Banking Resilience: Building Cyber Incident Response in the Finnish Financial Sector

Jade Karrila and Ilona Ilvonen
Tampere University, Finland

jade.karrila@gmail.com
ilona.ilvonen@tuni.fi

Abstract: Cybersecurity incidents in the financial sector pose systemic risks to economic stability and societal continuity. Despite extensive regulatory oversight and generally high cybersecurity maturity, recent incidents in Finland have revealed persistent weaknesses in incident response and recovery. Using a recent incident at the Nordic bank Nordea as a descriptive case, the study examines governance structures, role allocation and skills coordination during cybersecurity incidents at the sectoral level. The research data consist of document analysis of public incident-related material and six semi-structured interviews with cybersecurity professionals experienced in the financial sector. The analysis is informed by established cybersecurity governance and incident response frameworks. The data were analysed using thematic analysis to identify key patterns and gaps in incident response practices. The findings indicate that while preventive controls in the Finnish financial sector are well-developed, effective incident response is constrained by rigid structures, fragmented accountability, and limited application of skill-based roles. Incident response is frequently managed within functional silos, reducing shared situational awareness and slowing adaptive decision-making. The study contributes to cybersecurity and crisis management literature by contextualising the European Cybersecurity Skills Framework within financial-sector incident response and highlighting the importance of continuous learning, clear role coordination, and flexible governance mechanisms.

Keywords: Cybersecurity incident response, Financial sector, Organisational resilience, Cybersecurity governance, European cybersecurity skills framework

1. Introduction

Cyber security and cyber resilience are increasingly important in the operating environment of contemporary organisations. The financial sector is part of critical infrastructure, which makes it an especially attractive target for cyberattacks (Didenko, 2020). For this reason, the industry operates under heavy regulatory oversight from both international and national bodies, which enforce security and resilience measures. The European Union Agency for Cybersecurity (ENISA) provides coordination, threat intelligence, and support for implementing EU-wide directives such as DORA (Digital Operational Resilience Act).

Nationally, Finland's cybersecurity landscape in the financial sector is shaped by Traficom's National Cyber Security Centre and Financial Supervisory Authority (FIN-FSA), which guide, assist, and supervise organisations with implementing cybersecurity best practices in the industry. In Finland, the financial sector has previously been reported to be the third most advanced industry in terms of cybersecurity, after telecommunications and ICT and software (Huoltovarmuuskeskus, 2022). However, the pressure on the already targeted industry has grown. Internationally, cybersecurity attacks, especially denial-of-service (DoS) attacks, have increased both in size and volume over the past few years (de Neira et al, 2023). National Cybersecurity Centre of Finland has reported that the number of denial-of-service attacks has grown in Finland; however prolonged attacks disruptive to organisations are still rare (Kyberturvallisuuskeskus, 2024).

This paper analyses the regulatory and best practice landscape of the Finnish financial sector and uses the prolonged DoS attacks against the finance company Nordea in 2024 as an illustrative case. The paper aims to answer the question: How could the European Cybersecurity Skills Framework be used to identify and address skills gaps in incident response? The paper reports the results of a Master's thesis written by the first author.

2. Incident Response and Skills Coordination

2.1 Incident Response and Cyber Resilience

Cyber resilience refers to the ability of an organisation to absorb, adapt to, and recover from cyber disruptions while maintaining continuity of critical functions (Dupont, 2019; Petrenko, 2019). Unlike traditional cybersecurity, which prioritises prevention, resilience acknowledges that not all incidents can be avoided and emphasises response, recovery, and organisational learning (Björck et al, 2015).

In the financial sector, resilience is particularly important due to systemic interdependencies and the potential cascading effects of localised incidents (Carilo, 2023). Cyber disruptions may result not only in operational downtime but also in reputational damage and broader economic instability (Varga et al, 2021). Consequently,

incident response must extend beyond technical containment to coordinated organisational action across multiple functions.

