making an *insecure* or a *less* secure choice (Kirlappos, Parkin and Sasse 2014) — but is forced to approximate a ‘good enough’ behaviour because of the difficulty in complying with policy.

- **Information cascade behaviour.** When during a decision-making process the decision-maker no longer considers their private information or signal, and simply follows the identical behaviour of others, an information cascade emerges (Çelen and Kariv 2004). During an information cascade, the chosen
behaviour may contradict the decision-maker’s private information but because this information is ignored, decision-makers are likely to make suboptimal choices (Baddeley and Parkinson 2012). Negative externalities may appear, which in the context of security, could put the organisation at risk if the decision-maker is following a choice that actively ignores policy or security breaches (Caulfield, Baddeley and Pym 2016).

- **Herding behaviour.** In comparison to information cascade behaviours, herd behaviour occurs when the decision-maker can make an identical decision to others, but not necessarily by ignoring their own information (Çelen and Kariv 2004). Hence, herd behaviour supports the opportunity for social learning and access to social information about others’ decisions (Caulfield, Baddeley and Pym 2016). However, herding behaviours become difficult when decision-makers follow the herd even when they have unambiguous information about the behaviour being incorrect (Baddeley 2010). Reasons for following an incorrect herd may include social pressure or a decision-maker’s preference for conformity (Baddeley and Parkinson 2012).

Figure 3.3 also points out behaviours that may be perceived as viable policy choices by the decision-maker. Informal resources in a social environment may influence the decision-maker’s policy compliance when such resources originate from peers or managers within the organisation (Warkentin, Johnston and Shropshire 2011). A decision-maker’s perception of security may be changed by the viewpoints of co-workers or supervisors, which may then be perceived as directives (Ifinedo 2014). We distinguish between two types of perceived policy choices:

- **Communicated behaviour.** This behaviour originates from various communications the decision-maker may have received about how to do something. It primarily concerns new decision-makers in an organisation, dependent on the instructions of others at the time of their arrival. The decision-maker may observe the behaviour from the person leading their induction day, or from the colleague who is doing their handover for a new role. For a new employee, the absence of security advice — or a dismissive comment about policy compliance, may be perceived as a cultural cue of ‘how things are done around here’.

- **Inherited hierarchical behaviour.** This behaviour may be perceived — although not verified as such — as a viable policy choice primarily because it is inherited from a person of authority; a supervisor, a manager, or even a significantly more experienced colleague. The decision-maker may assume that more senior employees ‘know what they’re doing’ and are a sufficiently
trustworthy source of security behaviours. Also, these inherited behaviours might have potentially been made more specific to the local working conditions in order to make directives actionable (Reeder, Ion and Consolvo 2017) and are perhaps easier for the decision-maker to follow.

Preferences also factor into the final choice of a decision-maker. A decision-maker’s preferences can be influenced by their lack of knowledge or inexperience relative to a particular decision (Caulfield, Baddeley and Pym 2016). This may then prompt them to use information from other, more senior decision-makers. When faced with uncertain decisions, people tend to believe that others are better equipped than they are to make the right choice (Baddeley 2010). The bounded decision-maker might follow others because they trust that choice more than their own interpretation of the security policy.

Decision-maker preferences can also be influenced by cultural factors such as shared values, beliefs, or even tasks (Schein 2010). Behaviours are often created based on social interactions with others (Palinila, Siponen and Mahmood 2007). In organisations where social bonding between coworkers is stronger, individuals or groups are more likely to adopt identical behaviours because of social pressure (Ifinedo 2014; Robinson and O’Leary-Kelly 1998).

In cultures where teams or groups engage in communication and social interactions, some security choices may be a result of discussions between several non-experts. While such security choices can be risky and potentially cost the influencer, the decision-maker may prefer to avoid social costs at the expense of a security gain. Bearing the social cost of ‘not fitting into the culture’ may be worse for the decision-maker than the potential costs of non-compliance with security.

### 3.5.2 Framework implementation

We describe a framework that can be applied as part of a strategy to better anticipate employee security-related behaviours under bounded security decision-making conditions. A goal here is not to dictate how decision-makers (the employees) should behave, but to provide solutions in a consistent manner, with the aim of reducing the likelihood of the decision-maker being in a position of having to use their limited resources to make up for gaps and inconsistencies in security provisioning. If an influencer can understand pertinent decision points in work processes, and identify ways to support both productivity and security needs, then they can create a system of mutual advantage, rather than a potentially hierarchical approach of nudging or ‘prodding’ employees toward an outcome that benefits only security (Renaud and Zimmermann 2018). In this way, the intervention can address conscious decisions
about their security behaviours, with the aim of achieving a natural fit with working practices. In the spirit of mutual advantage (Sugden 2008), the security influencer can only succeed if their security provisions benefit decision-makers.

Here we describe steps for applying the framework (as in Figure 3.4). We note that smaller organisations may not have the resources to maintain an overview of systems and system usage (more so if elements are outsourced (Parkin, Fielder and Ashby 2016)).

1. **Capture decision-maker process**

   **Justification:** Influencers must understand the decision-maker’s process and consider the decision-maker’s current knowledge of the system (Figure 3.2), whether it is as individuals or discernible groups of users. Security managers in organisations may be unaware of the range of factors in bounded secur-
ity decision-making if they assume that the only possible choices are those provided in the formal policy. Thus, influencers should acknowledge that (1) there is in fact a decision-making process for employees that impacts the outcome of security behaviours, and (2) there are co-existent factors that impact the bounded rational decision-maker (other imperatives alongside security). In short, assumptions about the technical expertise of the decision-maker must be checked against what a representative sample of employees/groups is capable of doing.

*Implementation steps:*

1. Depending on the size of the organisation, set up an initiative to engage with individual or groups of employees;
2. Acknowledge the existing information asymmetries and moral hazard in the organisation to gain a better overview of who is currently carrying security risks (e.g., employees carrying risk on behalf of the organisation) — this will help clarify, determine, and communicate risk ownership within the organisation;
3. Discuss with employees the challenges of behaving securely in order to understand and capture their decision-making process (including here perceived costs, gains, losses, as well as employee preferences);
4. Evaluate the skills, knowledge, available resources, and time that employees have for security;
5. Discuss and identify available, perceived, decision-maker choices with employees (including here examples of communicated or inherited behaviours, as well as shadow security, information cascade, and herding behaviours).

2. **Adapt policy choices to decision-maker**

*Justification:* Policy choices must be adapted to the decision-maker’s current level of understanding and supported with concrete information. This requires a focus on the decision-maker’s current state of knowledge and resources, rather than the desired security behaviour end-state. It may be that the influencer will not acknowledge any viable behaviours outside of the formal security policy (Reinfelder, Landwirth and Benenson 2019; Ashenden and Lawrence 2016), in which case a way to make the policy more flexible should be explored. For example, more than one single choice for a security behaviour could be offered (as happens with fallback authentication meth-
ods, for example). This rests on the influencer having ensured that the policy choices are genuinely feasible for employees in light of the information gathered in the first step.

*Implementation steps:*

1. Consider the bounded rationality of employees by simplifying policy choices so that they correspond with the knowledge and skills of a representative sample of employees;
2. Utilise previously collected information about individual and groups of employees such as their cognitive, time, resource, and information constraints to better align policy choices to their decision-making processes and constraints;
3. Evaluate the perceived and decision-maker choices that have been identified, and consider whether they can qualify as viable policy choices and be supported by the organisation.

3. **Realign policy choices with stakeholders**

*Justification:* Collaboration must be established with stakeholders to determine which other imperatives exist for decision-makers, where these are other pressures on decision-making resources alongside security. If security and other competing imperatives are not aligned, there is a risk that the decision-maker is left responsible for ensuring that an advocated security behaviour is a possible choice in the presence of other imperatives. In this step it would be crucial to consult with authoritative employees such as managers or supervisors (Kirlappos, Parkin and Sasse 2014), or any employees who act as a local security champion representing a team of employees (Becker, Parkin and Sasse 2017). These stakeholders are likely to have more visibility of barriers and ‘dilemmas’ (Blythe, Coventry and Little 2015) experienced in adapting security policy choices to work activities, as well as more insight on how to tailor security behaviours to fit local working conditions (Reeder, Ion and Consolvo 2017). In practice, this may be a cycle of learning and adapting (Kirlappos, Parkin and Sasse 2014; Zimmermann and Renaud 2019).

*Implementation steps:*

1. Collaborate with relevant stakeholders from other parts of the organisation — such as managers — to understand competing policy expectations;
2. In collaboration with other stakeholders, identify, based on different em-
ployee roles and responsibilities, potential compromises for policy requirements, such that time and resources are allocated adequately;
3 Revise available policy choices and requirements with stakeholders and employees.

4. Enable business objectives

*Justification:* Security influencers must be supported by the larger organisation to ensure that security policy choices do not interfere with other business expectations. When business and security goals are misaligned, decision-makers experience friction (Demjaha et al. 2019). Employees should not be forced into a position where they would have to break security rules to maintain productivity (Kirlappos and Sasse 2014) or complete other primary tasks. Having competing policies and expectations is essentially a failure in organisational strategy, which is bound to occur if security requirements are not aligned with business expectations at an executive level (Kirlappos and Sasse 2014; Rothrock, Kaplan and Van Der Oord 2018). There is a need to support security management teams to understand and resource security policies alongside non-security workplace policies.

*Implementation steps:*

1. Assure employees that aligning security requirements with business objectives is a priority for the organisation;
2. Address time and resource constraints of bounded decision-making by budgeting time and money for required security activities such as training, or even mandatory software updates (e.g., by creating a designated time-allocation code that employees can use to log these hours);
3. Address employees’ cognitive constraints by empowering IT and security staff to proactively support them in their security efforts;
4. Revisit security expectations and the decision-making processes of boundedly rational employees continuously to align policy choices accordingly.

### 3.6 Worked example

We apply the framework to a pertinent case study — keeping software up-to-date — and demonstrate examples of both individual and group decision-making. This case study is derived from the top online security controls advocated by security
experts, as prompted by Reeder, Ion and Consolvo (2017). At the time of writing, this is also the top piece of advice advocated by, for example, the UK government\(^1\).

The behaviour of enacting software security updates has been selected as there is evidence that knowing what impact an update will have and when to install it is a complex decision for employees (Beautement, Sasse and Wonham 2009). Decisions around installing updates are also fraught with intrinsic uncertainty, especially concerning the impact an update can have on an employee’s ability to perform their immediate work tasks if they follow the advice. For instance, employees may not be able to work while a software or security update is installing (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016). Specifically to workplaces, if employees are busy, it is arguably difficult to find an appropriate time to install an update as far as work imperatives are concerned (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016), unless the update activity is surfaced, discussed, agreed, and facilitated within the organisation.

3.6.1 Process

Skills, knowledge, and time. Applying updates as soon as possible is seen as achieving the best results (Ioannidis, Pym and Williams 2012). However, advocating to ‘keep software up-to-date’ or to ‘apply updates immediately’ does not accommodate consideration of preferences for committing time to other tasks (such as primary work tasks). Some employee groups may not have sufficient time to retrieve and install software updates during work hours. It may also be that some employee groups are using a complex collection of applications, all impacted by an update to another application (Morris, Becker and Parkin 2020), or the underlying operating system, making the update process complicated to assess in advance.

A bounded security decision-making approach would provide step-by-step guidance to match skill levels, and potentially the version of software that is currently on a device. Automation could also be considered, if the update process is complex or requires technical skill. Where there are different groups of employees, it may be possible to ‘fingerprint’ a range of typical software configurations, and provide clear instructions for each.

If staff use a range of applications, it would be helpful to calculate the time it would take to install an update and be able to use the machine again, alongside a checklist of steps for staff to follow. The checklist would ideally be separated into discrete steps as much as possible to allow tasks to be followed whenever time is available. An employee can then plan for following a more predictable process. This

\(^1\)As at the National Cyber Security Centre (NCSC) website.
already differs from existing advice, which predominantly assumes in its framing that software updates have no associated cost, that security imperatives are ahead of all other objectives (such as completing work) or that there are no impacts of installing an update.

If it is not possible to make the update process more predictable for employees, a simpler option would be to provide an estimate of how much time each critical update would take, so that at least this estimated time could be negotiated for, or by, staff and their managers. Staff could then be asked to report if the estimate was accurate. In terms of informing ‘good enough’ decisions, the approaches above would eliminate guesswork in planning use of time and employees’ computing resources.

**Perceived costs, gains, and losses.** In organisations, system patches are first deployed to a test-bed (Ioannidis, Pym and Williams 2012), to ensure that they do not create problems (losses). Direct advice to employees to ‘keep systems up-to-date’ ignores this consideration to test patches first. Simplified advice about patching neglects the need for a user to already know how to install patches, and when. It may be that users also do not consider updates as a concern (Vaniea, Rader and Wash 2014), so may not be motivated to do it at all unless the connection to their primary work is made clear.

A **bounded security decision-making** approach could provide an assurance that the latest updates have been tested on a system similar to the one the receiver of the advice is using for their work. This is so that they do not have to establish whether the patch works without problems themselves. Ideally a patch would also come with sufficient explanation of any features or applications which have changed due to the patch, reducing any sense of potential loss of cognitive automation, which would require a user to rebuild their cognitive maps of how software works (Bergman and Whittaker 2017).

It would be necessary to convey that an up-to-date system protects specific assets that the decision-maker wants to minimise losses for (where top-management or asset-focused messaging could help). One approach here is to explicitly state that an update has been tested and will work and, if necessary, list any changes to core applications that employees can expect to see (e.g., a menu option has moved to a different menu or looks different). This does not completely eliminate employees feeling a need to check, but may at least encourage them that the cost of installing the update is more predictable. Additionally, if an update is being rolled out across many employees’ machines, providing dedicated technical support for that update — and communicating that this has been provided — would reduce uncertainty as
Incomplete information. The minimal advice does not declare how to check or how often to check updates, assuming a rational approach. If an update seems to be taking a long time, a decision-maker may not know if the problem is with the machine (requiring support) or personal expectations (and not being able to troubleshoot problems (Wash et al. 2014)). There is also an assumption that the user may know the changes that updates will create in advance, when it could impact them in a range of ways (Bergman and Whittaker 2017). In a corporate environment, an employee cannot know if all networked services or systems they wish to interact with are also up-to-date, or will work with a newer version of the software they are using. Indeed, if other systems are not kept up-to-date — which an employee cannot know — this also could prevent different systems from working together. Conversely, the provisions of the organisation may lag behind what an individual is capable of doing — corporate systems may be behind on versions, limiting how ‘far ahead’ an employee can go in keeping their own software updated.

A bounded security decision-making approach could involve informing the user of how long each update takes to install (Mathur et al. 2016), (especially if a restart is required), based on testing on a comparable setup (including machine performance, available disk space (Mathur et al. 2016), and provisioned software). It may be that updates can be scheduled centrally (Mathur et al. 2016), for instance to occur when employees are most likely to have their computer on but in use (if the organisation has scheduled workplace lunch breaks, for instance). Efforts in this direction may reduce the perceived costs to work activities when a patch is installed.

Ultimately, finding a time to install updates and avoid disruption is increasingly difficult to find in a PC-computing work environment. The above approaches are subtly different to the standard ‘progress bar’ and timing information provided by operating systems, by working to reduce individual costs and also reduce uncertainty about those costs. This moves in the direction of better matching updates to the work context, i.e., how operating system updates interact with corporate applications and systems, and how updates can fit into the work day of employees. This would be akin to knowing employees’ ‘Active Hours’ (as is already seen within Windows 10 home installations (Morris, Becker and Parkin 2019)), and assessing whether these hours make it feasible to install the updates within the working day.

Loss-averse evaluation of risks. A rational approach does not accommodate the chance that the user has had prior bad experiences with updates (Vaniea, Rader and Wash 2014). It also does not provide assurances that the update will not cause
software to cease working properly, and does not declare how much (paid/salaried) time the update will take (assuming this to be none/negligible).

A bounded security decision-making approach would provide support for creating backups before updates, and point to the existence of the backups (to assuage concerns about losses). A user may simply choose to delay or ignore the installation of an update (Vanier, Rader and Wash 2014), so there would be a need to convey or imply why this is not an appropriate option to consider. This is most readily achieved by presenting the options that the user perceives relative to each other. Across different groups of employees, it may be possible — if not necessary — to ensure that the organisation can still function while updates are occurring, and that there is declared support in case of problems that are discovered after the update has been installed.

This does not remove the uncertainty of whether problems could occur, but changes the deliberation of the employee to that of whether they are willing to risk needing help after an update. This is opposed to a user risking installation of an update and then needing to fix it on their own. The delegation of security to others seen as better-placed to manage it has been seen elsewhere (Dourish et al. 2004), and can inform ‘good enough’ decisions around installing updates by reducing the perceived costs of potential outcomes.

### 3.6.2 Available policy choices

Rational advice to keep a system up-to-date does not consider that modern systems may already be doing (some or all of) this without user involvement, so advice may, for example, need to consider specific operating system software. Unless an operating system or application provides separate feature updates and security updates, the value of updates for security may not allow a decision-maker to consider clear choices (Morris, Becker and Parkin 2019).

A bounded security decision-making approach would acknowledge how updates work on the system the decision-maker is using. It would also recognise the other options that are available to the decision-maker, from the perspective of their personal preferences and not solely the one ideal preference of the security function (influencer).

To better approach ‘good enough’ behaviours, the benefit of installing an update must consider the (declared) costs and risks of installing the update (such as time waiting for installation), but also the cost of delaying or ignoring the update. If the machine continues to function without the update, an employee may see that an update only brings costs.
With security controls such as forced software updates, an information cascade behaviour may be imposed on decision-makers by the technical policies of the organisation, and the collective workplace practices. This would leave no other available choices, especially if it is necessary to maintain software that is compatible with the applications used between employees or with collaborators elsewhere.

As a result, employees would be forced into an information cascade of simply updating their device, even if their own individual judgement indicates that they would want to do otherwise. This creates a negative externality that imposes additional costs upon the decision-maker’s primary task.

3.6.3 Decision-maker choices

If workplace security choices are framed for a rational decision-maker, and are not made explicit and compared meaningfully, the bounded security decision-maker may construct the set of choices in an ad-hoc fashion. These choices come from their own perspective, with little to no information about the consequences of taking action or not, based on the non-expert knowledge they personally have (Kirlappos, Parkin and Sasse 2014), which is not as informed as that of the security function.

Competing work and social pressures may urge the decision-maker to make improvised choices. When working in a group or a team, the decision-maker attempting to comply with the security policy may be instructed by colleagues or more senior members of their team to delay updates until work activities are completed. This can then create a moral hazard because the choice benefits the decision-maker (who manages to both complete their work and seem to comply with policy), but imposes the risk of not updating the software in a timely fashion which may in turn pose a risk to the organisation. Another option would be for the IT team to ensure that updates can be installed in such a way that prior operating system and application state would be reinstated once the update has been installed. This opens up options to identify tasks where a computer would not be used, for instance prompting staff to install updates together before an in-person team meeting or similar event where computers would not be used.

3.7 Related work

There is a growing body of research advocating the application of economics concepts to security generally, as a means to understand complex challenges. Foundational work by Gordon and Loeb asserted that traditional economics can inform optimal investment in security (2002), whereas here we apply a similar approach
to a combination of economic models in order to reposition investment challenges related to security behaviour management. Beautement, Sasse and Wonham articulate how employees have a restricted ‘compliance budget’ for security, and will stop complying once they have reached a certain threshold (2009).

Acquisti and Grossklags apply behavioural economics to consumer privacy in order to identify ways in which to support individuals as they engage in privacy-related decision-making (2007). Similarly, Baddeley applies behavioural economics in a management and policy setting, finding, for example, that loss-aversion can be leveraged in the design of security prompts (2011). Other concepts from behavioural economics have been explored within the domain of information security and privacy, such as the endowment effect (Thaler 1980) — a bias that causes people to value something more if they already own it, and framing — another bias that influences people’s choices depending on whether the options are presented in a negative or positive manner (Grossklags and Acquisti 2007; Anderson and Agarwal 2010). Anderson and Agarwal (2010) identify potential in the use of goal-framing to influence security behaviour, where commitment devices have since been explored as a way to influence behaviour change (Frik et al. 2019). Verendel applies behavioural economics principles to formalise risk-related decisions toward predicting decision-making problems, positing that aspects of usable security must also be explored (2008).

In addition to understanding security and privacy behaviour through behavioural economics, some have advocated the influencing of such behaviour through the application of nudge theory, which suggests the use of positive reinforcement and a choice architecture to influence people towards better decisions (Acquisti 2009; Turland et al. 2015). Through empirical modelling of behavioural economics, Redmiles, Mazurek and Dickerson effectively advocate for identifying and presenting options that are optimal for the decision-maker, and making the risk, costs, and benefits of each choice transparent (2018). Here we explore where there are ‘gaps’ in realising these capabilities, which must be closed in order for organisations to support secure behaviours.

With regard to capturing the dynamic between a decision-maker (here, an employee), and the security function — an ‘influencer’ — Morisset et al. present a model of ‘soft enforcement’, where the influencer edits the choices available to a decision-maker toward removing bad choices (2014). Here we acknowledge that workarounds and changes in working conditions occur regularly, proposing that the range of behaviour choices is effectively a negotiation between the two parties.

Research has often observed that people have a tendency to cluster their behaviours (Baddeley and Parkinson 2012). Engaging in collective behaviours —
often referred to as herding, frequently arises from communication between individuals (Baddeley and Parkinson 2012). Despite these findings, in economics, the decision-maker is most commonly modelled as an individual, rather than as a member of a group (Kocher and Sutter 2005). In real life, however, the decision-maker is normally part of a group, such as an executive board, a family, or a work team (Kocher and Sutter 2005; Kugler, Kausel and Kocher 2012). Group decisions are not necessarily smarter or more rational than individual ones, but groups can learn faster than individuals (Kocher and Sutter 2005), and experiments show that individuals sometimes follow others’ decisions despite having unambiguous private information that contradicts that decision (Baddeley and Parkinson 2012).

In the context of organisational security, groups could make sub-optimal decisions (Baddeley and Parkinson 2012) in relation to security policy compliance, which can in turn have negative implications for security if herd behaviour ensues (Caulfield, Baddeley and Pym 2016). To motivate adequate security behaviours in an organisation, it is important to consider the security culture (Vroom and Von Solms 2004). Schein’s model of organisational culture (2010), which has been largely applied to security (Schlienger and Teufel 2002; Furnell and Thomson 2009; Kraemer and Carayon 2005), refers to the shared values and behaviours of a group. According to Vroom and Von Solms, in order to change the security culture of the organisation, it must be changed both at the individual and group level (2004). If group behaviour begins to alter, it can then influence individual behaviour too (Vroom and Von Solms 2004). Therefore, both levels of behaviour should be evaluated when designing targeted behavioural interventions.

There is a need to reconcile the advancements in the application of economics to security with how management of behaviour change strategies in organisations is conceptualised. Here we fill in the gaps, where currently there are contradictions and shortcomings that act against both the organisation and the individual decision-maker whether that individual makes choices for themselves or with input from others in their official or informal group.

3.8 Summary

This chapter has looked at security decision-making through the lens of behavioural economics and portrayed the non-expert employee as boundedly rational. The conceptual framework outlines factors to consider when provisioning security choices, toward supporting the employee to choose ‘good enough’ behaviours under constraints on knowledge and resources. The next chapter presents a case study of a
single organisation and highlights aspects of security decision-making both on the
level of employees as well as the company board.
A Case Study of Post-Breach Security Changes

‘Roughly speaking, losses hurt about twice as much as gains make you feel good.’

(Richard H. Thaler 2016)

4.1 Introduction

As businesses and organisations become ever more dependent on their information infrastructure and assets, the importance of well-considered and -implemented security measures also increases. Organisations that are unable to protect their information systems and confidential data can suffer severe economic or reputational damage. For organisations who do not particularly focus on security — along with many that do — suffering a security breach can be a turning point in terms of how they think and act in relation to information security.

This chapter presents results from a case study of an organisation that suffered a breach as a result of an insider attack and rapidly changed its attitude towards security as a way of preventing future re-occurrences. The case study, conducted through long-term diary studies and interviews with security managers, explores how employees perceive the company’s approach to security provisioning as directed by its executive board. Typically, reactions to breaches are only captured in external statements and actions by companies — often to reassure customers and shareholders. This study offers a unique perspective of an organisation’s post-breach security changes and consequences.

The study shows that although the company is able to devote significant financial and human resources to its security function, there is a great deal of friction between
employees’ primary tasks and security tasks, which can lead to non-compliance with security policies (Beautement, Sasse and Wonham 2009). This suggests that a rapid and high investment in security, without considering how these changes will affect employees, may be inefficient. A more measured effort that accounts for how employees perceive and interact with security policy and controls can be expected to be more effective.

As noted in the Introduction (Section 1.1), this chapter explores the research questions through a unique case study showing a company’s culture after experiencing a breach. This chapter highlights the importance of effective communication in security management by presenting a misalignment between the role of security and the organisational objectives and the value of identifying and managing this misalignment for security practitioners and decision-makers. The need for promoting an aligned approach and communication across the organisation is further emphasised.

The rest of the chapter is structured as follows:

• In Section 4.2, we provide a brief discussion of how other organisations have responded to breaches in the past;
• Section 4.3 presents the case study, and includes a detailed description of the organisation as well as the applied methodology;
• Following that, Section 4.4 presents and discusses the identified themes relating to the security culture in the organisation;
• Finally, Section 4.5 summarises the chapter.

The content of this chapter is an edited version of the following publication:


## 4.2 Reactions to security breaches

Literature on post-breach analysis is limited, and the majority is not academic, but rather industrial and regulatory. While some work has been done in this area, what actually happens to the security function of a company after a breach, is rarely discussed in the research community. There is work which discusses log analysis of post-incident data (Haggerty and Hughes-Roberts 2014), the financial impact of IT security breaches (Garg, Curtis and Halper 2003), and the economic cost of publicly known data breaches (Campbell et al. 2003). Knight and Nurse propose
a framework for effective corporate communication to assist companies with their response and communication after experiencing a security breach (2020).

The work of Hsu and Wang suggests that the likelihood of information security breaches can be impacted by the board (2014). There is a relationship between the likelihood of breach incidents and the level of risk aversion of a Chief Information Officer (CIO) (Feng and Wang 2019). This relationship is significantly stronger when the CIO is also a part of the board (Feng and Wang 2019). According to Shaikh and Siponen, high costs associated with breaches can result in both increased top management attention towards cyber security and a greater likelihood of conducting an information security risk assessment (2023).

The number of breaches has drastically increased over the years (Finnerty et al. 2018), with at least fifteen — if not more — severe data breaches in the UK.¹ A previous major data breach which has left its mark in the UK is the TalkTalk breach, a company which largely failed to protect the data of its customers. The Information Commissioner’s Office was seriously involved and even published a report² containing the analysis of the breach and future recommendations. TalkTalk’s CEO claimed that the breach was an eye-opener and it strongly impacted the company’s security strategy. According to one of the board members, things changed in the following way:

‘From cyber security being an item on the board meeting to being a lens through which all decisions are viewed.’³

Although TalkTalk have been encouraged to make substantial security improvements, they have not excluded the possibility of another breach occurring in the future. In the words of the CEO:

‘You can’t say you are 100 percent certain that your measures are going to keep everything secure. Criminals only have to get lucky once.’⁴

Target’s data breach, on the other hand, was an internationally infamous one. Shu, Tian, Ciambrone et al. provide a detailed analysis of how the breach happened and what went wrong (2017). As a result of the breach, Target hired a new CEO and invested 100 million dollars for improving security by deploying chip and pin technology, upgrading insecure point-of-sale machines, improving network segmentation, etc. (Shu, Tian, Ciambrone et al. 2017).

⁴https://www.silicon.co.uk/security/cyberwar/talktalk-security-talktalk-dido-harding-182393
Many companies have suffered great financial loss due to data breaches. In addition, those companies have had to invest a large number of resources to improve security. For example, after a terrible breach and attempting to cover it up, Uber claimed that they added the following human resources:

‘Earlier this year we hired our first chief privacy officer, data protection officer, and a new chief trust and security officer. We learn from our mistakes and continue our commitment to earn the trust of our users every day.’

Each company reacts and invests differently after a breach. However, there is no silver bullet against data breaches (Shu, Tian, Ciambrone et al. 2017); and even high levels of investment cannot guarantee an absence of breaches in the future.

4.3 Case study

This case study takes an in-depth look at a single company. This section gives a description of the company and its reaction to a security incident, as well as details about the approach and methodology that were used in the study.

4.3.1 About the organisation

The company — hereafter referred to as Company A — is a medium-large company in the financial sector. It is based in the United Kingdom and only operates within the country. The company places great value on its information assets, upon which its business success depends. As such, Company A takes security seriously. The company has significantly grown over the last two decades, with its original start-up mentality slowly shifting to a more corporate one, and is now heading towards having a thousand employees.

