Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2309–2315
https://doi.org/10.54941/ahfe1007043

Cybersecurity Standards in Critical Infrastructure Protection: A Maturity Model for Finnish SMEs

Kim Rejman[1] and Markus Sihvonen[2]

[1]IBM Finland, Helsinki, Finland
[2]University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

The protection of critical infrastructure such as energy grids, water supply systems, and transportation networks has become a central concern in national and organizational security strategies. These systems form the backbone of societal functionality, and disruptions can lead to severe economic losses, safety risks, and societal instability. As digitalization accelerates, their vulnerability to cyber threats increases, making cybersecurity standards essential for both operational resilience and strategic preparedness. This study investigates whether Finnish companies utilize cybersecurity standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework to safeguard critical infrastructure, and how their adoption influences strategic decision-making, operational practices, competence development, and stakeholder collaboration. These standards support regulatory compliance and unify practices across sectors, but their effective implementation requires leadership commitment, resources, and continuous development, especially in environments where regulation may lag technological change. The findings show that standards are widely adopted, but the extent and effectiveness vary significantly depending on organizational size, industry, and cybersecurity maturity. Larger organizations tend to integrate standards into strategic decision-making and risk management, whereas smaller firms often apply them reactively. The effectiveness of standards is highest when combined with continuous improvement, maturity assessments, and targeted training. Cybersecurity standards are not merely technical guidelines but strategic tools for leadership, planning, and culture-building. To enhance their impact, companies should integrate standards into business strategy and governance, invest in staff training and competence development, leverage expert networks and collaborative partnerships, and actively engage stakeholders, especially in sectors where cybersecurity directly affects operational continuity. This research provides actionable insights for companies, policymakers, and security professionals aiming to improve national resilience through standardized and proactive cybersecurity practices.

Keywords: Cybersecurity standards, Critical infrastructure, Cybersecurity strategy, Cyber readiness, Strategic decision-making, Risk management, Cybersecurity culture language

INTRODUCTION

Protection of critical infrastructure such as energy supply, logistics, healthcare, and payment systems has emerged as one of the most pressing societal security challenges. With increasing digitalization, these systems have become heavily reliant on technological solutions, making them vulnerable to a wide range of cyber threats. Disruptions can have serious consequences not only for individual companies but also for the functioning of society.

In Finland, a significant portion of critical infrastructure is managed by private companies, which makes corporate information security practices a vital component of national security. Information security standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide structured methodologies for risk management, threat mitigation, and continuity assurance. These standards support both internal information security efforts and external trust-building, but their effectiveness depends on executive commitment, resource allocation, and the organization's maturity level.

The research question is how Finnish companies utilize information security standards to protect their critical infrastructure. Specifically, it explores the practical challenges and benefits associated with the implementation of these standards, and how organizational characteristics such as size, industry, and information security maturity affect their application. Decision-making and practices are analysed from both strategic and operational perspectives to understand the role of standards as part of comprehensive information security efforts.

RELEVANT INFORMATION SECURITY STANDARDS

Information security standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework are well-established tools for enhancing organizational information security. Standards provide structured methodologies that support risk management and ensure internal continuity (Mäki-Maukola, 2023). Security standards improve organizational performance and competitiveness by promoting standardized practices (Podrecca et al., 2022). Information security certification is closely linked to strategic decision-making, particularly regarding financial performance and stakeholder trust (Wu et al., 2022). The adoption of these standards has been shown to improve organizational productivity, competitiveness, and resilience. However, their effectiveness depends on the underlying motivations for implementation, executive commitment, and the organization's maturity level (Barafort et al., 2017).

International approaches to critical infrastructure protection highlight the importance of multi-level collaboration and adaptability to evolving threats. The U.S. National Infrastructure Protection Plan (NIPP) emphasizes the need for coordinated national strategies and stakeholder engagement (Brem, 2015). The Swiss Critical Infrastructure Protection (CIP) model highlights the integration of risk management processes across sectors (Luskova et al., 2019). The Swedish planning context reveals blind spots in actor interaction and underscores the challenges of cross-sector collaboration (Große and Olausson, 2019).

