Qualitative Factors in Organizational Cyber Resilience

Srinidhi Vasudevan
Department of Computer Science
University College London
London, United Kingdom
s.vasudevan@ucl.ac.uk

Anna Piazza
Department of Computer Science
University College London
London, United Kingdom
a.piazza@ucl.ac.uk

Madeline Carr
Department of Computer Science
University College London
London, United Kingdom
m.carr@ucl.ac.uk

***Abstract*— Cyber resilience moves organizations away from efforts to guarantee security of all systems, towards an approach that acknowledges that systems are bound to fail with a focus instead on the impact of that failure on business objectives. While the work on cyber resilience is evolving, there is a lack of studies using qualitative data for investigating the concepts and themes pertaining to cyber resilience in organizations. The purpose of this study is to uncover the non-technical organizational factors that contribute to better cyber resilience. By adopting a qualitative approach of analyzing factors of organizational resilience, this paper uses primary data collected through 25 interviews at senior leadership or board-level to point out the extent to which these factors facilitate or impede cyber resilience. The study illustrates a Leximancer map of each factor that characterizes organizational cyber resilience, based on insights from cyber practitioner communities through narrative interviews. This research contributes to a better theoretical and practical understanding of how cyber resilience within organizations can be improved. The findings show that cyber strategy and skilled people play a key role in adoption of cyber culture at the management level, while communication between boards and security leadership as well as a clear reporting structure are signals for building cyber resilience.**

Keywords—socio-technical factors, qualitative data, organizational cyber resilience, Leximancer concept maps, board-leadership communication, skilled workforce

I. INTRODUCTION

Increasingly, organizational approaches to cyber threats are based on resilience rather than the ironically named “fail-proof” systems developed in the 1980s. Conventional wisdom now holds that businesses need to prepare for ‘when’ they will suffer loss associated with cybersecurity rather than ‘if’ they will. The challenges facing organizations of all types and sizes continue to evolve. Organizations are more and more dependent on digital technologies for their day-to-day operations which expands the threat landscape and exposure to cybercrime. This was exacerbated by the Covid pandemic as technologies and processes for remote working introduced new vulnerabilities. Novel attacks employing machine learning increased by 15% in this period [1]. Similarly, a study conducted by ThoughtLab [2] that evaluated the performance and cyber practices of 1200 organizations across 13 industries and 16 countries found that there has been a 15% rise in all cyber-attacks in 2021. 41% of these organizations believe that, while they have been taking up digital transformation rapidly, their cyber practices are still lagging behind. Towards the end of 2021, organizations had faced 925 attacks on average every week [3]. The problem is not going away.

A reactive cybersecurity approach leads to organizations lagging behind, and the balance of power remains firmly in favour of cyber criminals [4]. For organizations to stay ahead of criminals, a more holistic approach is required. A cyber resilience approach helps bridge this gap because it considers security as a strategic channel for organizations to achieve their business objectives and goals despite adverse situations and threats [5]. As such, cyber resilience does not aim to create fail-safe systems but looks at how failure impacts business objectives [6]. Even though the cyber resilience approach is seen as beneficial, the World Economic Forum reports that 59% of cyber professionals believe that the terms cyber security and cyber resilience are synonymous and do not understand the difference. Also, only 17% of the organizations surveyed are confident that they have adequate cyber resilience [7].

While several frameworks from both academia (for instance, see, [8,9,10]) and practitioner (for instance, see, [1,4,7]) perspectives have been developed through using data to quantify different metrices, researchers argue that there is a lack of studies using qualitative data for investigating the concepts and themes pertaining to cyber resilience in organizations. Furthermore, there are most studies focus on technical aspects of cyber resilience and this calls for further investigation into evaluating how different non-technical organizational factors contribute to better cyber resilience [11]. Responding to this gap, this study’s main goal is to distil - in a specific empirical setting - the factors that contribute to cyber resilience and how this can be built and maintained in organizations. The empirical context that has been selected to test the value of the study’s scope is based on original fieldwork and data that has been collected on perception and views on cyber security. Primary data was obtained through 25 semi-structured interviews that were conducted in 2021. These interviews were carried out with individuals in leadership positions or boards involved in cybersecurity decision making. This study relies on a new class of qualitative software: Leximancer to conduct a thematic and relational analysis of our interview data. This research contributes to a better theoretical and practical understanding of how cyber resilience within organizations can be improved. By turning this research into useful guidance, leadership and boards can use it to work together to ensure good organizational cyber resilience.