Company A’s serious attitude towards security has not always been present. In earlier stages of operation and growth, security was largely informal, with very basic security controls. Then, around four years ago, Company A suffered an information security breach in the form of an insider attack. The existing controls were, fortunately, sufficient to mitigate most financial and reputational damage to the company, but the incident highlighted how the organisation’s approach to security needed to be taken more seriously.

Following the incident, the company began to invest heavily in security, both in terms of personnel and technology, to ensure that a similar incident would not

occur in the future. Now, the increase in security is apparent around the offices: physical barriers control entry to and exit from the building, and CCTV cameras are present throughout the offices. The number of staff working on security has increased to ten percent of the organisation. This includes employees working on security architecture, engineering, incident response, risk, compliance, and physical security.

In addition to this, Company A also made efforts to formalise its security policy. However, this was done in a somewhat ad-hoc manner; there is no centralised security policy, but instead a number of different policies — sometimes conflicting — and in different locations. The policies differ on various terms: technicality, scope, and audience. There are certain policies that are too technical for anyone but the employees required to implement them. Other policies only concern the security of some company assets, while others only adhere to security employees.

The security policies concerning all employees regardless of their job type, can be found in the company’s handbook. Although some of the content in these policies is quite useful to read, especially for a new joiner, the majority is too long or overly complex. The rules outlined within this handbook are all contractual, meaning that breaking them can lead to disciplinary action. However, there is no formalised and systematised escalation process for acknowledging necessary disciplinary action. Therefore, some incidents may go unnoticed, while others may be escalated unexpectedly. Such an approach can raise doubt about the legitimacy of the policies and motivate employees to be less cautious about security compliance. There has been a recent initiative to address the security policy issues that are currently present. It has now been decided that a centralised security policy would better fit the new format of Company A. Such a policy will be based on known security frameworks such as NIST Cybersecurity Framework and ISO27002. Its main purpose is to achieve consistency among all security policies as well as make security rules more understandable for non-security staff.

4.3.2 Methodology

The methods that were used in this case study were influenced by the context of the engagement with Company A. The engagement with the organisation began when Company A’s CISO made observations about the security division and had questions about the impact of security on the company’s business processes. This led to discussions between the CISO and the thesis author about Company A’s security function, and they decided to research the topic together. As a result, the thesis author had the opportunity to work in the company’s security division for
six months. Therefore, it seemed natural to follow a methodology that is based on the participation and engagement of all stakeholders. Here the methodological focus was on the principles of participatory action research (Kemmis and McTaggart 2005) and humble inquiry (Schein 2013).

**Participatory action research**

Engaging methods such as action research and participatory action research (PAR) were first introduced to the field of information systems in the 90’s (Baskerville 1999). Since then, such creative engagement methods have been applied to security studies (Ashenden and Lawrence 2016; Heath, Hall and Coles-Kemp 2018). The purpose of these methods is to be playful, participative, open-ended, and democratic (Heath, Hall and Coles-Kemp 2018).

The methodology consists of a self-reflective, iterative process (Kemmis and McTaggart 2005) where changes are planned and then consequences are observed and reflected upon — leading to further changes. The process is reflective of the author’s activities at Company A as well as the ever changing environment within an organisation. It is important to note that the changes occurring at the company were not designed interventions but rather regular changes that happen in organisations.

PAR emphasises the importance of understanding the factors below (Kemmis and McTaggart 2005), which were particularly helpful throughout our research. An additional explanation is added for each factor in the context of Company A:

- What people do — a clear understanding of what employees do at Company A and what their daily tasks are;
- How people interact with the world and with others — an understanding of how the employees of Company A interact with their colleagues in their division as well as outside of their division;
- What people mean and what they value — a deeper account of the opinions and values that Company A employees hold;
- The discourses in which people understand and interpret their world — a written account of the descriptions Company A employees use to make sense of things.

In addition to these factors, PAR has other key features that have guided the research at Company A. The features are listed below, followed by a description of how these were considered in the research process:

**Participatory action research is a social process:** The relationship between individuals in the organisation and their social environment was deliberately observed due to the importance of this interaction in the concept of security culture.
The above statement implies that *individuation* cannot happen without socialisation and vice-versa; this is reflected in security culture due to the necessity of shared assumptions to form a culture, which can only be created as a result of socialisation.

**Participatory action research is participatory:** By examining employees’ knowledge, understanding, skills, and values, a better understanding of their actions and how those actions affect the company’s security provisioning emerged.

**Participatory action research is practical and collaborative:** The thesis author being employed at Company A enabled a collaboration with the other employees, who were simultaneously under observation. Thus, their social interactions were observed to explore how they may impact the organisation’s security and work dynamics.

**Participatory action research is reflexive:** It is common for companies to initiate change without thoroughly understanding what exactly should be changed and why. When conducting both the company-specific as well as research tasks, the application of an investigative approach to solving a problem was encouraged. The employees of Company A were assisted in making changes when necessary, through an iterative process of critical and self-critical action and reflection.

**Participatory action research aims to transform both theory and practice:** PAR does not treat either theory or practice in isolation. This last feature significantly benefits the company implementing the method. PAR aims to develop both theory and practice in relation to each other in order to create a feedback loop and subsequently improve both.

**The study**

The study consists of 15 *semi-structured interviews* conducted with members of security management at Company A. The main study objectives are 1) to define and evaluate the daily security processes in Company A, 2) to identify any friction and the reasons behind it, 3) to explore the meaning and role of security culture in general and within the organisation, and (4) to identify potential improvements. The study went through the university’s ethics review process. Participants were given information sheets and consent forms before the start of the interviews and participated of their own free will.

**Diary entries**

Although the key emphasis of the study is on the interviews, it is worth mentioning the diary entries as well. They were written as part of an observational task by the author working at the company. During the first few weeks at the company, the
4: A Case Study of Post-Breach Security Changes

author took the opportunity to become familiar with Company A’s security division and how things worked at the company in general. The diary entries consisted of notes describing the following: the working environment, the organisational structure, daily business processes, security policies, security measures, policy mandated behaviours as well as workarounds. Monthly diary entries were produced during the six-month period. Although those entries are not included in the thesis due to confidentiality reasons, they are used as a research aid in order to further contextualise our findings.

Participants

Fifteen participants were interviewed in total. In order to best understand the security practices at the company, the focus in this first study was around the members of the security management at Company A. Security management consists of roles such as senior heads, security managers, deputy managers, and group heads. There were sixteen employees at Company A which held such roles at the time. To avoid any selection bias and simultaneously enrich the data set, the entire security management team was asked to be interviewed. Fifteen out of the sixteen participants showed up for their interviews. One group head could not make the first interview due to being outside of the country and missed the second interview due to unexpected work obligations. Since the study period had finished, a third interview was not scheduled with the group head.

Interviews and humble inquiry

The length of each interview was initially set to 30 minutes due to the hectic schedules of the participants. However, there were interviews which lasted shorter and longer than 30 minutes, depending on several factors such as the participant arriving late, a mix-up with the interview rooms, having to clarify questions to a participant, etc. The average length of the interviews was approximately 21.8 minutes. The interview process continued once the participant had read the information sheet and ticked all the boxes on the consent form.

It was crucial to conduct the interviews in a way that reflects the principles of PAR. The interviews were not strictly designed to benefit our research, they were collaboratively designed with the employees of Company A. Therefore, the interview methodology had to mirror this collaboration and treat the participants almost as co-researchers rather than as interviewees. The method of humble inquiry used in this case study has not been previously applied to other security research.
Schein’s humble inquiry encourages positive relationships and effective communication (2013).

‘Humble inquiry is the fine art of drawing someone out, of asking questions to which you do not already know the answer, of building a relationship based on curiosity and interest in the other person.’ (p.2)

More specifically, the method relies on the concept of humility and inquiry. The type of humility relevant to this study is the ‘here-and-now humility’ which Schein describes as a situation in which the researcher, or the person asking questions is inferior to the participant because that participant has information which would help complete the task of the researcher (2013). The important thing is to acknowledge this dependency and build a relationship with the participant (in this case a Company A security manager) on the basis of curiosity and interest. Inquiry on the other hand, is described as the type of inquiry that goes beyond overt questioning. It is the type of inquiry that would lead to open communication. When in a situation of here-and-now humility, it is that dependency and temporary ‘inferiority’ that makes the participant feel more psychologically comfortable and likely to share the information that the researcher needs.

Humble inquiry aims to reduce bias — it does not influence what the participant has to say nor the manner in which it is said. This principle is crucial for attaining data which is not influenced by the researcher. If the content described by the participant is somewhat unclear, instead of leading the content to where the researcher wants, it is better to instead ask for an example. This is a powerful method of showing curiosity and interest and simultaneously clarifying the participant’s statements.

4.4 Results

The interviews were transcribed verbatim and thematic analysis (Braun and Clarke 2006) was used for the analysis. Although it stems from psychology, the use of thematic analysis has extended beyond that field and is now a widely used method for analysing qualitative data.

‘Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data. It minimally organises and describes your data set in (rich) detail.’ (p.6)

The main coding process using thematic analysis was conducted by the thesis author because of her detailed familiarity with the data. As a sanity-check, this was reviewed by an additional researcher, who agreed with the codes and themes generated by the process.
A total of 42 codes were produced — some of which were discarded when refining the analysis. Therefore, the final code-book has 38 codes in total (Appendix B.2). Below are a few example codes with their description and a matching quotation from the interview transcripts.

- **hierarchical influence**: This code is used whenever top management or board members are referenced. They are usually mentioned in the context of having an impact over something which is why the word influence is used.
  
  - ‘I mean you know it’s going back down to how do you get people to buy into security. And you either have the champions pushing that out there or you have mandated from the CEO downwards so that people know it’s important.’

- **purpose of having a security policy**: This code questions the purpose of having a security policy. It was generated in reference to employees not taking the policy seriously which makes the existence of a security policy questionable.

  - ‘Everybody has to understand that those policies are there for a reason and they must be enforced. If you need an exception to them, fine, go and get an exception through proper channels, don’t just ignore them.’

- **security is security’s job**: This code reflects the company’s perception about security only being the job of the security division and as a result, the rest of the organisation not taking part in the implementation of security or responsibility for it.

  - ‘So, if the board is clearly focusing its attention on the security function and saying that ‘security is security’s job’, well it’s not surprising that the rest of the organisation actually feels that.’

The codes that were related to one another were then grouped together to produce themes. Eight themes relating to Company A’s approach to security, and its employees’ perceptions and attitudes towards security resulted from the thematic analysis of the interview data. These themes are summarised in Table 4.1, which lists them and provides an overview of their meaning. The themes are then discussed in more detail.

### 4.4.1 Post-shock security

When responding to questions, almost every single participant refers to an incident that the company experienced several years ago. Often, this incident is the justification for their answers, as if it changed everything in the company — which it did. The security structure of Company A is completely determined by the aftermath of
that security breach. The majority of the security controls were put in place as a knee-jerk reaction to the breach itself, and because of the fear of losing everything. For businesses that generate profit from their intellectual property, IP theft is a great concern — and likely to be caused by a disgruntled insider (Nurse et al. 2014).

Such existing threats place information security at a level of priority for the board rather than it merely being an ‘IT concern’ (Rothrock, Kaplan and Van Der Oord 2018). Company boards are increasingly being encouraged to become involved with the security management of their organisation (Von Solms and Von Solms 2005). However, when it comes to insider attacks, many companies underestimate them and fail to report them when they occur (Nurse et al. 2014). Company A, however, is on the other side of this spectrum. The CEO and the board became very much involved after the breach, and if anything, have been overestimating insider threats since.

### Table 4.1: Produced themes from thematic analysis.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-shock security</td>
<td>The effect of a security breach on the current security structure and practices at Company A</td>
</tr>
<tr>
<td>Security theatre undermines policy</td>
<td>The consequences of implementing security controls for the sake of ‘security theatre’</td>
</tr>
<tr>
<td>Security is like detention</td>
<td>The non-security employees are treated as ‘enemies’ when it comes to the security of company</td>
</tr>
<tr>
<td>Security is a blocker</td>
<td>Employees of other divisions often struggle to be productive because of the blocking nature of the security controls</td>
</tr>
<tr>
<td>Lack of effective communication</td>
<td>The importance of security is not effectively communicated across the organisation</td>
</tr>
<tr>
<td>Zero risk-appetite</td>
<td>The appetite for taking security risks is next to zero in the organisation</td>
</tr>
<tr>
<td>Sensible security is likely to work</td>
<td>Security managers believe that more sensible security controls are likely to increase compliance</td>
</tr>
<tr>
<td>Behaviour change is required</td>
<td>Behaviour change is required across the organisation to create better security habits</td>
</tr>
</tbody>
</table>
Therefore, the entire company, and especially the security division, reflect the fear that still lingers on as a consequence of the breach. The controls resemble barriers and it is visually clear that security is present once you enter the company due to the ubiquity of cameras in every space. This is intentional, of course, as the board wants to spread the message that the company is secure and it is almost impossible to breach that security. However, even the security managers believe that this post-shock approach is too much. Participant 9 says the following about the visible security measures:

‘So I think there’s something about making it visible and visceral to people, in a way that resonates with them. But there’s also something about making whatever security knowledge you’ve got rational to meet the risk in the first place, because some of them just aren’t.’ - P9

‘The advantage of this culture is that it keeps the board happy. And I don’t think it, my experience in security, even in this long time, it’s doing security this way, doesn’t make you more secure.’ - P9

In other words, it is perceived that the security controls are there predominantly to decrease the board’s fears of another breach. Although some of those controls might actually be beneficial to the security of the company, the majority of them are there to create a feeling of security rather than practically protect against a threat. Having taken the attack quite personally, the board often takes emotionally-driven decisions that are directly linked to the specifics of the breach. No financial investment appears too big as long as history does not repeat itself. The executives are often caught up in technical reports (Rothrock, Kaplan and Van Der Oord 2018), and spend too much time and money implementing technical controls while losing sight of the importance of people and processes.

4.4.2 Security theatre undermines policy

This theme follows the observation that most security controls in Company A are there for show, rather than for achieving actual security. In the words of Schneier, security theatre refers to those security measures that are intended to create a feeling of security rather than concretely improve security. Such measures can often unintentionally decrease the level of security because of their undermining nature. Namely, employees (or some of them at least) will realise at some point that certain measures are ineffective, and they will find ways to circumvent them. Once they

---

learn how to do this, they will get in the habit of continuously bypassing certain
security mechanisms.

This type of attitude also reflects badly on new joining employees. Once they pick up on these circumventions, that brings along a new generation of non-compliers who are trying to ‘fit in’ (Kirlappos and Sasse 2014). It is then difficult to convince people to comply with a policy that is unrealistic and clearly being breached by the majority of the company, most likely security employees too. Participant 3 explains this further:

‘You know if you’re not careful, it’s the classic thing of you write a policy, it’s maybe got ten points, maybe nine of them are actually valid, the tenth one isn’t valid at all and isn’t enforced because actually it’s universally accepted within the organisation that you breach that one because it’s a real pain. Whenever a new person comes into the organisation, they see the ten rules, they say oh everyone routinely breaches this rule, well obviously the policy isn’t enforced, we don’t really care about policy. Actually, do you know, rule number three is a real pain for me so I’m gonna breach that one. Rule number three might be a really really important one...’

- P3

The reason why this theme holds this title is because employees are usually blamed for undermining security policy, when in fact, the company undermines its own policies by 1) implementing security theatre, and 2) allowing non-compliance to become prevalent behaviour (Kirlappos and Sasse 2014). Some managers tolerate their trustworthy employees in circumventing the burdensome polices and follow their own shadow security to stay secure (Kirlappos, Parkin and Sasse 2014).

Once security violations become a norm (Kirlappos and Sasse 2014), it does not take long for employees to see through some of the faux security mechanisms at the company. When they do, they can challenge the integrity of those security mechanisms and further question the company’s seriousness about security. If the company is implementing measures that do not actually improve its security, then employees will feel even less responsible for acting in a secure manner (Bulgurcu, Cavusoglu and Benbasat 2010).

Perceived consequences have a significant impact on employees’ decision about complying with security (Bulgurcu, Cavusoglu and Benbasat 2010). They must be shown that policies are there for a sensible reason and purpose and that they must be enforced — by everyone. However, Company A seems to be in the habit of acknowledging and identifying breaches but not systematically following up on them. Participant 2 confirms this:
‘I think it’s probably that nothing is happening to the members of staff. There’s no consequences. A hundred percent. So, yeah, if there was something where if they have done it multiple of times and something happened then I think we will have a much lower... much lower [non-compliance]. So I think, for us personally, I think we should have some escalation or something.’ - P2

When employees see that non-compliance is going unpunished, that encourages them to continue bypassing policy. The real danger happens when policy rules that are genuinely important start being breached as a result of other ‘less important’ rules being circumvented. It is therefore more effective to have fewer rules in the policy that actually must be complied with, rather than adding a larger set of rules, some of which are inevitably going to be broken (Vance, Siponen and Pahnila 2012; Kirlappos and Sasse 2014; Kirlappos, Parkin and Sasse 2014).

4.4.3 Security is like detention

Regardless of the obvious security theatre in the company, non-security employees are still treated like bad students in detention, having to re-read the same policy multiple times until they decide to stop breaking the rules. Some of these employees might not have broken the rules thus far, but are implicitly expected to do so in the future. Such a severe attitude towards the employees’ security behaviour may have an undesired, opposite effect. Employees respond better to intrinsic motivation-based approaches than to sanction-based approaches (Son 2011). That level of distrust is risky as it could build resentment. One participant comments on this:

‘Because we apply such a low level of trust to individuals, that can feel insulting at times. So I think you almost get the reverse of what you’d expect.’ - P9

Furthermore, in relation to the overemphasised monitoring:

‘We’ve talked about it very much in the terms of I don’t trust you, so I’m watching you. That’s what my department was when I started — I’m watching you.’ - P9

This approach did not seem to be working at Company A, as non-compliance had increased in the last few months. The majority of employees in organisations tend to be trustworthy (Kirlappos and Sasse 2014) — treating them as untrustworthy components is counterproductive (Kirlappos, Beauthem and Sasse 2013) and merely leaves employees feeling untrusted (Kirlappos and Sasse 2014). It is
likely that even employees who are willing to make the effort and invest a portion of their time into security, are deterred by this almost patronising approach. It is not beneficial for either party to continue working with fear as their primary driver (Son 2011). Without trust and collaboration, it is difficult to achieve effective and inclusive security (Ashenden, Coles-Kemp and O’Hara 2018).

4.4.4 Security is a blocker

Employees in an organisation have primary (production) and secondary (enabling) tasks (Pfleeger, Sasse and Furnham 2014). As an example in this particular context, an employee’s production task would be to produce intellectual property, whereas their enabling task would be securing that intellectual property. The completion of a secondary task is not necessary for the completion of their primary task. Rather, in this case, a secondary task is an investment to protect the assets of the individual and of the organisation. But, employees have a limited budget for spending time and effort on secondary tasks (Beautement, Sasse and Wonham 2009), especially since they were hired for their primary one. When a secondary task, in this case security, prevents one from completing their primary task, it is natural for that individual to view security as a blocker rather than as an enabler. In Company A, even the security managers agree with this:

‘I think actually it is quite common, quite common thought in this business that security is a blocker to progress in this company.’ - P3

‘You know the disadvantages of [the security approach] are obviously people see that as a roadblock to being able to do your job. If you can’t trust people, you’re not necessarily using people as effectively as they can. You’re paying a lot of smart people to do a lot of smart things and basically you’re handcuffing them and not allowing them to do those things, if you do that.’ - P7

‘Most of security here is still blocking rather than enabling.’ - P9

When faced with a secondary (security) task, employees have to make a choice between complying with that task or bypassing it (Weirich and Sasse 2001). This decision-making process will usually include some low-level cost-benefit analysis from the employee’s perspective to determine the amount of effort they are willing to sacrifice for security compliance. Due to the lack of any personal gain coming from this compliance, employees exceed their compliance threshold soon enough and refuse to comply any further. Thus, in an attempt to increase their work productivity, they put the organisation’s security at risk. However, they are not to
4: A Case Study of Post-Breach Security Changes

blame — such situations occur when business and security goals are misaligned and friction is introduced as a result (Beaumont, Sasse and Wonham 2009). Employees should not have to break security rules for productivity reasons (Kirlappos and Sasse 2014).

In addition to blocking employees’ production tasks, security can also affect other parts of the organisation. For example, many managers mention that security restrictions such as ‘no homeworking’ and ‘no personal devices in the work space’ have made some employees leave the company while preventing others from joining it:

‘I think no home working is too restrictive. We can deliver that in a safe and secure way.’ - P11

‘I’m sure there’s been one or two people or ten or twenty or thirty people who have decided to resign or don’t work here just because they can’t have their smartphone or whatever.’ - P1

‘And one thing that changed for us fairly fast after our data breach was that homeworking was disabled and that’s turned out to have quite an impact on the hiring. It doesn’t actually bother me but for a lot of people it does.’ - P15

4.4.5 Lack of effective communication

The participants mention lack of proper communication as one of the factors negatively impacting the organisation in general, and security in particular. This may involve different types of communication lines, such as communication between different security teams, different members within a security team, security division and other divisions, and the board and the rest of the organisation. A lack of communication further instils a lack of trust within the organisation and creates an environment of uncertainty.

One reason why there is a lack of effective communication in Company A is the fast growth of the company. Employees used to know each other by name and walk across the room to talk to the person they needed, whereas now it is physically difficult to reach people from other teams due to several new floors being added. Effective communication was simpler when Company A was small (Williams 2009), and the communication process has suffered from this across the organisation.

An additional reason as to why having effective communication in an organisation is important is due to the circulation of information. As mentioned before, some employees may not follow security policy because they do not understand its pur-
pose, or what may happen if they do not comply with such a policy. It is difficult to have the motivation to invest in a secondary task, without properly understanding why you are being asked to do so.

*I think sometimes the understanding of why things are being done the way they’re done hasn’t always been communicated.* - P13

If the board believes that security is important and an integral part of the company, it must ensure that this message is communicated throughout the organisation. The communication should specify that security protects the business and is integral to the entire organisation (Kirlappos and Sasse 2014). In other words, the communication of Company A’s risk aversion and strict controls should come directly from the people driving them, in order for people to understand their true importance. Otherwise, the non-security employees will be convinced that ‘security is security’s job’ and rely heavily on their expertise whilst taking no responsibility themselves (Blythe, Coventry and Little 2015). It is natural for such an opinion to be formed if everything about security comes from security division rather than its original source — the board. Participant 8 summarises this argument very well:

‘[The board] put a lot of the security responsibility on the security division and they don’t talk about it as much to other divisions, the message that other divisions hear coming from the board is all about “deliver us these functional requirements, deliver us these new capabilities” but they don’t hear the board saying “deliver it securely” or “make sure you are thinking about security”. So then the security divisions come along, I will come along, or the CISO will come along and say to those divisions “well we need to actually do that securely”. But they’re hearing that requirement second hand. And I don’t think the board get that, they need to be saying to those divisions, even at the moment “security is tremendously important, you need to work with the security division to make sure that your services are secure” . . . even just saying that message I think would go a long way even at the moment with a centralised security model.’ - P8

4.4.6 Zero risk appetite

The most unanimously-mentioned term amongst the participants is risk appetite. It is always mentioned in the context of the company having very little to almost none of it. After the breach, one of the board’s knee-jerk reactions was to severely reduce appetite for security risk. By trying to almost completely eliminate security
risks, and over investing in security controls, the board is convinced that such an incident will not occur again. Once again, the emotional reasoning takes over the rational one and even extremely low risks are not taken due to the incredibly low probability of there being an identical attack again.

All necessary measures have been put in place to carefully assess security risks, on several levels, by several people. Very rarely is any risk accepted; big risks are never accepted even if their likelihood is extremely low. Participants 3, 9 and 12 disagree with this approach:

‘If the risk to the business is very very low, don’t put the security in place. If the cost to security is going to be higher than the risk of loss, risk of a breach, or risk of whatever it might be, then just accept it, that’s the cost of doing business, try and reduce it... obviously but don’t hurt the business because of it.’ - P3

‘I think we overplayed some of the threat, so we’ve kind of said we’ve got to do security here cause this could happen. But actually when you think about it, it could happen, but it’s really really unlikely’ - P9

‘I think historically the company has been very reluctant to accept risk and it’s still on a place that certain risks are not even considered to be accepted although the benefit would hugely overtake the actual risk. And I think that part of the problem is the understanding of the risk is not as well understood as it should be and that kind of comes in the way.’ - P12

Having a non-existent risk appetite frustrates the majority of the security managers. They believe that such an approach hinders the business from thriving. When asked what they would like to change in the company’s security strategy, more than one manager made reference to the company’s lack of risk appetite. Participant 3 continues to talk about the issue:

‘Because I think at the moment our... the risk function doesn’t actually understand the business drivers and so their risk appetite is prohibitively low. As in, it stops the business from progressing.’ - P3

Having a low risk appetite does not only impact the security division — it impacts the employees who are trying to do their jobs. The security managers are aware of the frustration that a low risk appetite causes to non-security employees, but it is out of their hands to change this reality:
4.4: Results

‘I think most of the divisions still see that our risk appetite is too low—and they’d want us to take more risk rather than the level it is at now which is extremely low from a security point of view. So I guess it would be a frustration with a lot of people that they can’t just get on and do what they do.’ - P9

‘Would a non-security person look for something different? I think non-security people would just want less security and more risk appetite.’ - P15

The two main issues that arise from such a risk-averse approach to security are that employees lack the proper understanding about why the company’s risk aversion is at this level and are left frustrated, and, employees believe that this approach is driven by the security division and ultimately blame them for always saying ‘no’.

This relates to the previous theme — lack of effective communication. The reasons for having such a low risk appetite have not been properly communicated throughout the company and employees are often left confused. They do not comprehend the importance of rejecting certain security risks and how accepting those risks could potentially lead to a second breach. Severity of threat often impacts employees’ non-compliance (Vance, Siponen and Pahnila 2012). Thus, it is important to educate employees on the potential security consequences their non-compliance can lead to (Vance, Siponen and Pahnila 2012).

4.4.7 Sensible security is likely to work

Generally, in security, it is the security professionals that insist on heavy and technical security controls. However, in Company A, this is not necessarily the case. The interviewed participants are almost unanimous in the opinion that the current controls are overplayed and thus, they are not particularly shocked that non-security employees are not happy to comply with them. On the contrary, while the board are demanding extreme measures, the security professionals are trying to shift towards more sensible security. They believe that if security controls are sensible, employees are more likely to comply with them.

