Crisis Communication Guidelines to Support Cyber Resilience

Eveliina Hytönen and Harri Ruoslahti
Laurea University of Applied Sciences, Espoo, Finland

eveliina.hytonen@laurea.fi
harri.ruoslahti@laurea.fi

Abstract: Cyber-attacks have become a prominent issue in the digital society. Attacks can result in losses for individuals and organisations. Cyber-attacks such as data breaches can create a very real threat to all stakeholders with a strong perception of vulnerability because potential loss of sensitive data. Such crises place unique demands for crisis management and communication. Communication is crucial for promoting awareness and sharing information and instructions to stakeholders. Consequently, effective communication can help build dynamic organisational cyber resilience. The research question of this paper is: How can crisis communication help manage cyber incidents? To respond to the research question, this paper draws on earlier research on cyber security-related communication. In addition, two semi-structured group interviews were conducted to collect views from expert participants in the field of cyber security management and communication. The data were analysed thematically. The findings from the interviews support earlier research on cyber security communication. To help manage cyber incidents, cyber crisis communication should be timely and open, express empathy to stakeholders, show accountability and commitment to securing the data and to resolving the incident. Clear instructions and information about protective actions are also required from effective communication. By synthesising findings from earlier research literature and the interview data, this paper proposes preliminary communication guidelines that can assist in identifying effective strategies and requirements for cyber security communication within organisations. The guidelines can help prepare for and respond to cyber crises and consequently support organisational cyber resilience.

Keywords: Crisis communication, Cyber security communication, Cyber incident, Organisational resilience, Cyber resilience

1. Introduction

In today's information-rich world, many organisations are affected by complex and ill-structured threats and crises. Cyber incidents such as ransomware attacks and data breaches, rank as the top global risk to business continuity management in the Allianz Risk Barometer in 2024 (Allianz Risk Barometer, 2024). The early hours of any cyber crisis are crucial for crisis management to mitigate reputational impacts, regulatory risks, and business disruptions (Miller and Pearlson, 2024). Cyber-attacks can create a very real threat to all stakeholders with a strong perception of vulnerability because potential loss of sensitive data (Coombs, Holladay and White, 2020a). Stakeholders no longer see the breached organisations as victims but as not properly protecting their data (Coombs, Holladay and White, 2020b). Therefore, cyber incidents force organisations to reconsider their approaches to crisis management and communication.

Organisational resilience becomes particularly apparent during a crisis, as an organisation communicates to mitigate the impacts (Doerfel et al., 2020). Communication can support resilience by providing necessary information, fostering self-sufficiency, relieving emotional reactions, maintaining reputation, and strengthening legitimacy (Vos, 2017; Tasic et al., 2020; Olsson, 2014). Given the increasing frequency and severity of cyber incidents, and their demands for crisis management, there is a need to further explore cyber security-related communication. The aim of this study is to gain understanding on communication in managing cyber incidents and in organisational cyber resilience. The research question of this paper is: How can crisis communication help manage cyber incidents?

Following this introduction, relevant literature on crisis management and on the role of communication supporting organisational resilience is presented in section 2. Section 3 then explores previous research on cyber security-related communication, followed by section 4 about the methodology of the study. Section 5 outlines the results, and section 6 discusses the results by drawing on previous research literature and the interview data of the study. Finally, section 7 provides a conclusion of the paper highlighting key issues and suggesting directions for future research.

2. Crisis Management and Communication Supporting Organisational Resilience

In the academic discussion on crisis management, there has only been a modest interest in viewing cyber related events as crises (Kuipers and Welsh, 2017). According to Knight and Nurse (2020) a cyber crisis results from a data breach or other similar cyber incident. Coombs, Holladay and White (2020a) view data breaches as sticky crises, that create a very real threat to most or all stakeholders and may take time to resolve.

