The Life Cycle Approach to Effective Crisis Communications in Mitigating Cyber Threats and Attacks

Jussi Toivanen and Vilma Luoma-aho
University of Jyväskylä, Finland

Jussi.t.toivanen@student.jyu.fi
Vilma.luoma-aho@jyu.fi

Abstract: Cyberattacks pose multifaceted risks, including physical, digital, economic, reputational and societal harm. Often starting as an attack on an organization's intangible assets but quickly spreading to endanger tangible assets, cyberattacks are increasingly common globally. Once an attack becomes public, the targeted organizations face intense scrutiny from employees, customers, the media, the wider public and the authorities. At this point, effective crisis communication becomes critical for mitigating damage and recovering from the crisis. Decision-making and communication during cyber incidents are complicated by uncertainty, operational issues, incomplete information, and even the potential for attackers to shape narratives through extortion or leaks. This paper examines communication challenges in cyber crises through the lens of framing theory and situational crisis communication theory (SCCT). Based on data analysed from interviews with key experts of eight organizations during recent Finnish cyberattacks, the paper identifies key factors that constitute effective cyber crisis communication. These include (1) organizational preparedness, (2) efficient information sharing and coordination, (3) a deep understanding of target audiences and the information environment, and (4) the essential role of communication in leadership. The findings highlight the importance of proactive, transparent and coordinated communication to maintain trust and boost organizational resilience. Practical recommendations in the form of three "no-L-principles" are provided: 1. Do not lessen, 2. Do not lie, and 3. Do not linger. Practical recommendations are provided to enhance crisis communications preparedness, improve real-time crisis communication, reduce risks, and strengthen organizational capacity to manage cyber crises.

Keywords: Cyber crises, Cyberattacks, Resilience, Communication, Crisis communication, Framing, Preparedness

1. Introduction

Vastaamo ("response place" in Finnish) was a Finnish psychotherapy business that became the target of a large-scale data breach in 2020 and filed for bankruptcy in 2021. The hacker managed to obtain the centre's entire database, which contained highly sensitive information on 33,086 clients (Poliisi, 2023). He extorted both the organization and clients by threatening to publish the patient records unless his financial demands were met. The stolen database was published on the dark web, casting a lifelong shadow for victims (Kleeman, 2026). For the organization Vastaamo, the hack was its death strike, with the legal process still ongoing in 2026.

While some cyberattacks may serve military or political objectives (Li and Liu, 2021, p. 8176), often their purpose is disruption or financial gain (Europol, 2025, p. 6, 11). Examples include hacking, ransomware, malware, distribute denial of service (DDoS) attacks, phishing, scams, data breaches and financial fraud (Lallie et al., 2021). The actors behind cyberattacks are multiple, ranging from state actors to organized groups and even individuals (Desa, Juremi and Jenalis, 2025, p. 23). Cyber incidents can trigger many different types of crises, with damage that may remain limited to the digital realm, affecting data, systems and networks but can also extend beyond cyberspace, impacting people, institutions and physical infrastructure (Berg and Kuipers, 2022, p. 21). In severe cases, disruptions can impact international supply chains and escalate into national supply security risks (Turvallisuuskomitea, 2025). Cyber crises can be highly complex and prolonged, potentially accompanied by sustained intensity (Backman, 2020, p. 436). Beyond financial losses, cyber-attacks can erode trust and reputation and harm societies by disrupting social unity, inflicting psychological trauma, and fostering division (Shandler and Gomez, 2023, p.1, 369).

In today's digital environment, the capacity to safeguard consumer and stakeholder data, uphold privacy and maintain strong cybersecurity is increasingly seen as a clear marker of broader social responsibility (Khan, Lee and Liu, 2025, p. 1371). For organizations under attack, attacks are often handled through crisis communication to mitigate the crisis and comply with legal restrictions and requirements (see, e.g., EU NIS2, DORA and GDPR). The organization must ensure that victims receive timely and accurate information without compromising investigative processes or exposing additional vulnerabilities (Traficom, 2025), p. 39). Miller and Pearson (2024) state that in a cyber crisis, the clock starts ticking once the attack has been detected. We argue that from the organization's perspective, the clock actually starts ticking the moment the vulnerability enabling the attack emerges.

In the management of cyber crises, communication plays a central role. The paper asks: What kind of crisis communication is needed to manage cyberattacks? Building on Knight and Nurse (Knight and Nurse, 2020) and the process-like nature of cyber incidents, we structure this paper into three stages: before, during and after crisis communication.

2. Organizational Cyber Crisis Communications

As everyday life becomes more deeply intertwined with cyberspace, even small cyber incidents can lead to significant and wide-ranging crises (Berg and Kuipers, 2022, p. 21). The uncertainty created by a crisis places psychological strain on stakeholders. This strain can be reduced by providing timely, clear information about what happened and what steps will be taken to prevent a similar crisis in the future. (Coombs, 2007, p. 165). Crisis communication has been defined as "the ongoing process of creating shared meaning of among and between groups, communities, individuals and agencies within the ecological context of a crisis for the purpose of preparing for and reducing, limiting, and responding to threats and harm" (Sellnow and Seeger, 2021, p. 17).