Cyber resilience is a key component of critical infrastructure protection, referring to the ability to detect, respond to, and recover from cyberattacks (Dawson et al., 2021). The CIERA model provides a comprehensive framework for assessing resilience in critical infrastructure elements, emphasizing interdependencies and systemic vulnerabilities (Rehak et al., 2019). A dynamic resilience framework integrates prevention, control, and recovery mechanisms to enhance organizational preparedness (Labaka et al., 2015). Network-based analysis can be used to identify and prioritize vulnerabilities in complex infrastructure systems (Chopra et al., 2016). A multi-hazard resilience assessment framework for transport infrastructure highlights the importance of scenario-based risk management in evaluating critical assets (Argyroudis et al., 2020).

Sector-specific studies indicate that the application of cybersecurity standards varies significantly across industries. The NIST Cybersecurity Framework offers flexibility and adaptability, making it suitable for complex industrial environments (Al-Dhanhani et al., 2021). In the healthcare industry, existing standards often fall short in supporting leadership development and fostering a strong security culture (Glisson et al., 2015). Research gaps have been identified in this sector, particularly regarding the integration of information security practices into organizational culture and strategic leadership (Ahouanmenou et al., 2023).

In summary, information security standards are not merely technical guidelines. They can serve as strategic instruments for enhancing organizational performance, resilience, and culture. Their impact depends on the organization's ability to integrate technical and organizational measures and to apply the standards both strategically and operationally.

RESEARCH METHODOLOGY

The survey was designed based on research questions and included both structured multiple-choice questions and open-ended responses. It covered topics such as standard selection criteria, implementation barriers, and perceived business impacts. The target group consisted of companies operating within sectors defined as critical infrastructure (Lewis, 2006).

The survey was distributed via open invitation on LinkedIn, resulting in a self-selected sample of information security professionals from various industries, including energy, telecommunications, and manufacturing. While this introduces limitations in generalizability, the responses provided valuable insights into current practices.

Data was collected using the Webropol platform and analysed through a combination of basic statistical methods and qualitative content analysis. Expert review of the survey instrument by representatives from the Finnish Information Security Centre, the Confederation of Finnish Industries, Technology Industries of Finland, and Ernst & Young, a global professional services firm, enhanced its relevance and reliability.

Despite the limited sample size, the study adhered to ethical research principles, including informed consent, anonymization, and compliance with

GDPR and Finnish data protection legislation. The data was securely stored and handled in accordance with best practices.

RESULTS OF THE QUESTIONNAIRE

Most respondents reported using ISO/IEC 27001 and NIST Cybersecurity Framework with selection driven by regulatory compliance, customer requirements, and strategic alignment. Implementation challenges included limited resources, lack of management commitment, and skills gaps. More mature organizations applied standards strategically, while others focused on compliance and reactive updates.

Larger and more mature organizations integrated standards into strategic planning, risk management, and investment decisions. Smaller companies tended to apply standards operationally, focusing on audits, basic controls, and compliance. The presence of a dedicated information security team was associated with a more structured and proactive application of standards.

Energy sector emphasized regulatory compliance, risk analysis, and collaboration with authorities. IT sector focused on automation, continuous improvement, and advanced training. Manufacturing showed limited strategic integration, with emphasis on technical updates and basic awareness.

Information security awareness was promoted through regular training, simulations, and campaigns. However, training quality and depth varied by maturity level. High-maturity organizations combined strategic and operational approaches, while low-maturity ones relied on basic education and ad hoc initiatives.

Effectiveness was assessed through audits, metrics, and certifications. Advanced organizations used penetration testing, incident analysis, and feedback loops. Standards supported continuous improvement, but their impact depended on organizational readiness and leadership engagement.

