PROCEEDINGS OF THE INTERNATIONAL
CRISIS AND RISK COMMUNICATION CONFERENCE
MARCH 10-12, 2025. CLEMSON SC, USA

Cyber Crisis Readiness Unpacked: A Qualitative Exploration of Organizational Approaches and Mindsets

Albena Björck

ZHAW School of Management and Law
Winterthur, Switzerland

Carlo Pugnetti

HSLU Institute of Financial Services Zug
Rotkreuz, Switzerland

Béatrice Vogel

ZHAW School of Management and Law
Winterthur, Switzerland

Marco Lopez

ZHAW School of Management and Law
Winterthur, Switzerland

Abstract: The study qualitatively explores the complex nature of cyber crisis readiness and proposes strategies to develop and sustain it in organizations. Using a qualitative research approach, the authors conducted in-depth semi-structured interviews with cybersecurity experts and managers across five industries in Switzerland, ranging from telecommunications to insurance. Our findings demonstrate the importance of a structured preparedness, proactive prevention, and adaptive foresight to promote vigilance, continuous learning, and proactive cybersecurity measures. They point out to specific challenges in the cyber context such as resource constraints, collaborative approaches to prevention, and the nuanced role of leadership in cultivating a foresight mindset. To our knowledge this is the first study to explore cyber crisis readiness and the process to achieve it.

Keywords — collaborative crisis management, crisis readiness, cyber preparedness, leadership mindset

---

SUGGESTED CITATION: Björck, A., Pugnetti, C., Vogel, B., Lopez M. (2025). Cyber crisis readiness unpacked: A qualitative exploration of organizational approaches and mindsets. *Proceedings of the 2025 International Crisis and Risk Communication Conference, 13(*1) 39-42. https://www.doi.org/10.69931/001c.142836

INTRODUCTION

Cyber crises represent a distinct and complex category of threats that can undermine the foundations of our digitalized economic systems, necessitating a strategic and informed response [1, 2]. Due to their complexity and extensive impact across various domains, cyber crises pose significant challenges to traditional crisis management strategies [3]. According to Prevezianou [4] cyber crises extend beyond the capacity of standard incident management. Originating from vulnerabilities in cyberspace, they often remain undetected, crossing territorial, sectoral, and temporal boundaries.

ISSN: 3068-6539
© 2025 Copyright is held by the owner/author(s).
Publication rights are licensed to ICRCA.
https://doi.org/10.69931/001c.142836

While the broader concept of crisis readiness is relatively nascent, the exploration into organizational cyber readiness is even less developed. This paper defines cyber readiness as a strategic capability based on systemic preparedness, proactive and collaborative prevention and an adaptative mindset fostered by emotional and hybrid leadership. Furthermore, the paper illuminates the critical role of crisis management and communication as well as cyber leadership.

THEORETICAL FRAMEWORK

The concept of crisis readiness extends existing crisis management frameworks such as preparedness and introduces a novel proactive approach. Jin et al. [5] see crisis readiness as a multidimensional construct with three pillars at its core: multilevel efficacity, mindset and dynamic process. The mindset pillar highlights the psychological readiness and proactive attitude required for leaders and teams to engage effectively in crisis management, emphasizing the importance of emotional leadership and mental adaptability. Multi-level efficacy builds on this by developing confidence and capability at the individual, team, and organizational levels, ensuring that efficacy at one level reinforces efficacy at others, thereby enhancing the organization's overall crisis response capability. The dynamic process pillar focuses on the flexibility and adaptability of crisis management strategies, promoting agile responses that can adapt as situations evolve and new threats arise [5].

In a recent review research Björck et al. [6] further elaborated on the boundaries of the crisis readiness concept by introducing three process-oriented building blocks: crisis preparedness, crisis prevention and foresight mindset. Achieving and sustaining crisis readiness is an overarching organizational capability that is developed and close the circle of crisis management – before, during, and after a crisis. Building on these insights, Björck et al. [6] developed a strategic process to achieve crisis readiness. This model comprises ten interdependent steps that guide companies toward crisis readiness when implemented sequentially [6]. The model incorporates several elements of crisis management, and it highlights additional practices as crucial for fostering the foresight mindset already mentioned by Jin et al. [5].

As technology evolves, cyber crises have emerged as a unique challenge that traditional crisis management strategies struggle to address. De Vittoris [1] defines a cyber crisis as a distinct organizational crisis marked by greater opacity, immediacy, and complexity, severely impacting digital domains. Backman [3] classifies cyber crises as transboundary, transcending political and temporal boundaries to escalate rapidly, spread across jurisdictions, and impact various sectors and infrastructures. These crises challenge conventional management approaches due to their complexity and broad, cross-domain effects. Prevezianou [4] highlights that cyber crises often surpass standard incident management capacities, triggering simultaneous emergencies and undermining public trust in institutions when they surge into political prominence.