‘But also, sensible reality. A lot of people, if they think something is sensible, won’t need educating. I’m trying to give a security example—most people, most people don’t pile up rubbish in front of fire escapes because you understand why you shouldn’t do that, because you’re going to burn to death. And even if there isn’t a big sign on the door saying do not pile rubbish here, there’s a very good chance if there is somebody
who does, somebody else will move it because it’s sensible and everybody can understand it.’ - P9

In other words, if the implemented security controls actually make sense, and they are properly explained to employees, it should come more naturally for them to comply with those measures. When security is sensible and designed with the purpose of assisting people rather than blocking them, they are more likely to take sensible decisions (Kirlappos and Sasse 2014). Rules that keep getting broken are likely unfit to support the company and should be re-designed to fit employees’ primary tasks (Kirlappos and Sasse 2014; Kirlappos, Parkin and Sasse 2014). Participant 12 states:

‘You want people to take sensible, common sense decisions in their everyday work. So you don’t want to have a very deterrent security culture that makes them always want to bypass every little thing, you want something that helps them do what they need to do but also supports them in doing that in the right way.’ - P12

In order to introduce sensible security into the organisation, the people running security must also join this approach. An important part of it is communicating the reason why the security division is implementing something and how not implementing it may risk the company. Ideally, employees should have the freedom to make suggestions to security employees about controls that affects their work. In relation to this, participant 6 states the following:

‘So it just makes easier working life for everyone, if you raise awareness, push awareness about why we’re doing things, invite people to look at what we’re working on and the reasons behind that not just “you can’t do this thing”… there’s actually a reason behind why you can’t do this thing. “Here’s the reason, here’s the main reason, here’s the way it may leave us vulnerable”. Once they kind of understand that, they’re kind of “okay, that kind of makes sense”. Or let’s work out how to achieve still the same level of security but maybe in a better working way for the person or the customer or whoever is trying to get work done.’ - P6

4.4.8 Behaviour change is required

This is not the last theme by coincidence — the rest of the above themes are an indication that Company A requires behaviour change, both of the board, and its employees. In order to leave behind the current security culture and move on to a more preferable one, a period of behaviour change is necessary. Such change can
take a lot of effort and time (Schein 2010). Participant 9 states that somebody has
to be told the same thing seven times before they actually listen to it. Participant
10, on the other hand, comments on how long cultural change takes:

‘To change the culture it takes between, around 2 years or more, on
average 2 years. To change the culture, the way people think.’ - P10

Before any change can be truly initiated, there’s the challenging bit of unlearning
people’s behaviours and discarding their old habits. According to Schein, a cultural
transformation primarily requires the unlearning of current behaviours in order to
move on to new ones (2010). A few participants shed light on the difficulty of
changing security behaviours:

‘I think it’s harder for people that used to work in a certain way to change. I’m
guessing if you come from a company that’s a lot more open and a lot more
flexible in the working approach because of the nature of the business or what
they’re working on, I can understand that but I think also for people that have
been here a long time and going through change I think can be a challenge for
some as well.’ - P6

‘I think the sense of a shared... some level of a shared responsibility for secur-
ity was there [in participant’s previous company] from the start. So, I think
the potential damage that’s being done here by pushing a heavily centralised
security model had never happened there.’ - P8

The statements above point out that change is difficult and time consuming.
People have their habits and those cannot be broken over night (Vance, Siponen
and Pahnila 2012). There are certain security behaviours at Company A which
need to be changed, but because they were encouraged from the very beginning,
that change will require timely persistence. A crucial step in this change process
is to let employees know exactly what the company is intending to change, which
specific behaviours, and why. Once that has been clearly communicated, employees
will need assistance and constant reminders to achieve that change. A systematised
transformational process is required to accomplish desired cultural results, as well
as sufficient time (Schein 2010). The majority of participants suggest training and
education efforts to achieve behavioural change. Although those measures will be
necessary, they are not sufficient in isolation. Employees must be given the adequate
understanding and skills to be able to change their behaviour.
4.5 Summary

This chapter has provided a unique perspective of an organisation and its culture after experiencing a breach. The case study has highlighted the importance of communication in security management and the friction that can arise if that communication is ineffective. It has additionally focused on the consequences of ad-hoc security decisions, and emphasised that financial and human resources are not always sufficient for achieving the desired security culture. The next chapter presents a co-design methodology for exploring the relationship between security behaviours and organisational culture and outlines how the case study presented in the current chapter has informed the methodology.
Co-design for Security Modelling

‘A problem well put is half-solved.’
(John Dewey 1938)

5.1 Introduction

Security managers are responsible for meeting the organisation’s security objectives. Most commonly, managers set a security policy as a way of clearly outlining these objectives and providing further guidance on how to follow them. While the security manager’s primary concern is to keep the organisation secure and ensure policy compliance, challenges arise from complex factors that may impede the effectiveness of the security policy. Factors obstructing compliance with security policy may include how the policy itself is written, the level of difficulty associated with compliance, the organisation’s security culture (or lack thereof), or irrelevant threats represented in the policy. Unfortunately, these factors are often unknown at the time of policy design and security managers face the challenge of setting and championing a security policy that may have undesirable consequences for the organisation. The inability to predict such consequences may create uncertainty and risk for the security manager. Modelling provides the opportunity to explore the consequences of a particular decision. Models can help system owners (in this case security managers) manage the complexity of their system by creating appropriate simplifications of the system and its components. In increasingly complex and dynamic environments, it is important to identify ways of exploring potential consequences of decisions before making decisions. Modelling, a ‘tool for thinking’, is a way of managing uncertainty and risk associated with decisions. By using a range of concepts from security (be-
Co-design for Security Modelling

behavioural) economics as well as mathematical systems modelling, models can be built to make predictions about policy choices and aid security managers in future security decisions.

However, rigorous and useful modelling presents many challenges. Typically, on the one hand, the system’s managers wish for it to be modelled in order to answer questions about its design or behaviour. They may be experts in the system’s design, its behaviour, or its domain of application, but may have little or no knowledge of the languages, methodologies, or data-capturing requirements of modelling. On the other hand, modellers, experts in the languages and methodologies of modelling, may have little understanding of many aspects of the behaviour of the system, the context within which the domain experts’ questions are asked, and little knowledge of what data may be available to be collected.

It is, therefore necessary that in order to construct models that capture the system and its behaviours accurately, capture the system’s managers’ questions adequately. To do so in such way that the required supporting data can be collected, it is necessary that the system’s managers and the modellers cooperate in the construction of the model.

Our thesis is that this requirement can be addressed rigorously by introducing the concept of co-design into the classical modelling methodology, as depicted in Figure 5.1. We summarise here the necessary modifications, which are explored in detail in Section 5.4.

- We introduce — see Figure 5.2 in Section 5.4 — a translation zone in place of the simple ‘induction’ of models step;
- This translation zone is the space in which the stakeholders — system owners and users and modellers — interact in order to co-design an adequate model;
- The translation zone supports the development of shared understanding of the system, the questions about the system, the modelling methodology and its limitations, and the availability of relevant data.

Security provides a systems perspective that is both quite generic and for which co-design is particularly important. Although there is evidence to suggest that security culture drives policy compliance (D’Arcy and Greene 2014), cultural and behavioural aspects of security are not commonly considered when modelling security policy. The importance of culture in security has been highlighted long ago (Martins and Elofe 2002); however, its representation is often oversimplified (Reid, Van Niekerk and Renaud 2014), or too complex to model usefully.

Modelling security culture through a co-design approach can help facilitate the required system and context knowledge to represent culture more accurately. Oppor-
tunities to capture observations of the cultural and behavioural aspects influencing security policy can be identified by engaging stakeholders from an early stage. Constructs from traditional and behavioural economics can then be used to characterise those observations in ways that are better suited for modelling by considering theories such as bounded rationality and herd behaviour (Caulfield, Baddeley and Pym 2016).

This chapter addresses the research questions (Introduction, Section 1.1) directly as it proposes a novel methodology for co-design which aims to more accurately capture the behavioural and cultural aspects of security in organisations. The methodology aims to bridge the gap between research and practice by engaging stakeholders in a process of mutual learning, co-creating the objectives of the model and incorporating the insights and perspectives of all stakeholders involved. The remainder of this chapter is structured in the following way:

- In **Section 5.2**, we introduce the role of modelling in understanding and supporting policy-formulation and decision-making in security. We consider the challenges that can be observed in coordinating the identification and collection of relevant data and the design and construction of models;
- We explain the impact of culture and behaviour on security policy compliance in **Section 5.3**, and summarise why behavioural and cultural aspects should be captured when modelling security. We then observe the challenges that may arise when attempting to characterise culture less vaguely and model it in a way that is useful in practice;
- Before introducing a new methodology in **Section 5.4**, we first provide an overview of co-design and discuss existing co-design work in modelling and security. We introduce the approach in the form of a co-design methodology that is a modification of the classical modelling cycle;
In Section 5.6, we present a case study which largely shaped the understanding of co-design presented in this thesis — previously published in (Demjaha et al. 2019). Through reflections, we discuss the methods and approaches that worked, as well as shortcomings. Finally, we summarise the contents of this chapter in Section 5.8.

The content of this chapter is an edited version of the following publication:


### 5.2 Modelling for security

Models play an important role in the way we understand, analyse, and make decisions about security. We can identify many types of models that arise in this setting. Here are a few key examples.

- **Access control models**: these are typically formulated using algebraic or logical methods. For example, Bell-LaPadula, Biba, and the many models they have inspired, use algebraic methods. An alternative approach is to use logical methods to specify access control rules. This too has been developed quite substantially in a large literature;

- **Models of attack–defence strategies**: these are typically game-theoretic, in which the game’s players represent attackers and defenders with varying assumptions about the knowledge of the players and their levels of investment;

- **Policy models**: these illustrate the consequences of policy choices on, for example, trade-offs between performance and security attributes. Often these are simulation models, such as impulse–response models, which explore the response of a system to attacks under varying policy régimes;

- **Behavioural economics models**: these illustrate behavioural choices within organisations. For example, the compliance budget (Beautement, Sasse and Wonham 2008), which can also be analysed logically (Anderson, McCusker and Pym 2016), examines the trade-off between the commitment of individuals’ (limited) resources to organisational operational objectives and those committed to compliance with organisational security policies;

- **Conceptual models**: these typically describe the components of an ecosystem, their relationships, as well as their evolution. Conceptual models are often expressed in informal, yet rigorous terms and can be represented through pictures, natural language, and/or diagrams;
5.2: Modelling for security

- Penetration models: these may use, for example, stochastic processes to capture an attacker’s expected degree of penetration in a system with a given defensive posture.

In all these examples, albeit to differing extents, constructing the models adequately requires their co-design by the system’s owners, users, and modellers.

5.2.1 Challenges of modelling

There are many problems that can arise when constructing models, and many of them have been described and explained in the work of Michael Pidd — see, for example — Pidd 1997 and the many articles in Pidd 2004. For a more mathematical perspective, see — Collinson, Monahan and Pym 2012 and for a ‘systems thinking’ perspective on engineering, see — Lawson 2010.

Challenges can arise during the initial phases of modelling, when the purpose and specification of the model is decided, during the construction of the model, and also during the eventual use of the model.

Before a model can be built, it is necessary to understand what its purpose is and what it should do. Beginning model construction or data collection before the purpose of a model has been identified can lead to a number of problems:

- Collecting data before determining the modelling approach to be used. The required data can vary significantly depending on the chosen modelling approach. By collecting the data in a silo, the data that has been collected may not be adequate for the modelling method in mind;
- Conducting large-scale data collection prior to determining the purpose of the model. When this occurs, the problem identification is driven and restricted by the data that has been already collected. Important contextual knowledge may be missing in the data-set because of the data collection happening prior to any careful objective identification;
- Neglecting communication with stakeholders (e.g., the system owner) at an early stage can lead to an incomplete identification of the problem to be modelled. The system owner is likely to hold critical information about the system and its issues, and can help with identifying modelling objectives.

Prior to model construction, it is essential to identify the data that are required and the limitations to what can be collected. Failure to do so can lead to the following problems:

- Deciding to model a system without considering the expert knowledge of the system stakeholders. Stakeholders might hold critical knowledge about
whether constructing such a model is even a possibility given the limitations of data availability;

• Some models may require the understanding of processes for which data cannot be collected. The system stakeholders may have the required understanding of the processes even if data collection about those processes is not possible. This further emphasises the importance of stakeholder involvement;

• The necessary data collection may be too expensive to conduct or require a long time to set up. This may mean that the data becomes unusable or irrelevant by the time it has been collected.

There are problems that can impact the eventual use of the model:

• Lack of stakeholder involvement may lead to a disconnect between the identified model objectives and the real-world issues present in the system. If the model objectives are not aligned with the real-world problems, the model might end up being useless for the system stakeholders;

• When modelling as part of interdisciplinary work, there is a risk that domain experts will work in a disjoint manner. If the objectives of the expert collecting the data and the modeller are not aligned, the end result of the model might not be useful for either.

Finally, a few generic issues are always present: ‘the map is not the territory’ (Korzybski 1958); the level of detail/complexity of the model must be appropriate to address the problem — Einstein’s principle; the model should be available when needed — a less good model that is available when needed may be more useful than a better model that is not; and cost-effectiveness — cost of creating the model should be justified by the benefits of having the model.

Looking carefully at these problems it is possible to see that they are in some sense circular: the data that needs to be collected depends on the purpose of the model and the modelling approach selected, but these choices are in turn constrained by the availability of data and affected by the modeller’s understanding of the system. The challenge is to develop an approach to modelling that resolves this circular dependency; we propose to do this by involving modellers and stakeholders in an iterative process of co-design that creates a shared understanding of the system to be modelled, identifies the purpose of the model, and ensures that the specified model is aligned with the needs of the stakeholders and fits within the limitations created by data availability.
5.3 Modelling behavioural and cultural aspects of security

Compliance with security policy is largely affected by employee behaviour and the elements that influence these behaviours (Beautement, Sasse and Wonham 2008). The behaviour and decision-making of people are already complex and can be further complicated by social, cultural, or other influencing factors in the organisation.

Insights from behavioural economics can aid the understanding of people’s decision-making and interaction with the system, which subsequently help better modelling of such behaviour (Caulfield, Baddeley and Pym 2016). Simplified abstractions of complex phenomena such as security culture may particularly benefit security managers and other system owners tasked with the management of security behaviours in ever-changing ecosystems. Modelling certain dimensions of security culture, or groups interacting within that culture, may help characterise security culture in a more meaningful and practical way for system stakeholders.

5.3.1 Challenges of modelling behavioural and cultural aspects

The complexity of security culture creates certain challenges when trying to model it. The following are some examples of such challenges:

- The concept of culture is complex and difficult to articulate in a tangible manner (Dignum and Dignum 2014). Although culture has been studied for a very long time and is a widely used concept, its meaning is often portrayed in an intangible way. When modelling culture, there is a need to focus on tangible components of culture, which can be used to establish cultural and behavioural parameters (Dignum and Dignum 2014);

- There is no accepted and practical definition of security culture (Malcolmson 2009). Originating from organisational culture, the concept of security culture has received a lot of attention in security research and the literature has expanded rapidly. However, work on security culture rarely provides a more in-depth explanation about how the adapted model of organisational culture translates to the context of security (Reid, Van Niekerk and Renaud 2014). This further complicates modelling cultural aspects of security;

- Culture is a dynamic phenomenon, often impacted by unexpected change or turbulence (Schein 2010). Culture may have stable components, but it is dynamic in nature and continuously changing. While it may be a more difficult and lengthier process, the stable components of culture may change as well under unexpected and extreme circumstances (Schein 2010). When modelling culture, it may be dif-
ficult to anticipate such extreme circumstances, which could significantly impact the cultural parameters in the model;
• Representing culture in a model could introduce a two-fold risk. The first would be ending up with a reductionist view — taking an approach that is too simplistic in representing the influence of culture on behaviour. This would produce yet another insufficiently detailed representation of security culture. The second would be that of over-elaboration — creating an overly complex representation of culture, perhaps rendering the model unusable in a real-world context (Dignum and Dignum 2014).

The complex nature of culture in general — and that of security culture in particular — is what makes the opportunity to model culture appealing. The ability to represent culture more practically — in a model — has the potential of becoming a useful tool for system owners challenged with the task of managing security behaviours in a complex and dynamic ecosystem. A possible representation of culture could be in the form of cultural and behavioural parameters derived from moving components of culture, or by categorising system stakeholders into distinct behaviour groups.

While the benefits of modelling culture in a practical manner may be obvious, there are inhibitors — similar to the modelling challenges above — that may limit the ability to do so. In order to represent cultural components or behaviour groups adequately and accurately, there is a necessity for real-life observations of that very culture. In addition to the observations of culture, there is a requirement for an in-depth understanding of the ecosystem. The availability of such knowledge is often limited, whereas the collectability of such data is sometimes not a possibility for various reasons.

System owners and other stakeholders hold critical knowledge about the ecosystem and the moving components of that system. The experience, knowledge, and information of the stakeholders about the system — as well as culture to be modelled — complement the expertise of the modeller. By involving stakeholders from the stage of problem identification, and obtaining their willingness to participate, much more accurate representations of culture and system components can be produced for the model. The complexity of a system — and culture — can be captured more correctly through a process of mutual learning between the system stakeholders and the modeller.
5.4 Co-design for security modelling

For the convenience of the reader, this section serves as a reminder of the content presented in Chapter 2, focusing on the origin of co-design, and its relationship with security and modelling, providing context to the methodology presented in this chapter.

5.4.1 What is co-design?

Co-design is normally associated with user-centred design and participatory design (David, Sabiescu and Cantoni 2013). As it is largely influenced by the latter, co-design is often considered to be an updated term for participatory design (David, Sabiescu and Cantoni 2013). The core principle of co-design is that it encourages collaboration between all stakeholders in the design process. As noted in Chapter 2, Section 2.5, a useful definition that thoroughly captures the process of co-design is that by Kleinsmann and Valkenburg (2008, p.2–3):

‘Co-design is the process in which actors from different disciplines share their knowledge about both the design process and the design content. They do that in order to create shared understanding on both aspects, to be able to integrate and explore their knowledge and to achieve the larger common objective: the new product to be designed.’

Benefits such as improved creativity and idea generation, as well as better knowledge and cooperation between stakeholders, have been associated with co-design (Steen, Manschot and De Koning 2011). Steen argues that co-design can be viewed as a process of abduction (2013). Dorst provides a similar perspective by arguing that abduction is fundamental to design thinking (2011). When using abduction as a technique in co-design, problems and potential solutions are explored in an iterative process whereby problem and solution co-evolve (Steen 2013, p.18).

5.4.2 Co-design and modelling

The closest representation of co-design in modelling work can be found in participatory modelling (PM) which can be defined as ‘a purposeful learning process for action that engages the implicit and explicit knowledge of stakeholders to create formalised and shared representations of reality’ (Voinov et al. 2018, p.1). PM emerged as a result of the realisation that stakeholders can contribute useful knowledge, experience, and skills — and that stakeholders are more likely to comply with policies if they are engaged in the process of developing those policies (Voinov et al. 2016).
Participatory modelling is sometimes referred to as collaborative modelling or co-modelling, terms which are often used interchangeably as there is no clear distinctions between them (Basco-Carrera et al. 2017). Basco-Carrera et al. attempt such a distinction and associate collaborative modelling more strongly with co-design as it is better suited for contexts with high cooperation (2017). PM, on the other hand, involves a lower level of cooperation.

Methods such as participatory and collaborative modelling have come into use because of an increased emphasis on stakeholder involvement in fields such as water resources management. In fact, the majority of PM work has been done in areas such as environment and planning, water resources management, and resource and environmental modelling (Landström et al. 2011; Basco-Carrera et al. 2017; Voinov et al. 2016; Voinov et al. 2018).

An ideal approach to PM would be to involve stakeholders in most (if not all) stages of modelling (Voinov et al. 2016). However, this is not always the case, and there are different ‘ladders’ of stakeholder participation which distinguish between different levels of involvement (Basco-Carrera et al. 2017). In contrast to PM, co-design focuses more strongly on high participation, which suits our methodological approach.

5.4.3 Co-design and security

To the best of our knowledge, there is a scarcity of work in security research that focuses on participatory modelling or co-design. Ionita et al. implement participatory modelling principles to evaluate whether such a collaborative approach would improve the quality of the final models (2015). They tested their approach in the context of risk assessment and got favourable results from the participatory modelling. Beautement et al. demonstrate the importance of capturing data that represents a real-world environment (2016). To achieve this, they propose a methodology consisting of passive and active data collection cycles — meant to collect accurate data about security behaviours and attitudes in organisations (Beautement et al. 2016). Heath, Hall and Coles-Kemp focus on the security design of a home banking system by intersecting aspects of co-design and participatory physical modelling. More specifically, participants interact with different security scenarios by using LEGO kits and achieve positive insights by doing so (2018).

While the above examples demonstrate co-design thinking (Beautement et al. 2016) — and attempts to create an interaction between co-design and modelling (Heath, Hall and Coles-Kemp 2018) — no comprehensive methodology has been proposed for co-designing security modelling, at least not one that reflects our understanding.
of co-design. Our approach focuses on a deeper involvement of stakeholders, by ensuring mutual objectives from early on, and continued participation — but also co-creation — throughout the entire co-design process.

5.5 Our methodology

In order to build a model, the modeller has three requirements: an understanding of the modelling objectives, an understanding of the system to be modelled, and the knowledge or data about the system required to construct the model. In order for a model to be useful for a system manager (the model user or ‘customer’), the modelling objectives must be aligned with the manager’s desired analysis. The modeller and the manager must have a shared understanding of the model objectives. The model must also fit within the limitations of what information the modeller can learn and collect about the system. A well-specified model with a shared understanding between modeller and manager is useless if the modeller has no access to the information required to build it.

These limitations on data collection come in two forms. First, there is information that is impossible to collect; this is a hard limit — perhaps because of time, monetary, or physical limitations that cannot be overcome. Second, there are limitations imposed by the willingness of system stakeholders to participate in the modelling process. In large socio-technical ecosystems, as frequently found in the security domain, there are many sources of data and many stakeholders, without whose cooperation it can be challenging to gain access to their knowledge of the systems of which they are a part.

We propose a process of model co-design that aims to facilitate the construction of models that meet these criteria. We start by giving a definition:

‘Model co-design is a process that engages modellers and system stakeholders cooperatively in the acts of objective identification and model specification, design, and construction with the aims of aligning model objectives with the needs of the stakeholders; and designing a model that is feasible given the limits of data availability, which are discovered as part of the process.’

We can express this process as a modification of the classic modelling cycle, which is shown in Figure 5.1. The classic modelling cycle starts at the point of observation — it assumes the objectives of the model are already specified — and moves in a cycle. Observations of the system are made and a candidate model is constructed; the consequences of the model are interpreted as real-world (or domain) consequences and then validated against observations of the real system. If the
Figure 5.2: Modelling cycle, translation zone, and co-design.

<table>
<thead>
<tr>
<th>Modelling Cycle</th>
<th>Description</th>
<th>Stakeholders</th>
<th>Modellers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>The cycle starts when a stakeholder, such as a system manager, has questions about a system. Observations about the architecture and behaviour of the system. Observations about the availability of data. Data collection. Induction of candidate model via techniques such as abduction and dialogue between stakeholders and modellers. Interpretation against observations. This is the translation zone. Design of a candidate model subject to observations and available data. Deduction from properties of the candidate model alone. A collection of properties of the candidate model that can be interpreted back in the domain. Interpretation of candidate model properties as domain properties. A collection of properties of the domain implied by properties of the candidate model. Validation of the implied properties of the domain against observed properties of the domain. Candidate model meets objectives, passes validation, and therefore becomes the model.</td>
<td>Stakeholders may have questions about the design or behaviour of the system.</td>
<td>Modellers accept that there is a prima facie case for the applicability of their techniques.</td>
</tr>
<tr>
<td>Observation &amp; Candidate Data Availability</td>
<td>- Share their knowledge of the system and the questions they have about it. - Express their desired outcomes from the modelling process. - Share insights about available data and its limitations. - Support the translation of observations into candidate model structure and parameters.</td>
<td>- Interpret the requirements from the stakeholders. - Learn about the system from stakeholders. - Share capabilities and constraints of the modelling tools and process. - Design the candidate model.</td>
<td>- Responsibility of the modellers.</td>
</tr>
<tr>
<td>Interpretation</td>
<td></td>
<td>Observe what properties of the model are derived.</td>
<td>Extrapolate preliminary consequences from the candidate model.</td>
</tr>
<tr>
<td>Induction</td>
<td></td>
<td>Collaboratively establish a method for translating properties of the model to properties of the domain. Express properties of the domain that are implied by properties of the model.</td>
<td></td>
</tr>
<tr>
<td>Candidate Model</td>
<td></td>
<td>Compare the properties of the domain that are implied by the model with the observed properties of the domain.</td>
<td>Observe the validation because they need to understand its result for the next step of the iteration of the candidate model. Evaluate the model in reference to the objectives.</td>
</tr>
<tr>
<td>Model Consequences</td>
<td></td>
<td>Understand the model sufficiently and can use it in the domain.</td>
<td></td>
</tr>
</tbody>
</table>
model does not match the real system, the candidate model is refined and the process repeats. When the modeller is satisfied that the model performs appropriately the cycle is finished. The perspective of this classic cycle is very modelling- and modeller-centric.

In our conception of co-design, modellers and stakeholders work together to determine the objectives of the model, which are refined based on observations of the system, the data required to produce a model, and the limits of data availability. Figure 5.2 presents our co-design cycle.

The co-design cycle starts when a stakeholder, such as a system manager, wants to understand something about the system. This may, for example, be due to a desire to understand an aspect of observed system behaviour, or a question about policy choices or system management. The stakeholder then begins to work with a modeller, if the modeller believes their techniques are applicable. The modeller can be a person or a team, and possibly be unfamiliar with the system of interest.

Next come the main elements of the co-design cycle: observation of the system and candidate data availability, which leads to the construction of a candidate model. In a change to the classic modelling cycle, we create a sub-loop between these two stages, and it is this sub-loop that forms the translation zone in the modelling co-design process. Here, system stakeholders work with modellers to:

1. make observations about the architecture and behaviour of the system;
2. make observations about the availability of data;
3. perform data collection;
4. refine the goals of the model based on these observations, data, and data availability;
5. design (or induce) a candidate model, and;
6. interpret the candidate model against observations — returning to (1).

We define this as the translation zone because of the interactions and cooperation of the modellers and stakeholders during this sub-loop. The stakeholders share their knowledge of the system with the modeller; the modellers learn about the system from the stakeholders. Modellers express their requirements for information and data; the stakeholders share their insights about data availability and limitations. The stakeholders share the questions they have about the system and express their desired outcomes from the modelling process; the modellers interpret these requirements as a specification. The modellers share the capabilities and constraints of the modelling tools and process; the stakeholders refine their requirements based on this understanding of what can be modelled. The modellers design the candidate model; the stakeholders support the translation of observations into model structure and parameters.
The candidate model is then interpreted by stakeholders and modellers against observations, and the cycle repeats. This is an iterative dialogue between stakeholders and modellers that seeks to converge on a shared understanding of the system, of the data available, and of the objectives and capabilities of the model.

The rest of the co-design cycle closely follows the classic modelling cycle, but we define the roles that stakeholders and modellers play during these parts of the process, as shown in Figure 5.2. The modellers deduce the model-consequences from the candidate model, while the stakeholders observe this step to learn more about the operation of the model. These are consequences in terms of the model, not in terms of the system itself, so they must be interpreted. The modellers and the stakeholders collaboratively establish a method for translating properties of the model to properties of the domain; the result are the domain properties that are implied by the properties of the model.

Next comes validation. Here, the stakeholders must compare these model-implied domain properties to the observed properties of the model. The modellers observe this because understanding validation failures — where model-implied properties and observed properties do not match — is important for the construction of a new candidate model in the next iteration. If validation is successful, the candidate model is accepted and the cycle is complete.

**What the co-design cycle achieves.** Sub-sections 5.2.1 and 5.3.1 described a number of challenges that often arise during modelling. This co-design approach has the potential to help modellers and stakeholders to overcome some of these challenges. Many of the challenges arise because of of uncertainty on the part of the modeller: about which data should be collected, what data is available, and even what problem should be modelled. Other challenges arise because of the stakeholders’ lack of involvement: stakeholders may ask an initial question, but it might not be the right question to arrive at answers that will be useful to them, or they may have necessary insights into the system that get ignored because they are never asked. For security problems, organisational culture is often a very important factor (for example, in the way policy decisions will play out); without the engagement of stakeholders, it may be impossible to capture the culture sufficiently well enough to make a good model.

A co-design modelling process will bring both modellers and stakeholders together in a cooperative process to produce a model that deepens the understanding of all stakeholders involved; it helps understand the system and helps make better decisions about it. Part of the value of building models of things is that it enforces a careful consideration of the thing itself — it actually forces one to think about
what it is, in ways that are perhaps more rigorously characterised than they would
be otherwise. This careful consideration also applies to the formulation of ques-
tions about the system of interest: it will encourage a more rigorous, more precise,
more reflected formulation of questions. Co-creating the questions (or problem)
is just as important as co-creating the model. Better questions allow for a better
understanding of what a model needs to do, and what data is needed for it.

Co-design also makes it more likely that more data will be available to the
modellers: stakeholders may have a great deal of knowledge about the system, and
in the case of modelling culture, the stakeholders’ behaviour is the data that is
needed. A process that creates an understanding of why data is needed, through
a shared understanding of the model and its purpose, can help gain access to the
stakeholders who have this information, as we show below.

5.6 Case study: Reflections

To demonstrate how an attempt to co-design looks like in a real-world context,
as well as reflect on potential improvements, we revisit the in-depth case study of
Company A which was first presented in Chapter 4.

5.6.1 The organisation

Here we provide a brief profile of Company A, focusing on the historical security
context of the organisation as well as their current security structure, policies, and
processes. A more detailed description of the company can be found in Chapter 4.

Profile: Company A is a medium-large sized company operating within the
finance and technology sector. Company A is based in the United Kingdom and
specialises in financial forecasting. The company has grown significantly over the
last few years — the start-up mentality it had in the beginning has slowly shifted
to a more corporate one. Starting at around two hundred employees about two
decades ago, it now has close to a thousand employees.

So far, Company A has been incredibly successful in the work that it does. In
order to protect the work that it produces, the company also places great value
on its information assets by investing heavily on security measures. They have
developed their security expertise throughout the years — so much so that — it is
often mistaken for a security company rather than a finance and technology one.

Security context: Company A’s security measures were almost non-existent in
the beginning. The company had a much more informal attitude towards security
and only basic controls. Then, Company A suffered an information security breach
in the form of an insider attack. This breach seriously threatened the company’s financial and reputational stability and could have potentially ended the business. Fortunately they were able to predominantly contain the breach and the damage. However, this particular experience emphasised the necessity for a better security strategy and more mature processes.

Fast forwarding some years after the incident — Company A resembles almost a completely different organisation. It has a post-shock organisational security structure. This means that the security structure was created as a result of a shock, that being the breach in this particular case. To ensure that a similar breach does not occur again, Company A invested significantly in security technology and staff. The security increase is also noticeable when entering the premises of the organisation as there are multiple CCTV cameras and physical barriers to control movement in different areas.

**Structure, policies, and processes:** The security division comprises around ten percent of Company A. The increase in size changes the security communication and impacts the processes and policies. After the incident, several security policies were created — some of them are redundant, some are jargon-heavy, some contradict others, and most are located inconsistently. Security rules are also outlined in the staff handbook, to which all newcomers and existing employees are contractually bound.