II. EVOLUTION OF ORGANIZATIONAL CYBER RESILIENCE

A decade ago, the idea of cyber resilience was put forth by the World Economic Forum and since then there has been a growing interest amongst practitioners and academic researchers in how cyber resilience can be applied to organizations to enable them to deal better with the evolving threat landscape (refer Table 1). The initial framework designed by the World Economic Forum contained a checklist for C-suite executives looking at three key areas namely Governance, Program, and Network and these areas considered both procedural and managerial aspects of cyber along with management of external relationships [12]. Enhancing this further, in 2015, a cyber value-at-risk model was developed which additionally allowed for organizations to evaluate the loss from a cyber-attack. In 2016, the cyber resilience model of WEF extended the work of [13] to account for the four organizational domains; physical, social, cognitive, and information. Researcher [14] looked at different stages in cyber resilience namely planning, absorption, recovery, and adaptation and focussed on response and recovery factors to evaluate cyber resilience. In other words, organizational factors for cyber resilience encompass those characteristics of the organization such as decision-making processes, organizational structure, knowledge and skills that employees within the organization possess, influence of managers, as well as organizational culture [15].

While several models have been proposed and applied in organizational contexts, there are several non-technical resilience factors that are consistently mentioned in the literature as outlined in Table 1.

TABLE I. ORGANIZATIONAL CYBER RESILIENCE MODELS IN LITERATURE

Reference	***Factors discussed***
[16],[17],[18],[19], [20]	***Security awareness/training***
[21],[22],[23],[24], [25],[26]	***Governance process, oversight, board engagement***
[18], [27],[28]	***Cyber investments***
[29],[30],[31]	***Knowledge sharing within and outside organizational boundaries; stakeholder management***

Considering the non-technical factors of organizational resilience, primary data was gathered through interviewing 25 participants at senior leadership or board-level to identify the extent to which these factors contribute to or impede cyber resilience through qualitative analysis. A protocol with open-ended questions to frame the interviews has been employed by this study. The interview protocol was organized around three different themes. The first theme focused on challenges pertaining to cybersecurity. The second theme focused on board involvement in cyber security and board-leadership communication. The third theme was used to investigate cyber strategy and how organizations respond to incidents as well as their business continuity.

The twenty-five interviewees were conducted between March and May 2021. All interviews lasted approximately 40 minutes. The participants were chosen from different types of organizations, and business sectors within UK to investigate the non-technical factors that organizations face and that impact on their cyber resilience. The interviews were conducted through Microsoft Teams and were all recorded and later transcribed verbatim to capture non-verbal behavior, to obtain a sequential observation scheme recording the real-time of interactions and communication [32], and facilitate detailed content analysis. The participation was voluntary, the data were kept in strict confidence and in line with the Data Protection Act and had approval from the Ethics Committee at University College London. The research team adopted an empathic neutrality [33] and were available throughout this phase of the data collection process to address any questions or concerns from the participants. The interviewees were then pseudo-anonymised and referenced using the acronym INT followed a numeric code 0XX. All quotes used in this research thus only provides the pseudo-anonymous code to avoid identification of individuals.

This research employs a tool called Leximancer which systematically reviewed the 25 interview transcripts, automatically detected keywords, identified other terms that these keywords co-occur with, and then grouped these together into broader 'concepts' [34, 35]. This is in contrast to NVIVO which asks the researcher themselves to code the themes. Concepts thus can be seen as connect words that have something in common. These connected words are visualised together as a concept map [34]. Employing Leximancer as a qualitative software over other software tools (e.g. NVIVO) for analysis was advantageous as this was completely automated with no intervention required for handling data. This was preferred as it avoids researcher bias [36]. Furthermore, from the raw data, it was possible to see how different concepts emerge and to assess which organizational factors were predominantly applied in the context of cyber resilience. Analysing each concept individually was also possible through obtaining text excerpts for each of these concepts. The analysis revealed for main concepts as shown in Figure 1:

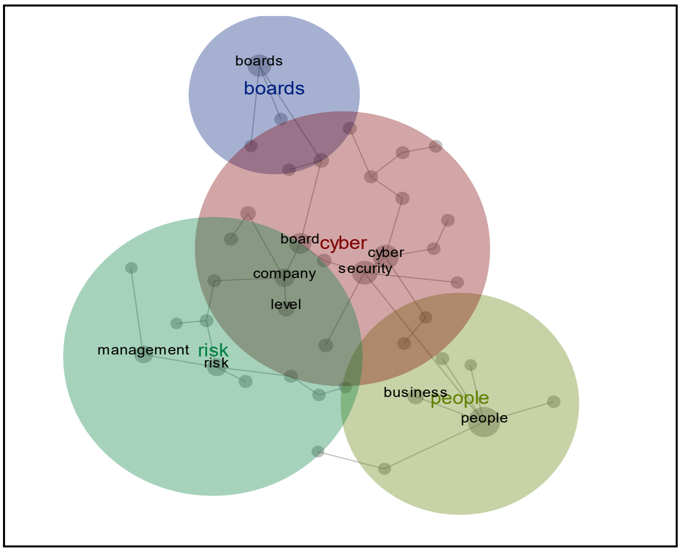

Fig. 1. Leximancer concept map

The organization of the bubbles in this diagram is significant including their size, position on the map, and relationship to one another, as is the proximity of the terms. All of this is generated by the software and there is some preliminary analysis to be done based on the physical characteristics of this map. The distance between the 'Board' bubble and the 'People' bubble can be seen, which indicates that terms that fall into the 'board' bubble did not tend to be discussed adjacent to issues related to people. It also shows that there is a distance between 'Board' and 'Cyber'. Indeed, in the interviews, it was found that participants perceived the distance in terms of communication gaps with boards, or in terms of individuals being separated from the boards in terms of cyber decision-making. Also, contextually, these words were not found to be mentioned together, which is a reflection of participants' perceptions. The lines in the diagram can be seen as conceptual paths that connect different concepts and this reflects the "proximity" of the concepts. The size of the bubble is representative of the importance of the words based on word-frequency.

A. *Concept Group 1: Level and company*

The first concept and the most prominent one that participants discussed was "level" within the organization and how interaction between and across levels impacts on cyber resilience. This broad concept comprised of several sub-topics namely organizational structure, different committees, audit levels within various organizational units. One clear example emerged in terms of the hierarchical communication between cybersecurity practitioners and senior business leaders. Looking at the role of the CISO, one interviewee points out "Until recently, the role of the CISO did not exist. Even now, if you think about it, CISO is largely a technical person reporting to the CFO or CIO. If a cyber-attack can lead to businesses being shut down, it is no longer a technical or operational risk. It is a strategic risk. CISOs need better reporting structure and better access to the CEO or even the boards" (INT024). Another interviewee says not having direct communication with the board makes cyber reporting difficult adding, "And that is another challenge, is that the CFO is not an IT person. So, I need to give him the material and he is the one communicating to the Board. Then he is getting questions, feedback, input, which I am getting afterwards. I do not have direct communication" (INT002). Governance also emerged as a key 'level' issue. One interviewee says "When you think about a resilient organization, one concept that is often overlooked is cyber governance. How effective is the organizational design? How can we have the right structures and decision-making processes that improves accountability of the boards and CEO? How can behavior at the top bring a positive change?" (INT025).

From looking at further interview excerpts, the main learning point is that when the role of the CISO is obfuscated by design, this leads to poor insight on cyber and reporting to other C-Suite this hinders or even dilutes its strategic importance. Building resilient organizations requires discussions that connect reporting structures for governance of cybersecurity with accountability and the fiduciary responsibilities attached to the board and CEO. This is in line with the literature on governance structures and its impact on cyber resilience [21-26].