Effective cyber crisis management demands specialized practices tailored to the digital landscape, requiring crisis readiness to adapt to cyber-specific scenarios. Traditionally defined within a military framework, cyber readiness refers to a country's preparedness to counteract cyberattacks. At the organizational level, Neri et al. [7] highlight the importance of cybersecurity awareness, culture, and resilience. Unlike national readiness, supported by centralized resources, organizational readiness must address resource constraints and adopt a culturally integrated approach to cybersecurity. While technical defenses are vital, human factors such as education, policy awareness, and a proactive security culture are equally critical for effective organizational responses to cyber threats [7].

METHODS

This study uses an exploratory qualitative methodology to examine organizational cyber readiness, leveraging qualitative research to explore complex phenomena like cyber crises and leadership dynamics [8]. Given the limited research on cyber readiness, an exploratory approach is crucial [8].

Our research is based on 13 in-depth, individual, semi-structured interviews with seven Chief Information Security Officers (CISO), two IT Heads, one CEO, two cybersecurity consultants and one head of Risk, Governance and Audit. Participants represented 13 companies across five sectors, including Information and Communication, Financial and Insurance, and Education, primarily based in Switzerland (11 out of 13). Organization sizes ranged from one small company (<49 employees) to ten medium (>250 employees) and two large (>5,000 employees). To ensure confidentiality, pseudonyms were assigned to participants, and organizations were anonymized.

RESULTS

The analysis of the interview data identified 20 codes, grouped into eight key themes: cybersecurity preparedness, training and awareness, actor's responsibility and leadership, cyber culture, integration with strategy, crisis communication, external stakeholders, and post-crisis learnings.

While the results show commonalities in these eight key themes, the 13 interviews also highlight differences in resource allocations, process formalization, leadership roles and embedding a cyber culture. Some examples of contextual differences are mentioned hereafter for five key themes.

1. In terms of *cybersecurity preparedness*, all participants recognized the necessity of proactive planning to handle cyber threats effectively. While small organizations often focus on basic checks and in-house monitoring, using internal

algorithms to detect anomalies, they lack external testing or simulations. On the other hand, larger organizations adopt more comprehensive approaches, involving external partners for realistic scenarios such as white-hat penetration tests.

2. *Awareness training* is essential for equipping employees with the knowledge and skills to effectively handle cyber threats. Training can take several forms depending on the goals the organization wants to achieve and the targeted audience. Larger companies invest in formal training through external providers, particularly for IT staff and those in security roles. In contrast, smaller firms rely on informal methods such as team discussions and resources like the specialized podcast.

3. When looking at *actors' responsibility and leadership*, our sample shows that cybersecurity roles were defined at various levels of responsibility, with crisis management structures emphasizing leadership during incidents. In smaller teams, shared responsibilities were common, with leaders like the CEO directly reassuring employees and leading during crises – visible approach suited to resource-limited settings. Larger organizations distributed leadership across structured teams, such as a crisis cell, where an incident manager oversaw responses and reported to leadership. Furthermore, increased frequency of discussions about cybersecurity at the board level reflects a shift in understanding its significance within the corporate governance framework.

4. Enhancing the *cyber culture* within companies is paramount to fostering a proactive and prepared organizational environment, rather than one that merely reacts to incidents as they occur. Small companies leveraged intrinsic motivation and close team dynamics within a startup culture, naturally fostering collaboration with minimal formal efforts. However, their limited resources hindered the spread of a cybersecurity-first mindset across functions. In contrast, larger firms relied on formal programs to build awareness and accountability. For example, one company integrated cyber-awareness into organizational communication, including C-level meetings. Aligning departments with differing priorities required significant effort to overcome silos.

5. *Integrating cybersecurity into strategic management* creates a holistic approach to readiness, embedding it as a core element of business operations rather than an afterthought. This alignment ensures cybersecurity initiatives support business objectives and are seamlessly integrated into operational and strategic frameworks. Larger firms historically prioritized and invested in cybersecurity, while smaller companies saw it as less critical due to funding constraints. However, this is changing, as medium-sized enterprises face growing security incidents they are unprepared to handle, exposing significant maturity and capability gaps.