According to the policies, non-compliance with security leads to disciplinary action, but Company A has no formal and systematised way of tracking non-compliance — some incidents may go unnoticed, while others receive unexpected disciplinary action. An inconsistent approach to disciplining non-compliance may negatively impact the legitimacy of the policies and, in turn, lead to increased workarounds. In addition, having a set of scattered policies rather than a single central policy can further complicate employees’ ability to comply with security. Given these observations, there has been an initiative at Company A to centralise the security policy in order to achieve consistency.

### 5.6.2 Methodology

The engagement with the organisation started when the CISO of Company A had made certain observations about the security division and had questions about the impact of security on the company’s business processes. The CISO and the thesis author had been discussing the questions about Company A’s security function. As a result of mutual interest in the topic — as well as the author’s capabilities to capture the factors they had discussed — they decided to research the questions by
constructing a conceptual model of Company A’s security processes, policies, and behaviours, focusing on the following objectives: (1) to explore and evaluate the daily security processes in the company, (2) to identify potential friction, (3) to explore the meaning and role of security culture in general and within the organisation, and (4) to identify potential improvements.

The research for this case study was led by the thesis author who was embedded in Company A for a period of 6 months. By working at the security division, she was able to immerse in the role of a security employee and simultaneously conduct research. The methods used were guided by the engagement with Company A and the context of the organisation. While the case study was conducted during the early stages of the co-design development, there was a clear understanding of the importance of focusing on the engagement and participation of stakeholders and existing methods were adopted to achieve this.

The study: The case study at Company A consists of long-term diary entries and semi-structured interviews with security staff. The following methods were used during the research: participatory action research (PAR) (Stephen et al. 2000), humble inquiry (Schein and Schein 2021), and thematic analysis (TA) (Braun and Clarke 2006). The diary entries served primarily as a process of familiarisation with Company A and its processes, and as a way to contextualise the findings. Semi-structured interviews with fifteen security managers at Company A were conducted focusing on the objectives that were agreed on with the CISO. The interview questions were guided by regular discussions with the CISO as well as independent observations.

Participatory action research, humble inquiry, thematic analysis: Participatory action research is an approach to action research that focuses predominantly on the action and participation of stakeholders impacted by the research (Stephen et al. 2000). In exploring issues and questions that are significant to stakeholders, PAR emphasises their role as co-researchers in the process of inquiry and research. PAR encourages the understanding of factors such as: what people do, how they interact with the world and others, what they value, and the discourses through which people understand and interpret their world (Stephen et al. 2000). These factors are much akin to those required to understand the culture of an organisation.

At Company A, the researcher had the opportunity to observe the employees on a daily basis — absorbing a detailed account of their actions, values, and interaction with the world. The PAR factors above — in line with the model objectives — were additionally explored during the interviews with the security managers. Other principles of participatory action research further guided the case study at Company A — PAR is a process that is social, participatory, practical and collaborative, emancipatory, critical, reflexive, and transformative.
As the co-design understanding developed, Schein and Schein’s method of humble inquiry, which encourages effective communication and positive relationships with participants, was used to conduct the interviews (2021). It treats participants as co-researchers rather than as interviewees. Interviews conducted in this way are meant to benefit both parties by having a conversation based on curiosity and honesty.

Thematic analysis — a widely used method for analysing qualitative data — was used to analyse the interviews with the security managers. The purpose of TA is to identify patterns in the data by creating codes that are later on grouped into relevant themes. The method consists of several steps such as data familiarisation, the generation of the initial codes, the search and revision of themes, up to the naming of the final themes (Braun and Clarke 2006). Having detailed knowledge of the data, the thesis author conducted the primary coding, which was then reviewed by another researcher. The final themes were agreed upon.

5.6.3 Main findings

Eight themes were produced from the thematic analysis of the interviews. The themes relate to Company A’s overall approach to security and the employees’ perceptions and attitudes towards security. The main findings from Demjaha et al. (2019) are briefly summarised in Table 5.1.

5.6.4 Reflections

The Company A case study was designed and conducted during the early stages of developing our co-design methodology for security modelling. The study was preliminary, aimed at developing a conceptual model, and meant to be followed up by larger-scale research, which might have involved more mathematical types of modelling. Unfortunately, because of organisational restructuring, the co-design with Company A ended earlier than expected.

Important lessons, which significantly shaped our understanding of co-design, emerged from conducting this case study. The individual methods that were implemented, such as participatory action research and humble inquiry, provided insights on which aspects of co-design would work and which should be improved. The work done with Company A provided an interesting perspective and valuable reflections, which significantly influenced the co-design work presented here.

The reflections are summarised below.
Table 5.1: Themes from thematic analysis.

<table>
<thead>
<tr>
<th>Theme and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Post-shock security</strong></td>
</tr>
<tr>
<td>The impact of the information security breach is reflected in the security structure and practices of Company A.</td>
</tr>
<tr>
<td><strong>Security theatre undermines policy</strong></td>
</tr>
<tr>
<td>The heavy implementation of visible security controls for the sake of <em>appearing secure</em> undermines the legitimacy of the security policies at the company.</td>
</tr>
<tr>
<td><strong>Security is like detention</strong></td>
</tr>
<tr>
<td>Non-security staff are treated as <em>enemies</em> when not complying with security, which leads to a blame culture in the company.</td>
</tr>
<tr>
<td><strong>Security is a blocker</strong></td>
</tr>
<tr>
<td>The productivity of non-security staff often suffers because of restrictions imposed by security controls.</td>
</tr>
<tr>
<td><strong>Lack of effective communication</strong></td>
</tr>
<tr>
<td>The justification behind implementing such strict security controls is not adequately communicated across the organisation.</td>
</tr>
<tr>
<td><strong>Zero-risk appetite</strong></td>
</tr>
<tr>
<td>The tolerance for taking security risks is almost non-existent in Company A, which often compromises productivity.</td>
</tr>
<tr>
<td><strong>Sensible security is likely to work</strong></td>
</tr>
<tr>
<td>The security division believes that less strict but better suited security controls are likely to increase compliance with security policies.</td>
</tr>
<tr>
<td><strong>Behaviour change is required</strong></td>
</tr>
<tr>
<td>Unlearning of old behaviours and behaviour change is required in order to create better security habits over time.</td>
</tr>
</tbody>
</table>

5.6.4.1 Co-creating objectives

The research objectives for the Company A case study were created jointly with the CISO. This was to ensure that the questions the CISO wanted to explore were aligned with our research goals and vice-versa. These aligned objectives were agreed upon early on and the methods were then adapted based on the context and other organisational factors. For example, one factor that impacted the method of the research was the availability of the security managers. Compromises were made jointly to ensure that the objectives were followed and that the research was beneficial for all actively involved stakeholders. There was a barrier during the attempt to co-create the objectives. Although there was initial buy-in for the research from the senior executives, the long-term objectives were not agreed with them in the same way they were agreed with the CISO. This led to a misalignment of goals later on and influenced the continuation of the co-design.

5.6.4.2 Involvement in research

The collaboration with the CISO and other relevant stakeholders was present throughout the research. Continuous discussions with the CISO helped shape the design of
the interviews and encouraged the managers’ willingness to participate. The interview study was approved as well as championed by the CISO of Company A. This simplified the arrangement of the interviews with the participants and set a positive tone for the conversations during the interviews. Furthermore, the involvement of the security managers in the research carried on as they were keen to contribute to the research and be informed of the outcomes.

5.6.4.3 Building relationships

In addition to the CISO’s involvement and support, something else that positively impacted the experience was the author’s opportunity to build relationships with the employees of Company A, including the security managers. The ability to work alongside the participants for months before interviewing them meant that relationship could be built based on trust and mutual goals. Building such relationships also enabled the authenticity of the cultural and behavioural observations and the possibility to make such observations in the first place.

5.6.4.4 Mutual learning

When embedded in the company, the author worked on several projects and tasks that were not directly related to the research. This was an opportunity to work alongside many employees from the security division as well as other departments. During these collaborations, there were many instances of mutual learning. The security division were able to learn about the human factors of security, while the author learned a lot about how the security systems and processes worked in practice. This process of mutual learning created a space for symmetric relationships functioning through translation zones between both technical and human-centred security — as well as between security research and application. A shortcoming of the mutual learning process was the lack of formalisation during the initial phases of learning while the author was getting familiar with the systems and processes. More structure and documentation of the knowledge exchange between the system owners and the author would have benefited the construction of the conceptual model.

5.6.4.5 Mapping case study reflections to our co-design process

Our co-design methodology was directly informed by the methodological principles and reflections at Company A. Below we map the components from the case study to the corresponding components of our methodology (as shown in Figure 5.3).

1. The process of co-creating the objectives with the CISO of Company A, as well as the inability to co-create the objectives with the rest of the senior execut-
ives, emphasises the importance of clarifying the mutual objectives from the very beginning. This maps to the first stage in the modelling cycle — Observation and Candidate Data Availability. Here the observations or questions about the system originating from stakeholders, are communicated to modellers to explore collaboration opportunities. If there is alignment between the questions the stakeholder wants to ask and the modelling techniques the modeller aims to apply, they co-create the objectives towards a mutually beneficial aim.

2. In between the first and second stage of the modelling cycle, lies the translation zone between the stakeholders and the modellers. This space of the co-design methodology corresponds to the multiple levels of mutual learning at Company A. In the translation zone, stakeholders and modellers exchange knowledge and experiences.

3. The reflections on involvement in research and building relationships highlight the significance of involving stakeholders in the research end-to-end. An extended interaction creates opportunities to build relationships and trust, as was the case with the author and the employees of Company A. Strong relationships create better collaboration opportunities while the involvement of stakeholders throughout the entire process improves the feasibility and quality of the research. As such, these two components correspond to all the stages in the co-design process.

Even though some of our reflections suggest that there is space for improvement, the experience at Company A has been largely positive. It provided an opportunity to trial a set of methods, the principles of which closely relate to our understanding of co-design — and further emphasise the necessity for stakeholder involvement. The engagement of stakeholders at Company A was worthwhile as it enabled observations and data collection from a wide range of people and significantly aided our understanding of the system. As a result of this early co-design process, mutual conclusions were drawn — from the observations and conceptual modelling — summarised in Section 5.6.3.

The biggest shortcoming was the inability to continue the co-design process, which stopped at the stage of designing a conceptual candidate model. The later stages of the co-design process, such as developing a more accurate model as well as validating it, are missing from the current case study. Another study must be repeated in the future in order to apply all the stages of our co-design process.
5.7 Candidate model

The candidate conceptual model of Company A, presented in the form of an entity-relationship (ER) model in Figure 5.4, aims to partially represent the interview themes summarised in Table 5.1 by capturing the entities, attributes, and relationships of the system. The study captured, first and foremost, the view of security management at Company A and their perceptions about the security processes, policies, and interactions within the organisation. The candidate model therefore predominantly reflects the viewpoint of security management and the board, while the perspective of non-security staff is underrepresented in the model.

For example, the link between the entity The Board and the entity Policy denotes the relationship Mandated by, to show that policy is mandated by top management. The link between the entity The Board and the entities Security Team and Non-security Staff facilitates the Communicates relationship, which is a positive relationship when linked between The Board and the Security Team and a negative one when linked between the Board and Non-security Staff. This shows that the board only communicates their security mandate to the security team/security management, and there is a lack of communication between the board and the non-
security staff. The entity *Security Breach* is linked by the *Influences* relationship to both The Board and Non-security Staff. This indicates the influence of the security breach on the board’s risk appetite as well as the productivity of non-security staff. The entity *Security Team* is linked through the *Implements* relationship to the entity *Security Controls*, which has *Restrictions* and *Security Theatre* as attributes. Lastly, the link between the entity *Policy* and *Security Controls* depicts the *Undermine* relationship to reflect that policy is undermined by the security controls which are largely implemented for the sake of security theatre.

![Diagram](image)

**Figure 5.4:** The candidate conceptual model in the form of an entity-relationship (ER) model representing the interview themes from Company A.

The model shows as much as was possible to reflect at this point in the co-design process. Given the methodology, this is not a point at which we would draw
any conclusions, but rather hypothesise from the model’s point of view. This is a candidate model that is mostly of meaning to the modellers at this stage of the methodology and would require further validation in order to draw any conclusions. Whilst it is possible to draw the candidate model in its current form, care should be taken as it does not necessarily follow that the final model will be consistent with the current one.

5.8 Summary

In this chapter, we have seen a new co-design methodology for security modelling. The chapter has identified important challenges with modelling generally, and modelling security culture specifically. The methodology addresses these issues by engaging stakeholders in a process of mutual learning. The chapter has also outlined how the case study from Chapter 4 has characterised the proposed methodology. In the next chapter, we apply the co-design methodology at a large university through several rounds of interviews with distinct user groups.
A Case Study Examining the Role of Security Practices in Organisational Culture

‘The map is not the territory.’
(Alfred Korzybski 1931)

‘All models are wrong, but some are useful.’
(George Box 1987)

6.1 Introduction

Organisations provide IT infrastructure for employees to use in their day-to-day work activities. This infrastructure includes security controls, which include policies and guidance to follow when interacting with digital assets that are to be used within regular, everyday tasks. Most recognisable of these would be managed account systems, which dictate access to IT systems, and associated account credentials, such as company usernames and passwords (Beautement, Sasse and Wonham 2008).

Security controls in organisations can be complex. Inescapable in this complexity is that people are using these systems. Making sure that humans can use security provisions is critical, especially where they are often supporting primary work activities. This is further complicated when considering that employees and teams can differ in their needs, especially in larger organisations. For over two decades, research into the human factors of security in organisations has highlighted impacts and frictions that are created when there is a bad fit of provisioned security with working practices (Adams and Sasse 1999; Beautement, Sasse and Wonham 2008; Blythe, Coventry and Little 2015). It remains that security managers con-
6: A Case Study Examining the Role of Security Practices in Organisational Culture

tinue to lack appropriate tools for understanding and addressing these challenges constructively (Zimmermann and Renaud 2019), so that a rift between end-users and system managers persists (Ashenden and Lawrence 2016) even when managers acknowledge that they lack that understanding (Reinfelder, Landwirth and Benenson 2019). It has been evidenced that security managers are eager to engage with an understanding of human behaviours as long as that understanding relates directly to decisions they make around the security infrastructure that they manage (Parkin, Van Moorsel et al. 2010; Reinfelder, Landwirth and Benenson 2019).

We posit that directly relating security management decisions to employees’ experience of security in the setting of a large organisation can not only identify improvements, but specifically improvements that are feasible within that same infrastructure. That is, the aim is to work with stakeholders within an organisation, to identify workable security controls that stem from actionable decisions, reasonable within the remit of the security management team or function. Such an approach requires identifying the commonalities between end-user experiences and security controls; this is embodied in the infrastructure provided to users (as controls, policies, etc.), and the decisions made about that infrastructure.

In this work, we apply a co-design approach — couched in terms of a structured methodology of modelling — to gathering data from stakeholders in the IT-security ecosystem and constructing models of the interaction of those stakeholders with technological and policy infrastructure. In so doing, we seek to provide structured evidence to inform decision-making in the management and provisioning of employee-facing security measures. Prior work has been facilitated by various organisations and findings have been reported as valuable insights into the workings of organisation security (Beautement et al. 2016; Blythe, Coventry and Little 2015). Here, we engage with the managers responsible for the security infrastructure in a large partner organisation in order to elicit their challenges and inform the decisions they make about security. Evidence is gathered through qualitative research in the form of semi-structured interviews with employees and IT/security support teams. Qualitative data is framed within a structured modelling approach, such that successive rounds of data-collection build up conceptual models, detailing the security artefacts of the organisation and how people interact with them. The ultimate aim is to empower security managers with systematically gathered evidence, through research activities, so that they can relate human factors to their existing decision-making processes.

In this chapter, the research questions (Introduction, Section 1.1) are addressed through a case study of a university where the role of security in organisational culture is represented in a conceptual model of the organisation. The co-design
methodology is applied at the university through interviews with administrative staff, support staff from local and central IT and IT-security teams, as well as senior security decision-makers. The co-design methodology reveals the significance of bridging any existing gaps in security support and aiming for alignment between stakeholders by fostering effective communication, trust, and relationships between security providers and employees. The rest of the chapter is arranged as follows:

- An appraisal of organisation security issues for employees is presented in Section 6.2, including a review of prior attempts to reconcile use and provisioning of security in the workplace, and co-design approaches;
- Details of our co-design and modelling methodology are found in Section 6.3;
- Section 6.4 presents the conceptual model built from our engagement with employees, support teams, and security decision-makers;
- Section 6.5 revisits our aims and distils recommendations, and Section 6.6 summarises the chapter.

The content of this chapter is an edited version of the following publication:
- The trivial tickets build the trust: A co-design approach to understanding security support interactions in a large university by Albesë Demjaha, David Pym, Tristan Caulfield and Simon Parkin (working draft — to be submitted).

6.2 Background and related work

Through a review of related research, we set the scene for how security in organisations is experienced by employees, and how this sits relative to the view of security management in organisations. We then complement this by outlining how prior co-design approaches can inform the translation of security human factors to the decision-making processes of security managers in organisations.

6.2.1 Organisational security

Employees in organisations, especially larger organisations, will be working in an environment with provisioned IT-security measures that they will be expected to use. This typically includes corporate IT accounts, provisioned laptops, and smartphones, etc. How to use these provisions, and which security-related behaviours to follow when interacting with digital assets, will often be defined as rules or advisories in one or more security policies (or as part of other IT-related policies).

Security rules and advice are not always workable in practice alongside productive tasks (Kirlappos, Beaument and Sasse 2013); employees may adapt or
circumvent prescribed security tasks and instead follow ‘workarounds’. Employees might otherwise create their own ‘shadow security’ solutions (Kirlappos, Parkin and Sasse 2014), especially if there is a lack of visible support or understanding from the organisation. In this sense, following the mandates of security managers and working securely are often assumed to be the same thing, but little attention is given to how best to design security rules so that employees can work both effectively and securely (Beautement et al. 2016; Ashenden and Lawrence 2016). Non-compliance with rules does not imply that the employee is working insecurely in all cases, and there is often scope to design security policies that provide security, can be complied with, and which do not add a burden to productive work tasks (Beautement, Sasse and Wonham 2008). Security policies have been the subject of a great amount of research, as they are regarded as the main thread connecting security management decisions to employee activities within organisations. As such, much effort has been invested in developing instruments to measure security behaviours and user compliance with policy, such as with the HAIS-Q behaviour scale (Parsons et al. 2017).

In terms of how to improve security and productivity in tandem, the foundational research of Adams and Sasse in 1999 noted the need to consider the human aspects of security provisions in organisations, having exposed problems that employees had with provisioned credentials (1999). The work highlighted that security managers did not understand their users, but also that there was no common ground between both sides or institutional means to reliably communicate issues from one side to the other. The work proposed a user-centric approach, whereas security provisioning to this day remains very much one-way, outwards from the security team to employees. We propose to address the continued lack of an understanding of the employee experience and a view of the organisation environment built from the perspectives of both decision-maker and employee.

A key aspect of improving the usability of security measures within organisations is the design of the security apparatus (Beautement, Sasse and Wonham 2008); this in essence comprises the ‘hard’ security controls (Pallas 2009). Employees may also be subject to ‘soft’ controls such as regular online training courses, formal presentations (as during onboarding), etc. (Bauer, Bernroider and Chudzikowski 2013). There are various ways in which these initiatives can fail to resonate with employees (Bada, Sasse and Nurse 2019), where communication is a key aspect in ensuring that employees are aware of (security) behaviours expected in the workplace (Beyer et al. 2016).
6.2.2 Holistic views of organisational security

Through studies of security managers and support teams, recognition has been seen among practitioners of the need to consider employee needs (Parkin, Van Moorsel et al. 2010; Brostoff 2005). As found by Reinfelder, Landwirth and Benenson, security managers can often lack a view of the end-user experience, which only serves to create distance between them and the users they are meant to support (2019). Ashenden and Sasse noted that security managers can seem unsure of how to approach the human side of the organisation, even while at the same time they are confident of their approach to managing security-related technologies (2013). This then requires dedicated approaches to bringing together the views of both sides, as in the ‘security dialogues’ work of Ashenden and Lawrence, which through focus groups explored a shift from unquestioned compliance with policy, toward security concordance: input from both sides can contribute to user-facing solutions which secure users’ work and are doable at the same time (2016). Here we examine the threads that connect ‘central’ security policymakers, via support teams, to employees who are using provisioned IT systems; that is, the existing elements of an organisation which have the potential to enable secure working.

Many aspects of security managers’ work demonstrate attention and care for how security is maintained (Kocksch et al. 2018), including where improvements can leave the security apparatus in a temporarily weakened state as it ‘oscillates’ to a new form. Adapting to users’ needs while also securing the organisation must then be done carefully, involving many such transitions between secure and non-secure states. Solutions are ideally found which enable employees to go about their work, and be able to do so securely (Beautement et al. 2016), but with care for how this can be maintained over time (Kirlappos, Parkin and Sasse 2014). From a study of two organisations (including a university), Blythe, Coventry and Little (2015) stress the importance of focusing on building up specific workplace security behaviours, as do Pollini et al. (2021), who engage with managers and employees to understand the differences in their knowledge about advocated security behaviours in the workplace. Regarding a university setting, Wang et al. interviewed multiple types of university worker around account-sharing practices, noting the importance of making sure that security messaging resonates with employees (2022).

6.2.3 Co-design of organisational security solutions

In an organisational setting, the aforementioned ‘security dialogues’ work of Ashenden and Lawrence created dedicated focus groups for security staff and their users in the same organisation (2016). This then served as a space for the experiences of multiple
groups to be shared, hearing out each other’s perspectives on security. A disconnect was highlighted where, for one, neither side had the sense that their needs were being listened to by the other. Beaumont et al. demonstrate the importance of capturing data that represents a real-world environment and the workplace ‘dilemmas’ within; this data was ultimately communicated to security managers after analysis, resulting in targeted improvements to existing security-related infrastructure (2016).

Heath, Hall and Coles-Kemp utilised LEGO kits to support engagement between participants from different parts of the same organisation, responding to a range of different security scenarios using a shared LEGO kit (2018). This then informed each participant’s knowledge of others’ perspectives on what the larger ‘whole’ of the organisation was and their involvement in it. The LEGO approach gives participants the constructs of a model (where each type of LEGO block had a particular meaning or purpose) and prompts them to develop a shared view, an instantiation of the model. Here we address the development of a whole-system view by engaging with stakeholder groups in their own terms through qualitative research, and deriving the constructs of the model from that data. This is done through a translation zone that maps the end-user perspective to the constructs or artefacts in the translation zone that represents decisions which can or cannot be made to directly improve the system in response.

Our approach has parallels with participatory modelling (PM), ‘a purposeful learning process for action that engages the implicit and explicit knowledge of stakeholders to create formalised and shared representations of reality’ (Voinov et al. 2018, p.1). Methods such as participatory and collaborative modelling have come into use because of an increased emphasis on stakeholder involvement, where the majority of PM work has been done in areas such as environment and planning, water resources management, and resource and environmental modelling (Landström et al. 2011; Basco-Carrera et al. 2017; Voinov et al. 2016; Voinov et al. 2018). To the best of our knowledge PM has not been applied in information security, yet we note here a comparable need to involve various stakeholders in complex environments and identify the best of the available choices to meet a broader need, in this case the provision of workable security measures in organisations.

PM aims to leverage the knowledge and experience that stakeholders can contribute, positing that policy compliance is more likely to emerge from engaging stakeholders in the process of developing those policies (Voinov et al. 2016). Participatory modelling is also at times referred to as collaborative modelling or co-modelling (Basco-Carrera et al. 2017). Participatory modelling informs researchers in gathering evidence to direct long-term system improvements; here we focus on an approach that directly relates stakeholder experiences to the decisions that a system
6.3 Methodology

For this work, we use an overarching methodology that combines established methods in order to identify, relate, and meaningfully evidence employee-facing security management decisions in an organisation setting. We apply an iterative *co-design modelling process*, generalising the well-established modelling methodology as explained in, for example, (Demjaha, Pym and Caulfield 2021; Caulfield, Ilau and Pym 2022b), that aims to bring modellers and the stakeholders of an organisation together, adopted from (Demjaha, Pym and Caulfield 2021; Caulfield, Ilau and Pym 2022b). This approach guides the building of a model of the organisation environment (as relates to security). Evidence of human-facing experiences and processes is then substantiated with evidence collected from qualitative research, in this case semi-structured interviews; here we employ humble Inquiry (HI) (Schein and Schein 2021), whereas for interview analysis we refer to the widely used thematic analysis (TA) method (Braun and Clarke 2020).

6.3.1 Co-design modelling process

Security managers are faced with the challenge of managing security apparatus within dynamic socio-technical environments. Yet, security managers must often take decisions in the interest of security that impact this complex environment, without always being aware of the potential outcomes. Modelling, whether conceptual or otherwise, can be used as a tool for managing uncertainty associated with security decisions (as with e.g., information security investments (Fielder et al. 2016), or exploring physical access improvements (Caulfield and Parkin 2016)). There are, however, challenges with modelling in a useful and rigorous way in general, and modelling cultural and behavioural aspects of security in particular (Woods and Böhme 2021).

While the managers of an organisation’s security apparatus may have extensive knowledge of that apparatus and expertise in its domain of application, they may lack knowledge of the necessary methods and data collection requirements for modelling (Hubbard and Seiersen 2016). Modellers, on the other hand, experts in the latter, may have limited understanding of the system under observation, the available data to be collected, and the context of the domain. This can limit a modeller’s capacity to model a system in a useful way that can arrive at actionable
recommendations in practice (hence such things as the popularised ‘spherical cow’ metaphor coming to be 1).

In an effort to address these linked challenges, and facilitate better opportunities for capturing the behavioural and cultural aspects influencing security in organisations, we apply the co-design approach for security modelling which was presented in Chapter 5.

6.3.2 Co-design modelling components

It is important to further emphasise the key differences as well as similarities between our understanding and definition of ‘model co-design’ and previously used methods such as participatory design (also referred to as co-design) (David, Sabiescu and Cantoni 2013) in the HCI and design community, as well as participatory modelling (Voinov et al. 2018).

Traditionally, participatory design has been used as a way of sharing knowledge between stakeholders of different disciplines, and often potential users of a product, with the aim of integrating this knowledge into a final product (Kleinsmann and Valkenburg 2008). Similarly, participatory modelling engages in a process of learning from stakeholders — and integrating their knowledge into formalised representations of reality. Our approach focuses more heavily on a process of co-creation from the very beginning, including the problem identification, objective setting, and model design and construction.

PM differentiates between three types of modelling method selection (Voinov et al. 2018): an ‘expert approach’ driven by the modellers’ own preferences for tools and methods; an ‘experimental approach’ developed and piloted specifically within an engagement between modellers and stakeholders, and; a ‘participatory approach’, wherein all stakeholders, including modellers, decide about the modelling tools and methods to be used. The PM community then recommends an approach which incorporates elements from all 3 types (Voinov et al. 2018). While the PM community considers the stakeholders’ ‘lack of (modelling) expertise’ as a potential challenge when choosing tools and methods, our approach embraces the expertise of our stakeholders in their own domain of practice, as a strength.

We treat the expert stakeholder as an expert stakeholder all the way through our process. In this sense, we embrace the participatory approach of PM, but with a greater focus on co-design, rather than potential participation. In a way, our work has parallels with both co-design and participatory modelling, applied in the field of security, more specifically in the modelling of behavioural and cultural aspects

1https://en.wikipedia.org/wiki/Spherical_cow
6.3: Methodology

Figure 6.1: The co-design process applied in this study (adapted from Demjaha, Pym and Caulfield 2021; Caulfield, Ilau and Pym 2022b).

A security manager at the university had questions about security practices.

Initial conversation with security manager to understand the infrastructure of the system. Discussion about the data available for collection.

Interviews with administrative staff to gain a deeper understanding of security behaviours. A subsequent cycle included interviews with IT and security staff to fill in the knowledge gaps identified in the first candidate model. Translation zone between us and the stakeholders.

Design of candidate model based on interview observations and data.

Deduction/recommendations from properties of the candidate model based on the interviews.

A summary of the candidate model properties created by us sent to the security manager so that it can be interpreted back in the domain.

Collaborative interpretation of the candidate model properties as domain/security properties with the security manager.

A collection of security properties implied by the candidate model properties. Recommendations based on candidate model.

Validation of the security manager’s assumptions of the domain against observed properties of the domain. Validation with two security managers.

Candidate model met its objectives and therefore became the model. Improvements were discussed for the next iteration.

of security in organisations. The focus of our approach is on representing decisions related to the management of employee-facing security, and how these relate to infrastructure, requiring a rigorous modelling approach with models constructed to inform decision-making, and how it feeds back into subsequent cycles — all in co-design with the expert stakeholder (here, the security managers in a participating university). The approach of iteratively collecting more evidence to reach more well-informed decisions that build on existing understanding of the system can improve investments and security risk management practices (Hubbard and Seiersen 2016).