When an organization becomes a target, it immediately forfeits part of the symbolic capital that reputation represents (Perera et al. 2022, p. 2). In public discourse, attacks are judged not only by technical details but by the narrative built around them. Communication becomes a crucial part of the impact chain: it can soften the crisis or intensify it. Cyber incidents are demanding because information is often incomplete, fragmented and unreliable (Traficom, 2025). The situation becomes clear only as the investigation progresses, so communication is built largely on uncertain information (Traficom, 2025). Silence can be harmful: if an organization fails to communicate clearly, stakeholders and the media may perceive secrecy or guilt, damaging organizational reputation (Pang, 2013, cited in Woon and Pang, 2017, p. 331). Therefore, it is crucial for the organization to communicate promptly about what has occurred, even if all the details are not yet known, often balancing uncertainty with swift communication (Knight and Nurse, 2020, p. 13).

Previous studies on cyber crises and communications have explored various topics – including the impact of data breach announcements on stock prices (Rosati et al., 2017), the role of corporate reputation and crisis response strategies in managing data breaches (Gwebu, Wang and Wang, 2018), resilience and its significance in managing cyber incidents (Calder, 2023; Joinson et al., 2023; Tzavara and Vassiliadis, 2024), testing perceptions on organizational apologies after a data breach (Bentley and Ma, 2020) – and provided behavioural recommendations (Zhang and Borden, 2020). Further, studies (Agrafiotis et al., 2018) have categorized cyber-related long-term harms around five key themes: physical or digital harm, economic harm, psychological harm, reputational harm and social harm. They define cyber harm as "the damage that arises as a direct result of an attack conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of" (Agrafiotis et al., 2018, p. 2).

From the practice side, Knight and Nurse (2020) propose a cyber-crisis communication framework for the pre-crisis and during-crisis phases, drawing on an extensive literature review and expert interviews that provide an empirical foundation for their recommendations on preparedness and communication. In addition to research-based guidance, practical CERT/CSIRT-oriented guidelines also support preparedness, response and recovery, for example, NIST's widely used Incident Response Recommendations (SP 800-61), whose third updated version was published in April 2025 (Nelson et al., 2025). However, these technically oriented guidelines tend to approach communication narrowly and often only superficially. When communication is viewed merely as support for technical functions and operational recovery, crisis management suffers because the organization overlooks the human dimension at the core of crises – how people interpret events and how they respond.

3. Theoretical Framework

Cybersecurity is not just about technology. It also involves the people who use technology and ensure it is implemented and operated correctly (Chaudhary, Gkioulos and Katsikas, 2022, p. 1). Research on cybersecurity spans multiple disciplines, ranging from technology and law to psychology and sociology (Fujs, Mihelič and Vrhovec, 2019, p. 1). An important question is where the focus of cybersecurity research should be directed. A human and social science perspective (Fujs, Mihelič and Vrhovec, 2019) on this technological topic is valuable, as it enables a broad analysis – both quantitative and qualitative – of the multidimensional human-technical context and offers insights accordingly.

As Triplett (2022, p. 575) states, "People and cybersecurity are inseparable". Therefore, communication constitutes a core capability for building and maintaining organizational cybersecurity (Triplett, 2022, p. 575) and for conveying attacks, their impacts and action guidance to employees and potential victims (Knight and

Nurse, 2020). Crises and crisis management likewise concern organizational reputation, conditioned by how employees, stakeholders and the media interpret and make sense of events (Coombs, 2007, p. 164). Accordingly, organizations should recognize that crisis situations and their management are not only operational processes but also intrinsically communicative. Also, as Coombs, Holladay and White (2020, p. 41) point out, effective crisis responses need to demonstrate empathy towards those affected, as showing empathy helps build trust between crisis managers and their stakeholders.

The growing use of digital channels, especially social media, has created new challenges for effective crisis communication (Coombs, Holladay and White, 2020, p. 35). Also, numerous actors seek to shape the information environment for their own purposes, and digital technologies give them capabilities that far surpass the public's understanding of what is possible or already underway (Wanless and Pamment, 2019, p. 1). At the same time, classical computer-mediated communication is expanding into artificial intelligence–mediated communication (AI-MC), in which AI is not merely a conduit but an active participant that can modify, augment or even generate messages so that people can better achieve their communicative goals (Hancock, Naaman and Levy, 2020, p. 90–91). Against this backdrop, it becomes crucial in crises to understand how public frames are constructed and processed (van der Meer, 2018) and how an organization's own actions and communication influence stakeholder interpretations (Coombs, 2007, p. 171).

Therefore, organizations must recognize that cyberattacks, despite their technical nature, function as communicative acts that shape the information environment. Regardless of the attacker's motives, their actions inevitably convey a message (Traficom, 2025). This means that cyber incidents must be interpreted not only as technical disruptions but also as meaning-making events that influence perceptions, trust and stakeholder expectations.

3.1 Framing the Cyber Incident

One challenge in crisis communication is that people interpret events differently, so messages may be misunderstood or tied to unrelated narratives despite the organization's intent, known as framing. Chong and Druckman (2007, p. 104) define framing as "the process by which people develop a particular conceptualization of an issue or reorient their thinking about an issue".