Most standards structure incident response around detection, response, and recovery processes; however, some argue that formalised procedures alone do not guarantee adaptive performance during real incidents (Adetunji & Chinonso, 2025). Effective response requires situational awareness, flexible decision-making, and the capacity to integrate lessons learned into future preparedness (Petrenko, 2019).

Resilience therefore depends on dynamic organisational capabilities rather than static compliance mechanisms. The ability to reconfigure roles, maintain coordinated communication, and institutionalise post-incident learning distinguishes resilient organisations from those relying solely on formal controls (Uddin et al, 2020).

2.2 Governance and Role Clarity

Cybersecurity governance encompasses the structures, policies, and decision-making processes through which cybersecurity activities are directed and monitored (Cortez & Dekker, 2022). In the financial sector, governance is shaped by extensive regulatory oversight, including requirements that emphasise management accountability for cybersecurity risks (Calliess & Baumgarten, 2020). Despite formal structures, governance deficiencies may emerge in fragmented accountability and unclear role definitions. During disruptive incidents, ambiguity regarding decision authority and escalation pathways can delay coordinated response efforts (Akinsulire & Ohakawa, 2024). This suggests that governance effectiveness depends not only on regulatory compliance but also on operational clarity.

Research further indicates that compliance-driven cybersecurity cultures may prioritise audit readiness over adaptive capability (Peihani, 2022). Although institutions may satisfy formal requirements, coordination challenges can persist in practice, particularly when responsibilities are distributed across technical teams, management, communication units, and external stakeholders (Varga et al, 2021). Moreover, governance mechanisms are embedded within organisational culture and behavioural norms (Weickert et al, 2023). Without shared understanding and clearly articulated responsibilities, even well-designed governance frameworks may fail to translate into effective incident coordination. Strengthening incident response therefore requires aligning governance structures with real-time operational demands and clarifying roles across hierarchical and functional boundaries.

2.3 The European Cybersecurity Skills Framework

While governance structures define accountability, effective incident response also depends on clearly articulated competencies. The European Cybersecurity Skills Framework (ECSF), developed by ENISA, provides a structured taxonomy of cybersecurity professional roles and associated knowledge, skills, and competences (European Union Agency for Cybersecurity, 2022a). It aims to harmonise role definitions across Europe and support workforce development within cybersecurity functions (European Union Agency for Cybersecurity, 2022b). However, competence frameworks are often implemented primarily as human resource instruments rather than as integrated elements of cybersecurity governance (Olutimehin, 2025).

Incident response requires multidisciplinary coordination, including technical expertise, crisis communication, risk assessment, and leadership capabilities (Varga et al, 2021). If roles are ambiguously defined or competencies misaligned with operational demands, response effectiveness may be compromised. Structured role frameworks can therefore support clearer allocation of responsibilities and identification of capability gaps.

Although existing research emphasises governance and technical controls in financial cybersecurity (Didenko, 2020; Uddin et al, 2020), limited attention has been paid to the integration of structured skills frameworks into incident response governance. Connecting ECSF-defined competencies with governance mechanisms may strengthen situational awareness, clarify escalation responsibilities, and support adaptive recovery processes. This integration provides a conceptual foundation for examining how skills coordination contributes to resilient incident response.

3. Research Design and Method

This study seeks to generate analytical and actionable insights to improve incident response capabilities from literature, documentary sources, and empirical material. The pragmatist approach of the study accommodates both the descriptive aim to depict how incident response is organised, and the prescriptive aim to identify how it could be improved (Farjoun et al, 2015; Goldkuhl, 2012). Document data, such as standards, media articles, and public reports, provide insight into official narratives, institutional framing, and sector-level expectations,

while expert interviews reveal practitioners' situated interpretations, reasoning, and tacit knowledge that are often absent from formal documentation (Eriksson & Kovalainen, 2008; Puusa et al, 2020; Yin, 2018).

