

Cyber Crisis Readiness: How Collective Internalization Emerges Through Interactive Communication

Béatrice Vogel

ZHAW School of Management and Law
Winterthur, Switzerland

Albena Björck

ZHAW School of Management and Law
Winterthur, Switzerland

Carlo Pugnetti

HSLU Institute of Financial Services Zug
Rotkreuz, Switzerland

Abstract: This experimental study explores how employee-focused interventions can enhance organizational cyber readiness amid rising digital risks. Despite strong technological defenses, human behavior remains a key vulnerability, making cybersecurity culture essential. Using the IDEA Model (Internalization, Distribution, Explanation, Action), four interactive workshops were conducted with 70 employees in a Swiss insurance company to address responsibility and fallibility in cyber risk behavior. Findings show that emotional engagement – such as curiosity and concern – combined with collaborative exercises and peer influence significantly increased awareness and strengthened behavioral intentions. These results highlight the effectiveness of interactive, socially driven risk communication over traditional passive approaches, demonstrating how emotional and collective processes can bridge the gap between knowledge and action and improve both individual and organizational cyber crisis readiness.

Keywords — collaborative crisis management; collective internalization; crisis readiness

SUGGESTED CITATION: Vogel, B., Björck, A., & Pugnetti, C. (2026). Cyber Crisis Readiness: How Collective Internalization Emerges Through Interactive Communication. *Proceedings of the International Crisis and Risk Communication Conference, USA, 14(1)*. <https://www.doi.org/10.69931/001c.164603>

INTRODUCTION

According to *PwC's 29th Global CEO Survey*, Chief Executive Officers (CEOs) have expressed growing concern regarding a range of near-term threats, including macroeconomic volatility, geopolitical conflict, and cyber risk, with the latter emerging as one of the most salient challenges facing firms [1]. About a third of CEOs report that their organizations face a high or very high exposure to the risk of significant financial losses resulting from cyber threats within the forthcoming year. As a response, a large majority of CEOs are prioritizing improvements in enterprise-wide cybersecurity practices to mitigate these escalating threats [1].

Despite these efforts, cybersecurity remains critically influenced by human behavior. Employees often constitute the primary entry point for attacks such as phishing and social engineering, making their perceptions and responses to cyber risks a key determinant of organizational cyber readiness. This highlights the need to move beyond generic training approaches toward interventions that more effectively influence risk perception and behavior [2].

This study examines how interactive risk communication and activation mechanisms – specifically those incorporating emotional engagement and peer interaction – affect employees' cybersecurity awareness, behavioral intentions, and internalization of responsibility toward cyber risks within a high-risk organizational context.

ISSN: 3068-6539

© 2026 Copyright is held by the owner/author(s).

Publication rights are licensed to ICRCA.

<https://doi.org/10.69931/001c.164603>

LITERATURE REVIEW

CYBER RISKS

Cyber risks represent a dynamic and evolving threat to organizations, driven by increasing digitalization and the expanding attack surface of information systems. While cyberattacks have been a long concern, advances in artificial intelligence (AI) have reshaped this landscape. AI has strengthened organizational capabilities in cyber defense and threat detection, but it has also been leveraged by adversaries to enhance the sophistication and effectiveness of their tactics and malicious campaigns [3].

Recent research has increasingly framed cyber risks not only as technical or operational issues, but also as organizational crisis readiness challenges. Björck et al. [4] conceptualize crisis readiness as an organization's capability to anticipate, prevent, respond to, and learn from crises through the integration of leadership, communication, culture, and adaptive organizational processes. Their framework emphasizes that readiness is not solely dependent on formal procedures or technical safeguards, but also on the organization's ability to foster shared understanding, collaboration, and proactive behavioral norms across all levels. Building on this perspective, Björck et al. [5] apply the crisis readiness framework to the cyber context, providing empirical insights into how organizations understand and operationalize cyber crisis readiness in practice. Their findings highlight the importance of leadership in cultivating adaptive and inclusive cultures that support collective responsibility, learning, and readiness in the face of cyber threats.

BEHAVIORAL VULNERABILITIES

Although technological defenses remain essential, they are insufficient on their own, as a significant proportion of cyber incidents originate from human error and everyday employee actions [6]. Behavioral vulnerabilities – such as susceptibility to phishing, weak security practices, or lack of vigilance – are frequently exploited by attackers, underscoring the importance of user behavior in cybersecurity outcomes [2].

These vulnerabilities are shaped by underlying attitudes, perceptions, and cognitive biases. Research indicates that knowledge alone does not guarantee secure behavior; rather, employees' internalized beliefs, motivation, and perceived responsibility play a decisive role [7]. Consequently, generic and normative training approaches often fail to produce lasting behavioral change [8]. More effective strategies require diagnosing these underlying attitudes and delivering targeted, context-specific interventions that align with employees' mental models and everyday work practices.