In contemporary digital societies, individuals can access, generate, circulate and reinterpret information through a wide range of online platforms, reshaping how meaning is constructed (Johansson et al., 2024; Neuman et al., 2014). As a result, framing becomes more dynamic and increasingly difficult for organizations to manage. This difficulty is further intensified by the digitalization of networked framing processes, which significantly influence interpersonal and organizational communication across both online and offline environments. These dynamics shape how groups emerge and divide, process new information, and remain vulnerable to misinformation. (Entman and Usher, 2018, p. 299). From the perspective of planning and implementing crisis communication it is essential for organizations to recognize and understand the diversity of framing and the ways in which frames emerge and evolve within a digital society.

According to media framing theory, the media can shape how the public interprets complex issues by selectively emphasizing certain elements (Zhang and Zhang, 2024, p. 13). In the era of social media, traditional media still retains an important role. As Roulet and Clemente (2018, p. 328) describe the role of traditional media as producing common knowledge about various events. In the context of social media, people then interact and respond on the basis of this shared knowledge. This process creates a continuous interplay between traditional media and social media.

Snider et al. (2021, p. 2) point out that past cases have shown that in many cyberattacks, the public internalizes the details of the attack immediately after it occurs, when media coverage is at its peak. Even though more accurate information is released later, fear and concern have already taken hold. From an organizational perspective, it is essential to provide sufficient contextual information when communicating about an event. Furthermore, according to White (2009, p. 187), when the media report issues without organizational context, negative framing tends to intensify, elevating issue salience and perceptions of crisis severity. If issues are not managed proactively, external audiences often adopt the media's perspective. Finally, in crises, the way an organization shapes its communication and provides contextual information can influence how the media frames and portrays a crisis (White, 2009, p. 178).

3.2 Situational Theory of (Cyber) Crisis Communication

The importance of communication becomes especially clear in times of crisis, when organizations must respond quickly, maintain trust and manage uncertainty. Coombs and Holladay (2022, p. 259–260) emphasize that crisis communication is a strategic tool that enables organizations to adapt to disruption, protect stakeholders and regain focus on core objectives. Whereas crisis management refers to the actions taken to address a crisis, crisis communication is the mechanism through which those actions are carried out and made meaningful to those affected (Coombs and Holladay, 2022, p. 259-260).

Widely used in organizational crisis communication research, situational crisis communication theory (SCCT) provides a model for anticipating how stakeholders will react and what kind of reputational threat the crisis may pose (Coombs, 2007). The theory highlights how key aspects of a crisis situation influence attributions related to the crisis and stakeholders' perceptions of the organization's reputation (Coombs, 2007). This is important in managing crises.

From this perspective, according to Coombs (2007, p. 166), three factors influence the reputational impact of a crisis: how responsible the organization is perceived to be, whether it has experienced previous crises, and what its reputation was like before the crisis. The more responsibility and negative history the organization has, the greater the reputational threat. SCCT highlights the importance of perceived responsibility and how it shapes reputation. Knight and Nurse (2020, p. 15) note that in the context of data breaches, organizations may be inclined based on SCCT to portray attackers or other external actors as those at fault, thereby positioning themselves primarily as victims.

Drawing from recent literature and real-world cases in Finland, this paper applies framing theory and situational crisis communication theory to analyse organizational crisis communication and its challenges concerning cyberattacks.

Research questions

The paper states that clear crisis communication strategies can be identified that organizations have used to manage and mitigate cyber incidents. These strategies are shaped by the specific characteristics and severity of the case, the organization's own features, its level of preparedness, general crisis readiness, previous crisis history, and the leadership's understanding of cyber threats. This paper analyses these approaches and is guided by the research question: "How can effective crisis communication be used to mitigate cyber risks and threats?" These insights aim to enhance organizational preparedness and crisis leadership from a crisis communications perspective.

4. Research Method

Multiple challenges relate to cyber security studies. In cybersecurity contexts, the target of an attack may be reluctant to disclose details about the incident due to concerns about operational issues, reputation, legal implications or the challenges of attribution (Lilli, 2023, p. 6). The data collection for this paper also involved challenges, which are described below.

For this study, a qualitative, semi-structured thematic interview method was selected to explore events and their underlying factors in depth, as the method enables participants from a limited number of organizations to share their personal perspectives, interpretations and meaning (Tuomi and Sarajärvi, 2018).

Grounded in SCCT and framing theory, the developed interview guide covered the full crisis life cycle through thematic sections, assessing preparedness, leadership and situational management. Questions related to communication practices, constraints, reputation, trust, resilience and accountability were asked. It also examined public framing and included questions on post-crisis recovery, communication and evaluation. Follow-up questions were asked to deepen understanding based on the interviewees' responses.

The study examined Finnish public- and private-sector organizations hit by high-visibility cyberattacks since 2020. Incidents spanned DDoS, phishing/scam campaigns, data breaches and ransomware, with several organizations facing recurring attacks, often repeated phishing and DDos, over subsequent years. The interviews focused on the attack types most relevant to each organization.