DISCUSSION AND CONCLUSION

To define cyber readiness, we compared our findings with the three pillars outlined by Björck et al. (2024). While both emphasize structured preparedness, proactive prevention, and adaptive foresight, key differences emerged, particularly regarding resource gaps in smaller firms, collaborative prevention approaches, and leadership's role in fostering foresight. Our study contributes to the emerging discourse on cyber crisis readiness by offering a nuanced understanding of how organizations in various contexts design and cultivate cyber readiness. Our findings illustrate that cyber readiness is not a static capability, but a dynamic, adaptive process shaped by resources availability, organizational culture, and leadership ethos.

A central insight is the critical role of leadership – not only in responding to cyber threats but in fostering a mindset of anticipation and learning. Emotional intelligence, visibility, and distributed leadership structures emerged as key enablers of cyber resilience, especially in environments where formal processes are less developed. While larger firms benefit from structured programs and dedicated crisis management infrastructures, smaller organizations demonstrate that agility, intrinsic motivation, and team cohesion can also form effective foundations for readiness, albeit with limitations in scalability and formalization.

Furthermore, our research extends the conceptualization of cyber crisis prevention beyond internal risk controls. A novel, ecosystem-level approach encourages inter-organizational exchanges to address shared cyber risks. Unlike traditional internal-focused frameworks, cyber threats necessitate collaboration, such as industry-wide forums and partnerships. Such ecosystems of collaboration represent a shift toward a more collective, proactive, and systemic approach to managing cyber threats – an evolution that traditional siloed models of crisis prevention may struggle to accommodate.

In the field of cyber preparedness, our research confirms the importance of practical, systematic strategies like crisis management plans, training, scenario planning, and awareness exercises. However, the fast-evolving nature of cyber crises complicates cost estimation for preparedness, posing challenges. Neglected in the literature is the need for cutting-edge infrastructure combined with high preparation standards, highlighting flexibility and improvisation as compensatory strategies.

In defining the characteristics of cyber readiness – preparedness, prevention, and mindset – our research confirms the multidimensionality of the construct and support the extension of traditional crisis readiness frameworks to digital contexts. Particularly noteworthy are the overlooked but vital aspects of infrastructure readiness, organizational improvisation, and the integration of cybersecurity with strategic business objectives.

While this study provides valuable empirical insights, its findings are contextually bounded and of limited generalizability. Most participating organizations are based in Switzerland and represent specific industries. Future research could benefit from broader geographic and sectoral comparisons to test the generalizability of our findings. Moreover, longitudinal studies could trace the evolution of readiness practices over time, especially in response to major cyber inci-

dents. Another promising avenue for future research is the deeper exploration of the cultural and psychological dimensions of cyber readiness. As our study shows, mindset and motivation are as critical as technological investments – yet these human factors remain underexplored in both academic and practitioner literature.

Cyber readiness is increasingly becoming a strategic imperative rather than a technical-only pre-condition. Organizations must go beyond reactive postures and instead develop integrated, anticipatory approaches to cybersecurity. By articulating the interconnected roles of process, leadership, and mindset, this study offers a foundation for more adaptive and resilient organizational responses to the fast-evolving cyber threat landscape.

Author Biography

Dr. Albena Björck, Dr. oec., University of St. Gallen (Switzerland), currently working at the Zurich University of Applied Sciences, School of Management and Law (Switzerland), bjoe@zhaw.ch.

Dr. Carlo Pugnetti, PhD Stanford University (USA), currently working at the Lucerne School of Business, Institute of Financial Services Zug (Switzerland).

Béatrice Vogel, MSc International Business, Zurich University of Applied Sciences, currently working at the Zurich University of Applied Sciences, School of Management and Law (Switzerland).

Marco Lopez, MSc International Business, Zurich University of Applied Sciences, currently working at Corsano Health (Switzerland).

REFERENCES

[1] de Vittoris, R. (2022). La gestion de crise cyber et classique, entre similitudes et divergences. *UCA.HAL.Science*. https://uca.hal.science/hal-03879148/document

[2] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), Article 15. https://doi.org/10.3390/s23156666

[3] Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

[4] Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards & Crisis in Public Policy, 12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

[5] Jin, Y., Shivers, B. N., Wang, Y., Coombs, W. T., & Van Der Meer, T. G. L. A. (2024). READINESS as a new framework for crisis management: Academic-industry integrated expert insights from practitioners and scholars. *Journal of Communication Management*. https://doi.org/10.1108/JCOM-02-2024-0034

[6] Björck, A., Bläse, R., & Bastida, P. (2024). Becoming crisis-ready: A systematic literature review on corporate crisis readiness and the process to achieving it. *Journal of Contingencies and Crisis Management*, *32*(3), e12614. https://doi.org/10.1111/1468-5973.12614

[7] Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information & Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

[8] Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed). New Age International (P) Ltd., Publishers.