Document analysis is used to examine the incident response of the financial sector through news articles, standards, and public reports for the descriptive case study. In total, 99 documents were included in the analysis. The document dataset consists primarily of publicly available news articles as well as public reports and decisions by FIN-FSA. A key inclusion criterion was the potential of the document to provide insight into the Nordea incident and related incident response practices. Table 1 shows examples of thematic coding linked to the documents.

Table 1: Document analysis coding example

Main Theme	Subtheme	Example Codes	Frequency
Leadership and the role of management	Leadership taking responsibility	Leadership visibility during crisis, communication roles	15
Skills and ECSF Roles	Competence management	Unclear division of responsibilities, need for specific skills	5
Organisational resilience and incident response	Evolving operational environment	Increased number of attacks	10
	Recovery from service disruptions	Lessons learned and improvement actions	20

In this paper the thematic coding of the document data presented in Table 1 is not very strongly visible due to space constraints. Individual materials from the data are used as example sources in the findings, but they represent findings from a larger pool of articles as seen in the table.

Semi-structured interviews were selected as another data collection method to complement the document data and enable an in-depth exploration of expert perspectives on incident response practices in the financial sector. Recommendations by Hair (2023) and Flick (2021) for forming interview questions that guide the discussion but remain open to interpretation were considered. In total, six experts with varying backgrounds and experience were interviewed in this study. Providing themes in advance to the interviewees was considered beneficial for directing attention to specific areas within the broad scope of incident response, while withholding detailed questions preserved the spontaneity and authenticity of the discussion (Puusa et al, 2020). The interviewees are given the identifiers I1, I2, I3, I4, I5 and I6 in the findings section of this paper. The thematic analysis of the interviews is shown in table 2.

Table 2: Interview analysis example

Raw Excerpt	Initial Code	Subtheme	Main Theme
"Companies must have crisis management plans in place in case, for example a cloud service provider experiences security issues"	Third-party risk identification	Outsourcing management and third-party coordination	Organisational resilience and incident response
"It does not make sense to keep forensic experts in-house, as they have work once or twice a year, and their skills need to be maintained"	Balancing outsourcing Cost-benefit of external expertise	Balancing in-house and outsourced capability decisions	Skills

The data were analysed with a thematic analysis process guided by the research questions (Braun, 2022). Qualitative interpretation is inevitably shaped by the researcher's prior understanding and assumptions (Patton, 2023). Therefore, reflexive notetaking and journaling were used to document analytical decisions. Thematic coding was conducted from the interviews by combining codes and sub-themes as illustrated in Table 2. The interview questions were based on the document analysis, but this type of coding was made to ensure as much independence between the analyses of the datasets as possible.

4. Findings

4.1 Incident Response and Cyber Resilience

Document data revealed mixed perceptions of Nordea's resilience and incident response capabilities. Experts questioned the technical explanations given publicly, and many noted that Nordea had experienced recurring mobile and online banking disruptions on most days over several weeks (Oukanen, 2024). At the same time, Nordea consistently framed its response as evidence of resilience, repeatedly emphasising ongoing investment in defence capabilities and the iterative strengthening of systems as attacks evolve (Nordea, 2025a).

The disruptions affected not only online banking but also Nordea's authentication application (Suutari, 2025). Because bank credentials are the dominant method of strong authentication in Finland, customers were temporarily unable to access unrelated essential services such as government platforms. From a resilience perspective, this reflected a system-level single point of failure rather than a Nordea-specific technical limitation. Document data highlighted that authentication via the Mobile Certificate requires prior activation using bank credentials, making it unusable as an alternative once the disruption began, and unavailable to many users due to operator constraints. Customer support channels were also impaired, as chat services required online-bank authentication (Mäntylä, 2024). This highlights the dependencies that are created within systems over time and emphasises the role of banks as a critical part of the entire digital society in Finland.