Experts were selected based on their roles and incident-management involvement, identified either directly or through organizational referrals. Personnel changes sometimes required redirecting interviews to those with first-hand experience. Interviewees typically prepared by consulting internally with CISOs and other specialists involved in the response.

Despite varied job titles, all interviewees participated in planning or executing crisis communication for cyber incidents. Crisis-team structures differed across organizations, reflecting organizational design and role allocations between communication and cybersecurity experts.

Table 1: Interviewed organizations, sector and expert roles, and attack types

Organization	1	2	3	4	5	6	7	8
Attack type	Ransom ware	Data breach and ransomwar e	Data breach and ransomwar e	Data breach	Data breach and ransom ware	DDoS /scams/Phi shing	Ddos/scams/P hishing	Data breach and ransomwar e
Intervie wed	Technical Director, Administr ative Director and occupatio nal safety officer	Director of communic ations	CIO and vice president (global marketing and communica tions)	Communic ations director	Chief	Communic ations director and communic ations manager	Corporate and customer communicatio ns lead	Head of security and external communic ations manager
Sector	Public	Public	Private	Public	Private	Private	Private	Private

Seventeen organizations were approached for interview participation. Two declined at the initial contact. One organization initially consented but did not engage with subsequent scheduling communications. Three organizations did not respond to either the initial invitation or the follow-up message. One organization initially accepted but cancelled and deferred the interview upon receipt of the advance questions and did not subsequently reinitiate scheduling. One organization redirected the request to an external communications agency that had supported the organization's crisis communication during the cyberattack. For one organization, an interview could not be arranged within the data-collection period due to scheduling constraints.

Participants received the interview questions in advance and retained the right to decline specific items or withdraw entirely. The interviews lasted 45–120 minutes and were conducted primarily via Zoom or Teams, with one held in person. All sessions were recorded and stored securely in encrypted form on the University of Jyväskylä's network drive and then deleted after transcription. During transcription, anonymization procedures ensured that neither organizations nor individual experts could be identified.

Given the interviewer's cybersecurity background and prior familiarity with some cases and interviewees, special care was taken to ensure that participants could speak freely and steer the discussion without undue influence. To preserve anonymity, the industries of the organizations are not reported, as such details could enable identification, given the small number of publicly known cyberattacks in Finland. Safeguarding anonymity was a central consideration throughout the study.

Following the interviews, the material was transcribed and analysed using the inductive method (Thomas, 2006). An inductive approach was selected, as it was considered particularly well suited for analysing interview data. Instead of relying on predefined theories, the aim was to allow the material itself to guide the process, identifying naturally emerging themes and categories directly from the transcripts. These insights could then be used to construct a framework that reflects the participants' perspectives and experiences (Thomas, 2006, p. 238).

5. Cyber Crisis Communications

5.1 Communication Before a Cyber Crisis

Proactive communication and building awareness are essential when preparing for and responding to cyberattacks. Based on the interviews, proactive communication helps employees and external parties understand how the organization prepares for and responds to cyberattacks. It also provides customers and partners with guidance for safeguarding their own data and devices. Such communication strengthens trust and improves the ability to withstand and recover from cyber crisis (Hytönen and Ruoslahti, 2025). Investing in intangible assets before any crisis is a key means of building resilience and securing support when disruption occurs (Canel, Luoma-aho and Barandiarán, 2020, p. 171–172).

Cyber incidents often remain undetected for extended periods, allowing vulnerabilities to persist until an attack or accident escalates into a full-scale crisis, leaving decision makers little time to prepare or respond (Berg and Kuipers, 2022, p. 14). High uncertainty and ambiguity further complicate management: attacks can originate anywhere, unfold instantly and produce immediate effects, unlike more predictable threats with warning signs. The lack of early indicators hinders prevention and complicates both preparedness and effective crisis response (Berg and Kuipers, 2022, p. 14).

The interview data indicate that effective pre-incident communication entails the following: (i) mapping plausible cyber-threat scenarios and associated impacts; (ii) identifying priority audiences; (iii) integrating and analysing crisis history and existing trust capital; and (iv) planning across the entire threat life cycle, including post-incident recovery. To mitigate uncertainty, (i) organizations should draft scenario-specific frameworks that specify management and information (situational-picture) requirements at each organizational tier, (ii) bring external partners into case-specific preparedness planning, (iii) and pre-draft communications for different channels and audiences across likely scenarios. Given the likelihood of a prolonged disruption, respondents emphasized the following: (i) redundant channels, (ii) clearly assigned management and communications roles with deputies, (iii) offline storage of essential materials, and (iv) processes that are deliberately designed, documented and regularly exercised.

Awareness-building is likewise central to preparedness. Effective communication improves risk comprehension (Chaudhary, Gkioulos and Katsikas, 2022), as underscored in Interviews 6 and 7. By proactively educating staff and customers, organizations can build trust and strengthen their readiness. Routine preparedness messaging also shapes stakeholder perceptions during a cyberattack (Interviews 6 and 7).