Pugnetti et al. [2] extend this perspective by proposing a diagnostic approach that combines deep metaphor interviews with the IDEA risk communication model [9] to identify and operationalize behavioral cyber risks in organizational settings [2]. Their findings demonstrate a link between diagnosed employee attitudes and effective cyber risk behavior, highlighting the value of integrating behavioral diagnostics into cyber risk management practices.

IDEA MODEL

In this context, the IDEA model (Internalization, Distribution, Explanation, Action) provides a structured framework for designing communication that supports behavioral change [9]. By emphasizing personal relevance (internalization), clear and credible information (explanation), appropriate communication channels (distribution), and actionable guidance (action), the model supports the design of messages that not only inform but also motivate behavioral change. Applying such an approach enables organizations to translate risk awareness into concrete, risk-averse actions, thereby mitigating behavioral vulnerabilities and strengthening overall cybersecurity.

METHODS

Building on prior research on diagnosing and mitigating behavioral cyber risks (hereafter referenced as phase one [2]), this study was conducted within two organizational units of a Swiss insurance company. The selected organization provides a relevant high-risk context due to its access to sensitive personal and financial data, as well as the presence of operational units – such as a customer assistance call center – that require frequent, real-time handling of confidential information, thereby increasing exposure to cyber threats and human-related vulnerabilities.

The experimental design comprises two workshop-based interventions. The first intervention, consisting of three workshops with a total of 55 participants, addressed how employees have a responsibility to protect the organization from cyberattacks. The topic was selected based on the responses of phase one of the project, as one of the most important attitudes correlating risk behavior. The second intervention, with 15 participants, focused on the theme of making mistakes in the cyber context.

All workshops followed the same structure. Participants were first introduced to the results of phase one of the project, followed by a brief Q&A session. They were then divided into four groups; each assigned a specific statement or a question for discussion. Groups recorded their key insights on flip charts, which were subsequently presented in plenary. Participants voted on the two most important insights, and the workshop concluded with a summary of results and a final feedback round. Each session lasted approximately one hour.

The workshop design was guided by the IDEA model. The introductory presentation addressed the current internalization of cyber risks (I), while the group activities aimed to explain the risk in a relevant manner (E), or activate employees for the correct behavior (A). The workshop format itself provided the distribution element of the model (D).

Following the interventions, both risk attitude and risk behavior were measured and tested using a phishing campaign centered on Black Friday offers. This scenario was selected due to its seasonal relevance and the effectiveness of similar interventions during phase one of the study. The outcomes of the phishing campaign were subsequently compared between workshop participants and non-participating employees to evaluate whether the interventions influenced cybersecurity-related attitudes and behavioral responses.

RESULTS

The preliminary results indicate that structuring the workshops along the IDEA model enabled a progression from emotional engagement to collectively articulated behavioral intentions. In the internalization (I) phase, participants expressed curiosity, concern, and, in some cases, apprehension – emotions that are critical as they make cyber risks personally salient and motivate engagement. These emotional responses were further amplified through the distribution (D) phase, where interactive formats encouraged peer exchange and collective sense-making. Observing colleagues reflect on and discuss risks fostered social reinforcement, strengthening individual awareness and responsibility. The explanation (E) and action (A) phases translated these reflections into shared insights and prioritized behaviors, as captured through the voting exercises. This dynamic illustrates how emotionally engaging and socially embedded communication can overcome the limitations of traditional, passive cybersecurity training approaches. This tendency was further reflected in the phishing campaign results, where workshop participants generally demonstrated lower rates of unreported phishing attempts compared with non-participating employees, suggesting a positive influence on cybersecurity-related behavioral responses.

In the first intervention, this progression is clearly reflected in the convergence of participant votes around concrete, action-oriented themes. The participants put the emphasis on proactively reporting suspicious activities to IT security, maintaining vigilance, recognizing cybersecurity as a shared responsibility, and understanding the risks inherent in every digital interaction reflects a strong awareness that cyber threats are pervasive and not fully mitigated by technical defenses alone. At the same time, the voting results also demonstrate how internalized risk perceptions were translated into collectively endorsed norms for action. Participants acknowledged that even routine online actions can create exploitable vulnerabilities, underscoring the need for continuous attentiveness and close collaboration with IT security functions. The prominence of reporting and vigilance suggests that the workshops successfully bridged the gap between risk awareness generated through explanation (E) and intended behavior (A), reinforced through group validation.

Similarly, the second intervention highlighted how the IDEA-based framing surfaced both organizational pressures and emotional barriers in shaping cybersecurity behavior. Discussions among participants around fear of making mistakes and the perceived severity of even minor errors point to strong internalization (I). Notably, the discussions revealed a relatively high level of anxiety making mistakes, coupled with the insight that increased awareness can help mitigate this fear. Through collective reflection and explanation (E), participants identified time pressure as a primary driver of mistakes, pointing to the tension between operational efficiency and security compliance. The voting results – emphasizing the exploitability of small mistakes and the importance of rapid response to limit potential damage – demonstrate how these insights were translated into actionable priorities. While formal guidelines were not explicitly emphasized, their implicit presence suggests either familiarity or limited salience in daily practice. Overall, these findings underline the importance of addressing both structural and emotional factors to enhance cyber readiness.