Nordea and external commentators framed the incident as a catalyst for strengthening resilience. Nordea highlighted defence mechanisms becoming "even more robust" (Oxvig, 2024), and even critical voices acknowledged the potential of the event to improve defences (Linnake, 2024). Nordea stated that thousands of updates and modifications are deployed annually, most invisible to customers, and that large-scale changes may occasionally require interruptions (Kärkkäinen, 2024). Nonetheless, documents also noted that service disruptions continued after the attack period, suggesting that the incident occurred amid broader infrastructural strain.

Although several major Nordic banks, including SEB, Danske Bank, Swedbank, and OP, were targeted during the same campaign, Nordea experienced the most prolonged and visible disruptions. Document data suggested contrasting interpretations. Nordea attributed the differential impact to its position as the largest Nordic bank and therefore the most attractive target (Oxvig, 2024), while some experts questioned whether Nordea's existing system fragilities amplified the effects. The observation that the strongest attacks were reported in Sweden, despite lower public attention than in Finland, reinforces the need to evaluate resilience not solely through media visibility but through structural preparedness and recovery capability across institutions (Raeste, 2024). Cybersecurity experts also cautioned that it is inherently difficult to assess an organisation's resilience from the outside. They noted that given the volume of attacks targeting Finnish entities, the relative scarcity of large-scale disruptions indicates strong baseline resilience in the country (Raeste, 2024). However, Nordea faced recurring issues throughout 2024 and early 2025 (Pietiläinen, 2024; Suutari, 2025), which may have shaped public perceptions and heightened scrutiny during the autumn incident.

4.2 Governance and Role Clarity

Both the document data and interviews suggest that incident response governance in the Finnish financial sector is generally well structured and closely aligned with regulatory expectations. In the Nordea case, governance was publicly framed through visible engagement with authorities and cross-institutional coordination, indicating that the incident was managed as a matter of national relevance rather than a purely technical disruption (STT-YLE, 2024). Nordea's interactions with authorities and the broader institutional attention given to the incident reflect a high level of formal coordination within the sector's governance ecosystem, involving key supervisors and national cybersecurity actors.

At the same time, the document data indicate that from a legal and supervisory perspective, the Nordea incident did not necessarily reveal a failure of governance as such, but rather the limits of what regulation can achieve. Public commentary and supervisory framing emphasised that oversight primarily evaluates whether required processes and controls exist and whether obligations are met, rather than how effectively practices function in real time under rapidly evolving conditions (Valkama, 2024). This creates a gap between formal compliance and experienced resilience, a phenomenon that has been previously documented in literature (He et al, 2022). Governance structures may appear sufficient from a regulatory standpoint, while stakeholders affected by disruptions may interpret the response as inadequate or unclear.

The interviews reinforce the view that Finnish financial institutions maintain mature and rehearsed governance processes and roles for incident response. Respondents described governance structures as formalised, role-based, and supported by pre-defined escalation pathways (I3). These structures were described as well-established and practised, supporting the broader perception of high cybersecurity maturity in the sector (I5).

However, the analysis also suggests that rigid governance does not automatically translate into adaptive incident response. Interviewees highlighted that real-world incidents often inspire unpredictability and require cross-unit coordination and prioritisation decisions that cannot fully be scripted. While governance structures support accountability and role clarity, the increasing specificity of obligations can also introduce complexity and additional workload during an active incident (I3). In practice, this may divert resources from operational response tasks to reporting and coordination routines. Even when these routines are necessary for compliance this may not be the optimal use of resources during the incident (I4).

Both datasets point to a visibility and trust challenge in the sector. Even where governance processes and roles exist and are exercised sector-wide, their effectiveness may not be evident to external stakeholders such as customers during service disruptions. Interviewees emphasised that stakeholder trust is fragile and that communication decisions carry reputational consequences, particularly if customers perceive responses as vague or unaccountable (I2). Unlike the interviews, the document data indicate that the clarity of governance roles was not consistently reflected in public communication during the Nordea incident. Updates to customers were described in media coverage as ambiguous, limited, and scattered around channels (Kärkkäinen, 2024). This contrast suggests that internally coherent governance structures do not automatically translate into externally coherent processes. In practice, role clarity within organisations may remain invisible to stakeholders if processes are not sufficiently integrated into incident response governance.