Crisis management can be defined as a set of measures to prepare for and respond to a crisis, and to reduce its impacts (Coombs 2019). Crises act as catalysts for resilience-building activities (Doerfel et al., 2020). Organisational resilience can be defined as the inherent characteristics of an organisation to be able to respond to and recover from adverse events more quickly or develop more unusual ways of doing business under pressure than others (Vogus and Sutcliffe, 2007). Organisational resilience depends on the organisation's internal stakeholders, i.e. the employees (Olsson, 2014; Sutcliffe and Vogus, 2003). Employees' problem-solving and decision-making competences, self-efficacy, and communication skills are essential for organisational resilience (Rodríguez-Sánchez et al., 2019; Sutcliffe and Vogus, 2003). Resilience requires strong relationships also with external stakeholders, e.g. creating awareness and building trust by collaborating (Tasic et al., 2020). Organisations benefit from building their crisis capacity and fostering strong relationships with stakeholders before crises occur. Preparedness and communication strategies play a crucial role in influencing stakeholder perceptions during a crisis (Diers-Lawson and Pang, 2021).

Cyber resilience extends beyond cyber security by focusing on how organisations prepare for, respond to, and recover from incidents to ensure survival (Björck et al., 2015). Cyber resilience can be viewed as "the capacity to withstand, recover from and adapt to the external shocks caused by cyber-risks" (Dupont et al., 2023, p. 1). Miller and Pearlson (2024) define a cyber-resilient organisation as "one that has prepared for a cyber incident, can recover swiftly with minimal damage, and communicates appropriately as part of the organisation's ability to bounce back".

Communication supports organisational resilience through several functions. Effective communication facilitates preparedness activities such as promotion of continuity management activities (Herbane, Elliot and Swartz, 2004), awareness building and training by clarifying risks and instructing how they are managed (Reynolds and Seeger, 2005; Veil et al., 2008). Communication enables mindful organising, where resilience is constructed through organisational practices, i.e. sharing values, norms, and continuous interaction (Weick and Sutcliffe, 2015). Collaboration enables monitoring the situation and establishing relationships to support the development of collective responses during crisis (Sánchez and De Batista, 2023). People make sense of the crisis through communication, i.e. through interaction and interpretative actions (Weick, 2001). Situational awareness is maintained through constant communication that helps recalibrate the situation (Weick and Sutcliffe, 2015). Communicating warnings and instructions and explaining the crisis to the stakeholders supports continuity management functions (Reynolds and Seeger, 2005; Veil et al., 2008). Resilience-oriented crisis communication focuses on reputation management by explaining and advocating an organisation's own perspective, thus strengthening its credibility and legitimacy, and on providing information to the affected stakeholders with the aim of increasing self-sufficiency, affirming collective identity and providing emotional support (Olsson, 2014).

3. Previous Research on Cyber Security-Related Communication

Cyber security-related communication has been studied from both internal and external stakeholder perspectives. The public often lacks awareness of cyber security issues (Zhang and Borden, 2020) and fails to take precautions due to ambiguous cyber security communication (de Bruijn and Janssen, 2017). Effective communication strategies should aim to increase understanding of cyber risks, their severity and likelihood, and people's confidence in taking protective actions (Gillam and Foster, 2020; Zhang and Borden, 2020; Dodel and Mesch, 2019). Also, raising awareness by highlighting past incidents and potential losses can improve cyber security behaviour (Fatoki, Shen and Mora-Monge, 2024). Message framing strategies such as avoiding exaggeration, identifying villains and heroes, linking cyber security to broader values like trust, and personalising messages to make them more relatable and tangible, can be useful for communicating about cyber security (de Bruijn and Janssen, 2017).

Data breaches as sticky crises create strong perceptions of susceptibility of harm for victims, and place therefore different demands for crisis management than many other types of crises (Coombs, Holladay and White, 2020a). In case of a data breach, the responsibility can be ambiguous: stakeholders might hold the organisation liable for not implementing adequate security measures, while others may blame the hackers (Coombs, Holladay and White, 2020b; Bentley, Oostman and Shah, 2018). Being slow in revealing data breaches and in offering support can evoke strong responsibility attribution among stakeholders (Coombs, Holladay and White, 2020b). Emotional reactions such as anger and disgust tend to heighten when the public perceives the organisation as responsible for the breach (Syed, 2019).