5.2 Communication During a Cyber Crisis

Interviews suggest that the early phase of cyber incidents is often marked by acute uncertainty: organisations may lack a consolidated situational picture - what happened, the scope, and which internal or external communication channels are safe to use. Technical constraints, legal obligations and ongoing investigations can restrict disclosure, creating significant challenges for determining what can be communicated, to whom, and at what point in time.

Effective crisis communication was generally seen as contingent on robust preparedness, clearly communicated command and management structures, regular exercises and dedicated expertise; it also benefits from alignment with stakeholder information needs and awareness of the broader information environment. Timely, level-specific and tailored situational picture was seen important for leadership, operational activities and communication.

Interviewees emphasised early stakeholder identification and the value of explicit communication coordination mechanisms; roles, responsibilities, and deputies are typically best defined and communicated in advance so that tasks, authority, and decision rights are clearer. It was considered important that internal personnel be informed first to support consistent responses, effective communication and customer care. In addition, worst-case contingency planning, including the possibility of a full data leak, was advised early on to keep messaging timely, coherent, and relevant amid evolving information. In parallel, organisations were advised to start planning and preparation for recovery communication, even while the investigation and corrective actions were in progress.

From the perspective of organizations, crises invariably raise questions of responsibility and reputation (Coombs, 2007) and trust (Siegrist, Gutscher and Keller, 2010). Beyond direct financial losses, cyberattacks cause significant intangible damage to morale and goodwill, which are far more difficult to measure (Perera et al., 2022, p. 2). Restoring trust requires transparent, evidence-based communication that does not downplay the incident (Knight and Nurse, 2020). Based on the interviews, common communication errors included evading responsibility, withholding information, minimising events, or issuing false statements. Existing trust capital, reputation and an organization’s crisis history were found to influence how audiences interpret events. It was also recommended that communication planning should consider concurrent events and stakeholder expectations. Organizations should also stay aware of the broader context and ongoing developments in the information environment to ensure that the timing, content, and tone of their communications are properly aligned. This helps preserve credibility, reduce ambiguity, and support reputational recovery.

5.3 Communication After a Cyber Crisis

Interviews showed that organizations' view post-incident communication as essential for employees, possible victims, customers and partners. Openness was the preferred strategy to rebuild trust and reputation, and one expert interviewed felt that sharing lessons learned during and after an attack generated positive feedback and helped restore trust and credibility (Interview 3).

Cyber crises can have lasting effects on personnel and operations. Reviewing the incident, especially with those most involved, was deemed important for learning and recovery. Staff may remain sensitive to minor technical issues, as shown by an organization recovering from ransomware (Interview 1). Operational impacts can persist, for example, when lost data cannot be restored (Interview 1), making it necessary to issue targeted communications that provide clear guidance and support to employees. Acknowledging employees' efforts after the incident was also considered important (Interview 2).

As one expert noted (Interview 5) crisis communication reveals more about an organization than any branding in normal circumstances because values, strategy and identity are tested in practice. Effective crisis communication therefore depends on shared values and a clear strategic direction, which enable responsible and coherent communication under pressure.

6. Recommendations for Managing Cyber Crisis Communications

Based on interviews and research literature, organizations are advised to use a life cycle approach to cyber crisis communication. Plan, implement and review actions across the preparedness, response and recovery phases. Clear roles, responsibilities and procedures with effective information flow are associated with more effective communication and leadership during incidents.

After a crisis, communication should continue with timely updates and audience-specific follow-ups for staff, affected individuals, customers and partners, acknowledging their different information needs. The next section explains how communication can help mitigate cyber threats and manage attacks.

The following recommendations are organized into (i) leadership, (ii) communication, and (iii) situational awareness. They align with the Finnish government's crisis communication guidelines (Prime Minister's Office, 2019), which were developed from post-analyses of crises affecting Finnish society since 2012 and emphasize the seamless integration of leadership, communication with effective information flow. This interconnection was further reinforced by the Finnish government's 2021 crisis communication development project (Valtioneuvoston kanslia, 2023), informed by broad stakeholder consultations and data collection.

Before the crisis

Leadership: Organizations should ensure preparedness and continuity planning for cyber threats, including activating a diverse crisis management team with clear roles, responsibilities and backup arrangements. Partners and relevant stakeholders must also be identified, cooperation should be agreed upon in advance, and coordination structures must be established.

Communications: Crisis communication plans must cover different attack types, identify spokespersons and substitutes, define core messages and prepare channel-specific communication materials in advance for various audiences. Backup communication channels should be tested and ready. Partners and relevant stakeholders must also be identified, cooperation should be agreed upon in advance, and coordination structures must be established.

Situational awareness: Processes for gathering and verifying information should be established, including alternative methods for maintaining situational awareness when systems fail. Plans should define what information is essential for decision-making and operations in different scenarios and for each level of the organization.

During the crisis

Leadership: The crisis team should be activated immediately to manage operations, ensure compliance, and maintain continuity. Leadership must coordinate decision-making and support recovery actions. During a crisis, management must consider the personnel's operational capacity, including their psychological well-being, by demonstrating support and understanding and by maintaining a visible presence. Leadership should take responsibility and remain visibly engaged with external stakeholders.