As seen in Figure 6.1, the methodology provides a structured approach for modeller–stakeholder interaction through the key phases of model construction. The key phases are Observation and Candidate Data Availability, Candidate Model, Model Consequences, and Domain Consequences — and their implementation is carried out through the processes of interpretation, induction, deduction, and validation. We create a sub-loop between the first two phases which represents the translation zone between the modellers and the security decision-
maker(s) (Spring, Moore and Pym 2017). Below we explain how the different stages of the co-design process were applied in this particular study, emphasising the importance of the translation zone.

The goal of each part of the framework (Figure 6.1) is as follows:

- **Observation and Candidate Data Availability**: identify mutually beneficial objectives, which can be pursued, and explore the data collection opportunities in the real environment.
- **Translation Zone**: engage in an iterative process of mutual learning, where modellers learn about the system from the stakeholders, and the stakeholders learn from us about the nature and bounds of our research (in this case, socio-technical security) as well as the required data and information to substantiate the model.
- **Candidate Model**: construct an initial candidate model based on the collected data (here, qualitative data from interviews) and information.
- **Model Consequences**: deduct preliminary consequences from the candidate model which resonate with the stakeholders.
- **Domain Consequences**: interpret the domain properties that are implied by the properties of the model (consequences relating to the real-world environment).
- **Validation**: validate the domain properties that are implied by the model against the observed properties of the domain.

The framework described above can be used to develop all of the key types of model — mathematical, computational, and conceptual (Caulfield, Ilau and Pym 2022b). In the case of the work reported here, a conceptual model has been constructed, and the components of that conceptual model (represented in Figure 6.4) are the following:

- An in-depth understanding of the system;
- An understanding of the interaction between different stakeholders in the organisation;
- Knowledge of the organisational structure and policies intended to be applied to the system.

We demonstrate how to use this conceptual model to extract recommendations that can inform security policy design, communication, and decision-making.
6.3.3 Supporting security management decision-making

Engagement was facilitated with the acting security manager — CISO — at a participating university, and the co-design approach was applied in the process. The overall aim was to support decisions about how to manage and invest in information security infrastructure, which is a common challenge (Hubbard and Seiersen 2016). Here we specifically examined the management of employee-facing security, where our examination of Related Work (Section 6.2) has detailed the additional complexities here, as well as reasons why it is critical to anticipate and avoid problematic security provisions. A capacity to model a system and to some extent forecast the outcomes of decisions then have additional importance.

In the initial engagement with the security manager, the manager had made some assumptions about the security behaviours and practices at the university but had, at the same time, a lot of questions, believing that knowing more about working practices in the organisation would better inform decisions around investments in employee-facing controls and improvements. That is, there were elements of the workings of the organisation — around employee activity — that the security manager believed they (i) did not understand because they were not observable as part of their existing (technical) infrastructure, and (ii) did not have the methods or capacity to measure. This naturally led to opportunities for human factors research to gather and structure information from the environment. Working in the spirit of the related work section discussed earlier, the goal was to examine the role of behavioural aspects in organisational security, toward finding ways to reach workable security solutions in practice.

These challenges were complicated further by the decentralised nature of the university infrastructure (with some user support and IT decisions happening within faculties or departments); the security manager had a less detailed overview of the system than if all infrastructure was directly under their control (as in a completely centralised environment), and was thus unable to support these assumptions or explore them further from their ‘central’ position.

The interaction began by exploring the opportunity for collaboration. Initially, we, as modellers, and the security manager as a stakeholder, each had our own representation of reality, which was, for the purposes of this research, regarded as being each side’s candidate model of the system and its socio-technical interactions. These models were predominantly characterised by our areas of expertise. For example, the modellers brought in knowledge about the human factors of security, and questions to be asked about security culture and practices. The security manager, on the other hand, brought in observations of the system, and different elements of
infrastructure relevant for the security behaviours at the university. As shown in Figure 6.2, while both sides had their own understanding of the system, and areas of expertise, exchangeable artefacts were identified to facilitate the translation zone.

The concept of the translation zone stems from that of trading zones (Galison 2010), which was introduced to bridge the communication gap between sciences. The purpose of a translation zone is to identify a shared language between communities in order to facilitate conversation and collaboration in specific contexts (Parkin, Arnell and Ward 2021). Having been previously proposed to solve a range of challenges in the security community — e.g., (Spring, Moore and Pym 2017; Parkin, Arnell and Ward 2021; Caulfield, Ilau and Pym 2022b), we similarly adopt the concept of the translation zone and exchangeable artefacts, to establish a meaningful conversation with the security manager. This exchange would be meaningful insofar as the researchers gathering human factors data within the organisation in a targeted fashion, and constructing a model of the environment that is then discussed with the security manager. By identifying these artefacts, the modellers and stakeholder were able to interact within the translation zone through commonly understood concepts, which are outlined in the intersection of the union in Figure 6.2. As can be seen in Appendix C, the artefacts identified within the initial engagement became the basis for the general structure of interviews conducted with employees as part of later evidence-gathering activities.

Figure 6.2: Exchangeable artefacts between modellers and stakeholders in the translation zone.
6.3.4 Interview study (substantiating the model)

6.3.4.1 Interview structure

In total, 21 semi-structured interviews with employees were conducted, the design of which was guided by Humble Inquiry — an approach which facilitates relationships based on interest and curiosity, and focuses on asking instead of telling (Schein and Schein 2021). HI goes beyond traditional interviewing and aims to create an atmosphere of trust and empathy. It is also guided by similar principles to the methodology here, such as truly learning what the other person knows and thinks and why — making it an adequate choice for this study. By using HI, the interviews facilitated open and honest conversations with our participants, and learned more about the context of their work in relation to security practices. Rather than merely following structured questions, the focus was on constructing open-ended questions, and prompts, to facilitate an interactive and honest conversation with our participants, while acting to build implicit trust. On average, the interviews lasted for approximately 55 minutes.

Opening questions aimed to understand employee experiences through organisational culture and ‘how we do things around here’ (Deal and Kennedy 1982). A definition of ‘security culture’ is also useful for scoping what was explored, as the ‘attitudes, assumptions, beliefs, values and knowledge’ of employees and their interactions ‘with the organisation’s systems and procedures’ that result in security-related behaviours (Da Veiga et al. 2008). However, we note that rather than there being ‘a collection of people’ to define organisational culture, the words community, group, or team are better suited to indicate some level of culture formulation (Schein 2010). Informed by existing studies of security in organisations, the interviews also explored interaction with security policies and training, and how employees manage primary work tasks alongside security expectations (as in Appendix C). The interviews with support staff were informed by the interviews with administrative employees and further explored security practices and interactions at the university, including the ticketing system, which is a way of managing user queries at the university (Appendix C).

6.3.4.2 Participants and recruitment

Interviews were conducted with employees holding active roles in the partner university. The interviews were anticipated to provide a foundational understanding of security-related practices among administrative as well as IT and security support staff at the university, while being a large enough cohort to characterise issues rel-
evant to particular security processes and technologies. Considering that the aim was to interview several ‘hard to recruit’ participant groups, the total participant number depended on their availability (a challenge noted in other studies with active professionals (Reinfelder, Landwirth and Benenson 2019)). Fourteen administrative staff and seven IT and security support staff were interviewed, in addition to iterative discussions with two security managers responsible for information security strategy.

The first group of interviewed participants are administrative staff who work across departments and faculties at the university, in a wide range of services such as finance, HR, and communication. The second group of participants — which we refer to as IT and security support — consists of staff in the central university helpdesk, security group, and local/departmental IT teams. Overall, the participants that were recruited represent a variety of roles, departmental as well as central functions, and level of seniority (ranging from administrator to manager level).

The two security managers with whom there were continuous interactions are a part of the security group which governs the security of the entire university. They are responsible for managing different functions within the group, such as awareness, incidents, and governance, which support both staff and students in their daily management of information security.

Senior managers in administrative services were asked to promote the study as a normal part of communications with teams, where care was taken to ensure that any such communication is framed in a collegial manner for the good of the organisation, removing any sense of pressure to participate. In addition to this channel of promotion, the interview study was promoted via the university newsletter, using a combination of brief study recruitment text and advance sight of the participant Information Sheet, to provide potential participants with information about the study and its aims, so that they could make an informed decision whether to participate. There was a focus on speaking to administrative staff in this engagement as they work with important data assets. Security managers suggested to focus in this area first.

6.3.4.3 Research ethics and Covid-19 measures

The study was approved through the university ethics committee review process. The principles on the Menlo Report were followed (Kenneally and Dittrich 2012): Respect for Persons through anonymisation, right to retract from interview, conducting interviews online, etc.; Beneficence through anonymity, etc.; Justice by hearing both sides, etc.; Respect for Law and Public Interest by respecting the policies of the
organisation during the study. All interviews were recorded and transcribed by the thesis author and transcripts were redacted to remove any identifying information.

Because of changes to research conduct during Covid-related ‘lockdown’ restrictions over the course of the study, it was necessary to conduct human-subjects research online. The interviews were conducted between April of 2020 and November 2021. Because of the changes and uncertainty in the way of working following Covid, the recruitment and interviewing cycle lasted longer than expected. This means that experiences were captured at different points during the pandemic. Having remote as well as hybrid working conditions may have impacted the responses of participants. Recent studies (Kaur et al. 2022; Delfino and Kolk 2021) have reported on the impact that the pandemic has had on employees and their working practices. In particular, Kaur et al. focus on how system administration work was affected (2022). Their findings largely align with those presented here, in that, for example, many system administrators did not experience the shift to remote working to be a significant change in terms of carrying out tasks, but they did experience longer working hours. Many of them communicated with users via e-mail or phone prior to the pandemic, and this type of communication continued during remote working. Coordination with colleagues, especially new joiners, proved to be more challenging during remote working, as even small exchanges had to be done via the phone or MS Teams. This also impacted the ability to provide or receive help from other colleagues or teams. Lastly, a notable difference was the decrease in human interaction, both with colleagues and users, where particularly in our case, this was more visible for local administrators who were used to walk-ins and informal interactions with users.

6.3.4.4 Data analysis

The interviews were transcribed verbatim and analysed through a process of thematic analysis (Braun and Clarke 2006, 2020). A hybrid approach of reflexive and code-book thematic analysis was adopted. The focus was mostly on reflexive TA, an open coding approach, where themes are the final outcome of an iterative theme development and coding process (Braun and Clarke 2020). Additionally, a code-book was developed during the coding process to document the analysis. Unlike other approaches to TA, neither code-book nor reflexive thematic analysis use inter-rater reliability as a measure of quality (Braun and Clarke 2020).

Two separate code-books were constructed, one for each of the two main participant groups. Through a process of refinement and regular coding discussions, the final code-book for administrative staff consists of 73 codes (Appendix C.2.1),
whereas the one for IT and security staff consists of 37 codes (Appendix C.2.2). It should be noted that the original code-book for IT and security staff consisted of 56 codes. However, some of the coding was meant for purposes outside of the thesis scope and these codes were not directly mapped to the themes in this chapter. Based on groupings of the codes, several themes were identified for both user groups: 5 themes from the interviews with administrative staff, and 4 themes from the interviews with IT and security support. The themes for both groups are summarised in Table 6.1, and the outcomes of our interviews in the next section are arranged according to these themes and represented in a conceptual model (Figure 6.4).

6.3.5 Qualitative data collection and the modelling framework

We relate the interview activities and qualitative research to our framework (Figure 6.1) in the following ways:

- **Observation and Candidate Data Availability**: the observation phase started with preliminary conversations with the security manager to capture their perception of how the existing IT/security systems were being used by employees and other users, and their questions about how human factors research — and research techniques — could be helpful to inform management decisions. This centred around understanding better which potential changes, and in turn decisions, could encourage engagement with security provisions, and how to avoid deploying controls which frustrate — and not support — users. During this conversation, there was a discussion about what should be achieved with the modelling process and the objectives for the work were agreed. Opportunities for data collection were also discussed, and the security manager helped with identifying other relevant stakeholders who could provide a realistic picture of the system, as well as brokering contact with specific teams.

- **Translation Zone**: the translation zone depicts instances of interaction between researchers/modellers and the security manager, which occurred several times throughout the co-design process. The placement of the translation zone in the context of the traditional modelling process is summarised in Figure 6.3, adapted from Caulfield, Ilau and Pym (2022b). Figure 6.1 gives a more detailed description of the co-design process that Figure 6.3 presents, emphasising the role of the translation zone.

- **Candidate Model**: after consultation with the security manager, the first round of interviews with administrative staff was conducted, and they were
able to provide an in-depth account of security interactions at the university, as a stakeholder group which both (i) made direct use of provisioned IT systems, and (ii) worked with sensitive data (such as student records), and so ought to have secure systems at their disposal. Administrative staff engagement acted as the first iteration of the translation zone that supported the fuller approach. The knowledge gained from this interaction enabled the construction of the first candidate model, based on the analysis of the interviews. When going back to the main stakeholder — the security manager — gaps as well as areas of interest were identified from the interviews. In further conversation with the security manager, the next group of stakeholders to engage was identified, specifically the IT and security support staff. This demonstrates the sub-loop between the translation zone and the candidate model, as seen in Figure 6.1. The candidate model was updated in light of new knowledge emerging from the second phase of interviews.

- **Model Consequences**: The analysis of both sets of interviews led to the extraction of potential recommendations from the candidate model that could be applicable in the domain (of managing IT-security in a university).
- **Domain Consequences**: During our interactions with the security manager, the properties of the candidate model were collaboratively observed and translated into domain properties. In more concrete terms, there was a dis-
cussion about the method of translating the findings into appropriate and useful recommendations that could inform future security decision-making in the university (the ‘domain’). Once it was determined how to translate the properties from model to domain, the main findings stemming from the candidate model were instantiated. The purpose of the co-design process was intended to be mutually beneficial and the recommendations were hence not formulated in a silo. Therefore, the final formulation of the recommendations was shaped towards the end of the co-design process, in interaction with the main stakeholders, and based on existing constraints (e.g., budget) and realistic opportunities.

- **Validation**: In the final stage of the co-design, another security manager engaged in addition to the one who was part of the interactions from the very start. The second security manager had recently joined the university and was interested in gaining insights that would inform future security initiatives and decisions. Both security managers confirmed that the findings from our candidate model were in line with their own assumptions. They were also positive about the knowledge sharing that had occurred as a result of the co-design process and were keen to use the recommendations extracted from the candidate model. Although we completed two cycles of our framework, the engagements with the security managers pointed to other groups to engage with should further cycles be possible (as reported on later in Section 6.4).

### 6.4 Results

Here we present the outcomes of our interviews with employees working in administrative teams (PE##, Section 6.4.1), and IT and security support staff (PS##, Section 6.4.2). The outcomes contribute to a conceptual model (Figure 6.4), which supported the interactions with security decision makers, and which here act as an overview of the identified entities, attributes, and relationships in the organisation which are relevant to the security practices at the collaborating university. The model comprises 9 themes in total, which are also summarised in Table 6.1.

As the legend depicts, the model consists of 4 different shapes which portray the entities, attributes, relationships and links in the model. For example, the link from the entity **Users** to the entity **Central Services** facilitates the relationship **Communicate**, and **Not Preferred** is an attribute of that relationship. We describe the conceptual model below through each individual theme and reflect on its evolution throughout the next sections. Section 6.4.3 then summarises the closing
6.4 Results

Figure 6.4: The conceptual model in the form of an entity-relationship (ER) model representing the interview themes.

discussion with security managers, incorporating paraphrased statements from that interaction.

6.4.1 Administrative employees

6.4.1.1 Use of technology

Most of the administrative participants see technology as a fundamental part of their daily work. They mention the importance of technology when communicating with others, such as through e-mail or Microsoft Teams, the use of content creation tools, as well as several university systems used for administrative purposes. Administrative staff provide a nuanced view of their experience with technology, with examples of advantages — where using a tool enables more effective work — but also
Table 6.1: Themes identified during thematic analysis.

<table>
<thead>
<tr>
<th>Administrative Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviour is not guided by policy directly</td>
</tr>
<tr>
<td>Central mandates, made actionable locally</td>
</tr>
<tr>
<td>Personal relationships with IT and security support build trust</td>
</tr>
<tr>
<td>Relating security to every day tasks</td>
</tr>
<tr>
<td>Impact of GDPR on security awareness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT and Security Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local support teams build relationships</td>
</tr>
<tr>
<td>Giving assurance rather than guidance</td>
</tr>
<tr>
<td>Asking for security advice is common</td>
</tr>
<tr>
<td>Security of behaviours varies between individuals and groups</td>
</tr>
</tbody>
</table>

barriers that may be introduced when using IT systems and services. For example, participant PE1 explains that they must often rely on colleagues for getting access to certain reports, because of restricted access as a temporary employee. PE3, on the other hand, appreciates the physical presence of the security guards, when ‘the technology sometimes doesn’t work’ and they are unable to use their access card.

The topic of change is also present in the conversation about technology. Some participants observe that there are people in the university who are sceptical towards change, and meet technology advancements with strong feelings of resistance. Such people usually need longer time and additional support to adapt to the use of new technologies and ways of working. The ‘four rooms’ concept refers to a similar phenomena (Weisbord 2004), where employees may not be as willing to change if they are content with how their workplace is currently established.

6.4.1.2 Role of security

Most participants seem to believe that their current workplace is secure. This includes an implicit trust that the university’s own systems are secure, and that this trust extends to the external systems used by the university, in other words — ‘the university have put their trust in the software’ — PE13. Participants are not able to articulate thoroughly what they mean by ‘secure’, but some associate a state of security with the lack of experiencing a compromise. This is in contrast to the notion of ‘counterfactuals’ in security, as ‘what-if’ scenarios (Herley and Pieters 2015); that is, if there is no experience of compromise, then what is being done currently must be secure.
In addition to placing trust in the organisation’s security provisions, participants are also generally understanding towards its limited IT and security resources. Although it may often be inconvenient to experience a long waiting time (e.g., to regain access to a locked device or account), participants are aware of the university’s limited resources and, in turn, their propensity to prioritise certain tickets over others. One participant summarises this sentiment: ‘When I have tried with [central help-desk], it’s been a very mixed bag. Sometimes, if it’s something very specific, you can solve it over phone but if you turn it into an e-mail ticket it can take a while. [...] But at the same time, it’s nothing that I hold a grudge about, [...] it’s not a big department and these are the less urgent things.’ — PE6.

6.4.1.3  Behaviour is not guided by policy directly

Representation in model:  The link between the entity Users and the entity Policy denotes the relationship Guided, which in this case is a negative relationship, as the link states. The link from the entity Users to the entities Local IT and Security Support, Managers and Co-workers facilitates the Guided relationship, only this time it is a positive relationship. For example, Initiatives is an attribute of the entity Managers, and users are guided by manager initiatives. In addition, there is a recursive relationship between users, meaning that users are also guided by their own awareness.

Participants’ security behaviours and practices are generally not guided by a specific policy but rather by other factors such as personal security awareness, co-worker behaviours, manager initiatives, or guidance from local IT and security support. The overwhelming majority of participants are not explicitly aware of a security policy. There was, however, some mention of awareness of policies relating to physical security, data retention, health and safety, as well as data protection. No direct connection was made between such policies and information security. After direct prompting, participants acknowledged that there is likely a security policy in place, but almost none claimed to have seen it or have substantial knowledge of it. These findings then represent knowledge derived from the working environment that the security manager would benefit from, as employee experiences are disconnected from some of the tools they control, such as security policies.

Instead of a specific policy, several other sources of guidance emerged. For instance, when asked about the source of their security behaviours and practices, PE13 noted that ‘it’s also from talking to colleagues, like my manager, who is also knowledgeable about these sorts of things, as well. So, it’s probably come from a mixture of experience, my own practical experience and learning from reading’. Kirlappos,
Parkin and Sasse noted the role of middle managers in communicating security behaviours (2014), and Blythe, Coventry and Little have noted the potential of security culture to act as ‘the way we do things here’ (2015).

6.4.1.4 Central mandates, made actionable locally

Representation in model: The link from the entity Central Services to the entity Local IT and Security Support facilitates the relationship Enforced, and Mandates is an attribute of that relationship.

How security is managed centrally or locally relates to a broader issue within the university, distinguishing between preparation and action. Participants mention several IT and security initiatives that were mandated and communicated centrally in the past, such as the implementation of the General Data Protection Regulation (GDPR) or the introduction of Microsoft Teams. Several participants frame rules as becoming ingrained once they are related to local context, such as PE9:

‘It’s that combination of the things we all sort of vaguely know we should do because the people at the top have sent out these messages like […] change your passwords, etc. But then when it is sort of talked about and enforced locally, then it becomes more of a culture, and it becomes more obvious how it affects your work and the work of the people around you.’

— PE9.

Some participants imply centrally-communicated security rules and recommendations may be ignored or remain unclear, until they are taken a step further by local managers, and linked to the local work context at the level of a team. These findings identify a potential ‘local’ point of action for centralised policies, in local managers. This again reflects previous findings (Kirlappos, Parkin and Sasse 2014) relating to how security-related practices are informed by managers, but also relates to conversations around the role of ‘security champions’ within companies (Becker, Parkin and Sasse 2017).

6.4.1.5 Personal relationships with IT and security support build trust

Representation in model: The link from the entity Users to the entity Local IT and Security Support facilitates the relationship Communicate, and Relationship and Trust are attributes of that relationship.

Participants mentioned that they may avoid communication with central services if it is seen as involving a longer waiting time. Also, the majority of participants believe that it is important to have more of a personal relationship with IT and security staff, in order to build trust and effective communication. The participants
that do have a local IT person or a departmental IT team report a more frequent and positive interaction, in comparison to the participants whose only recourse would be to contact the central service desk. For example, PE13 explains the difference in behaviour when interacting with local vs. central support:

‘We had our own IT team and the benefits of that are, you know the guys, you know they’re just down the corridor from you. You know those IT guys well and you trust them. What used to happen, when I was based there, [...] if I saw an e-mail that I thought looked like a phishing attack, I would forward the e-mail to them and then say, flag it as this looks dodgy, to them. And then they would deal with it. They would make people aware you know be careful [...] But, now that [central help-desk] is a bit more remote [...] I mean they’re not physically down the corridor from me and I don’t really know those people face to face.’ — PE13.

When participants were asked whether they would prefer asking for help locally or from central services, most of them preferred a local alternative, unless they needed help with something quite specific, as ‘the local IT manager is maybe more pertinent to me because I know the person, [they are] a colleague of mine.’ (PE11). Crucially, several participants mention that they feel more comfortable and potentially less embarrassed to get help from somebody they feel they know or somebody who is physically located closer to their office. A preference for seeking IT help from someone who is seen as having an existing understanding of personal IT needs has been noted for home users (Poole et al. 2009; Nthala and Flechais 2018). Kirlappos and Sasse observed that trust between employees can clash with the trust promoted by following top-level policies (e.g., if a policy requires screen-locking even in the midst of colleagues); here we find that support teams serve a purpose as a mediator between the two (2014).

One participant specifically mentioned an approach called ‘management by walking’, suggesting someone from central help-desk could walk around and introduce themselves to staff. The participant believes this would make the experience more human and future interactions more approachable. The work of Harvey Molotch in assessing, for example, airport and subway safety, advocates such an approach also for understanding how infrastructure is experienced ‘on the ground’ by those who must use it (Molotch 2013).

6.4.1.6 Relating security to everyday tasks

*Representation in model:* The link from the entity *Users* to the entity *Policy* represents the relationship *Associate*, and *Tasks* is an attribute of that relationship,
meaning that users associate security policy with their tasks.

An immediate takeaway from the interview results is that participants associate security with various terms and concepts, most frequently with tasks familiar and relevant to them personally. When first asked about security, most participants mention data privacy or data protection as well as physical campus security. Almost reflexively, they then link these concepts to their daily work and give examples of tasks they usually complete to stay ‘secure’ in the workplace, for example, ‘I guess the only security part of it is monitoring visitor access cards.’ — PE3.

Although many participants do not immediately mention security tasks, most appear familiar with security when prompted further. Overall, any lack of knowledge or awareness about security practices cannot be attributed to a lack of interest or awareness about the importance of security. On the contrary, the majority of participants acknowledge the importance of being secure at the workplace and do not object to the additional effort that may be necessary. However, a difficulty conveyed by participants was in mapping security to concrete tasks. This appeared to stem from participants’ lack of knowing all the ways in which security was involved in their daily tasks.

As a constructive example, many participants mentioned GDPR when the topic of information security was brought up, for example, PE5, ‘we are being very careful about GDPR and [...] try not to leave anything on our desks.’, and ‘Security fits into my day because, as you might expect, I see quite a lot of confidential information. So, on the most basic level [including payment details] that’s GDPR level of personal information.’ — PE10. These excerpts demonstrate where participants saw a direct relation between a tangible workplace behaviour and a set of rules issued by the organisation. Participants took the opportunity to suggest ways to make these connections more often, such as through scenario-based content, tailored messages, and real-world examples. Another suggestion is to provide easy checklists, or ‘golden rules’ to follow, with very clear messaging, but, crucially, so that less is left up to the reader’s interpretation.

### 6.4.1.7 The impact of GDPR on security awareness

*Representation in model:* The link from the entity *Users* to the entity *Policy* facilitates the relationship *Impacts*, and *GDPR* is an attribute of that relationship.

Awareness of GDPR among participants was strong, with this being attributed to a clear organisation-wide buy-in, and the link to everyday tasks seeming to be clear: ‘Everyone’s thinking quite a lot about GDPR, [...] that message has come down very strongly. [...] Because a lot of people in our office work with student
records [...] people are fairly cognisant of the need to be sensitive with data and things like that.’ — PE9.

Moreover, the introduction of GDPR practices appears to have had an influence on security practices as well. For instance, some of the GDPR training materials helped to clarify the motivation behind using certain security controls, such as a Virtual Private Network (VPN): ‘I think probably GDPR did a lot in terms of information security because it spread the awareness of the few basic principles of you know, who is this information related to, who needs to see it and what level of access I give to people.’ — PE7.

Generally across the participants, there was an association of security tasks and policies with data protection, as most participants are obliged to comply with GDPR as part of their job. In contrast, those who did recall receiving security training almost exclusively related this to their induction when joining the university: ‘with GDPR it kind of clarified what [current workplace] systems were because I was a bit confused with the Sharepoint, OneDrive, VPN, Dropbox, all these things. So, this tutorial, [current workplace] mandatory training was very beneficial in explaining different systems and why they needed to be used.’ — PE11.

When asked whether security comes up in conversations with co-workers, the association with GDPR would often surface again, as for PE8: ‘It does come up, particularly in HR areas and sort of GDPR areas, for want of a better term. So, it’s like we can do this, we can’t do this because of GDPR. And I know it’s not exactly the same as information security, but it makes you think about what information you can and can’t pass down and how secure information is. [...] I think will I put this on an e-mail, will I put it on the Dropbox [...] what is the most secure way of putting that information which is confidential so that only certain people can access it?’ — PE8.

6.4.1.8 Summary

The themes presented in Section 6.4.1, namely, Behaviour is not guided by policy directly, Central mandates made actionable locally, Personal relationships with IT and security support build trust, Relating security to every day tasks, and Impact of GDPR on security awareness, were produced in the first iteration of the translation zone cycle.

The overall themes from the qualitative work were aimed to be distilled as — or related to — exchangeable artefacts. For example, in the theme Behaviour is not guided by policy directly, behaviour was our side of the translation zone, and policy was on the stakeholder’s side, whereas guidance was the exchangeable artefact
6: A Case Study Examining the Role of Security Practices in Organisational Culture

in the translation zone. It was communicated to the security manager that local understanding was important to employees, as was being able to put security advice into context; this highlighted the role of managers ahead of policy in communicating security, for instance.

Another example is the theme *Relating security to every day tasks*, where the stakeholder had knowledge of security practices at the university, the modellers modelled the everyday tasks through the interviews, and the relationship between the two was discussed in the translation zone. These themes were taken into the next discussion with the stakeholder and it was agreed that more information was necessary and the next important cycle would be to conduct interviews with IT and security support. Managers were guiding employees’ security behaviours locally, where a relationship with ‘central’ security policy was missing, there was instead a reliance on IT support teams to provide relevant security-related guidance. What was seen in practice with administrative employees was in essence along the same lines of a a primary recommendation in earlier research of ‘Shadow Security’ behaviours (Kirlappos, Parkin and Sasse 2014), informing locally-derived working practices with security knowledge, rather than supplanting those behaviours entirely with security-focused behaviours, which dismiss the need to maintain productivity and applicability to local context.

6.4.2 IT and security support

6.4.2.1 Local support teams build relationships

*Representation in model:* The link from the entity *Local IT and Security Support* to the entity *Users* represents the relationship *Communicate*, and *Relationship* is an attribute of that relationship.