Sticky crises require a near-instant response, and almost continuous adjustment of response strategies as the crisis evolves (Reber et al., 2021). The public should be notified about a cyber incident as quickly as possible,

because it helps address feelings of vulnerability (Knight and Nurse, 2020) and prevent potential disinformation from spreading (Backman, 2020). Fast information exchange within internal and external networks can improve cyber incident response (Dupont et al., 2023). Balancing between accuracy and timing is needed, but it might be better to over-estimate to get the message out fast before the media (Knight and Nurse, 2020).

Cyber crisis communication should prioritise the well-being and relief of stakeholders by demonstrating empathy and commitment to resolving the issue. This can diffuse negative emotions and reduce the blame placed on the organisation (Syed, 2019). Recognition of the violation helps rebuild trust (Coombs and Tachkova, 2019). When framing the message, the organisation should show responsibility, and apologise, because they are the custodians of the stakeholders' data (Knight and Nurse, 2020). The organisation and its leaders should take ownership of the situation by acknowledging it and sharing appropriate information to build goodwill among stakeholders (Miller and Pearlson, 2024). Crisis responses should also include advice to stakeholders on protective actions (Bentley, Oostman and Shah, 2018), and information about the corrective actions by the organisation (Bentley and Ma, 2020). Downplaying the incident and blaming others should be avoided, because that might be perceived as not taking the breach and cyber security seriously (Knight and Nurse, 2020). Humanising the message by adding a real person's name could help gain stakeholders' forgiveness and trust (Bentley, Oostman and Shah, 2018). Additionally, the language of the messages should be tailored, clear and understandable; jargon should not be used (Knight and Nurse, 2020).

All available channels should be used for communicating about the incident (Knight and Nurse, 2020; Miller and Pearlson, 2024). The appropriate channels for communication should be assessed during the crisis; alternative channels might be needed, if the prior planned channels are unavailable (Miller and Pearlson, 2024). Further, strategic use of social media to share real-time information and to monitor reactions, is needed because message framing affects public opinion (Syed, 2019). Organisations should also monitor how their initial response strategies are portrayed in the media especially regarding severity and controllability of the incident, because media framing can significantly impact public views on organisational responsibility (Kim, Johnson and Park, 2017).

4. Method

This study uses a case study approach (Yin, 2003) and qualitative research methods for data collection and analysis. The data were collected by conducting group interviews (Denzin and Lincoln 1994). This study and the research question (How can crisis communication help manage cyber incidents?) uses an academic approach to focus on practitioner interests, as is recommended by Baskerville and Myers (2009).

Two group interview sessions were held in the spring 2024. An open invite to the interview sessions was sent to the project DYNAMO (DYNAMO, 2025) consortium members and they were asked to promote the sessions to the people they considered relevant and suitable for the topic. The interview sessions were also promoted in the project's webpage and social media sites. There were altogether ten participants in the group interview sessions. The participants were professionals working in the field of cyber security management, and communication management and training. The sessions were held online in Microsoft Teams and lasted approximately 2 hours. The interviews were recorded and transcribed. Each interviewee was asked for informed consent before the start of the session and only data from interviewees who consented were included in the final sample.

The interview protocol was based on earlier literature about cyber security-related communication. The interviewees were asked to describe the functions and role of communication and the characteristics of effective and ineffective cyber security-related communication when preparing for and responding to cyber incidents. With a question such as 'What are the essential communication practices in preparing for and responding to cyber incidents or crises?' the interviewees were asked to express their opinions and experiences on practical aspects such as roles, responsibilities, target groups and content of communication related to cyber security. Additionally, the interviewees were encouraged to share examples and perspectives on both successful and unsuccessful cyber security communication they had encountered or observed in the media. They were asked to elaborate on their views regarding the effectiveness of those communication efforts. They were also asked, what kind of recommendations and advise they would give to organisations regarding cyber security communication.

After transcribing the recordings, the authors conducted a cross-case analysis of the data. The data was first narrowed down to a Data Extraction Table (DET), that was designed for this study based on the research

question. Then the data were further analysed thematically to find common themes and aspects of communication in managing cyber incidents.