Communications: Communication should be timely, accurate and consistent across channels. Employees should be informed first, and designated spokespersons should deliver messages supported with prepared materials. Backup channels should be used if primary systems are compromised. Communication coordination networks must be activated, and the flow of information between them must be ensured. The communications function must have access to an up-to-date operational situational picture.

Situational awareness: Organizations must identify the attack type, scope and impact quickly, update the situational picture continuously, and share it with relevant audiences. Monitoring internal and external impacts and supporting leadership decisions are critical. The flow of situational awareness information must be ensured between all actors and organizations involved in the situation.

After the crisis

Leadership: Assess the impact on operations and stakeholders, implement recovery measures, and document lessons learned for future preparedness. Attention should be given to restoring normal operations and supporting staff in the recovery process. Senior management must engage in active stakeholder communication.

Communication: Post-crisis communication should demonstrate accountability and inform stakeholders about actions taken. As the situation is clarified and the investigation progresses, the instructions are refined as needed. Sharing communication lessons learned internally and externally supports resilience.

Situational awareness: Continue monitoring direct and indirect impacts. Analyse the incident to compile lessons learned and improve future situational awareness processes.

7. Conclusion

Cyberattacks disrupt organisations' operations, decision-making, and communication. Interviews across sectors and attack types revealed consistent themes: managing uncertainty, addressing fear, communicating with incomplete information, safeguarding continuity, and protecting intangible assets such as reputation and trust. As highlighted in the interviews, victims' and customers' perspectives must be considered, and guidance should be clear, practical, and action-oriented. Irrespective of the attack type, customers and other external stakeholders consistently expressed concern that sensitive data might fall into the hands of attackers.

According to the interviews, it was notable that, regardless of attack type, the same kinds of concerns consistently emerged. This suggests that variations in attack modalities did not significantly alter the core requirements for crisis communication. Across contexts and cases, the fundamental communication practices remained largely the same. We took this observation into account when developing our framework: the general principles we identified are applicable across different types of cyberattacks.

Our findings extend the framework proposed by Knight and Nurse (2020) by specifying a distinct post-crisis phase in which communication continues to play a central role: providing updates, supporting those affected, rebuilding trust, and strengthening resilience. Investing in post-crisis communication is essential, as it plays a vital role in ensuring organisational continuity, recovery, and the long-term restoration of reputation and trust. Employees also emerged as a distinct audience requiring focused attention in preparedness and in every crisis phase.

Interviews highlighted that cyber crises place heavy demands on managers, requiring situational leadership in fast-changing conditions. Communication was seen as a crucial enabler, with supervisors playing a key role as the closest link to employees and the frontline. Overall, the interviews underscored that communication is a core leadership task in cyber crises: open, empathetic, two-way dialogue sustains trust, reduces uncertainty, supports wellbeing, and strengthens organisational resilience.

Based on the interviews, cyber crisis communication can be summarized into the three "no-L principles": do not lessen, do not lie, and do not linger. The idea is that in a crisis situation, an organization must be honest, direct, and timely, without trying to downplay or hide the problem. This builds trust and enhances the organization's ability to manage and recover from the crisis more effectively.

AI declaration: Generative AI was utilized to improve the clarity and language of the text. Following this, the author thoroughly reviewed and revised the content to ensure its accuracy, taking full responsibility for the final version.

Ethics declaration: The ethical guidelines of the University of Jyväskylä were followed throughout the study.

References

Agrafiotis, I. et al. (2018) 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*, 4(1), p. tyy006. Available at: https://doi.org/10.1093/cybsec/tyy006.

Backman, S. (2020) 'Conceptualizing cyber crises', *Journal of Contingencies and Crisis Management*, 29. Available at: https://doi.org/10.1111/1468-5973.12347.

Bentley, J.M. and Ma, L. (2020) 'Testing perceptions of organizational apologies after a data breach crisis', *Public Relations Review*, 46(5), p. 101975. Available at: https://doi.org/10.1016/j.pubrev.2020.101975.

Berg, B. van den and Kuipers, S. (2022) 'Vulnerabilities and cyberspace: A new kind of crises', in *Oxford Research Encyclopedia of Politics*. Available at: https://doi.org/10.1093/acrefore/9780190228637.013.1604.

Calder, A. (2023) *Cyber resilience: Defence-in-depth principles*. First edition. Ely: ITGP. Available at: https://research.ebsco.com/linkprocessor/plink?id=fbb74d3d-f862-37b2-8a4c-e319d5b5bbbd (Accessed: 9 September 2025).

Canel, M.-J., Luoma-aho, V. and Barandiarán, X. (2020) 'Public sector communication and publicly valuable intangible assets', in *The Handbook of Public Sector Communication* (eds V. Luoma-aho and M.-J. Canel). https://doi.org/10.1002/9781119263203.ch6

Chaudhary, S., Gkioulos, V. and Katsikas, S. (2022) 'Developing metrics to assess the effectiveness of cybersecurity awareness program', *Journal of Cybersecurity*, 8(1), tyac006. Available at: https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603

Chong, D. and Druckman, J. N. (2007) 'Framing theory', *Annual Review of Political Science*, 10, pp. 103–126. Available at: https://fbaum.unc.edu/teaching/articles/Chong-Druckman-FramingTheory.pdf

Coombs, W.T. (2007) 'Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory', Corporate Reputation Review, 10(3), pp. 163–176. Available at: https://doi.org/10.1057/palgrave.crr.1550049.