Local support teams have the opportunity to build a relationship with their users. They are ‘just down the corridor’, and as PS5 put it, they are: ‘*friendly, local, and quick*’. According to IT and security support, users prefer to approach someone they know and trust, rather than a stranger who has no understanding of their history (as noted elsewhere in discussion of ‘informal’ technical support (Poole et al. 2009)). In terms of employees adopting secure behaviours, users are seen as often feeling embarrassed about asking ‘stupid questions’, and a choice to talk to local support is in part due to feeling that they will not be judged, and ‘*Yeah, we are not exactly going to broadcast it, what comes to us stays with us.*’ — PS7.

Local support staff such as PS7 would make an effort to get to know their users, learning about their way of working, and thus providing a more personalised experience: ‘*there is that connection. There is not this nameless faceless person,*
who doesn’t maybe know my history or even just [that] the way I work is quirky or different.’ — PS7.

The ‘lockdown’ restrictions related to the Covid-19 pandemic have made it difficult to maintain the same type of in-person communication. While most local teams usually have an ‘open-door’ policy, Covid-19 ‘lockdown’ practices have limited users’ opportunity to pass by with queries in an ad-hoc manner (as noted in research with system administrators in the immediate aftermath of the pandemic (Kaur et al. 2022)). Local support staff expressed that they continue to maintain interactions, either through the phone or via Teams, and still try to accommodate physical appointments when possible and in accordance with the restrictions (for instance, knowing when employees will be at the office, to then also be there if support might be needed).

### 6.4.2.2 Giving assurance rather than guidance

*Representation in model:* The link from the entity Local IT and Security Support to the entity Users facilitates the relationship Provides, and Assurance is an attribute of that relationship.

Support participants stated that there is guidance for a variety of topics, which has been made accessible, either on the central university website, on local sites or forums, or via e-mail correspondence. However, these materials were seen as lacking a level of assurance. Users prefer to get confirmation from a person that what they are doing is correct, rather than interpreting the guidance themselves. This was represented in that there may be many tickets about topics for which there is already guidance available, and the tickets would often be seen as trivial to solve, from an IT and security perspective; this was in essence laying the groundwork of a safe space for users, so that they would reach out if faced with something more serious later. One participant elaborates this further:

‘Without the trivial engagement, when someone is new and you’ve given them their password, or their new laptop, [...] it’s what creates community, and it’s what gives that person the understanding that they can come to us down the line that’s going to be more beneficial for them. But, having engaged with us on the trivial, I think makes them more likely to come to us with the more complex stuff where we can actually help them where they couldn’t help themselves.’ — PS3.

Although there is value in trying to make guidance more appropriate and engaging for users, IT and security support believe that sometimes even if guidance is available in abundance, there are users who need human interaction and assurance.
When they are unsure of how to do something securely, it helps to receive some type of approval from the experts whom they trust:

‘Absolutely, yeah there are some people that just want to make sure because when they read that information, they are not confident enough to make a decision. So, maybe they just need some approval or confirmation that okay you’re doing the right thing [...] they’ll tell you oh I just wanted to make sure.’ — PS2.

Blythe, Coventry and Little note that response efficacy was an issue for their participants, as to whether individuals behaviours were believed to be effective; here we find instead that there is hesitancy about knowing what the approved behaviours are (2015). Blythe, Coventry and Little mention the importance of feedback as of further interest, where here we find an existing interaction point for this in workplaces; that is, support teams (2015). We then find evidence that self-efficacy and the belief a person has that they can enact a behaviour can be encouraged by leveraging existing (local and informal (Poole et al. 2009)) processes. Similarly, where Das, Dabbish and Hong have explored the socialisation of security (2019a), and learning through communication with others, here we see that within that communication, there can be a purpose in explicitly legitimising or approving a learned behaviour as secure.

6.4.2.3 Asking for security advice is common

Representation in model: The link from the entity Users to the entity Local IT and Security Support denotes the relationship Ask, and Advice is an attribute of that relationship.

In line with the theme above, almost all participants reported that one of the most frequent security queries or tickets that they receive is users seeking advice. They often walk into the local office — for example, to ask the local IT and security support for any advice on working securely abroad when they are travelling to another country. Others may send an e-mail when they are about to procure a new piece of software asking which one is the most secure one.

On the other hand, IT and security support also make recommendations proactively and advise users on whether they should stop or start doing something in order to be secure. One participant working in local capacity says:

‘People will often ask us for advice, they’ll say look I know what to do but I just want to check. And that’s because of that culture that we’re put in, ask us, we’re busy, but ask as anyway, we’d rather you get it right than get it wrong. And I’d say probably 25% of the time we do pick up
on something and advise somebody and say that was a good point, but actually, did you know you could do it better’ — PS5.

This proactive dispensing of advice where it is known it will be relevant is again similar to findings from ‘informal’ technical support for members of the public (Poole et al. 2009).

6.4.2.4 Security of behaviours varies between individuals and groups

Representation in model: The link from the entity Users to the entity Security facilitates the relationship Varies, meaning that the security behaviours of users vary.

There is an overall view that users differ in terms of whether and how they contact IT and security support regardless of the issue, and those who will take a few steps on their own first before deciding to contact support. The people in the second category might first try to search online for information about an issue, or ask their colleagues, consult their manager, etc.. Several participants elaborate on this, for example:

‘It’s not just security related, but it’s sort of evidenced in security matters, there’s one sort of person that gets in touch at the first sign of needing to, or there being any IT issue. And there’s another sort of person who leaves it and tries to figure stuff out and only gets in touch when it becomes an actual problem. And, I think, for the security type stuff, probably people in the second groups, means we don’t actually see everything that’s going on.’ — PS3.

That some users may prefer to take matters into their own hand, and try to resolve or abandon the issue rather than contact support, may then mean that IT and security support do not always have oversight over non-secure behaviours. A reluctance to reach out to support or even report something may sometimes be due to long-term aspects of workplace culture ‘that we’ve always done it this way’ — PS2, where ‘It’s not easy to change those individuals to adapt to better ways of doing things […] Especially if they feel like it’s always been working for them’ — PS2.

PS3 summarised a general order of how queries may reach them, where ‘they’d rather talk to each other, and then they’d rather talk to local IT support, then they might talk to central, but they might not’ — PS3.

6.4.2.5 Summary

Similarly to the previous cycle with administrative staff, the interviews with support staff were analysed, adding further detail to themes developed for the trans-
A Case Study Examining the Role of Security Practices in Organisational Culture

The role of assurance and availability/visibility of support staff were key findings from this round of interviews.

The themes were then taken back into another discussion with the stakeholder, as well as an additional stakeholder transitioning into a similar role. All themes were part of that discussion, having been enriched by a second iteration of the translation zone.

6.4.3 Reflection by policy decision-makers

The two security managers, responsible for higher-level security strategy such as security policies and procurement decisions, reflected upon the themes from the interviews (Sections 6.4.1 and 6.4.2), as presented to them.

Discussion with security managers was guided by the overall themes in Table 6.1. The conceptual model (Figure 6.4) was then useful for the discussion — the translation zone — as specific elements could be ‘zoomed in’ on within the themes when the security managers explored the meaning and available next steps in response to individual themes. This is reflected in the expansion of each theme in individual subsections of the interview Results.

It was noted that IT cannot drive a change of culture alone, and that IT teams ‘do not have the tools to achieve the change’, with this being about remit rather than power. The managers spoke instead of supporting the mission of the organisation, that security is not the primary purpose of the organisation, and although ‘security is important’, this is because of what the rest of the organisation is doing that their teams are supporting. This in turn pointed to the alignment of security messaging with the organisation’s strategic direction, to values in terms of enabling people to do their job safer, in a more compliant way, or as an improvement; for example, being able to send data in a safer way.

An additional area of focus was on rolling out secure technologies, ‘to be more secure from the outset’, and ‘if something goes wrong we can stop and help’, rather than security being everybody’s responsibility. This relates to the distinctions made by Pallas on organisational security provisioning, between large one-time investments in security technologies, and lower-cost user-level activities such as training, where the latter can nonetheless involve higher costs due to the need to proactively manage for non-compliant behaviours (2009). Regarding employees generally, it was seen as ‘it’s about how we get the same message to people in a way that is relevant to them’, in terms of understanding local risks; Beris, Beaument and Sasse make a distinction between sentiment toward security apparatus, and ability to recognise risks in the workplace which then activate interaction with security controls (2015).
When considering our study as a first step in a continuous process of using models to empower security management, the security managers suggested to look externally in further work, and involve security solution vendors. Specifically, vendors may argue that deciding how much security to have is an organisation’s choice as a consumer; however, the argument was made here that ‘security should not be a bolt-on any more; allow choice with a baseline.’ That is, ensure that a reasonable level of security is provided by default, then allow additional options on top of that.

In line with the support staff interviews (Section 6.4.2), the managers stressed the importance of ‘removing the stigma of raising questions about security’, and employees reaching ‘a comfort level to be able to ask when they don’t know’. The managers believed this relied also on engagement from their side, and ‘becoming a visible business partner’. The managers also discussed the role of policy in light of our findings; that is, that ‘policy is for taking someone to task; even if people ask for an exception to do things in a better way’. The key point in this is to drive engagement and find workable solutions. This is in line with existing research (Beautement et al. 2016; Zimmermann and Renaud 2019). However, here it is noted that support staff also may have questions about how things work, so it is necessary to provide support outwards from the security experts to support teams as well as employees. The managers noted that our co-design methodology ‘confirmed their intuition’, but that the evidence was useful for them, for informing and bolstering decision-making in the company of other stakeholders. The managers would have the co-creation process go into generating more information that is of practical use; for example, ‘how do we resolve some of this?’ or ‘how do we test whether we’re doing it right?’ This points to a further element of our approach; research producing scientific evidence, but also evidence that can inform real-world security decisions, where the two are not necessarily synonymous without an integrated approach that considers the working ‘model’ of stakeholders responsible for managing the systems that are being researched.

6.5 Discussion

Reflecting upon the interviews with employees (Section 6.4.1), participants noted security as important, but it was often discussed relative to daily tasks and terms relating to data privacy and protection rather than security details directly. The majority of participants implied that they had limited recollection of security policy and security training, but that experience and intuition played a role in guiding their security behaviours. Sources of guidance linked more closely to how they worked had the greatest utility, such as help from co-workers and managers (where the latter
may include arranging training), the local IT person/team or potentially a mixture of all of these.

Several participants also noted their own initiatives and security practices in the organisation as well as how they help co-workers with security. Ultimately, security behaviours are not embodied in one policy document alone, but are a sum of information, help from people who understand personal working practices and needs, and a kind of ‘oscillation’ (Kocksch et al. 2018) between being non-secure and secure, of signalling when not sure of how to do something, as well as being guided toward how to work securely in what may be an unfamiliar situation, or one that implies caution should be taken. Such a view, of care for the security-related norms and values in an organisation, goes beyond present references to the concept of a ‘security culture’ as being ‘how we do things around here’.

When in need, participants will call upon local IT support where it is available. In general, most participants are more likely to ask for help from someone they already know, such as their manager or a tech-savvy co-worker, rather than approach a relative stranger at the service desk. As noted in the interviews with both employee groups, this has parallels with informal technical support for individual members of the public (Poole et al. 2009). Here, this support is attributed to the opportunities for building relationships with local people in general. More specifically, there is a mutual understanding between the users and the local IT and security support that their relationship is built on openness and trust. These types of interactions with local support may positively influence users’ willingness to ask for security advice, or even to get in contact when something goes wrong. If support is not actionable or not visible, employees may develop their own ‘shadow security’ approaches to working securely (Kirlappos, Parkin and Sasse 2014).

When discussing the availability and adequacy of guidance with IT and security support, there seemed to be a shift throughout the conversation; although they saw value in tailoring guidance to users, as well as making it more practical, they also highlighted the importance of giving assurance to users. Local support staff claimed that many queries and tickets are trivial to solve from their perspective, but although the guidance is predominantly available, and often fit for purpose, many users require a level of confirmation that what they are doing is what was intended. They prefer to be reassured that their behaviour or practices are secure rather than having to make that judgement about themselves, upon themselves. This relates to contradictions in how security is typically managed in organisations, deciding that employees need to be trained, but that they know security well enough to adopt secure practices with incomplete information as if they are experts (Demjaha, Parkin and Pym 2022).
In the shift to remote working, there is less visibility of security practices as well as perceived barriers to communication. When the ‘lockdown’ was introduced, administrative staff worried about how they would get anything done, as collaboration with others was part of their way of working. An important part of that collaboration is the ability to communicate effectively. One participant reflected on how ‘you could normally raise your head above the screen and ask a question’ (PE7), whereas during the ‘lockdown’ they became more reluctant to reach out to each other remotely to avoid being bothersome. While technology has enabled communication during Covid-19 in one way, it has also hindered it in another way, by reducing opportunistic communication.

In terms of IT and security support, remote working seems to have impacted interactions between users and local services more than those between users and central services. This may be due to the differences in communication style to begin with, with local support always keeping their door open for physical interactions, and central services communicating remotely most of the time. Local staff continue to make efforts in accommodating their users, where a big part of this accommodation is in facilitating in-person support every now and then, in line with Covid-19 restrictions and recommendations.

Previous research indicates that when there is a need for IT or security support, people may also choose to ask their friends or family for advice (Poole et al. 2009). During the interviews, administrative staff acknowledged that they often observe the behaviours of others, be it family, or co-workers, and sometimes learn about security through these observations. This further emphasises the importance of visibility in security support, and the championing of secure behaviours in the organisation.

6.5.1 Limitations

It was made clear to all participants that summary themes could be communicated to the security management decision-makers, under conditions of anonymity. There is potential for this to have acted as a barrier to engagement by employees, but the participants voiced concerns nonetheless and offered alternatives to the existing security provisions. Similarly, support staff often talked positively about how they support employees, which may have indicated a bias in praising their own work, but they also provided concrete examples of positive engagements and of where negative outcomes could arise. They were also able to relate their experiences as reasoning to explain phenomena seen in, for example, the ticketing system (such as why there would be a great number of seemingly trivial tickets for issues where guidance was already provided, as a signal that direct assurance was amiss).
To consider this engagement as a specific case study (Morgan 2014), here the focus has been on a large university; it has many thousands of active users, like other large organisations, but is decentralised and not necessarily governed by one centralised IT system, much like smaller businesses (Parkin, Fielder and Ashby 2016). In consultation with the security managers, employee participant groups were knowingly selected based on their use of managed infrastructure, where most organisations will have teams dedicated to working with sensitive or high-value information.

6.5.2 Recommendations

Below are recommendations which emerged from the research study, which can be regarded as interrelated.

- **Security communication first, then security policy after.** Communications are often used to convey policy, but it is a reference document, not the lived experience of security. Security policy is a useful tool for articulating compliance expectations, but is not the way employees ‘live’ security. Communication efforts can then strengthen intentions of policy, where this includes supporting IT and security teams in ways to be more personable; this was seen in the interviews as being a way to encourage engagement and reduce the likelihood of unexpected incidents. Where there is a lot of dialogue about ‘security culture’, an embodiment of secure working has roots in there being visible support and a dialogue with security (Ashenden and Lawrence 2016), which is not the same as one-way communication of policy and training.

- **Leverage the approachability of local expertise.** Although local IT teams are referred to in terms of their proximity to employees’ work, the interviews surfaced that what was of great value was the approachability that this engendered. Local representatives are a conduit for two-way communication of security concerns, but also for validating behaviours and legitimising security behaviours for non-expert employees when they have learned them, providing a highly-valued confirmation that a behaviour is correct. Support staff would provide a prompt (Fogg 2019) to employees that they are ‘correct’ and have approval to activate their existing motivation and ability, so that employees actively practice the behaviour. This represents ‘knowing I’m doing the thing right’, as opposed to only ‘knowing the right thing to do’. This builds on the behaviour dimension of actionability as described by Redmiles et al. (2020), by activating actionable behaviour through assurance from
someone who understands the person’s existing behaviours (Poole et al. 2009) and has the expertise to ‘approve’ the behaviour.

- **Maintain an awareness of the wider security ecosystem and related infrastructure decisions.** The co-design process followed during this work helped create a conceptual model of the organisation, which captured the entities, attributes, and relationships of the system. This approach, including the translation zone, led both researchers/modellers and stakeholders to a more systematic understanding of the organisation, including the effectiveness of policies, how groups within the organisation interact, and where changes and improvements can feasibly be made, i.e., the decision points in the system. Maintaining such a systematic understanding — in this case via a conceptual model — then informs how an organisation designs future (security) policy changes effectively.

### 6.6 Summary

This chapter has detailed the application of the co-design methodology at a large university. The study consists of interview with 14 employees working with high-value data with specific security needs; 7 support staff across both local and central IT and IT-security support teams; and two senior security decision-makers in the organisation. In this chapter we highlight the importance of communication, trust and building relationships when providing security support to employees. The next chapter brings together the thesis work and discusses the overall findings in light of existing research, as well as the methodological implications of the thesis.
'Like a circle in a spiral, like a wheel within a wheel, never ending or beginning on an ever spinning reel.'

(Noel Harrison 2003)

7.1 Introduction

This thesis has explored the relevant security components of organisational culture, which then characterise security culture. It has linked the nebulous concept of security culture to workplace environment decisions, behaviours, and policies with the aim of representing ‘security culture’ in a more tangible manner. All of this exploration has been done through a process of co-design, alongside stakeholders working with security in organisations. This chapter is a space to discuss — in more detail — the background of the work, the common thread in the thesis, and the value of the methodology and findings.

7.2 Summary of work

The co-design methodology, economics framework, and the two studies presented in this doctoral dissertation, explore the relationship between security provisioning and the culture of an organisation, including the response to expectations from non-security related policies (e.g., administrative duties and deadlines). The organisational culture, or the ‘how we do things around here’, refers to the conversation around ‘security culture’, and its relationship to the skills and expectations associated with other non-security behaviours in the workplace. The economics
work demonstrates how current approaches to security behaviour provisioning in organisations mirror rational-agent economics, even where behavioural economics is embodied in the promotion of individual security behaviours. The economics framework aims to accommodate bounded security decision-making, within an ongoing programme of behaviours which must be provisioned for and supported. The two studies explore security practices and expectations in real organisations, focusing on distinct user groups such as employees, security managers, and IT and security support. They provide insights on the complex and interconnected nature of supporting workable security practices, both from the perspective of users and decision-makers. Finally, the co-design methodology aims to facilitate a better understanding of these phenomena, by emphasising the importance of stakeholder involvement when studying behavioural and cultural aspects of security.

7.3 How to understand people in organisations: crossing boundaries at security trading zones

A security policy embodies security decisions made centrally within an organisation. These central directives are intended to be followed by all members of the organisation. Regardless of investment, the enactment of security policies may not realise the protection intended during design due to lack of adoption by employees. Users may (knowingly or unknowingly) circumvent provisioned solutions, or create their own solutions based on what is available to them. If security provisioning does not consider the needs of users (generally, or as a discernible group of users), challenges in encouraging adoption may arise (Kirlappos, Beautement and Sasse 2013). Having an understanding of the controls which can fit existing user needs, as well as the process of identifying and investing in these controls at a policy level, can inform effective organisational security.

Supporting the user is increasingly seen as capable of contributing to a genuinely secure working environment (National Cyber Security Centre (NCSC) 2017; Standards and Technology (NIST) 2017, p. 31). Employees in organisations have primary work tasks to complete — an employee may base decisions about compliance and non-compliance on whether the controls mandated by policy are perceived as being aligned with completion of these tasks. From an economics standpoint, such user decisions can be seen to involve cost-benefit decisions, between personal benefits and security compliance for the good of the wider organisation (Beautement, Sasse and Wonham 2009). Once understood, these trade-offs can be modelled (Beautement et al. 2009) to anticipate the tensions between wider organisational pressures and
security tasks.

There is then a need to reconcile policy investment and employee security behaviours. Policy decisions within security policy management can benefit from the application of behavioural economics, to realise a structured understanding of context-specific security behaviours.

There are hard questions about security usability in organisations which most policymakers do not have the answers for, to for instance be able to account for the total effort that employees put into security throughout their working day (Beaumont, Sasse and Wonham 2009). Yet, not facing these challenges leaves policy managers with a reduced sense of how well they are supporting the workforce in their organisation:

1. Where are our employees now, in terms of both the security they have and the security they believe they need?
2. How much of employees’ time is security using, relative to other tasks?
3. Are there other controls which we do not know about which employees might be using, and if so, why might that be?
4. Where are employees taking or avoiding risks in their business tasks because of a bad fit with security?

This dissertation shows how a shift in thinking, and an exploration of these hard questions, could be supported by taking an interdisciplinary approach. Here we study the human factors of security, through a lens of behavioural economics, and with tools from modelling. Taking such an approach provides a broader understanding of the problems and questions that we explore in the thesis. As a result of incorporating different viewpoints and considering new perspectives, our co-design methodology facilitated new branches of knowledge. While from an academic context we take the relationship between human-centred security, behavioural economics and modelling — this being an interdisciplinary relationship — their application to concrete organisational cultures takes us into the transdisciplinary.

**What is transdisciplinary research?** According to several definitions, the core of transdisciplinarity is characterised by a process of collaboration between academics and practitioners working together to address a real-world problem, in a manner that combines interdisciplinarity with participatory approaches (Klein et al. 2001; Burton, Rønningen and Wedderburn 2008; Walter et al. 2007). Transdisciplinary approaches can be used to bridge the gap between scientific knowledge and organisational decision-making when addressing real-world problems. It has been shown that the involvement of non-academic stakeholders brings new types of knowledge
and expertise when solving research problems (Bracken, Bulkeley and Whitman 2015). However, for such collaboration to be meaningful, researchers must break down communication barriers between them and researchers of other fields, as well as non-academic stakeholders (Schmachtel 2019). For co-designing projects or research, a mutual way of communication must be created to achieve progress (Schmachtel 2019).

It is important to make the distinction between identifying a mutual way of communication and developing a common language. Several fields contribute knowledge and understanding to security — from economics to psychology to modelling — and the translation between these fields is vital (Spring, Moore and Pym 2017). But, as Spring, Moore and Pym highlight: ‘that does not create a common language any more than translating between German and French creates a combined language; it just creates a translation’ (2017, p. 13). The anthropological term trading zones was borrowed by Peter Galison, to address the issue of translating between sub-fields of physics (Peter and Mario 1999; Galison 2010). Galison argued that although physicists from different sub-fields speak different languages, with their own characteristics, they can still productively share ideas through the development of a trading zone (Galison 2010). The purpose of the trading zone is to translate ideas into a shared language from both sides which can then be translated back to the respective fields (Spring, Moore and Pym 2017). Trading zones are also applicable to the field of security (Galison 2012).

We have brought the concept of trading zones into the transdisciplinary by incorporating it into our modelling co-design process. We refer to it as the translation zone. Our methodology intends to bridge the disconnect between research and practice by creating new ways of collaboration. We introduce the concept of co-design into the classical modelling cycle and incorporate the translation zone to enable the development of a shared understanding. The translation zone is developed through the identification of exchangeable artefacts between the modellers and the stakeholders. At Company A, the thesis author brought in knowledge from economics of security and human factors, and the CISO was interested in understanding the impact of security on employees’ productivity, the artefacts were then trade-offs, costs, losses and gains related to security and the organisation. At the university, the exchangeable artefacts included, for example, organisational culture, policy, and security practices. As the co-design process continues — through the translation zone — the model construction evolves up to a point where all stakeholders (including the modellers) collectively agree that the model sufficiently and reasonably represents reality.
7.4 Bringing it all together

The previous section discussed the need for an interdisciplinary approach to address the complexity of designing security policies which accommodate user needs and their bounded decision-making. While an organisation has policies, which can be managed, there are also informal practices and norms which can be local and not necessarily written down. The ability to capture such informal practices and behaviours is very important in the aim to better inform policy decision-making. With our economics work in Chapter 3, we map out what the moving parts are in improving user-facing policies. Using constructs from both traditional and behavioural economics is a way to represent a system and how it interacts. The economics work highlights the necessary motivations for the modelling co-design methodology. The purpose is not to detail how to do an intervention, but rather detail how to design an intervention so that it has a higher chance of success. The economics framework indicates what should be taken into account during an intervention, but it also indicates who needs to be involved. By deconstructing the idea that employees are rational decision-makers, as per traditional economics, we highlight the elements to account for in the bounded decision-making process. Our framework aims to support non-expert employees to find and follow appropriate security behaviours. It also facilitates a way for the distant managers to relate to the local view of the employees — by using economics as a theoretical translation zone. However, while we use economics as one type of modelling for security, we recognise that it lacks the capacity to co-design. The CARE implementation model presented in Chapter 3 does not provide a sense of feasibility and co-design is critical for understanding the feasibility. This further motivates the need for a translation zone, where the artefacts of the organisation are critical to the translation zone.

The first study, presented in Chapter 4, took an exploratory approach towards identifying the link between security and organisational culture, while simultaneously exploring ways to actively collaborate with the stakeholders at Company A. Those observations complement our economics framework by providing an example of inadequate policy design which failed to consider the boundedly rational employee. The reflections from Company A were then utilised in Chapter 5, as a way of informing and further developing our understanding of modelling co-design. Our co-design approach for security modelling can help identify in advance the unexpected consequences of policy design as a way of managing decision-making risks and uncertainties. To that aim, we conduct our second study, presented in Chapter 6, at a large university, using our novel modelling methodology based on co-design principles and incorporating qualitative, user-centred research. Here, we implement the
methodology presented in Chapter 5 and instantiate the ‘translation zone’ with the stakeholder. Through a process of mutual learning with the stakeholder, we design a conceptual model of the security interactions at the university. The model represents how employees and IT and security support teams interact through policy, or lack thereof. The conceptual model helped produce a range of co-explored recommendations for improving security decisions, policy design, and communication in the organisation.

7.5 What are the success factors for co-design?

Beautement et al. demonstrate the value and importance of capturing data that represents a real-world environment and the workplace dynamics within that environment (2016). Conducting research, especially user studies, in a real-world setting can be challenging and time consuming. Data collection in organisations often requires the help of ‘hard to recruit’ groups — employees who are subjected to notable work pressures and time constraints. Recruiting participants who work in the field of security can be additionally challenging due to the strict requirements for confidentiality and a simultaneous expectation to report insecure behaviours or incidents. These expectations may deter employees from becoming participants in the first place, particularly in cases where the incentive for participation may be little.

These challenges are important to emphasise in co-design research such as the one presented in this dissertation, due to employees’ critical role in its success. Often, the inability to research one single organisation for long enough can disrupt the methodological flow and leave unaddressed gaps. The existing barriers in capturing data in a real-world context makes the effort to do so all the more valuable. The fulfilment of research studies in real organisations makes an important contribution to security research and broadens the understanding of behavioural and cultural aspects associated with security practices and policy.

In the study at Company A (Chapter 4), our co-design methodology for security modelling was in the early stages of development. The pre-study with the security managers was very valuable in that it provided a snapshot of the security practices at Company A, and it identified several sources of friction. The case study shed light on a unique culture, where the policies and security measures were taken too far as Company A was operating with an organisational model from the past, rather than a current one. Working with Company A also gave us an understanding of what it was like to work with a stakeholder from the very beginning of a study, and co-design the aims and questions together. However, due to unexpected changes at Company A, mostly related to the organisational structure, our co-design journey
was unable to continue as planned. After the completion of the first interview round, the intended larger-scale study which aimed to explore the perspective of non-security employees was not feasible. This left us with a conceptual candidate model of the security culture at Company A.

The university study (Chapter 6) was a second opportunity to implement our co-design methodology. But, challenges with data collection and recruitment of participants were increasingly present. In addition to the above-mentioned challenges, the pandemic with all its difficulties, caused major disruption to employees’ ways of working. This severely delayed administrative research processes and further challenged the feasibility of face-to-face interviews and participants’ motivation to partake. However, what gave continuity to our co-design process was the continuous communication with the stakeholder (security decision-maker) and the strong goal alignment which had been established in the beginning. Although the decision-maker had clear concerns about the security practices at the university, and had an assumption about what the contributory factors to the issue could be, they lacked oversight and evidence about what was actually happening. With our knowledge, as exchangeable artefacts, through the translation zone, the decision-maker was able to speculate about what was already in his ‘model’. The initial candidate models, both ours, and the stakeholder’s, were a first attempt at identifying the relevant entities, attributes and relationships, which at that stage may have been lacking or incorrect. The purpose of the translation zone is to ultimately produce a refined version of the model which the stakeholders and modellers collectively agree upon as being a reasonable representation of reality. The translation zone represents an evolution of the candidate models and the relationships within them. The final conceptual model is used to represent what was translated between us and the decision-maker.

So, what are the success factors for co-design? Reflecting on these two studies and the challenges that accompanied them highlight important success factors for the co-design process. Chapter 5 identified several modelling challenges — those of modelling in general, and those of modelling behavioural and cultural aspects of security in particular. These challenges, alongside the lessons learned from the studies, serve as a guide for implementing the modelling co-design methodology successfully.