5. Results from the Group Interviews

Two main themes emerged from the data gained from the group interviews: preparation and awareness, and response and communication during a crisis.

5.1 Preparation and Awareness

The interviewees mentioned that organisations should have a strategy for building awareness. Employee training was emphasised as a means of preparing and creating awareness, and that employees should be instructed on how to prevent cyber incidents and on how to respond to them. One participant described their organisation's frequent interactive training sessions that emphasise the impacts of cyber threats. The sessions aim to create understanding of the severity of the threats and explain the reputational threats. One interviewee explained that there is frequent communication from the risk management team to create awareness and share instructions to the employees. The interviewees mentioned examples of advertising and contacting customers to increase awareness among all stakeholders. Examples included ads warning against trusting certain messages, organisations highlighting their strong security measures after another's breach, and using white hackers in PR events to raise awareness.

Collaboration within the organisation and with external stakeholders was considered important. When planning communication and communicating, collaboration between the CTI experts who can identify the risks, the IT managers who can provide strategies for minimising or mitigating risks, the HR and the communication department, is needed. One participant mentioned that it would be essential to collaborate with stakeholders or partners within the same industry, if there is an attempt of a cyber-attack. That would help prepare and monitor the environment.

5.2 Response and Communication During a Crisis

The interviewees described cyber crisis communication experiences and practices. Organisations should plan standardised approaches by creating scenarios, appropriate statements, and messages for communication. One interviewee stated that having a crisis communication plan is not enough. The organisation and the management must commit to putting the plan into practice. It was pointed out, that communication needs to be quick and show that the organisation is taking actions to resolve the incident. Proactive and transparent communication from employers reassures employees and builds trust. Similarly, prompt communication with external stakeholders fosters confidence in the organisation's ability to handle the situation. The interviewees noted that timing needs to be considered carefully. If the affected organisation lacks clarity about the incident and its resolution, only announcing that there has been a data breach could make the public feel unsafe, potentially eroding trust and damaging the reputation.

The roles and responsibilities in cyber crisis communication management should be defined in the crisis communication plan. The interviewees mentioned agreeing on a spokesperson or a point of contact and on the coordination of the communication together with the management and IT experts to ensure appropriate handling of the situation.

According to the interviewees, cyber crisis communication should express empathy and show the organisation actively taking responsibility. The organisation should not be presented as a victim. No-one should be blamed in the communication. Apologising for not being able to protect the stakeholders' data was seen important. As target groups for the communication, the interviewees mentioned the public, the affected people, customers, suppliers, internal stakeholders such as employees, board, media and the local cyber security authorities. The language of the communication should be simple and clear. One interviewee also said that the messages should be created by communications professionals and not by the IT management or lawyers. As communication channels, the interviewees identified email, video messages, press releases, holding statements, Q&A sessions, websites, phone calls. Other channels, such as WhatsApp messages or calling to the local media and asking them to disseminate the information, were mentioned, as they might be needed, if the company website or email systems are down.

6. Discussion

The interview results support earlier research on cyber security-related communication. The findings of this study, and of the previous research literature were consolidated to suggest preliminary crisis communication

guidelines that can help manage cyber incidents. Reflecting and comparing these against the literature on organisational resilience and communication contributing to resilience, insights into how strategic cyber crisis communication can help support organisational cyber resilience are provided.