4.3 The European Cybersecurity Skills Framework

While Nordea describes structured training programs and internal coordination models (Nordea, 2025b, 2023), there was little evidence of systematic alignment with the European Cybersecurity Skills Framework (ECSF) or comparable competence models found in the document analysis. This gap may hinder efforts to clearly assign, develop, and evaluate the roles involved in incident response. The lack of competence models might also hamper communication and reduce trust when organisational communication is inconsistent and ambiguous.

The Nordea case illustrates the multidisciplinary nature of incident response competencies. Media coverage revealed that individuals without explicit technical expertise responded to detailed questions about attack methods and defensive measures (Herrala, 2024; Linnake, 2024), which increased distrust and critique (Linnake, 2024). The absence of cybersecurity leadership in media contradicts with the ECSF's distinction between operational, communication, and strategic cybersecurity roles. This does not necessarily indicate a lack of expertise, but rather a potential misalignment between competence structures and their external enactment.

Broader public discussion during the incident further highlighted concerns about cybersecurity competencies within Finnish organisations, particularly regarding human error and cybersecurity awareness (Nyman, 2024). This reflects the ECSF's emphasis on defined competence areas across both technical and organisational domains.

Interview data confirm that financial institutions maintain strong technical capabilities, including internal SOC and CERT functions, while highly specialised expertise is often outsourced due to its infrequent use (I4, I5). Respondents emphasised that effective incident response requires not only deep technical knowledge but also communication and leadership competencies (I4, I5). Training was described as continuous and responsive to identified gaps (I5, I6). However, these practices appear to operate without explicit integration of structured competence frameworks such as the ECSF into governance mechanisms. The findings suggest that while the Finnish financial sector demonstrates high levels of cybersecurity expertise, competence management remains practice-driven rather than framework-integrated. This gap highlights the potential value of linking ECSF-defined competencies more systematically with incident response governance to enhance role clarity, situational awareness, and adaptive recovery.

5. Discussion and Conclusions

The comparison between the empirical findings and literature reveals that Finnish financial institutions largely adhere to the spirit of international best practices in but may fall short of implementing them in the systematic and accountable manner into governance processes. While interviewees consistently emphasised that DORA does not change anything substantial because the sector largely already follows international best practices, the

document data demonstrates that the practical application of these standards remains uneven, especially in accountability and post-incident learning. This gap invites a critical reflection on whether adherence to formal frameworks equates to genuine resilience in practice, or whether resilience depends on how incident response capabilities are used in real incidents.

Effective incident response encompasses preparation, detection, analysis, containment, eradication, recovery, and post-incident activity (ISO/IEC 27035, 2016; National Institute of Standards and Technology, 2024). Evidence from both datasets shows that Finnish financial institutions perform strongly in the preventive and detection phases. Interview data emphasised extensive monitoring capabilities, active participation in national exercises, and integration of threat intelligence into routine operations. These findings support previous research suggesting that Nordic financial entities demonstrate advanced detection maturity and inter-organisational cooperation (European Union Agency for Cybersecurity, 2025). However, the later stages of the incident response life cycle, particularly response, recovery, and post-incident learning, appear less consistent with the frameworks' intent, which raises the question of whether compliance-driven maturity adequately translates into agile and effective incident response (Computer Security Division, 2024) when confronted with complex incidents.

From a theoretical perspective, the findings both confirm and extend prior studies on the relationship between institutional maturity and adaptive response. Consistent with He et al (2022), the data suggests that high technical preparedness can coexist with limited strategic flexibility and lack of agility in incident response processes. However, this study extends the discussion by providing sector-specific evidence from Finland that even when frameworks are embedded at the policy level, their interpretive application varies depending on organisational culture and perceived reputational risk.