External experts were commonly used for audits and specialized tasks. Investment in resilience varied. Larger firms prioritized crisis management, incident response, and strategic planning, while smaller ones focused on basic technical measures. Real-time threat intelligence sharing and stakeholder engagement remain underutilized, especially among SMEs.

Statistical analysis using Chi-square and Fisher's exact test indicated significant correlations between organizational maturity and standard utilization, particularly in training, decision-making, and post-incident recovery. Companies with higher maturity levels viewed standards as development tools rather than compliance checklists.

DISCUSSION

The findings of this study confirm that information security standards are widely utilized by Finnish companies in protecting critical infrastructure. However, their strategic integration and operational effectiveness vary significantly across organizations.

The results highlight a clear divide between strategic use in mature, resource-rich organizations and operational compliance in smaller firms. The effectiveness of information security standards is closely linked to leadership commitment and the integration of risk management into organizational processes (Barafort et al., 2017). Organizational maturity and internal capabilities significantly influence the adoption and implementation of ISO/IEC 27001, particularly in terms of organizational readiness and long-term sustainability (Mirtsch, 2023).

While standards such as ISO/IEC 27001 and NIST Cybersecurity Framework provide structured frameworks, their effectiveness is contingent upon contextual adaptation. Organizations that view standards as development tools rather than compliance checklists tend to achieve better outcomes in risk management, resilience, and cultural transformation.

Sectoral differences were pronounced. Energy sector emphasized regulatory alignment and authority collaboration. IT sector demonstrated agility, automation, and proactive training. Manufacturing showed limited strategic adoption, often constrained by resources and awareness.

Organizational size and structure also influenced adoption depth. Companies with dedicated information security teams were more likely to implement standards holistically, while hybrid models struggled with role clarity and continuity.

Key challenges included resource limitations, training gaps, and inconsistent management support. These findings echo earlier studies that stress the importance of leadership, communication, and continuous learning in successful standard adoption (Van Wessel & de Vries, 2013). Opportunities lie in developing tailored support models for SMEs, enhancing stakeholder engagement, and promoting scenario-based risk analysis. The proposed three-level maturity model offers a practical framework for assessing readiness and guiding development.

The proposed three-level maturity model can help organizations assess their current state and define a development path based on size and industry (Rejman, 2025). It supports SMEs in evaluating and improving their cybersecurity posture:

- Level 1 – Basic: Internal audits, monitoring tools, regular training, and management support.
- Level 2 – Advanced: Automated updates, response plans, vulnerability testing, external audits.
- Level 3 – High: Attack surface management, collaboration with authorities, customer feedback, strategic leadership.

Information security standards should be seen as strategic enablers, not just technical guidelines. Their integration into business strategy, investment planning, and organizational culture is essential for long-term resilience. Real-time threat sharing, structured training, and cross-sector collaboration can significantly enhance effectiveness.

CONCLUSION

The findings confirm that Finnish companies utilize information security standards, but adoption is influenced by organizational size and maturity, industry-specific requirements, and leadership commitment as well as internal capabilities. Strategic integration is more common in large, mature organizations, while operational compliance dominates in smaller firms. Standards support risk management, resilience, and cultural development, but their effectiveness depends on contextual adaptation, continuous improvement, and stakeholder engagement.

To enhance the impact of information security standards on critical infrastructure protection, organizations should integrate standards into business strategy and investment planning, strengthen leadership commitment through structured governance, and invest in continuous training that combines technical and strategic perspectives. Utilizing maturity models to assess capabilities and guide development is also recommended.

Policymakers and support networks can contribute by developing tailored support models for SMEs, facilitating cross-sector collaboration, promoting scenario-based risk analysis, and encouraging proactive communication strategies aligned with international standards.

Ultimately, information security standards should be viewed as strategic enablers that support long-term resilience, not merely as technical checklists. Their full potential is realized when embedded into organizational culture, decision-making, and continuous development.