Coombs, W.T., Holladay, S.J. and White, C.L. (2020) The Handbook of Crisis Communication. 2nd edn. Wiley-Blackwell.

Coombs, W.T. and Holladay, S.J., 2022. 'Crisis communication as strategic communication: Process and insights', in J. Falkheimer and M. Heide (eds.) *Research handbook on strategic communication*. Cheltenham: Edward Elgar, pp. 259–273. doi:10.4337/9781800379893.00025

Desa, J.M., Juremi, J. and Jenalis, M.H. (2025) 'Understanding cyber threat actors: A review on classification, motivations, and behavioral profiling', in V. Bhateja et al. (eds.) *Innovations in communication networks: sustainability for societal and industrial impact*. Singapore: Springer Nature, pp. 23–30. Available at: https://doi.org/10.1007/978-981-96-5223-5_3.

Entman, R.M. and Usher, N. (2018) 'Framing in a fractured democracy: Impacts of digital technology on ideology, power and cascading network activation', *Journal of Communication*, 68(2), pp. 298–308. Available at: doi: 10.1093/joc/jqx019.

Europol (2025) *Steal, deal and repeat – How cybercriminals trade and exploit your data: Internet Organised Crime Threat Assessment (IOCTA) 2025*. Luxembourg: Publications Office of the European Union. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

Falkheimer, J. and Heide, M. (2010) 'Crisis communicators in Change: From plans to improvisations', in *The handbook of crisis communication*. John Wiley & Sons, Ltd, pp. 511–526. Available at: https://doi.org/10.1002/9781444314885.ch25.

Fujs, D., Mihelič, A. and Vrhovec, S.L.R. (2019) 'The power of interpretation: Qualitative methods in cybersecurity research', in Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19: 14th International Conference on Availability, Reliability and Security, Canterbury CA United Kingdom: ACM, pp. 1–10. Available at: https://doi.org/10.1145/3339252.3341479.

Gwebu, K.L., Wang, J. and Wang, L. (2018) 'The role of corporate reputation and crisis response strategies in data breach management', *Journal of Management Information Systems*, 35(2), pp. 683–714. Available at: https://doi.org/10.1080/07421222.2018.1451962.

Hancock, J.T., Naaman, M. and Levy, K. (2020). 'AI-mediated communication: Definition, research agenda, and ethical considerations', *Journal of Computer-Mediated Communication*, 25(1), 89–100.

Hytönen, E. and Ruoslahti, H. (2025) 'Crisis communication guidelines to support cyber resilience', *European Conference on Cyber Warfare and Security*, 24, pp. 222–229. Available at: https://doi.org/10.34190/eccws.24.1.3730.

Johansson, S., Johansson, B. and Johansson, J. (2024) 'The dynamics of information-seeking repertoires: A cross-sectional latent class analysis of information-seeking during the COVID-19 pandemic', *Mass Communication and Society*, 27(4), pp. 599–626. Available at: https://doi.org/10.1080/15205436.2023.2258863.

Joinson, A.N. et al. (2023) 'Development of a new "human cyber-resilience scale"', *Journal of Cybersecurity*, 9(1), p. tyad007. Available at: https://doi.org/10.1093/cybsec/tyad007.

Khan, W.N., Lee, J.K. and Liu, S. (2025) 'Is cybersecurity a social responsibility?', *Information Systems Frontiers*, 27(4), pp. 1367–1391. Available at: https://doi.org/10.1007/s10796-024-10565-z.

Kleeman, J. (2026) *A faceless hacker stole my therapy notes – now my deepest secrets are online forever*. BBC. Available at: https://www.bbc.com/news/articles/c62nzxqw45eo

Knight, R. and Nurse, J. (2020) 'A framework for effective corporate communication after cyber security incidents', *Computers & Security*, 99. Available at: https://doi.org/10.1016/j.cose.2020.102036.

Lallie, H.S. et al. (2021) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Computers & Security*, 105, p. 102248. Available at: https://doi.org/10.1016/j.cose.2021.102248.

Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Reports*, 7. Available at: https://doi.org/10.1016/j.egyr.2021.08.126.

Lilli, E. (2023) 'How can we know what we think we know about cyber operations?', *Journal of Global Security Studies*, 8(2), p. ogad011. Available at: https://doi.org/10.1093/jogss/ogad011.

Meer, van der T.G.L.A. (2018) 'Public frame building: The role of source usage in times of crisis', *Communication Research*, 45(6), pp. 956–981. Available at: https://doi.org/10.1177/0093650216644027.

Miller, K. and Pearlson, K. (2024) 'How to build a cyber crisis communications plan', *MIT Sloan Management Review*, 16 September. Available at: https://sloanreview.mit.edu/article/how-to-build-a-cyber-crisis-communications-plan/

Nelson, A. et al. (2025) 'Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile', *NIST Special Publication* (SP) 800-61 Rev. 3. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-61r3.