The European Cybersecurity Skills Framework (ECSF) provides a comprehensive structure for defining cybersecurity roles and competencies across organisations. Although it has not yet been widely adopted in the Finnish financial sector, the findings suggest that it could serve as a valuable tool for clarifying responsibilities, managing outsourcing relationships, and improving communication and accountability in incident response. Both document and interview data indicate that roles in the Finnish financial sector are currently defined through standards and regulations rather than through the ECSF. This observation aligns with assessment of ECSF (Polemi & Kioskli, 2023), which note that the frameworks' uptake has been limited across sectors despite its potential to harmonise competence requirements.

Across both datasets, ECSF was not explicitly recognised as a guiding structure. Interview data revealed that incident response roles are already well established within financial institutions, typically reflecting regulatory expectations and industry best practices. During the Nordea incident, several executives commented publicly on the situation, yet technical experts or the CISO did not take a visible role. This pattern contradicts the ECSF's approach, which emphasises clear role definition and accountability chains extending from technical experts to strategic management. This further contradicts with the interviewees' stance that the CISO often has a communicative role. However, the ECSF does not precisely define the communicative role and responsibility for stakeholder communication (European Union Agency for Cybersecurity, 2022a), which can be considered a major limitation especially in terms of its utilisation in incidents like the one in this study. Clarifying these responsibilities could directly strengthen communication as an incident response capability.

This study contributes to cybersecurity governance literature by contextualising the European Cybersecurity Skills Framework (ECSF) within financial-sector incident response and by highlighting the importance of integrating structured competence frameworks into governance mechanisms. Practically, the findings suggest that financial institutions and regulators should prioritise escalation clarity, cross-functional coordination, and systematic learning processes alongside regulatory compliance.

The study is limited by its reliance on publicly available documents and a relatively small interview sample, which may not fully capture internal organisational dynamics. Future research could examine longitudinal incident response development, compare multiple institutions, or explore how competence frameworks such as the ECSF can be operationalised in crisis communication and leadership practices.

Ethics Declaration: The research adhered to the ethical review guidelines of the home institution and did not require formal ethical clearance from an institutional ethics committee.

AI Declaration: AI tools were not used in writing of this paper.

References

Adetunji, P.A. and Chinonso, P.O. (2025) *The role of cybersecurity in safeguarding finance in a digital era*, World Journal of Advanced Research and Reviews, Vol. 25, pp 1542–1556. https://doi.org/10.30574/wjarr.2025.25.3.0909

Akinsulire, A.A. and Ohakawa, T.C. (2024) *Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance (2024),* International Journal of Advanced Multidisciplinary Research and Studies, Vol. 4 (6), pp 2127-2139, https://doi.org/10.62225/2583049X.2024.4.6.4264

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015) *Cyber Resilience – Fundamentals for a Definition*, Department of Computer and System Sciences, Stockholm University, Sweden, pp. 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

Calliess, C. and Baumgarten, A. (2020) *Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective,* German Law Journal, Vol. 21 (6), pp 1149–1179. https://doi.org/10.1017/glj.2020.67

Carilo, E.F.P. (2023) *Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform,* European Business Law Review, Vol. 34 (7), pp 1133–1166. https://doi.org/10.54648/EULR2023052

Computer Security Division and I.T.L. (2024) *Incident Response | CSRC* [online], CSRC NIST, URL https://csrc.nist.gov/projects/incident-response (accessed 5.29.25).