ACKNOWLEDGMENT

The first author would like to express his sincere gratitude to his supervisors at the University of Jyväskylä, Dr. Markus Sihvonen and Professor Tapio Frantti, for the opportunity to publish the research results in the AHFE Conference. Their guidance and support have been invaluable throughout the research process of this paper.

REFERENCES

Ahouanmenou, S., Van Looy, A., & Poels, G. (2023). Information security and privacy in hospitals: A literature mapping and review of research gaps. Informatics for Health and Social Care, 48(1), 30–46. https://doi.org/10.1080/17538157.2022.2049274.

Al-Dhanhani, M. J., & Mat Jizat, J. E. (2021). Review of cyber security on oil and gas industry in United Arab Emirates: Analysis on the effectiveness of the National Institute of Standards and Technology's (NIST) Information security Framework. Turkish Journal of Computer and Mathematics Education, 12(11), 714–720.

Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. Science of the Total Environment, 714, 136854. https://doi.org/10.1016/j.scitotenv.2020.136854.

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces, 54, 176–185. https://doi.org/10.1016/j.csi.2016.11.010.

Brem, S. (2015). Critical infrastructure protection from a national perspective. European Journal of Risk Regulation, 2(2015), 191–199. https://doi.org/10.1017/S1867299X00004499.

Chopra, S. S., Dillon, T., Bilec, M. M., & Khanna, V. (2016). A network-based framework for assessing infrastructure resilience: A case study of the London metro system. Journal of the Royal Society Interface, 13, 20160113. https://doi.org/10.1098/rsif.2016.0113.

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of information security in critical infrastructure sectors. Land Forces Academy Review, 26(1), 101. https://doi.org/10.2478/raft-2021–0011.

Glisson, W. B., Andel, T., McDonald, T., Jacobs, M., Campbell, M., & Mayr, J. (2015). Compromising a medical mannequin. Computerworld. https://www.computerworld.com/article/2981527/researchers-hack-a-pacemaker-kill-a-man-nequin.html, https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf.

Große, C., & Olausson, P. M. (2019). Blind spots in interaction between actors in Swedish planning for critical infrastructure protection. Safety Science, 118, 424–434. https://doi.org/10.1016/j.ssci.2019.05.049.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2015). A framework to improve the resilience of critical infrastructures. International Journal of Disaster Resilience in the Built Environment, 6(4), 409–423. https://doi.org/10.1108/IJDRBE-07–2014-0048.

Lewis, T. (2006). Critical infrastructure protection in homeland security: Defending a networked nation. https://doi.org/10.1002/0471789542.

Luskova, M., & Dvorak, Z. (2019). Applying risk management process in critical infrastructure protection. Interdisciplinary Description of Complex Systems, 17(1-A), 7–12. https://dx.doi.org/10.7906/indecs.17.1.2.

Mäki-Maukola, E. (2023). The ISO 27000 Series of Information Security Standards as Part of Modern Corporate Security Management (master's thesis). University of Jyväskylä.

Mirtsch, M. (2023). Adoption of the Information Security Management System Standard ISO/IEC 27001: A study among German organizations. International Journal for Quality Research, 17(3), 747–768. https://doi.org/10.24874/IJQR17.03–08.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry, 142, 103744. https://doi.org/10.1016/j.compind.2022.103744.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. International Journal of Critical Infrastructure Protection, 25, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003.

Rejman, K. (2025). Corporations' critical infrastructure and security standards, (master's thesis, University of Jyväskylä). Jyväskylä University Digital Repository. https://jyx.jyu.fi/bitstreams/5e70cbfe-7c34–41f7–8647-0cb669713994/download.

Van Wessel, R. M., & de Vries, H. J. (2013). Business Impacts of International Standards for Information Security Management: Lessons from Case Companies. Journal of ICT Standardization, 1, 25–40. https://doi.org/10.13052/jicts2245–800X.122.

Wu, W., Shi, K., Wu, C.-H., & Liu, J. (2022). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. Journal of Global Information Management, 30(3), Article 2. https://doi.org/10.4018/JGIM.20220701.oa2.