DISCUSSION

Emotional engagement and supportive group interaction have been shown to play a critical role in strengthening awareness and shaping behavioral intentions toward cyber risk mitigation. By fostering active participation, shared reflection, and collective sense-making, the workshops enabled individuals to internalize cyber risks more effectively and translate this understanding into actionable behaviors. Emotions such as concern, vigilance, and apprehension contributed to making cyber risks personally relevant, thereby reinforcing individual responsibility and motivating engagement beyond purely cognitive understanding. This interactive and affective dimension complements cognitive learning processes, thereby enhancing the overall impact of cybersecurity interventions.

Compared with the existing cybersecurity awareness literature, the results further suggest that the effectiveness of the intervention cannot be explained solely by emotional engagement at the individual level. A key contribution of the workshops was the collective and interactive nature of the exercises, which created opportunities for peer learning, social reinforcement, and the emergence of shared behavioral norms. Participants not only reflected on their own practices but also observed and responded to the attitudes and behaviors of colleagues. These dynamics are consistent with Social Learning Theory, which emphasizes that attitudes and behaviors are shaped through observation, social reinforcement, and interaction within groups [10]. This process appeared to strengthen collective responsibility, normalize desirable security behaviors, and create a form of informal social control in which vigilance and reporting behaviors became socially validated within the group. These findings also support recent research emphasizing that effective cyber risk mitigation depends not only on individual awareness but also on organizational culture, collaborative practices, and collective behavioral dynamics [2, 5].

These findings stand in contrast to the predominantly passive and indirect communication methods commonly

employed in cybersecurity contexts, such as standardized training modules or one-way awareness campaigns [8]. The limited effectiveness of such approaches may be attributed to their failure to engage individuals on an emotional level or to account for the social dynamics that influence behavior. Consequently, more participatory and emotionally resonant communication strategies offer a promising avenue for improving cybersecurity outcomes by addressing the cognitive, affective, and social dimensions of cyber risk awareness and behavior.

CONCLUSION

The study suggests that emotional engagement, when combined with collaborative exercises and peer interaction, significantly enhances awareness and fosters positive behavioral intentions toward cyber risk mitigation. In particular, structured risk communication approaches that integrate clear explanation, active engagement, and, crucially, interactive elements appear effective in bridging the persistent gap between knowledge and action. These results indicate that purely informational strategies are insufficient, whereas approaches that incorporate affective and social dimensions can more effectively influence behavior. By leveraging emotional resonance and group dynamics, such interventions strengthen both individual responsibility and collective preparedness, thereby contributing to improved organizational crisis readiness against cyber threats.

These findings align closely with the IDEA model and the results of previous research [5], as emotional engagement supports Internalization, interactive and peer-based formats facilitate Distribution, and structured risk communication enhances Explanation, ultimately enabling the translation of awareness into concrete Action. In this way, the workshops demonstrate how integrating all four dimensions of the model can effectively transform cognitive understanding into collectively reinforced behavioral change.

Author Biography

Dr. Alben 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).

REFERENCES

- [1] PwC. (2026, January 19). *PwC's 29th Global CEO Survey. Leading through uncertainty in the age of AI*. PwC. <https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html>
- [2] Pugnetti, C., Björck, A., Schönauer, R., & Casán, C. (2024). Towards Diagnosing and Mitigating Behavioral Cyber Risks. *Risks*, 12(7), Article 7. <https://doi.org/10.3390/risks12070116>
- [3] Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Gelei, D., Yang, L., Zhang, X., Pintor, M., Lee, W., Elovici, Y., & Biggio, B. (2023). The Threat of Offensive AI to Organizations. *Computers & Security*, 124, 103006. <https://doi.org/10.1016/j.cose.2022.103006>
- [4] 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>
- [5] Björck, A., Vogel, B., Pugnetti, C., & Lopez, M. (2025). Advancing cyber crisis readiness: context, microfoundations and the role of leadership. *Journal of Communication Management*. <https://doi.org/10.1108/jcom-01-2025-0006>
- [6] Borkovich, D. J., & Skovira, R. J. (2020). Working from Home: Cybersecurity in the Age of COVID-19. *Issues In Information Systems*, 21(4), 234–246. https://doi.org/10.48009/4_iis_2020_234-246
- [7] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- [8] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- [9] Sellnow, D. D., Lane, D. R., Sellnow, T. L., & Littlefield, R. S. (2017). The IDEA Model as a Best Practice for Effective Instructional Risk and Crisis Communication. *Communication Studies*, 68(5), 552–567. <https://doi.org/10.1080/10510974.2017.1375535>
- [10] Bandura, A. (1977) *Social Learning Theory*. Englewood Cliffs, NJ: Prentice-Hall.