Cortez, E.K. and Dekker, M. (2022) *A Corporate Governance Approach to Cybersecurity Risk Disclosure*, European Journal of Risk Regulation : EJRR, Vol. 13 (3), pp 443–463. https://doi.org/10.1017/err.2022.10

de Neira, A.B., Kantarci and B., Nogueira, M. (2023) *Distributed denial of service attack prediction: Challenges, open issues and opportunities*. Computer Networks, Vol. 222, pp 109553. https://doi.org/10.1016/j.comnet.2022.109553

Didenko, A.N. (2020) *Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond*, Uniform Law Review, Vol. 25, pp 125–167. https://doi.org/10.1093/ulr/unaa006

Dupont, B. (2019). *The cyber-resilience of financial institutions: significance and applicability*. Journal of Cybersecurity, Vol. 5 (1). https://doi.org/10.1093/cybsec/tyz013

European Union Agency for Cybersecurity. (2025) *ENISA threat landscape: finance sector : January 2023 to June 2024*, [online], Publications Office, LU, https://data.europa.eu/doi/10.2824/5410466

European Union Agency for Cybersecurity. (2022a.) *ECSF, European cybersecurity skills framework*, [online] Publications Office, LU, https://data.europa.eu/doi/10.2824/859537

European Union Agency for Cybersecurity. (2022b) *European cybersecurity skills framework (ECSF): user manual*, [online] Publications Office, LU, https://data.europa.eu/doi/10.2824/95989

He, Y., Zamani, E.D., Lloyd, S. and Luo, C. (2022) *Agile incident response (AIR): Improving the incident response process in healthcare*, International journal of information management, Vol. 62, pp 102435-. https://doi.org/10.1016/j.ijinfomgt.2021.102435

Herrala, O. (2024) *Nordean johtaja kertoo, mistä on kyse – 360 palvelunestohyökkäystä kuukaudessa, tekijällä kymmenien miljoonien eurojen resurssit,* [online], Tivi, URL https://www.tivi.fi/uutiset/nordean-johtaja-kertoo-mista-on-kyse-360-palvelunestohyokkaysta-kuukaudessa-tekijalla-kymmenien-miljoonien-eurojen-resurssit/343bc7e4-c5b7-47a1-89d6-dd12ebfcb6ed (accessed 2.20.25).

Huoltovarmuuskeskus. (2022) *Toimialojen kyberkypsyyden selvitys 20220 - Kansallinen koosteraportti*, [online], URL https://www.huoltovarmuuskeskus.fi/files/bbdecbcd7921768bd3ac5496af7992a0460a9f2b/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf (accessed 3.3.25).

ISO/IEC 27035. (2016) *ISO/IEC 27035-1:2022 - Information security incident management - Principles,* International Organization for Standardization.

Kärkkäinen, H. (2024) *Nordea, mitä on oikein meneillään? Nyt pankki vastaa,* [online], Ilta-Sanomat, URL https://www.is.fi/digitoday/art-2000010715956.html (accessed 5.13.25).

Kyberturvallisuuskeskus. (2024) *Palvelunestohyökkäystilanne Suomessa*, [online], Kyberturvallisuuskeskus, URL https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaystilanne-suomessa (accessed 3.3.25).

Linnake, T. (2024) *Asiantuntijalta kylmää kyytiä Nordealle – näin pankki puolustautuu,* [online], Ilta-Sanomat, URL https://www.is.fi/digitoday/art-2000010862819.html (accessed 5.18.25).

Mäntylä, J.-M. (2024) *Analyysi: Nordean asiakkaat saavat nyt kärsiä päätöksistä joita on tehty jo paljon aiemmin*, [online], Yle Uutiset, URL https://yle.fi/a/74-20116824 (accessed 5.16.25).

National Institute of Standards and Technology. (2024) *The NIST Cybersecurity Framework (CSF) 2.0 (No. NIST CSWP 29)*, National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.29

Nordea. (2025a) *Päivitys: Palvelunestohyökkäykset voivat aiheuttaa hitautta Nordean digitaalisiin palveluihin kirjautumisessa*, [online], Nordea, URL https://www.nordea.com/fi/uutiset/paivitys-palvelunestohyokkaykset-voivat-aiheuttaa-hitautta-nordean-digitaalisiin-palveluihin-kirjautumisessa (accessed 2.20.25).