Table 1: Overview of the results and literature

Interview results	**Earlier research on cyber security communication**	**Earlier research on organisational resilience and communication**
Preparation and awareness building		
Planning - create communication strategy for building awareness and a cyber crisis communication plan - create standardised statements and messages - define roles and responsibilities for communication	Organisations need a cyber crisis communication plan due to the unique demands of cyber incidents (Miller and Pearlson, 2024; Coombs, Holladay and White, 2020a).	Cyber-resilient organisations have a cyber crisis communication plan in place (Miller and Pearlson, 2024).
Training and instructions - train employees - share instructions on how to prevent and respond - emphasise the impacts of cyber incidents - create understanding of the severity of the threats - communicate about risk management	Effective communication increases understanding of cyber risks, their severity and likelihood, and confidence in taking protective actions (Gillam and Foster, 2020; Zhang and Borden, 2020; Dodel and Mesch, 2019). Employee cyber security behaviour can be improved by highlighting past incidents and potential losses (Fatoki, Shen and Mora-Monge, 2024).	Effective communication clarifies risks and instructs how they are managed (Reynolds and Seeger, 2005; Veil et al., 2008). Employees' problem solving and decision-making competences, self-efficacy, communication skills and behavior, are essential for resilience (Rodríguez-Sánchez et al., 2019; Sutcliffe and Vogus, 2003).
Collaboration and promotion - advertise, organise PR events, contact customers to share information - promote cyber security policies and practices - collaborate with all stakeholders on crisis planning and risk management	Linking cybersecurity to broader values, such as privacy, trust, and relating to tangible issues, can make the communication more understandable (de Bruijn and Janssen, 2017).	Effective communication facilitates collaboration in preparedness activities (Reynolds and Seeger, 2005).
Interview results	Earlier research on cyber security communication	Earlier research on organisational resilience and communication
Response and communication during a crisis		
Timing - commit to putting the plan in practice - consider timing carefully - prefer communicating quickly, if possible	Data breaches require near-instant response (Reber et al. 2021).	Effective communication mitigates reputational damages, regulation risks, and financial consequences (Miller and Pearlson, 2024).

Interview results	**Earlier research on cyber security communication**	**Earlier research on organisational resilience and communication**
Message framing - show that actions are taken - blaming others should be avoided - the organisation should not be presented as victim - express empathy - apologise for not being able to protect the stakeholders' data - prefer open and proactive communication to create trust and reassurance - be careful not to decrease trust, impact reputation or cause uncertainty or fear	Recognition of the violation helps rebuild trust (Coombs and Tachkova, 2019). Demonstrating empathy and commitment to resolving the issue can help diffuse negative emotions and reduce the blame placed on the organisation (Syed, 2019). Crisis responses should include instructions (Bentley, Oostman and Shah, 2018) and corrective actions by the organisation (Bentley and Ma, 2020).	A crisis requires situational awareness; resilience is built through constant communication to recalibrate the situation (Weick and Sutcliffe, 2015). Sharing instructions and explaining the crisis to the stakeholders supports continuity management (Reynolds and Seeger, 2005; Veil et al., 2008). Advocating the organisation's perspective strengthens its credibility and legitimacy (Olsson, 2014).
Channels and collaboration - consider target groups - use simple and clear language - communications professionals should create the messages -consider all channels and alternative channels	The organisation should take ownership of the situation and share information to build goodwill among stakeholders (Miller and Pearlson, 2024). All available channels should be used for communicating about the incident (Knight and Nurse 2020; Miller and Pearlson, 2024).	Collaboration enables monitoring the situation and developing collective responses during crisis (Sánchez and De Batista, 2023). Situational awareness is built through continuous interaction (Weick and Sutcliffe, 2015).

As seen above (Table 1) cyber incidents place unique demands for crisis management and communication. It is important that organisations plan for cyber crisis communication as part of their preparedness and resilience building. Based on the results, communication can help manage cyber incidents by enabling preparedness activities such as creating awareness by training employees, sharing information about risks and instructions on how to prevent and respond to cyber incidents. Organisations should also collaborate with their stakeholders and promote their cyber security principles and perspectives to build awareness. These communication practices enable creating and sharing situational awareness among all stakeholders, and fostering trust and legitimacy, which are essential in supporting continuity and resilience (e.g., Vos, 2017; Weick and Sutcliffe, 2015; Olsson, 2014).

The results imply that to manage cyber incidents efficiently, cyber crisis communication should be quick, accurate and contain relevant information. It should also show responsibility, reassure internal and external stakeholders of the organisation's commitment to resolving the incident, and express empathy. Open and understandable cyber crisis communication containing advice for stakeholders on protective actions is also required in case of a cyber incident. These communication practices help recalibrate and make sense of the situation (Weick and Sutcliffe, 2015). Recognition of the violation (Coombs and Tachkova, 2019) and emotional support (Olsson, 2014) help maintain trust, and build goodwill among stakeholders to manage reputational damages and continuity of the collaboration (Miller and Pearlson, 2024). Based on the results, all available channels should be used, and different target groups considered in the communication and collaboration. Strategic use of social media is recommended to monitor the discussions (Syed, 2019), which can enhance situational awareness and development of collective responses to crisis (Sánchez and De Batista, 2023).