B. *Concept Group 2: People and Business*

The second major concept was around "people" where discussions were around training and awareness, skills of individuals responsible, and the overall culture and values of the organization. A skilled workforce and relevant training were perceived as key to resilient organizations as highlighted by the literature on cyber resilience [16-20]. One interviewee points out, "It is making sure as well that the people internally who are looking after cyber security are sufficiently resourced and trained and appropriate to do the job" (INT012). Training needs to be sustained, throughout the organization and there should be a way to evaluate training efficacy through simulations. On this another interviewee says "I would suggest that it is not standard across the industry, it just happens to be part of how we are training and this is continual training, this is how we continue to brief colleagues, directors etcetera, and then we push that down through the organization. I think probably the biggest feedback we can give is to gamify it and actually start telling people that 27% of people clicked on that fake link so we would have had a cyber issue" (INT004). Finally, how people behave and carry out their tasks is part of the larger organizational and cyber culture. To this end, one interviewee postulates, "we are guided by the same core values. And we do have a young leadership team, we do have young people who are really willing to bring this company into the right place" (INT003). In short, another interviewee adds that cyber posture and resilience of the organization "is reflective of the culture" (INT007). Further to this, another interviewee points out how parochialism is a result of organizational culture where information is not shared fully among different organizational units or when silo mentality hinders communication and co-ordination across different organizations. The interviewee raised a concern about "cyber not being taken to the boards and looking at different committee results in siloed mentality." (INT025). Another interviewee adds further about information sharing culture saying, "When we setup an exchange of information for the industries in the UK to swap cyber security incidents the people who were the hardest to persuade to join in were the financial institutions. It was a sackable offence in most banks ever to even say you'd had an incident, but we're talking 15 years ago. It isn't the case now, but at the time it was. So they didn't feel empowered to be able to join in and talk about what had happened to them which would have been very useful" (INT015).

C. *Concept Group 3: Boards*

The third concept was about boards, their involvement with and understanding of cyber security within the organization and communication between boards and security leadership. The role that boards play in ensuring good cyber resilience has been emphasised both in academic literature [23,25] and in practitioner studies [4,7].

One interviewee mentions that boards tend not to be involved directly unless the there is an investment need that crosses the spend threshold or unless the issue is deemed serious. On this note, the interviewee says "No direct involvement [of the board]: I had very little contact except at the chairmen level and that was a direct relationship where I was asked to do briefings. But I have never presented to a main board, it has always been at the executive committee level (INT007). Another interviewee reflects that boards do not have the right knowledge saying, "The challenge is that you are highly unlikely to find a non-executive director who is expert in cyber security, and even if they were, how do they keep current, unless they are in a fulltime role and exercising a network" (INT005). Boards having adequate knowledge is deemed important as they are then able to question cyber practices. This has been mentioned by one interviewee who says "I think it's very important that the Board is able to ask the right kind of questions about ensuring that the management has the rigor in place as far as cyber security is concerned. And I think the problem that I see today is that the Board is unable to sometimes ask those questions and be able to inform themselves of that risk properly simply because they don't know what to ask" (INT0023).

Another interviewee points out about that CISO communication needs to transcend technical language and instead point out to how cybersecurity incidents may impact the business. "This is why boards get very frustrated about it and do not really understand it, because cyber strategy is really about how you run your business" (INT009) and CISOs should be able to communicate cyber "from a reputational perspective, from a business perspective, and of course programmatic type risks" (INT023). Apart from being able to speak the board's language, another interviewee adds that "the biggest challenge is around what level of details do we need to communicate to a Board. It has been an on-going challenge all the time" (INT002).

D. Concept Group 4: Management

This concept comprised of topics pertaining to risk approaches to cyber, alignment of security to organizational strategy, and cyber investments. Finally, one interviewee explains that good resilience can be achieved when a holistic risk approach is taken and there are adequate policies in place to govern and manage these risks. "Mechanisms by which risk can be managed [include] our policies and procedures, training people and equipping them to be able to identify risk, qualify, and then mitigate it. And then we have a mechanism by which we report risk, so we delegate risks" (INT008). Emphasising good risk management for better security management and improved resilience, another interviewee adds, "I do not think anybody has mentioned an enterprise management risk management system before. What is specifically the focus of doing an annual review on that, to actually really get assessment of how those risks have changed" (INT007).

While appropriate risk strategy is needed to achieve better resilience, another aspect of management is appropriate investment in cyber [18, 28]. Organizations need to have adequate investments in cyber and one interviewee says "The difficulty, of course, comes from the fact that however much awareness is there is always fierce competition for finance and investment and a lot of the issue is around precisely those two things. So, maintaining that level of awareness and willingness to see cyber security as a top risk, that is where the challenge lies"(INT007). Bigger budgets should not be seen as a solution for most cyber problems. This attitude signals that organizations have a reactive approach and cyber should focus on creating value and sustaining it. This is captured by one of the interviewees who says, "you will have individuals that want to see IT security as an insurance company. Like, you know, you buy something and you kind of hope it will work, kind of approach" (INT002).