Nordea. (2025b) *Detection, prevention, response - staying ahead of cyber threats,* [online], Nordea, URL https://www.nordea.com/en/news/detection-prevention-response-staying-ahead-of-cyber-threats (accessed 5.29.25).

Nordea. (2023) *Nordea On Your Mind: Cybersecurity II*, [online], Nordea, URL https://www.nordea.com/en/news/nordea-on-your-mind-cybersecurity-ii (accessed 5.29.25).

Nyman, M. (2024) *Tietoevry: Nearly half of Finnish companies have been targeted by serious cyberattacks* [online], Tivi, URL https://www.tivi.fi/uutiset/tietoevry-nearly-half-of-finnish-companies-have-been-targeted-by-serious-cyberattacks/a62447be-a920-4e8c-8bd3-5a8d03e60358 (accessed 5.16.25).

Olutimehin, A.T. (2025) *Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi)*, Social Science Research Network, Rochester, NY. https://doi.org/10.2139/ssrn.5133050

Oukanen, T. (2024) *Nordean pankkiongelmat jatkuvat,* [online], Yle Uutiset, URL https://yle.fi/a/74-20113097 (accessed 5.16.25).

Oxvig, M. (2024) *Nordea har været under cyberangreb 25 dage i træk,* [online], URL https://finanswatch.dk/Finansnyt/Pengeinstitutter/article17522707.ece (accessed 5.21.25).

Peihani, M. (2022) *Regulation of Cyber Risk in the Banking System: A Canadian Case Study*, Journal of financial regulation, Vol. 8, pp 139–161. https://doi.org/10.1093/jfr/fjac006

Petrenko, S. (2019) *Cyber resilience*, 1st ed. ed, River publishers series in security and digital forensics, River Publishers, Gistrup, Denmark

Pietiläinen, T. (2024) *Pankkihäiriöt | HS selvitti: Nordean viimeaikaiset ongelmat ovat vain jäävuoren huippu,* [online], Helsingin Sanomat, URL https://www.hs.fi/tutkiva/art-2000010750754.html (accessed 5.13.25).

Polemi, N. and Kioskli, K. (2023) *Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPRO European Efforts*, Human Factors in Cybersecurity, Vol. 91, pp 93–100.

Raeste, J.-P. (2024) *Pankit | Nordea: Verkkohyökkäysten voima ja kesto täysin ennennäkemätön, tarkoitus horjuttaa yhteiskuntaa*, [online], Helsingin Sanomat, URL https://www.hs.fi/talous/art-2000010761540.html (accessed 5.13.25).

STT-YLE. (2024) *Verkkopankkien käyttökatkoista järjestetään kuuleminen eduskunnassa,* [online], Yle Uutiset, URL https://yle.fi/a/74-20116728 (accessed 5.16.25).

Suutari, E. (2025) *Pankit | Nordea joutui palvelunestohyökkäyksen kohteeksi,* [online], Helsingin Sanomat, URL https://www.hs.fi/talous/art-2000011212898.html (accessed 5.13.25).

Uddin, M.H., Hakim, A.M. and Kabir, H.M. (2020) *Cybersecurity hazards and financial system vulnerability: a synthesis of literature*, Risk Management, Vol. 22, pp 239–309. https://doi.org/10.1057/s41283-020-00063-2

Valkama, H. (2024) *Analyysi: Tärkeä arjen toiminto kaatuilee jatkuvasti, mutta kukaan viranomainen ei ärähdä Nordealle*, [online], Yle Uutiset, URL https://yle.fi/a/74-20116834 (accessed 5.16.25).

Varga, S., Brynielsson, J. and Franke, U. (2021) *Cyber-threat perception and risk management in the Swedish financial sector*, Computers & Security, Vol. 105, pp 102239. https://doi.org/10.1016/j.cose.2021.102239

Weickert, T.D., Joinson, A. and Craggs, B. (2023) *Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice*, Computers & security, Vol. 128, pp 103130-. https://doi.org/10.1016/j.cose.2023.103130