7. Conclusions and Future Work

Cyber incidents place unique demands for crisis management and communication, necessitating the integration of cyber security communication strategies into preparedness and resilience activities. As cyber-attacks become more frequent and severe, effective communication is crucial for creating awareness,

coordinating responses, and maintaining trust. This study explored how crisis communication can help the management of cyber incidents and contribute to organisational cyber resilience.

The findings, synthesised from previous research literature and from the interview data, imply that proactive cyber security communication can support preparedness by raising awareness, training employees, and fostering stakeholder collaboration. During a cyber crisis, organisations should communicate promptly and accurately, providing internal and external stakeholders with relevant information while demonstrating responsibility and empathy. Clear and actionable messages, including instructions and support, helps stakeholders navigate the crisis and rebuilds trust. Consequently, strategic and well-structured cyber security communication can support organisational cyber resilience.

This study makes theoretical and practical contributions by increasing the understanding of cyber security-related communication and its role in organisational resilience. It offers organisations valuable insights for developing cyber crisis communication strategies that can enhance their ability to prepare for, respond to, and recover from cyber incidents. Despite these contributions, there are certain limitations in the study. The interview data is limited in scope, preventing broad generalisation across different organisational contexts. Future research should conduct industry-specific analyses, systematic literature reviews, and expanded interviews to elaborate on these findings. Further research on communication strategies in different organisations could offer frameworks and guidelines on how to best support organisational cyber resilience through communication management. Knowledge is also needed on how the frameworks and guidelines are applied to organisations' communication practitioners' work.

Acknowledgements

This study has received funding by the European Union project DYNAMO, under grant agreement no. 101069601. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Allianz Risk Barometer (2024) Allianz Global Corporate and Specialty (AGCS), https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf.

Baskerville, R. L. and Myers, M. D. (2009) Fashion waves in information systems research and practice. *Mis Quarterly*, pp. 647-662.

Bentley, J. M. and Ma, L. (2020) Testing perceptions of organizational apologies after a data breach crisis. *Public relations review, 46*(5), 101975.

Bentley, J. M., Oostman, K. R. and Shah, S. F. A. (2018) We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management*, *26*(1), pp. 138-149.

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015) Cyber resilience–fundamentals for a definition. In *New Contributions in Information Systems and Technologies: Volume 1*, pp. 311-316. Springer International Publishing.

Coombs, W. T. (2019) *Ongoing crisis communication: Planning, managing, and responding.* SAGE Publications.

Coombs, W. T. and Tachkova, E. R. (2019) Scansis as a unique crisis type: Theoretical and practical implications. *Journal of Communication Management*, *23*(1), pp. 72-88.

Coombs, W. T., Holladay, S. J. and White, R. (2020a) Corporate crises: Sticky crises and corporations. In *Advancing crisis communication effectiveness*, pp. 35-51, Routledge.

Coombs, W. T., Holladay, S. J. and White, K. L. (2020b) Situational crisis communication theory (SCCT) and application in dealing with complex, challenging, and recurring crises. In *Advancing crisis communication effectiveness*, pp. 165-180, Routledge.

de Bruijn, H. and Janssen, M. (2017) Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), pp. 1-7.

Denzin, N. K. and Lincoln, Y. S. (1994) *Handbook of Qualitative Research*, Sage Publications, Thousand Oaks, USA.

Diers-Lawson, A. and Pang, A. (2021) 11 Strategic crisis management: State of the field, challenges and opportunities. *Public relations*, *27*, 195.

Dodel, M. and Mesch, G. (2019) An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers and security, 86*, pp. 75-91.