Some of the main modelling challenges occur before the model construction. Those include collecting data prior to selecting the modelling approach, conducting large-scale data collection without identifying the purpose of the model, and failing to communicate with the relevant stakeholders when defining the problem to be modelled, to name a few. Determining the modelling approach and data collec-
tion requirements has implications for the entire modelling co-design process. It is therefore important to truly explore which modelling approach is the adequate one for a particular problem, rather than select methods and data out of convenience. There is an abundance of modelling tools and methods available, but not all will be suitable for addressing specific problems. Caulfield, Ilau and Pym categorise models and their interactions into three types: mathematical, executable, and conceptual (2022b). In this dissertation, we have predominantly focused on conceptual models, which can be expressed through rigorous natural language, pictures, and/or diagrams. The purpose of conceptual models is to describe the components and relationships of a system. It is also common to combine different types of models, especially in interdisciplinary work (Caulfield, Ilau and Pym 2022b). For example, if the research at Company A had continued, it would have been appropriate to combine the conceptual model of the security culture in the organisation and an economic model representing the trade-offs between security and productivity. A similar combination of models was done in Beautement, Sasse and Wonham’s ‘compliance budget’ (2009). For the university study, it was appropriate to keep the model conceptual, as it was the suitable model to facilitate the translation zone.

The careful consideration of data collection requirements and the modelling approach is one of the critical success factors for co-design. It would go against the principles of co-design to simply choose methods that the modellers are already familiar with, or utilise data which is readily available. In addition, the involvement of stakeholders as early as the problem identification stage is one of the core principles of our co-design methodology. It is also helpful to draw parallels with similar collaborative work in the field of security and critical success factors identified there. Security convergence (Anderson 2007), for example, refers to the convergence of two traditionally distinct security areas — physical security and information security — where both are integral for managing risk in organisations. Convergence is not the same as co-design in that it aims to integrate two distinct security fields permanently, whereas co-design aims to engage modellers and system stakeholders from other fields to work cooperatively through a process of mutual learning. However, they share important similarities, such as finding a commonality between two different security fields and the experts in those fields. Additionally, co-design and convergence share important similarities in the factors that are critical to their success, adapted from Boakes 2021:

- **A key person has a vision for convergence/co-design:** As it has been demonstrated in both studies, the co-design process starts when both a security stakeholder who is key to the management of security in an organisation, as well as a researcher or a modeller, have a shared interest in a security issue
that needs further exploration.

- **Senior management advocate for a converged/co-designed approach:** A continuous advocate for a co-designed approach is crucial for the continuation of the process, especially if the support comes from senior management with a decision-making function. The study at Company A showed that a senior management advocate was required for the continuation of the co-design, as was then showed by the university study.

- **Steps are made to engage with stakeholders:** For research or a model to be truly co-designed, engagement with stakeholders is paramount. This principle is at the core of our co-design approach, and an adequate facilitation of the stakeholder engagement is critical for the success of the methodology. Both studies showcased this element of co-design, where engaging with several stakeholders, primarily the CISOs, as well as other groups of employees (security managers, IT and security support, administrative staff, etc.) was one of the constants in our iterative process.

- **Converged/co-designed security aligns with the business:** Security research has established that a misalignment between security requirements and business expectations can cause friction in the organisation (Kirlappos and Sasse 2014; Rothrock, Kaplan and Van Der Oord 2018) — as was also shown with Company A. A similar principle applies to co-design, where the process might break down if the objectives of the study do not align with those of the stakeholder, as well as the priorities and strategy of the organisation. Often research studies offer recommendations for practitioners which are simply not feasible due to different types of constraints. There is no value in identifying security problems if there is no capacity to find solutions for those problems. Thus, aligning the objectives early on, both with the stakeholder and the business is critical for the success of co-design.

Looking back at the methodological reflections from Company A (co-creating objectives, involvement in research, building relationships and mutual learning — summarised in Section 5.6.4), they are aligned with the critical success factors listed above. Co-design is an iterative process which learns and improves with each iteration. Such a reflective approach has contributed to our current understanding, definition, and application of co-design which in turn aims to arrive to more accurate and accessible findings.
7.6 Reflecting on the findings and their value for future security research

It has been 23 years since Adams and Sasse argued against the view that ‘humans are the weakest link’ (1999). They highlighted that understanding users and considering their primary task will lead to more effective security rather than simply blaming them (Adams and Sasse 1999). The body of work and research community in human-centred security has since grown immensely, and there have been significant contributions to the field. However, when researching security in organisations, the need to get back to the basics — and articulate why users are not the enemy — is often still there.

7.6.1 Users ‘vs.’ managers

Reinfelder, Landwirth and Benenson report that security managers are well aware of the need to consider users when developing security measures, but user’s goals and daily workload are not formally considered when designing measures (2019). Security managers then feel frustrated — primarily due to their inability to account for usability in a structured manner, and secondly due to the lack of organisational support (Reinfelder, Landwirth and Benenson 2019). These results are in line with our findings at Company A, where the security managers were themselves concerned about the highly restrictive policies and security measures. Being under pressure to keep the organisation secure, and simultaneously distrustful of users and their behaviour, security managers often resort to implementing strict security and monitoring measures. This then leads to a vicious cycle of distrust, rigid measures imposed upon employees, and negative feedback on those measures (Reinfelder, Landwirth and Benenson 2019). A lack of trust towards employees was also present at Company A, where monitoring and fear-based approaches were common practice. Such approaches are likely to be counterproductive, as effective security requires trust and collaboration (Ashenden, Coles-Kemp and O’Hara 2018). In order to overcome the often observed ‘them’ vs. ‘us’ relationship, there is a need for reciprocal communication with employees and an acceptance that errors and mistakes will occur (Ashenden and Sasse 2013).

7.6.2 Communication

The first step towards building trust, and a culture of security, is open communication (Ashenden and Lawrence 2016). The findings from both studies highlighted,
7.6: Reflecting on the findings and their value for future security research

in various forms, the importance of communication when managing security in organisations.

7.6.2.1 Communication of security mandates

One main reason why the security managers at Company A were concerned about the current situation was due to the security division’s bad reputation. The frustrations that employees had because of security restrictions were all directed towards the security teams. This was predominantly due to lack of communication from the board of Company A, who were the actual advocates of such a restrictive security strategy. Communication is a key factor in ensuring that employees are aware of the security behaviours that are expected of them in the workplace (Beyer et al. 2015). Without communication from the board, employees at Company A found it hard to resonate with the policies and measures coming from the security division. Because of the perceived misalignment between the security and the business strategy, from the perspective of the employees, security was merely a barrier. Such perceptions occur when business and security goals are not aligned and introduce friction (Beautement, Sasse and Wonham 2009). In reality, the board considered security to be paramount, and was willing to compromise their risk appetite (the level of risk they were willing to accept) to avoid another breach — this was however not adequately communicated. Hence, the security mandates that were coming from the board, were uncommunicated, and perceived to be coming directly from the security department. Users are often collateral damage of insufficient or inadequate communication within organisations, not only when there is a lack of communication with them, but also when other groups of people fail to communicate between each other. The university study showed that the lack of communication between different IT and security support teams tended to impact users negatively. For example, local support staff were sometimes kept out of the loop when new policies were mandated centrally. As a result, local support staff would not be adequately prepared to support users upon requests related to new policies. In addition, there was a poor level of knowledge sharing between these teams, which once again affects users indirectly. One local administrator pointed out that there has been a recent improvement in the communication between central and local support, and that getting information about new developments beforehand improves their subsequent service to the users.
7.6.2.2 Communication of security context

Another thing which was not communicated to the employees of Company A was the context behind all the security measures. Although older employees recognised that the breach was the reason behind the security measures, this was not immediately evident to newer employees. Adams and Sasse point out that insufficient communication with employees can ‘cause them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate’ (1999, p.43). Having to comply with such strict security measures which often impede their work, without knowing the context as to why these measures are in place, is ineffective. Adequate communication should aim to change employees’ perception of security as something that is crucial to the business (Kirlappos and Sasse 2014). A positive example of communication and context-giving emerged from the university study, where the majority of study participants, who were university employees, were very aware of the importance of complying with GDPR. The employees attributed their awareness and knowledge of GDPR to the fact that it was communicated from all directions (both centrally and locally), and its clear relevance to their everyday tasks.

7.6.2.3 Communication of policy

Communication is an important part of the security policy lifecycle (Howard 2019; Paananen, Lapke and Siponen 2020). In fact, a security policy can in itself — as a collection of documented statements — be considered a communicative object (Karlsson, Hedström and Goldkuhl 2017). However, employees at organisations do not always receive sufficient communication in relation to security policies. The university study showed that the overwhelming majority of participants were not explicitly aware of a security policy. In other words, they were not aware of the policy document. From the interviews with administrative staff, we observe that it is the policy apparatus that drives secure behaviours, not the policy document itself. Participants were not necessarily unaware about the secure behaviours that they needed to adopt, but rather the source of those prescribed behaviours. They remembered what had been communicated to them about security by actual people — a colleague or their manager — but could not recall reading an actual policy. This highlights the importance and impact of personal communication on secure behaviours. Similarly, when new policies were launched at Company A, it was not the document itself which was the most important element — but the questions from employees that followed. Employees needed to communicate with security employees to properly understand the policy changes. Ultimately, the effectiveness
7.6: Reflecting on the findings and their value for future security research

of the security policy relies on how it is communicated to the users, rather than the content within it (Höhne and Eloff 2002), and policy communication should be therefore prioritised (Da Veiga 2016).

7.6.3 Centralised vs. decentralised

The ways in which communication is facilitated can vary depending on the organisational structure. The same applies to security communication. Company A and the university each represent a different security structure — the former being centralised, and the latter decentralised. Company A had one central security department which was responsible for the entire company. On the other hand, in addition to the central security function, the university had local or departmental IT teams covering a wide range of support, including security. There were significant differences between the local and central function, in the nature of communication and relationship with their users. It has been widely studied how people seek and receive help with technological issues in an organisational setting (Poole et al. 2009), and research has shown that people tend to seek help from familiar coworkers, local experts, or ‘gurus’, making technical help-seeking a highly social activity (Ackerman and McDonald 1996; Ackerman 1998; Allen 1977; Bobrow and Whalen 2002; Lang, Auld and Lang 1982; Lee 1986; Mackay 1990; Orr 2016). Our work shows that this is also the case when it comes to seeking security help.

A common observation from both studies was that the central IT and security functions were either invisible, or had a bad reputation. At Company A, security were seen as the blockers of productivity, whereas at the university, employees avoided getting in touch with the central help-desk. Interestingly, participants were not very much aware of the central security function, as many day-to-day security queries were being handled either by local support or the central help-desk. One phenomenon which was consistent in both interview rounds at the university was the relationship between the employees and their local support staff. Employees said they were much more keen to seek help from their local team because they are friendly, local, and quick. The interviews with local support staff confirmed that employees were more likely to approach them because they had an opportunity to build a relationship with them. Unless there was a query with which only central help-desk could assist, employees generally tried to avoid contacting them. They did not feel comfortable sharing their concerns with ‘strangers’ who had no understanding of their history. A lack of interaction between security practitioners and staff often leads to a lack of trust on both sides without which staff fail to engage with security issues or even actively avoid them (Ashenden and Lawrence 2016).
According to local support staff, employees may often feel embarrassed about asking ‘stupid questions’ — that being part of the reason for interacting with local support and getting judgement-free assistance. While central help-desk took a more formal approach and often referred employees to written guidance, local support staff provided them with in-person guidance and assurance. Going back to the concept of bounded rationality and employees’ limited understanding of security, there should not be an expectation for non-experts to interpret whether something has been done correctly. The need for practical assistance, in-person guidance, and assurance, sheds light on the boundedly rational employees and the effectiveness of local support staff accounting for their security limitations and needs — and responding to them adequately.

The role of top management is critical in championing the importance of security (Hu et al. 2012), while the role of local managers and staff is critical in implementing secure behaviour (Kirlappos and Sasse 2014). The study at Company A showed the negative consequences of having invisible security mandates coming from top management. On the other hand, the university study showed the positive interaction that can come from having engaged local support. Local managers, regardless of whether or not they are security experts, should be encouraged to shape an organisation’s security provisioning due to their considerable influence on their staff’s security decisions (Kirlappos, Parkin and Sasse 2014).

7.6.4 Security (of) culture

As discussed in previous sections, people’s security behaviours and practices are not directly guided by a policy document. They are mostly influenced by social interactions with others (Weirich and Sasse 2001; Furnell and Rajendran 2012; Dang-Pham, Pittayachawan and Bruno 2017) — both professional and personal. In addition to the influence from local support staff, both studies show that employees are influenced or guided by the behaviours of others — co-workers or managers. Das et al. found that half of all reported security behaviour changes were attributed to social interactions with others, where social triggers included observation of others, sharing access, and receiving advice from others (2014). These findings are alike those from the university study, where participants reported that they tend to observe and learn from the behaviours of their co-workers or managers. For example, one participant reported that they started using their pedestal for storing work documents and locking it after having observed that particular behaviour from a colleague. In this instance, imitating a colleague’s behaviour resulted in adopting a secure behaviour, which is not necessarily always the case. At Company A, employees were
7.6: Reflecting on the findings and their value for future security research

prone to circumvent security policies as a result of observing the non-compliance of others, highlighting the issue of negative influence.

Flechais, Riegelsberger and Sasse describe the concept of ‘social embeddedness’, which refers to new employees trying to fit in and mimicking the behaviours of others (2005). Once again, if the social environment is compliant, the new employees trying to fit it will also likely mimic compliance. Here we can refer back to our analysis in Chapter 3, Section 3.4.2, where we discuss the relevance of herding and information cascades in security decision-making. Security-related decisions can be influenced by herd mentality in situations of uncertainty (Vedadi and Warkentin 2020), which is often the case when it comes to security. Herding differs from social influence — while social influence originates from a group of known people — herding is based on popularity information which usually comes from strangers (Vedadi and Warkentin 2020). To put it in another way, herding may occur when new employees join and mimic the behaviours of others, whereas social influence is more likely to occur between existing coworkers. Das, Dabbish and Hong found that participants were four times more likely to share their own security behaviours with others when their behaviours were also reported to be socially triggered (2019b), which further emphasises the role of both herding and social influence in organisational security.

So, what is security culture? While security (of) culture is a complex phenomenon, it may most easily be summed up with Schein’s description of organisational culture, which is the way we do [security] around here (Schein 2010). An organisation’s culture consolidates employees’ responses to uncertainty through a system of shared beliefs and actions (Vasu, Stewart and Garson 2017). Security culture characterises what is socially acceptable or unacceptable — a dynamic set of security behaviours perpetuated by new employees joining the organisation. Understanding the role of security in organisational culture is a critical step towards identifying insecure behaviours and addressing them accordingly. Representing security culture accurately and in a useful manner is challenging due to its complexity (Dignum and Dignum 2014).

Chapter 5 identified several of those challenges and introduced our modelling co-design methodology as a way of addressing them. The exploration of cultural components in the real world provided a much better understanding of the role of culture in organisational security. Our continuous interaction with stakeholders in the translation zone led to an in-depth understanding of the organisational ecosystems. With the aim of representing cultural and behavioural aspects of security in a more tangible manner, a conceptual model was produced, representing the moving parts of security culture at the university.
The findings presented in this thesis were facilitated by our rigorous methodology of modelling co-design. We contend that the value of the findings is enhanced because of the methodology used to produce them — because it ensures that not only is the process of constructing the models a rigorous one — but also the representation of the domain to which the model is applied is robust.
Conclusions

Organisations are acknowledging the importance of human factors in the management of secure workplaces now more than ever. In increasingly complex and dynamic environments, it is difficult to predict potential outcomes of security policies. In addition, there are challenges in managing security infrastructures in which there may be centrally-mandated and locally-managed initiatives to promote secure behaviours. Security managers and other stakeholders are often challenged with designing and implementing security policies without knowing the consequences they may have for the organisation. While it has been established that developing a positive security culture can improve compliance with security policy, there is still insufficient practical guidance about how security culture should be approached by managers (Nasir et al. 2019). This thesis addresses a research gap related to the difficulty of studying and modelling cultural and behavioural aspects of security in a real-world context, and of producing meaningful guidance in that area for organisational stakeholders. It does so by taking an exploratory approach and addressing the following, open-ended, research questions:

*How does the role of security align with organisational culture, and how can we enhance our understanding and mapping of this relationship in a manner that is practical for practitioners and decision-makers? How can we establish a connection between security and other areas of the organisation, effectively bridging the gap and promoting an aligned and integrated approach?*
8: Conclusions

8.1 Overview of findings

The conceptual framework based on consolidated economics principles, identifies several considerations for decision-making in organisational security:

- the importance of capturing where an employee is, alongside where the organisation, or the policy-maker wants them to be;
- that a security choice architecture is essentially decentralised and cannot be wholly dictated by any one stakeholder;
- that, in organisations, security expertise can exist in places recognised by the organisation and also in places that are not; and
- that information asymmetries — for example, as constructed by information security teams — ought to be accounted for when assessing user behaviours.

The constructed framework can be used to improve the process of providing a set of advocated security behaviours. This is more doable for employees who work under conditions of uncertainty and workplace constraints.

The study with Company A shows that employees perceived security as a barrier to their work, some of whom also felt that they were being constantly monitored and treated as the ‘enemy’. Post-breach security changes should not merely aim to rapidly ‘increase security’, they should instead consider the long-term impact on the organisational culture and how those changes will interact with the effectiveness of proposed policies. One of the main causes of friction that the study identifies is the lack of effective communication around security. At Company A, the board saw security as high priority, but mainly communicated this to the security division and not other employees, who then became frustrated when their primary tasks — their paid jobs — were interrupted or blocked by the security controls. Without an approach considerate of how humans and security interact, even with high investment, attempts to change security behaviours within the organisation may be ineffective.

The proposed co-design methodology integrates the concept of co-design into the classical modelling cycle and provides a rigorous methodology for the construction of models, that captures the system and its behaviours accurately. This co-design approach aims to tackle the challenges of problem definition, data availability, and data collection associated with modelling behavioural and cultural aspects of security. It does so by capturing the system’s managers’ questions adequately, in such a way that the required supporting data can be collected, and the managers and modellers can cooperate in the construction of the model. Co-designing a security model in such a way focuses on more accurate and practical representation of behavioural and cultural aspects of security, which can help security managers with their policy decisions.
As a result of applying the co-design methodology at the university, the study culminates in a conceptual model that details the security artefacts of the organisation and how people interact with them. The components of the conceptual model are the following: an in-depth understanding of the system; an understanding of the interaction between different stakeholders in the organisation; and knowledge of the organisational structure and policies intended to be applied to the system. The study finds that cultural and behavioural factors have the potential to impact security behaviours. For example, the positive relationship between employees and their local IT and security support encourage employees to take a more active role in security. This is due to the level of trust built between the two, which makes it easier for employees to ask for help and guidance. The study also finds that communication is key in several aspects of security and that employees often remember what was communicated to them, rather than seeing a policy. Finally, another interesting finding is the identification of factors influencing security behaviours in lieu of policy, which in the case of this study are: employees’ personal awareness, the behaviour of co-workers, manager initiatives, and guidance from local IT and security support.

8.2 Summary of contributions

The studies — as well as the conceptual and methodological work presented in this thesis make several contributions to security research and methodology. The thesis highlights, first and foremost, the importance of understanding the role of organisational culture in security behaviours and compliance with security policy. Additionally, the thesis emphasises the importance of co-design and stakeholder involvement when attempting to capture data in a real-world context.

The main contributions of this thesis are the following:

8.2.1 Empirical and analytical contributions

- We identify a common contradiction in how security interventions are currently approached in organisations. Chapter 3 shows how current approaches to security provisioning and infrastructure reflect expectations from traditional economics, even when concepts from behavioural economics are applied to encourage individuals to adopt specific security behaviours. That is to say, even though interventions are often based on methods from behavioural economics — such as nudging — the assumption remains that employees are rational as per the definition of rationality from traditional economics. We address this
contradiction by designing a framework which views employees as boundedly rational and aims to better support ‘good enough’ security-related decisions for individuals and groups within an organisation;

• We present a unique case study in Chapter 4 which depicts an understudied perspective — the reactions of an organisation after experiencing a breach as well as the effect of those reactions on the organisational culture. The study shows the opposite of what has long been advocated in security research and industry — that the main barrier in achieving security is the lack of financial and human resources. Although the latter may be a common barrier, this thesis shows that there are other factors causing friction in the management of security in organisations. These factors include the lack of effective communication and a consideration of the trade-offs between security and productivity;

• The findings from the studies contribute new dimensions to human-centred security. Both studies highlight the role of communication in several aspects of security, such as the importance of communicating the context behind security controls to employees, and the need for an increased focus on the communication of policies rather than their design. The university study shows the role that an organisational structure can play in the day-to-day management of security practices. The results surface that employees value the qualities of local support in understanding their contextual needs, but also in accommodating their uncertainty with security by providing assurance rather than guidance. These findings highlight the role of care in IT security (Kocksch et al. 2018) and new, informal dimensions to technical support (Poole et al. 2009), including constructive engagement with employees who have doubts about doing the right thing for security (Kirlappos, Beaument and Sasse 2013).

8.2.2 Methodological contributions

• This thesis identifies important challenges in the different stages of modelling, such as data collection and application of the model. In addition, it identifies particular challenges in attempting to capture and model behavioural and cultural aspects of security.

• To address these challenges, this thesis proposes a novel co-design approach for security modelling (Chapter 5). Model co-design is a process that engages modellers and system stakeholders cooperatively in all stages of modelling with the aims of aligning model objectives with the needs of the stakeholders, and designing a model that is feasible yet useful for the stakeholders. The methodology is based on rigorous modelling principles as well as a strong requirement
that the agreed upon model has to accurately reflect the understanding of all stakeholders, not merely the views and perceptions of the modellers. This methodology facilitates an opportunity to capture knowledge about the cultural and behavioural aspects of security in organisations more accurately, as well as represent those aspects more meaningfully:

- The work in this thesis has captured several ‘real-world’ accounts of security practices and cultural factors that may influence security in organisations. This has been done through engagement with different stakeholder groups within two organisations. The approach is underpinned by rigorous modelling principles (Spring, Moore and Pym 2017; Caulfield, Ilau and Pym 2022b, 2022a), while also incorporating a translation zone between researchers and security decision-makers. This serves to produce a multi-stakeholder view of the complex security management in organisations, by linking the study of employees and support staff to security managers.

8.3 Recommendations

Lessons learned during this thesis work surface important recommendations for both researchers and practitioners working in the field of security.

8.3.1 Recommendations for researchers

Collecting security data that represents real-world contexts and engaging with organisation stakeholders is challenging. Researchers are often in a difficult position when it comes to data collection and that sometimes means that data which is readily available must be used instead of bespoke data. Despite it being challenging, time consuming, and sometimes unsuccessful, this thesis shows the value of attempting to engage with real organisations and their employees. We find value in engaging with decision-makers responsible for the environments under study, to better understand their decision-making processes. Co-designing a study with stakeholders in an organisation provides an opportunity for mutually beneficial research objectives as well as contextually useful results. A richer picture of the relationship between security provisioning and organisational culture can be produced as a result of facilitating a multi-stakeholder view. Thus, the main recommendation for researchers is to focus on building relationships with various stakeholders in organisations. Although this may not always be the case, stakeholders are often willing to engage with researchers, especially if the research can help address an existing problem in the organisation, or help identify unknown issues. When attempting to
facilitate a collaboration, it is important to acknowledge the domain expertise of
the stakeholders and engage in a process of mutual learning. A common challenge
with such engagements is that the contact with an organisation often hinges on one
individual. To address this issue, it may be more useful to focus the research goal
on the greater benefit of the organisation in order to ensure sustainability.

8.3.2 Recommendations for practitioners

• Current approaches of managing security behaviours tend to imply that em-
employees have resources available to complete security training and comply with
policies, but in an organisation employees are busy with their paid job. To
avoid ‘decision fatigue’ and the ‘hassle factor’ (Beautement, Sasse and Won-
ham 2009; Anderson, McCusker and Pym 2016) of complying with security,
we must acknowledge that for the busy employee, doing security requires a
loss to something else. If for the organisation it is equally important that
the employee completes their primary tasks and invests time in security, the
employee needs help negotiating where that cost will be borne from. In other
words, the organisation should ensure that the employee is given the resources
to meet all — or balance between — security and non-security expectations.

• The security function in an organisation must assume that employees are (se-
curity) novices. It is important for employees to be made aware of the ‘cost’
of security compliance and exactly what the steps are. Otherwise, the busy
employee will be required to guess the duration of an unfamiliar behaviour,
and exactly what constitutes the behaviour in its entirety. The findings of
this thesis show that employees value assurance more than guidance. This
means that even in the presence of guidance, employees may need reassurance
that they are following the guidance correctly. In addition, explicitly relating
security guidance to regular work tasks contextualises security policies for em-
ployees and can make it easier for them to adopt certain security behaviours.

• Leveraging the impact local support have on employees may positively af-
fect compliance with security policy. The university interviews show that the
presence of a local IT & security person or team is perceived very positively.
Local support can build trust-based relationships with employees if they are at
a close proximity and interact with them continuously. In turn, employees feel
more comfortable seeking help from a familiar face or find it more practical to
receive face-to-face assistance from someone. The relationship between local
support and employees should be leveraged by encouraging support staff to
increasingly focus on security locally.
8.4 Limitations

The limitations of each study are described in their respective chapters. To summarise, the two interview studies explored the relationship between security provisioning and organisational culture in the context of two distinct organisations. The findings and insights from these studies might not be completely applicable or generalisable to other organisations or contexts. In the first case study, with Company A, the biggest shortcoming was the inability to continue the co-design process and reflect other stakeholder perspectives within the same organisation — such as that of the non-security employees.

Another factor that may have impacted the interviews is the topic of security itself. Participants were informed that anonymised interview findings could be communicated back to the security management decision-makers. This may have potentially acted as a barrier during the interviews, but participants were nonetheless open when communicating about existing security provisions. Support staff sharing positive experiences with helping employees with secure practices may have indicated signs of bias in praising their own work, but these experiences were supported with specific examples of positive engagements as well as potential issues.

Lastly, the co-design in this thesis was carried out with several ‘hard to recruit’ participant groups: (1) security managers at Company A, (2) administrative staff working across university departments, (3) IT and security support staff at the university, and (4) two security managers (the co-designers) responsible for the university’s information security strategy. All of these groups consisted of people managing or providing security services to others and had hectic working schedules. Therefore, the total participant number, as well as the duration of the interviews depended on their availability (a challenge noted in other studies with active professionals (Reinfelder, Landwirth and Benenson 2019)). The process was lengthy due to these factors — finding times when the participants were available — and relaying back to the ‘co-designer’ at the university who was also a ‘hard to recruit’ participant.
8.5 Future work

Informed by human-centred security research — and the work presented in this thesis — we outline directions for how a security function in an organisation can consider the approaches suggested in this thesis. A security function cannot be assumed to have in-depth knowledge of the human aspects of security, but may nonetheless value it in security policy decision-making (Parkin, Moorsel et al. 2010), and benefit from methods and tools to do so (Reinfelder, Landwirth and Benenson 2019).

8.5.1 A security diet

A ‘security diet’ would document perceived occurrence and costs of advocated behaviours (for example, through a regular working day). Questions can be asked to reconcile these costs with expected behaviours elsewhere in the organisation (Karls-son, Karlsson and Åström 2017), to determine if time for security tasks is being taken from elsewhere (e.g. primary tasks). If security behaviours add to an already busy schedule, then time constraints, pressure, and stress increase the likelihood of errors (Reason 1990). This is akin to the Compliance Budget (Beautement, Sasse and Wonham 2009; Anderson, McCusker and Pym 2016), which supposes that there is a limit to the effort an employee will commit to security before they choose not to comply (and crucially, beyond which the organisation needs to commit additional resources to encourage a return to compliance).

Ideally, security is progressively revisited and redesigned to be achieved as part of core business tasks, targeting the burden of identifying appropriate behaviours — this would begin to achieve something closer to ‘Productive Security’ (Beautement et al. 2016; Anderson, McCusker and Pym 2016). Security diets may be populated by talking to a representative sample of employees across different teams, for instance, or team managers (rather than all employees for large organisations). This can bring the organisation closer to collecting system-level data to complement the experiences and perceptions of employees.

An individual arguably should not be expected to commit more than their full working day to all tasks including security. As mentioned, critically, security mandates demand the very same qualities from employees that diminish when available resources are exceeded. Security is then self-defeating if it leaves the employee to figure out how to make this possible, as the effort involved in identifying and following behaviours can induce errors from already-burdened employees. Consideration of how to manage security with other pressures can reduce this ‘gulf of execution’ (Renaud and Goucher 2014).
8.5.2 Co-design with stakeholders

Several aspects of the proposed co-design methodology can be further studied. Generally, the methodology requires several applications to be able to determine whether any improvements or changes are necessary. Further applications in varying security contexts are also necessary to explore how generalisable the methodology is. Another avenue for future research — which has not been addressed in this thesis — is specifying exit criteria to determine when a sufficiently accurate model has been produced (Caulfield, Ilau and Pym 2022b). Finally, the identification of the translation zone is a process that should be further explored in cases where the gap in understanding between the researchers/modellers and the stakeholders is greater than anticipated.