III. Conclusion

The threat landscape is ever evolving with attacks becoming more sophisticated than before. Combating these require a strong leadership (CISOs) able to focus on protecting the digital assets of the organization while ensuring that the business and strategic priorities of the organization are met. This research looked at the current state of cyber resilience across organizations through data gathered from interviewing cyber leaders. The findings are fourfold. First, this study looks at how well-placed cyber is on the board agenda. As such, the study shows that while most organizations follow industry-best practices and adhere to security frameworks, there is clear scope to improve in terms of board – CISO relationships and how cyber can be communicated in a way that is clearly linked to business objectives. The senior leadership thus need to possess a range of competencies and capabilities including effective communication with boards to ensure that organizations are cyber-ready and resilient.

This study also showed some CISOs are C-level in title only. They do not get face-time with the board and direct reporting to boards is obfuscated by organizational design. Secondly, it is the responsibility of the boards to ensure that good culture is built at an organizational level and our research shows that this is not yet in place. This is partly attributed to the fact that some organizations still treat cyber as a function of IT and hence are not risk-mature. At an organizational level, it is important to find the right alignment between business leaders extending to the board of directors and security-focussed executives. When there is an acknowledgement at high-level for cyber issues, cyber would become part of the priority for the business leading to organizations being more resilient.

Third, organizations still see cyber as a cost-function – as a necessary evil which is required to appease different stakeholders. While there is a huge difference in terms of cyber budgets across different organizations and sectors, the key question to ponder is the motivation behind spending on cyber. Not all organizations see it as a strategic investment and money spent for some organizations is considered as money down the drain or a mere box-ticking exercise. Higher investments does not equate to outcomes if they are not aligned strategically. Firms looking at it as a strategic investment are more "invested" in cyber and are proactive in defending the business, thus more resilient to attacks. Finally, organizations are now recognising that working in silos and trying to improve their resilience alone might not be enough. Understanding that attackers work together in collaborative environments and acknowledging that the sum is greater than its parts, organizations are now more open to create collaborative and information sharing cultures across industries to improve their overall resilience, although this is still not happening proactively.

Acknowledgment

The authors wish to acknowledge funding received by Lloyd's Register Foundation and the National Cyber Security Centre through the Research Institute for Sociotechnical Cyber Security (RISCS). The authors would like to acknowledge the contribution and support of Prof. Angela Sasse who was instrumental in collecting the interview data used in this research.

References

[1] Deloitte, "Impact of COVID-19 on cybersecurity", deloitte2.com https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (Accessed 22/08/2022

[2] Thoughtlab, "Cybersecurity Solutions for a riskier world", thoughtabgroup.com https://thoughtlabgroup.com/cyber-solutions-riskier-world (Accessed 23/07/2022)

[3] Check Point, "Check Point Research: Cyber attacks Increased 50% Year over Year", checkpoint.com https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (Accessed 22/08/2022)

[4] Accenture, "The nature of effective defense: Shifting from Cyber Security to Cyber Resilience", Accenture.com https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/en/accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf (Accessed 30/07/2022)

[5] Conklin WA, Kohnke A. Cyber resilience: An essential new paradigm for ensuring national survival. InICCWS 2018 13th International Conference on Cyber Warfare and Security 2018 Mar 8 (p. 126). Academic Conferences and publishing limited.

[6] Björck F, Henkel M, Stirna J, Zdravkovic J. Cyber resilience–fundamentals for a definition. New Contributions in Information Systems and Technologies. 2015. Vol. 353.

[7] World Economic Forum, “Global Cybersecurity Outlook 2022”, weforum.org https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (Accessed on 02/08/2022)

[8] Duchek S. Organizational resilience: a capability-based conceptualization. Business Research. 2020 Apr;13(1):215-46.

[9] Kantur D, Say AI. Measuring organizational resilience: A scale development. Journal of Business Economics and Finance. 2015 Sep;4(3).

[10] Sahebjamnia, N, Torabi, SA & Mansouri, SA 2015, ‘Integrated business continuity and disaster recovery planning: towards organizational resilience’, European Journal of Operational Research, vol.242, no. 1, pp. 261–273.