Doerfel, M., Harris, J., Kwestel, M. and Kim, M. (2020) Crisis communication and organizational resilience. In F. Frandsen and W. Johansen (Ed.), *Crisis Communication*, pp. 319-340, Berlin, Boston: De Gruyter Mouton.

Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023) The tensions of cyber-resilience: From sensemaking to practice. *Computers and security, 132*, 103372.

DYNAMO (2025) *Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors* -homepage. Available at: https://horizon-dynamo.eu/ [Accessed 23 Feb. 2025].

Fatoki, J. G., Shen, Z. and Mora-Monge, C. A. (2024) Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. Computers and Security, 141, 103812.

Gillam, A. R. and Foster, W. T. (2020) Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior*, *108*, 106319.

Herbane, B., Elliot, D. and Swartz, E.M. (2004) Business Continuity Management: Time for a Strategic Role? *Long Range Planning* 37(5), 435-457.

Kim, B., Johnson, K. and Park, S. Y. (2017) Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business and Management*, *4*(1), 1354525.

Knight, R. and Nurse, J. R. (2020) A framework for effective corporate communication after cyber security incidents. *Computers and Security*, *99*, 102036.

Kuipers, S. and Welsh, N. H. (2017) Taxonomy of the crisis and disaster literature: Themes and types in 34 years of research. *Risk, Hazards and Crisis in Public Policy*, *8*(4), 272-283.

Miller, K. and Pearlson, K. (2024) How to Build a Cyber Crisis Communications Plan. *MIT Sloan Management Review (Online)*, pp. 1-7.

Olsson, E. K. (2014) Crisis communication in public organisations: Dimensions of crisis communication revisited. *Journal of Contingencies and Crisis management*, *22*(2), pp. 113-125.

Reber, B. H., Yarbrough, C. R., Nowak, G. and Jin, Y. (2020) Complex and challenging crises: A call for solutions. In *Advancing crisis communication effectiveness*, pp. 3-16, Routledge.

Reynolds, B. and Seeger, M. (2005) Crisis and emergency risk communication as an integrative model, *Journal of Health Communication*, 10(1), pp. 43–55.

Rodríguez-Sánchez, A., Guinot, J., Chiva, R. and López-Cabrales, Á. (2021) How to emerge stronger: Antecedents and consequences of organizational resilience. *Journal of Management and Organization*, *27*(3), pp. 442-459.

Sánchez, M. A. and De Batista, M. (2023) Business continuity for times of vulnerability: Empirical evidence. *Journal of contingencies and crisis management*, 31(3), pp. 431-440.

Sutcliffe, K. M. and Vogus, T. J. (2003) Organizing for resilience. In K. Cameron, J. E. Dutton, and R. E. Quinn (Eds.), *Positive organizational scholarship*, pp. 94–110, Berrett-Koehler.

Syed, R. (2019) Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, *28*(3), pp. 257-274.

Tasic, J., Amir, S., Tan, J. and Khader, M. (2020) A multilevel framework to enhance organizational resilience. *Journal of Risk Research*, 23(6), pp. 713-738.

Veil, B., Reynolds, B., Sellnow, T. and Seeger, M. (2008) CERC as a theoretical framework for research and practice*, Health Promotion Practice*, 9(4), pp. 26S–34S.

Vogus, T. J. and Sutcliffe, K. M. (2007, October) Organizational resilience: Towards a theory and research agenda. In *2007 IEEE international conference on systems, man and cybernetics*, pp. 3418-3422. IEEE.

Vos, M. (2017) Communication in turbulent times: exploring issue arenas and crisis communication to enhance organisational resilience. Reports from the School of Business and Economics, (40).

Weick, K. and Sutcliffe K. (2015) *Managing the Unexpected: Sustained Performance in a Complex World.* Hoboken: John Wiley and Sons.

Weick, K.E. (2001) *Making sense of the organisation*, Blackwell, Oxford.

Yin, R. K. (2003) *Case Study Research, Design and Methods*, 3rd. Ed. Sage, Thousand Oaks, USA.

Zhang, X. A. and Borden, J. (2020) How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises, *Journal of Risk Research*, 23(10), pp. 1336-1352.