Perera, S., Jin, X. and Opoku, D-G. J. (2022) 'Factors affecting reputational damage to organisations due to cyberattacks', *Informatics*, 9(1), 28. Available at: https://www.mdpi.com/2227-9709/9/1/28

Poliisi (2020) Tietomurron tutkinta jatkuu – poliisi toivoo harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Available at: https://poliisi.fi/-/tietomurron-tutkinta-jatkuu-poliisi-toivoo-harkintaa-asiaan-liittyvien-yksityiskohtien-julkaisemisessa-1

Prime Minister's Office (2020) *Guidelines for enhanced government communications: Communications under normal conditions and during incidents*. Publications of the Prime Minister's Office 2020:9. Available at: https://julkaisut.valtioneuvosto.fi/items/735b999e-5579-466b-819d-435794dde21c

Rosati, P. et al. (2017) 'The effect of data breach announcements beyond the stock price: Empirical evidence on market activity', *International Review of Financial Analysis*, 49, pp. 146–154. Available at: https://doi.org/10.1016/j.irfa.2017.01.001

Roulet, T.J. and Clemente, M. (2018) Let's open the media's black box: The media as a set of heterogeneous actors and not only as a homogenous ensemble. *Academy of Management Review*. doi:10.5465/amr.2016.0537

Russell Neuman, W. et al. (2014) 'The dynamics of public attention: Agenda-setting theory meets big data: Dynamics of public attention', *Journal of Communication*, 64(2), pp. 193–214. Available at: https://doi.org/10.1111/jcom.12088

Sellnow, T.L. and Seeger, M.W. (2021) Theorizing crisis communication. John Wiley & Sons.

Shandler, R. and Gomez, M.A. (2023) 'The hidden threat of cyber-attacks – undermining public confidence in government', *Journal of Information Technology & Politics*, 20(4), pp. 359–374. Available at: https://doi.org/10.1080/19331681.2022.2112796

Siegrist, M., Gutscher, H. & Keller, C. (2010) 'Trust and Confidence in Crisis Communication: Three Case Studies', in Earle, T.C. & Gutscher, H. (eds.) Trust and Confidence in Risk Communication. United Kingdom: Taylor & Francis Group. Available at:

Snider, K. L. G., Shandler, R., Zandani, S. and Canetti, D. (2021) Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1), tyab019. Available at: https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745

Thomas, D.R. (2006) 'A general inductive approach for analyzing qualitative evaluation data', *American Journal of Evaluation*, 27(2), pp. 237–246. Available at: https://doi.org/10.1177/1098214005283748.

Traficom (2025) Miten viestiä kyberhyökkäyksistä? – kriisiviestintäohje organisaatioille. Traficom. Available at: https://traficom.fi/fi/julkaisut/miten-viestia-kyberhyokkayksista-kriisiviestintaohje-organisaatioille

Traficom and Supo (2025) *Cyber security threat level remains high – serious cases on the rise*. Available at: https://www.kyberturvallisuuskeskus.fi/en/news/traficom-and-supo-cyber-security-threat-level-remains-high-serious-cases-rise

Triplett, W.J. (2022) 'Addressing human factors in cybersecurity leadership', *Journal of Cybersecurity and Privacy*, 2(3), pp. 573–586. Available at: https://doi.org/10.3390/jcp2030029.

Turvallisuuskomitea (2025) Yhteiskunnan turvallisuusstrategia. Available at: https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Tuomi, J. and Sarajärvi, A. (2018) Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi.

Tzavara, V. and Vassiliadis, S. (2024) 'Tracing the evolution of cyber resilience: A historical and conceptual review', *International Journal of Information Security*, 23, pp. 1–25. Available at: https://doi.org/10.1007/s10207-023-00811-x.

Valtioneuvoston kanslia (2023) Kriisitilanteita koskevan kansalaisviestinnän kehittäminen: Työryhmän loppuraportti. Valtioneuvoston kanslian julkaisuja 2023:1. Available at: https://julkaisut.valtioneuvosto.fi/items/7bfd752c-ea0f-43ed-b94f-574e08733ef9

Wanless, A. and Pamment, J. (2019) 'How do you define a problem like influence?', *Journal of Information Warfare*, 18(3), pp. 1–14. Available at: https://www.jinfowar.com/journal-issue/volume-18-issue-3

White, C. (2009) 'Examining a crisis communication void: The role of context to mitigate issues', *Journal of Communication Management*, 13(2), pp. 176–190. Available at: https://doi.org/10.1108/13632540910951777.

Woon, E. and Pang, A. (2017) 'Explicating the information vacuum: Stages, intensifications, and implications', *Corporate Communications: An International Journal*, 22(3), pp. 329–353. Available at: https://doi.org/10.1108/CCIJ-10-2016-0066.

Zhang, Q. and Zhang, X. (2024) 'Media influence on public trust during crises: A comparative analysis of different media types and trust dimensions', *Journal of Contingencies and Crisis Management*, 32(3), p. e12624. Available at: https://doi.org/10.1111/1468-5973.12624.

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. Available at: https://doi.org/10.1080/13669877.2019.1646315