8.5.3 Security modelling and investment forecasting

Given the complexity of security policy choices and all the factors impacting them, it is difficult to predict the consequences different policy choices may have on the security of a system. Models are helpful in predicting the implications of design decisions. System models are particularly suitable here as they can represent the behaviour, structure and environment of a system, as well as the behaviour of employees interacting with it (Caulfield, Baddeley and Pym 2016). Lessons from behavioural economics are useful for improving modelling of people’s decision making.

Conceptual models, such as the ones presented in this thesis are useful for representing entities, relationships and processes in organisations in a meaningful way. Additionally, security modelling can begin to forecast the impact of investments in complex environments, before making infrastructure and provisioning changes (Caulfield and Pym 2015a). Security deployed is not security as designed; contact with the complex organisational environment will alter how successful a control is in practice, and how well it fits with other practices in the organisation. Incorporating employee perspectives into structured economic models will inform the viability of new controls before their deployment.


Beris, Odette, Adam Beautement and M Angela Sasse. 2015. ‘Employee rule breakers, excuse makers and security champions:: Mapping the risk perceptions and emotions that drive security behaviors’. In Proceedings of the 2015 New Security Paradigms Workshop, 73–84. ACM.


Bibliography


———. 2020. ‘One size fits all? What counts as quality practice in (reflexive) thematic analysis?’ Qualitative research in psychology, 1–25.


———. 2015b. ‘Modelling and simulating systems security policy’. In SIMUTOOLS 2015-8th EAI International Conference on Simulation Tools and Techniques. ICST.


Da Veiga, Adéle. 2016. ‘Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study’. Information & Computer Security.


Grossklags, Jens, and Alessandro Acquisti. 2007. ‘When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information’. In WEIS.


Herley, Cormac, and Wolter Pieters. 2015. ‘”If you were attacked, you’d be sorry” Counterfactuals as security arguments’. In Proceedings of the 2015 New Security Paradigms Workshop, 112–123.


Kaur, Mannat, Simon Parkin, Marijn Janssen and Tobias Fiebig. 2022. ‘” I needed to solve their overwhelmness”: How system administration work was affected by COVID-19’. In 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing. ACM.


Kirlappos, Iacovos, Simon Parkin and M Angela Sasse. 2014. ‘Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security’.


Koppel, Ross, Sean W Smith, Jim Blythe and Vijay H Kothari. 2015. ‘Workarounds to computer access in healthcare organizations: you want my password or a dead patient?’ In ITCH, 215–220.


Lim, Joo S, Shanton Chang, Sean Maynard and Atif Ahmad. 2009. ‘Exploring the relationship between organizational culture and information security culture’. In Australian information security management conference, 12.

Lim, Joo Soon, Atif Ahmad, Shanton Chang and Sean B Maynard. 2010. ‘Embedding Information Security Culture Emerging Concerns and Challenges.’ In PACIS, 43.


Malcolmson, Jo. 2009. ‘What is security culture? Does it differ in content from general organisational culture?’ In 43rd Annual 2009 international Carnahan conference on security technology, 361–366. IEEE.


Bibliography


Pahnila, Seppo, Mikko Siponen and Adam Mahmood. 2007. ‘Employees’ behavior towards IS security policy compliance’. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07), 156b–156b. IEEE.


Bibliography


Wang, Serena, Cori Faklaris, Junchao Lin, Laura Dabbish and Jason I Hong. 2022. ‘It’s Problematic but I’m not Concerned: University Perspectives on Account Sharing’. CSCW 2022.


Williams, Patricia A. 2009. ‘What does security culture look like for small organizations?’


Glossary: Economics Terminology

The definitions were derived from: Friedman 2012; Mankiw and Taylor 2006; Bate-
man and McAdam 2003; Thaler and Sunstein 2008; Shafir 2013; Vohs et al. 2014;
Johnson et al. 2012; Kahneman and Tversky 2013; Keynes et al. 1930; Chamley
2004; Çelen and Kariv 2004; Baddeley 2010; Baddeley and Parkinson 2012; Badde-

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>gain</td>
<td>A gain is an increase in the value of an asset.</td>
</tr>
<tr>
<td>loss</td>
<td>A loss is a decrease in the value of an asset.</td>
</tr>
<tr>
<td>cost</td>
<td>A cost signifies the using up of assets.</td>
</tr>
<tr>
<td>investment</td>
<td>The allocation or use of goods with the expectation of some benefit in the future.</td>
</tr>
<tr>
<td>rationality</td>
<td>The idea that an individual takes into account all information, probability, potential costs, gains or losses in order to take the most optimal decision</td>
</tr>
<tr>
<td>decision</td>
<td>The choice that results in the optimal level of benefit for the decision-maker.</td>
</tr>
<tr>
<td>rational decision-making</td>
<td>The process of making a choice that results in the optimal level of benefit for the decision-maker.</td>
</tr>
<tr>
<td>information asymmetry</td>
<td>When one party has more or better information about something than the other party.</td>
</tr>
<tr>
<td>moral hazard</td>
<td>When an individual takes more risks because someone else is responsible for bearing those risks.</td>
</tr>
<tr>
<td>principal-agent problem</td>
<td>When one individual has the ability to make decisions on behalf of another.</td>
</tr>
</tbody>
</table>

Table A.1: Traditional and behavioural economics terminology — part 1.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>externality</td>
<td>A cost or benefit that is imposed on a third party who did not agree to incur that cost or benefit.</td>
</tr>
<tr>
<td>information cascade</td>
<td>When an infinite sequence of individuals ignore their private information when making a decision.</td>
</tr>
<tr>
<td>herding</td>
<td>When an infinite sequence of individuals make an identical decision, not necessarily ignoring their private information.</td>
</tr>
<tr>
<td>perceived gain</td>
<td>A perceived gain is an increase in the value of an asset that is important and subjective to the decision-maker (as according to limitations of bounded rationality).</td>
</tr>
<tr>
<td>perceived loss</td>
<td>A perceived loss is a decrease in the value of an asset that is important and subjective to the decision-maker (as according to limitations of bounded rationality).</td>
</tr>
<tr>
<td>perceived cost</td>
<td>A perceived cost signifies a subjective value of an asset as according to limitations of bounded rationality.</td>
</tr>
<tr>
<td>risk</td>
<td>The possibility or likelihood of losing something valuable.</td>
</tr>
<tr>
<td>loss aversion</td>
<td>The concept that people are far more psychologically affected by a loss rather than a gain.</td>
</tr>
<tr>
<td>bounded rationality</td>
<td>The idea that humans have certain constraints; cognitive, time, and information/knowledge; that limit their decision-making processes; as such, boundedly rational agents turn to ‘satisficing’ rather than ‘optimising’.</td>
</tr>
<tr>
<td>choice architecture</td>
<td>The practice of influencing an individual’s choice by organising the context in which they make decisions.</td>
</tr>
<tr>
<td>satisficing</td>
<td>The act of making a decision which is satisfying and sufficient (given the constraints) rather than optimal.</td>
</tr>
<tr>
<td>social learning</td>
<td>When a person’s beliefs, decisions, or behaviour are affected or altered by some form of social interaction.</td>
</tr>
<tr>
<td>decision fatigue</td>
<td>Fatigue caused by the difficulty and effort required to make a choice.</td>
</tr>
</tbody>
</table>

Table A.2: Traditional and behavioural economics terminology — part 2.
B.1 Interview questions:

*Questions used in interviews with security managers.*

**General — security processes:**
1. How does security make you feel?
2. What are your daily responsibilities?
3. If you were to change one thing in the company’s security, what would it be?
4. Do you think that change would be different if you were a non-security employee?

**Security culture:**
1. How would you define security culture?
2. What do you think is the relationship between security culture and organisational culture?
3. How do you think your current company interprets the term ‘security culture’?
4. If you could choose one word to describe the security culture of this company, what would it be?
5. Please describe where you last worked without providing any specific details of the company.
   a) What security approach did the company have?
   b) What was the security culture like?
   c) How does it compare to your current company’s security culture?
   d) What are the advantages and disadvantages of both cultures and why?
## B.2 Code-book:

<table>
<thead>
<tr>
<th>Code</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Post-shock security</strong></td>
<td></td>
</tr>
<tr>
<td>Security culture definition</td>
<td>11</td>
</tr>
<tr>
<td>Incident from the past</td>
<td>7</td>
</tr>
<tr>
<td>Insider threat</td>
<td>2</td>
</tr>
<tr>
<td>Maturity of security processes</td>
<td>2</td>
</tr>
<tr>
<td>Reluctance to change</td>
<td>2</td>
</tr>
<tr>
<td>Organisational culture</td>
<td>1</td>
</tr>
<tr>
<td><strong>Security theatre undermines policy</strong></td>
<td></td>
</tr>
<tr>
<td>Fear of security</td>
<td>7</td>
</tr>
<tr>
<td>Robust vs. compliance-based</td>
<td>5</td>
</tr>
<tr>
<td>Nothing happens if you break policy</td>
<td>4</td>
</tr>
<tr>
<td>What is the purpose of security policy</td>
<td>4</td>
</tr>
<tr>
<td>Copying behaviour</td>
<td>2</td>
</tr>
<tr>
<td>Culture means being compliant</td>
<td>1</td>
</tr>
<tr>
<td>Security theatre</td>
<td>1</td>
</tr>
<tr>
<td><strong>Security is like detention</strong></td>
<td></td>
</tr>
<tr>
<td>Security vs. employees</td>
<td>7</td>
</tr>
<tr>
<td>Lack of trust</td>
<td>3</td>
</tr>
<tr>
<td>Non-compliance with security</td>
<td>2</td>
</tr>
<tr>
<td>Trusting your employees</td>
<td>2</td>
</tr>
<tr>
<td><strong>Security is a blocker</strong></td>
<td></td>
</tr>
<tr>
<td>Less security more productivity</td>
<td>7</td>
</tr>
<tr>
<td>Security as a blocker</td>
<td>7</td>
</tr>
<tr>
<td>Security and the people</td>
<td>5</td>
</tr>
<tr>
<td>Bypassing security</td>
<td>2</td>
</tr>
<tr>
<td><strong>Lack of effective communication</strong></td>
<td></td>
</tr>
<tr>
<td>Hierarchical influence</td>
<td>7</td>
</tr>
<tr>
<td>Fast growth</td>
<td>4</td>
</tr>
<tr>
<td>Security is security’s job</td>
<td>2</td>
</tr>
<tr>
<td>Cultural split</td>
<td>2</td>
</tr>
<tr>
<td>Security culture doesn’t exist in a vacuum</td>
<td>1</td>
</tr>
<tr>
<td><strong>Zero risk appetite</strong></td>
<td></td>
</tr>
<tr>
<td>Risk appetite</td>
<td>12</td>
</tr>
<tr>
<td>Culture means serious security</td>
<td>2</td>
</tr>
</tbody>
</table>
### B.2: Code-book:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paranoia</td>
<td>2</td>
</tr>
<tr>
<td>Security posture</td>
<td>2</td>
</tr>
<tr>
<td><strong>Sensible security is likely to work</strong></td>
<td></td>
</tr>
<tr>
<td>What is good security culture</td>
<td>4</td>
</tr>
<tr>
<td>Sensible security is likely to work</td>
<td>3</td>
</tr>
<tr>
<td>Culture means everyone doing security</td>
<td>1</td>
</tr>
<tr>
<td>Non-security people doing security</td>
<td>1</td>
</tr>
<tr>
<td><strong>Behaviour change is required</strong></td>
<td></td>
</tr>
<tr>
<td>Unlearning behaviour</td>
<td>7</td>
</tr>
<tr>
<td>Training and education</td>
<td>4</td>
</tr>
<tr>
<td>Culture means working together</td>
<td>3</td>
</tr>
<tr>
<td>Change is good</td>
<td>1</td>
</tr>
</tbody>
</table>
C.1 Interview questions:

C.1.1 Administrative employees

*Questions used in interviews with administrative employees.*

**Introductory questions:**
1. What do you do here?
2. How long have you been working here?
   a) Have you worked anywhere else that compares (or not) in some way?
3. Can you describe your typical working day at the university?
4. Where does your way of working come from?
   a) The way things have been done?
   b) A policy you know about or have read?
   c) Security awareness/training you have done?
   d) What is it that makes a behaviour adoptable?
   e) What would have to happen outside of that behaviour that would help you learn it?

**Security practices:**
1. How does technology factor in your work?
   a) Does it help in any ways?
   b) Does it get in the way of your work in any ways?
2. How does security fit in to your day?
a) Are there particular tasks you do in your work which are related to information security? / how often?
b) Probe: Sensitive data/information, clear desk policy and sharing workspaces, physical security/tailgating, passwords, sharing data/USB sticks and sharing by emails, phishing.

Decision-making and policies:
1. Is there a security policy within the organisation?
   a) Is this a departmental one or university-wide? (for people not in central services)
2. How much would you say you know about the content?
3. What security training, if any, have you received to date?
4. Have you ever received any security communication?
5. How effective was it in your view?
6. What do you see as the pros and cons of security policies?
7. Do the rules you follow work well?
   a) If so, in what ways?
   b) If not, what do you think should change, and in what way?
8. How often do you think people generally follow the policy rules?
9. If you see people behaving securely – how do you feel about that?
   a) Good, bad, waste of time.
10. Is it clear from the policy what non-compliance is?
11. Does the policy say anything about reporting an incident?
12. How does the culture compare to health and safety and physical security?
13. What risks do you think failing to comply with security policy poses to the org?

Organisational culture:
(General probe: (if applicable) how does this compare to other places you have worked at?)
1. How would you describe the working culture around here?
   a) What is important in that culture?
   b) What is recognised and rewarded?
   c) Do you see staff here pushing themselves in any way to meet those expectations?
2. How do you usually do things around here? (further probe – do you do them as you’re told, as others do them, or in your own way?)
   a) Probe: Shared beliefs/values
C.1: Interview questions:

b) Probe: Shared norms (ways of doing things)

c) Who are these approaches shared with (certain colleagues, an entire team, the university)?

d) How are these approaches shared? (e-mail, conversation, etc.)

3. Could you talk through an example of the way you work with others to get things done?
   a) Do they need to be done this way for a reason?

4. (If previous answers indicate they are a ‘new’ employee) Can you give examples of behaviours you are expected to adopt in order to fit in?
   a) Do you adopt these behaviours and why?

C.1.2 IT and security support

Questions used in interviews with IT and security support.

Contextual questions:
1. How long have you worked here?
2. Could you describe an hour of your working day? (focus: processes, way of working, routines)
3. How many people are there in your division/department? (e.g., central help-desk vs. security help-desk)
4. How many people are there in your team?

Ticketing system:
1. How many users do you have?
2. How are tickets assigned?
3. What are the different ways people can contact you with a query? (e.g., phone, e-mail, online form/another tool, dropping in, etc.)
4. Which is the most common way to submit a query/ticket?
5. Are all queries logged as tickets?
   a) If not (or if queries are logged informally), why/when does that happen?
6. Do users rank tickets by severity? (e.g., urgent, medium)
   a) If not, how are tickets prioritised?

Security tickets:
1. How much of the tickets that you get are security tickets?
2. What kind of security tickets do you get?
3. How many security tickets per day do you/your team receive on average?
4. How many security tickets per day do you solve on average?
5. How long does it take on average to resolve a security ticket?
6. Do you get certain security queries more than others?
   a) If yes, which are the 3-5 most common?
7. Do you often get security queries that are meant for another team/department?
   a) If yes, what is the process of handling such queries? (e.g., reject, help anyway, delegate, reject & redirect)
   b) Are there certain queries that you get by mistake more frequently? Why do you think that is?
8. Are security tickets prioritised over non-security tickets by default?
9. Do you ever notice an unusually low number of tickets?
   a) If yes, do you follow-up on that?
10. Do you feel that you ever have time to proactively support people? (i.e., without them having to log tickets)
11. Based on the things you just said, how would it affect your work if any of them went up or down?

Security behaviours:
1. Do you have any sense of what happens before people decide to contact you regarding a query?
2. Do you think they first attempt to solve it themselves?
3. Do you think they try to find help/guidance on your website?
4. Do you think they ask someone in their team before coming to you?
5. How frequently do people log issues that there is already guidance for?
6. Do you think...
   a) There are queries that would be trivial to solve if people have access to the right information?
   b) That there is guidance available, but they cannot find it?
   c) That there is guidance available, but they cannot understand it?
   d) That there is guidance available, they are able to resolve the issue, but prefer assistance?
7. Are there queries that would be trivial to solve but for which there is no available guidance?
8. How would it affect your work if they were able to find the guidance?
9. How often do people come back with the same problem? (e.g., a ticket that has already been resolved)
10. What would you say a ‘good’ number of queries/tickets would look like?
11. On a percentage scale, how secure would you say most behaviours are?
C.1: Interview questions:

12. Are there certain behaviours which are followed in a more/less secure way than others?
13. Do people ever log a ticket to seek advice (about how to do something securely) rather than to resolve a particular issue?
14. Do people ever log a security problem after it has broken their computer and they are terrified?

Remote working:

1. What has changed the most about your way of working since ‘lockdown’?
2. Do people come to you as much as before the ‘lockdown’?
3. With the new policy, have you seen people come to you with questions?

Additional group specific questions:

Central support staff:

(after remote working questions)
1. How was the policy launched and communicated to people?
2. Do you think it’s useful to have local IT teams/person?
   a) Why yes/no?
3. Have you noticed any key differences between departments that have vs. departments that do not have a local IT team/person?

Security support staff:

1. Are there any queries that can only be solved by the security help-desk?
2. Do you think people fully understand when they should explicitly come to you?

Local IT:

(after remote working questions)
1. Were you already guiding people on that?
2. Did you notice people coming to you more when the e-mail was sent out?
3. Have you noticed a lot of people having the same questions about it?
4. When a new policy is introduced, do you get a sense that it takes time to adapt to new practices?
5. Do you feel that people in the department trust you and feel comfortable coming to you with queries?
6. If yes, why do you think that is?
7. Do you think they prefer coming to you vs. central help-desk and why?
8. What fraction of queries are you able to solve without escalating to central IT?
9. What type of queries are most likely to be escalated to central IT and why?
10. Is there a local system of tracking queries?
11. What is the local culture like in terms of people asking for help?
12. Do you think that people ask each other what to do before calling someone?
13. Have you noticed specific groups that behave differently in this respect? (e.g., managers vs. other employees)

C.2 Code-book:

C.2.1 Administrative staff

The code-book consists of 73 unique codes. Some codes are repeated due to their applicability to several themes.

<table>
<thead>
<tr>
<th>Code</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviour is not guided by policy directly</td>
<td></td>
</tr>
<tr>
<td>Security policy</td>
<td>70</td>
</tr>
<tr>
<td>Security perceptions</td>
<td>70</td>
</tr>
<tr>
<td>Security behaviours</td>
<td>37</td>
</tr>
<tr>
<td>Asking colleagues/manager for IT or security help</td>
<td>30</td>
</tr>
<tr>
<td>Security risks</td>
<td>28</td>
</tr>
<tr>
<td>Security conversations</td>
<td>21</td>
</tr>
<tr>
<td>Learned behaviours</td>
<td>20</td>
</tr>
<tr>
<td>Prior experience with security</td>
<td>19</td>
</tr>
<tr>
<td>Expected behaviours</td>
<td>17</td>
</tr>
<tr>
<td>Shared values</td>
<td>8</td>
</tr>
<tr>
<td>Communication during lockdown</td>
<td>8</td>
</tr>
<tr>
<td>Toxic culture</td>
<td>8</td>
</tr>
<tr>
<td>Self-help</td>
<td>7</td>
</tr>
<tr>
<td>Security decision process</td>
<td>7</td>
</tr>
<tr>
<td>Trust uni to be secure</td>
<td>6</td>
</tr>
<tr>
<td>Culture is about freedom</td>
<td>6</td>
</tr>
<tr>
<td>Culture is about professionalism</td>
<td>4</td>
</tr>
<tr>
<td>Culture is about respect</td>
<td>4</td>
</tr>
<tr>
<td>Culture is about responsibility</td>
<td>3</td>
</tr>
<tr>
<td>Policy workarounds general</td>
<td>3</td>
</tr>
</tbody>
</table>
### Code-book:

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy workarounds other workplace</td>
<td>3</td>
</tr>
<tr>
<td>Culture mental model</td>
<td>2</td>
</tr>
<tr>
<td>Shadow security</td>
<td>1</td>
</tr>
<tr>
<td><strong>Central mandates, made actionable locally</strong></td>
<td></td>
</tr>
<tr>
<td>Security culture</td>
<td>45</td>
</tr>
<tr>
<td>Culture</td>
<td>31</td>
</tr>
<tr>
<td>Technology</td>
<td>23</td>
</tr>
<tr>
<td>Asking colleague or manager for help</td>
<td>17</td>
</tr>
<tr>
<td>Technology barriers</td>
<td>12</td>
</tr>
<tr>
<td>Adapting to change</td>
<td>11</td>
</tr>
<tr>
<td>Culture is about flexibility</td>
<td>11</td>
</tr>
<tr>
<td>Procedure for phishing</td>
<td>11</td>
</tr>
<tr>
<td>Organisational structure</td>
<td>9</td>
</tr>
<tr>
<td>Resistance to change/technology</td>
<td>9</td>
</tr>
<tr>
<td>Uni systems issues</td>
<td>9</td>
</tr>
<tr>
<td>Technology enablers</td>
<td>8</td>
</tr>
<tr>
<td>Reward and recognition</td>
<td>6</td>
</tr>
<tr>
<td>Uni systems</td>
<td>6</td>
</tr>
<tr>
<td>Uncertainty during pandemic</td>
<td>4</td>
</tr>
<tr>
<td>Description of culture</td>
<td>3</td>
</tr>
<tr>
<td>Technology perceptions</td>
<td>2</td>
</tr>
<tr>
<td><strong>Personal relationships with IT and security support build trust</strong></td>
<td></td>
</tr>
<tr>
<td>Security communication</td>
<td>49</td>
</tr>
<tr>
<td>Interaction with IT support</td>
<td>34</td>
</tr>
<tr>
<td>Interaction local vs. central support</td>
<td>25</td>
</tr>
<tr>
<td>Interaction with local IT support</td>
<td>23</td>
</tr>
<tr>
<td>Interaction with central help-desk</td>
<td>20</td>
</tr>
<tr>
<td>Culture is about communication</td>
<td>13</td>
</tr>
<tr>
<td>Interaction with security group</td>
<td>13</td>
</tr>
<tr>
<td>Culture is about support</td>
<td>12</td>
</tr>
<tr>
<td>Communication during lockdown</td>
<td>8</td>
</tr>
<tr>
<td>Interaction with campus security</td>
<td>6</td>
</tr>
<tr>
<td>Lack of IT knowledge</td>
<td>3</td>
</tr>
<tr>
<td>Covid implications</td>
<td>3</td>
</tr>
<tr>
<td>Culture is about appreciation</td>
<td>2</td>
</tr>
<tr>
<td><strong>Relating security to every day tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Security policy</td>
<td>70</td>
</tr>
</tbody>
</table>
C: University Study

Individual working 26
Working together 22
Disruption caused by security 20
Policy suggestion 14
Cons of security policy 10
Security way of working 9
Security and safety policy 8
Security procedure 8
Pros of security policy 7
Way of working 5
Lack of time for security 5
Communicating via technology 4
Disruptions during work 4

Impact of GDPR on security awareness

<table>
<thead>
<tr>
<th>Code</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policy</td>
<td>70</td>
</tr>
<tr>
<td>Security culture</td>
<td>45</td>
</tr>
<tr>
<td>Security training</td>
<td>34</td>
</tr>
<tr>
<td>Security risks</td>
<td>28</td>
</tr>
<tr>
<td>Induction/Training</td>
<td>27</td>
</tr>
<tr>
<td>Data protection</td>
<td>19</td>
</tr>
<tr>
<td>Relation to everyday tasks</td>
<td>15</td>
</tr>
<tr>
<td>Positive security example</td>
<td>11</td>
</tr>
<tr>
<td>GDPR training</td>
<td>11</td>
</tr>
<tr>
<td>GDPR impact on security awareness</td>
<td>7</td>
</tr>
<tr>
<td>Procedure for data breach</td>
<td>4</td>
</tr>
</tbody>
</table>

C.2.2 IT and security support

The code-book consists of 56 unique codes in total, and 37 unique codes within the scope of this thesis. Some codes are repeated due to their applicability to several themes. The codes that are located under the ‘Other’ category do not directly map to the themes presented in the thesis but are included for transparency.

<table>
<thead>
<tr>
<th>Code</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local support teams build relationships</td>
<td></td>
</tr>
<tr>
<td>Covid implications</td>
<td>28</td>
</tr>
<tr>
<td>Local support vs. central</td>
<td>19</td>
</tr>
<tr>
<td>Proactive support</td>
<td>12</td>
</tr>
<tr>
<td>Code-book</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>Impact if ticket numbers changed</td>
<td>11</td>
</tr>
<tr>
<td>Trust</td>
<td>10</td>
</tr>
<tr>
<td>Central help-desk interaction with local IT support</td>
<td>8</td>
</tr>
<tr>
<td>Local support physical interaction with users</td>
<td>6</td>
</tr>
<tr>
<td>Organisational changes</td>
<td>3</td>
</tr>
<tr>
<td>Way of working</td>
<td>3</td>
</tr>
<tr>
<td>IT Culture</td>
<td>3</td>
</tr>
<tr>
<td>Local IT support vs. security group</td>
<td>2</td>
</tr>
<tr>
<td>Mundane tickets</td>
<td>2</td>
</tr>
<tr>
<td>Collaboration between IT teams</td>
<td>2</td>
</tr>
<tr>
<td>Central help-desk physical interaction with users</td>
<td>2</td>
</tr>
</tbody>
</table>

**Giving assurance rather than guidance**

| Queries and guidance | 41 |
| Security of behaviours | 25 |
| Users behaviours | 21 |
| Remote working policy | 15 |
| Repeat tickets | 13 |
| Users panicking | 13 |
| Most common security tickets | 12 |
| Users seeking security advice | 8 |
| Improvement suggestions | 2 |

**Asking for security advice is common**

| Queries and guidance | 41 |
| Local support redirecting tickets | 16 |
| Remote working policy | 15 |
| Security group redirecting tickets | 13 |
| Types of security tickets | 12 |
| Formal vs. informal queries | 12 |
| Users seeking security advice | 8 |
| Central help-desk redirecting tickets | 6 |
| Security group physical interaction with users | 6 |
| Knowing who to contact | 4 |

**Security of behaviours varies between individuals and groups**

<p>| Security of behaviours | 25 |
| Users behaviours | 21 |
| Ways to log a ticket | 14 |
| Culture | 11 |</p>
<table>
<thead>
<tr>
<th>Issue</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perception of security tickets</td>
<td>8</td>
</tr>
<tr>
<td>Resistance to change</td>
<td>5</td>
</tr>
<tr>
<td>User awareness</td>
<td>3</td>
</tr>
<tr>
<td>Data protection</td>
<td>3</td>
</tr>
<tr>
<td>Why are tickets logged incorrectly</td>
<td>3</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
</tr>
<tr>
<td>Prioritising tickets</td>
<td>20</td>
</tr>
<tr>
<td>Team size</td>
<td>13</td>
</tr>
<tr>
<td>Process of assigning tickets</td>
<td>12</td>
</tr>
<tr>
<td>Low number of tickets</td>
<td>11</td>
</tr>
<tr>
<td>Number of users</td>
<td>10</td>
</tr>
<tr>
<td>Ranking by severity</td>
<td>10</td>
</tr>
<tr>
<td>Good number of tickets</td>
<td>9</td>
</tr>
<tr>
<td>Portion of security tickets</td>
<td>6</td>
</tr>
<tr>
<td><strong>Central help-desk</strong></td>
<td></td>
</tr>
<tr>
<td>Average security tickets per day</td>
<td>4</td>
</tr>
<tr>
<td>Average time to solve security tickets</td>
<td>4</td>
</tr>
<tr>
<td>Average security tickets solved per day</td>
<td>3</td>
</tr>
<tr>
<td>Central help-desk vs. security group</td>
<td>3</td>
</tr>
<tr>
<td><strong>Security group</strong></td>
<td></td>
</tr>
<tr>
<td>Average security tickets per day</td>
<td>5</td>
</tr>
<tr>
<td>Average time to solve security tickets</td>
<td>5</td>
</tr>
<tr>
<td>Security group specific tickets</td>
<td>4</td>
</tr>
<tr>
<td>Average security tickets solved per day</td>
<td>3</td>
</tr>
<tr>
<td><strong>Local support</strong></td>
<td></td>
</tr>
<tr>
<td>Average security tickets per day</td>
<td>9</td>
</tr>
<tr>
<td>Average time to solve security tickets</td>
<td>3</td>
</tr>
<tr>
<td>Average security tickets solved per day</td>
<td>2</td>
</tr>
</tbody>
</table>