[11] Bagheri S, Ridley G. Organizational cyber resilience: research opportunities. InACIS2017: Australasian Conference on Information Systems 2017 (pp. 1-10).

[12] World Economic Forum, “Partnering for Cyber Resilience”, weforum.org https://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf (Accessed 04/08/2022)

[13] Linkov I, Eisenberg DA, Bates ME, Chang D, Convertino M, Allen JH, Flynn SE, Seager TP. Measurable resilience for actionable policy.

[14] Roege PE, Collier ZA, Chevardin V, Chouinard P, Florin MV, Lambert JH, Nielsen K, Nogal M, Todorovic B. Bridging the gap from cyber security to resilience. InResilience and Risk 2017 (pp. 383-414). Springer, Dordrecht.

[15] Goodman PS, Haisley E. Social comparison processes in an organizational context: New directions. Organizational Behavior and Human Decision Processes. 2007 Jan 1;102(1):109-25.

[16] Wilding N. Cyber resilience: How important is your reputation? How effective are your people?. Business Information Review. 2016 Jun;33(2):94-9.

[17] Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. Cyber security awareness, knowledge and behavior: a comparative study. Journal of Computer Information Systems. 2022 Jan 2;62(1):82-97.

[18] Hausken K. Cyber resilience in firms, organizations and societies. Internet of Things. 2020 Sep 1;11:100204.

[19] Dupont B. The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity. 2019;5(1):tyz013.

[20] Annarelli A, Clemente S, Nonino F, Palombi G. Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy. In Intelligent Computing 2021 (pp. 818-832). Springer, Cham.

[21] North J, Pascoe R. Cyber security and resilience It's all about governance. Governance Directions. 2016 Apr;68(3):146-51.

[22] Hult F, Sivanesan G. What good cyber resilience looks like. Journal of business continuity & emergency planning. 2014 Jan 1;7(2):112-25.

[23] Armour C. Cyber resilience: Leadership matters. Cyber Security: A Peer-Reviewed Journal. 2017 Jan 1;1(2):134-46.

[24] Ingram M, Martin M. Guide to cybersecurity, resilience, and reliability for small and under-resourced utilities. National Renewable Energy Lab.(NREL), Golden, CO (United States); 2017 Jan 1.

[25] Gale M, Bongiovanni I, Slapnicar S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Computers & Security. 2022 Oct 1;121:102840.

[26] Branfield C. Cyber risk: Leveraging a multidisciplinary approach. Cyber Security: A Peer-Reviewed Journal. 2019 Jan 1;2(4):310-20.

[27] Carias JF, Borges MR, Labaka L, Arrizabalaga S, Hernantes J. The order of the factors DOES alter the product: Cyber resilience policies’ implementation order. InComputational Intelligence in Security for Information Systems Conference 2019 May 13 (pp. 306-315). Springer, Cham.

[28] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient systems: a systems security engineering approach. National Institute of Standards and Technology; 2019 Sep 4.

[29] Fenwick T, Seville E, Brunsdon D. Reducing the impact of organizational silos on resilience: A report on the impact of silos on resilience and how the impacts might be reduced.

[30] Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security. 2016 Jul 1;60:154-76.

[31] Shalamanov V. Towards effective and efficient IT organizations with enhanced cyber resilience. Information & Security. 2017;38:5-10.

[32] Mondada L. Challenges of multimodality: Language and the body in social interaction. Journal of sociolinguistics. 2016 Jun;20(3):336-66.

[33] Foley KM, Warin M, Meyer SB, Miller ER, Ward PR. Alcohol and flourishing for Australian women in midlife: a qualitative study of negotiating (un) happiness. Sociology. 2021 Aug;55(4):751-67.

[34] Conrad RA. Media coverage of crises faced by higher education institutions. University of Nevada, Reno; 2011.

[35] Rooney D, McKenna B, Barker JR. History of ideas in management communication quarterly. Management Communication Quarterly. 2011 Nov;25(4):583-611.

[36] Sotiriadou P, Brouwers J, Le TA. Choosing a qualitative data analysis tool: A comparison of NVivo and Leximancer. Annals of Leisure Research. 2014 Apr 3;17(2):218-34.