Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Role of It Management Competence in Enhancing Cybersecurity Preparedness in Financial Institutions

Arto Smedberg

ARTICLE INFO

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The research offers a systematic literature review evaluating the influence of IT management competence on increasing cybersecurity preparedness in financial contexts. The review develops findings applying the PRISMA Model from current empirical research and integrates them with expert perspectives from industry practitioners. The research determines seven major themes, ranging from purpose-based leadership and technical adaptability to continuous learning and communication skills, that jointly foster cyber resilience. The outcomes emphasize the requirement for an associated method that amalgamates technical skills with organizational adaptability, human-centric leadership, and strategic thinking. Moreover, this study facilitates practical applications for financial institutions intending to reinforce their cybersecurity stance via optimized culture-driven strategies, leadership development, and IT governance.

Keywords: Systematic literature review, strategic IT leadership, financial institutions, cybersecurity preparedness, IT management competence

Introduction

Background and Significance of IT Management in Cybersecurity

The financial sector is a core target for cybercriminals in the current decade because of its systemic interconnectedness, sensitive customer information, and high-value transactions. In financial institutions, cyber events account for a significant part of the sector-wide cyber losses, and individual attacks possess cascading financial effects throughout the interconnected process (Azura et al., 2025). Robust management of such critical risks pivots on effective IT management skills, which encompasses technical efficacy, and also risk-based decision-making, governance framework, and align with organizational strategy (Mızrak, 2023). At the same time, frameworks including ISO/IEC 27001:2022 and NIST CSF 2.0 (2024) are largely incorporated, underscoring consistent development, incident response, risk assessment, and IT governance as institutional supports of cybersecurity preparedness or awareness (Dimakopoulou & Rantos, 2024).

Significance to Financial Institutions

Financial institutions or organizations face significant regulatory and financial concerns from cybersecurity violations. Certain large banks possess an approximate annual loss from cyber-related circumstances that lead to address up to tens of millions. On the contrary, smaller institutions and fintech startups often reveal wider vulnerability and lower cyber maturity degrees (Adejumo & Ogburie, 2025). Furthermore, popular regulatory frameworks, including the US's CIRICA, the breach discourse protocols of the SEC, DORA in Europe, and NIS2, are growing the responsibility for senior board and management to directly supervise cybersecurity readiness (Singh, 2023). Additionally, operational stability, investor confidence, and regulatory stress are promptly associated with the inadequate preparedness, weak governance, and cybersecurity posture of the institution, leading to market penalties or reputational damage and weakening trust (Shaker et al., 2023).

Purpose and Scope of the Review

The study seeks to systematically review the present practitioner perspectives and peer-reviewed studies to elucidate how IT management competence, including soft skills, strategic alignment, technical expertise, and governance, contributes to cybersecurity awareness or preparedness in financial institutions.

The review intends to address the following:

- How IT leadership and governance frameworks foster robustness in association with business goals, incident response, and risk identification.
- What soft skills, like change leadership, resilience, and communication, promote user trust and cybersecurity decision-making.
- The major gaps in both practitioner and academic literature, especially about how IT competence converts into measurable resilience across diverse financial environments.

Moreover, the research contributes to a transparent basis for both practice and research by designing such competencies to particular cybersecurity readiness results and fixing supported directions for institutional capability-making initiatives and future empirical research.

Literature Review

IT Management Competence

Tran et al. (2025) outlined the development of cybersecurity in the banking sector from pre-Industry 4.0 to post-Industry 4.0, emphasizing a market transformation from separated and manual security operations to technology-based and associated systems. Cybersecurity largely depended on manual controls with restricted accuracy in the pre-Industry 4.0 era. On the contrary, post-Industry 4.0 developments presented IoT, Blockchain, and AI to promote multi-layered defence instruments and automate threat discovery. Banks face continuous barriers such as enhanced threats, high application expenses, and scalability concerns from standard cybercriminals. This research evaluates technological changes and also the interconnection of cybersecurity strategy, operational objectives, and IT management, facilitating an inclusive perspective of the sector's evolution. Moreover, this study summarizes the development of present policies and practices, and suggests improving cybersecurity competencies via strategic innovation and investment.

Gambo & Almulhem (2025) designed a PRISMA-based SLR ("systematic literature review") that evaluated a ten-year range of studies (i.e., 2016-2025) on ZTA ("Zero Trust Architecture"), a security framework developed on the belief of "never trust, always verify." This study introduced an organized classification of ZTA implementation, allowing technologies (including conditional access and continuous authentication), and determined major adoption barriers. The researcher emphasized the developments of ZTA in response to the challenges of conventional perimeter-driven frameworks, particularly in critical digital environments. At the same time, this study investigates the increase in interest regulated by cybersecurity consequences and the enhancing requirement for least-privilege, adaptive, and effective access controls. Moreover, this review facilitates a practical support for practitioners and researchers intending to associate ZTA with advanced cybersecurity models by fixing the implementation strategies, challenges, and trends.

Cybersecurity Preparedness

Javaheri et al. (2024) prepared an SLR that investigated the growing difficulty of cyber threats in the FinTech industry, regulated by the increasing incorporation of smart technologies and AI. Determining the challenges of conventional security approaches, this research presented an improved cybersecurity taxonomy and ascertained major defensive policies. This study examined 74 peer-reviewed articles, which showed 11 key threats demonstrated throughout 9 basic defence strategies, and 43 papers were comprehensive in 31 papers. The outcomes facilitate practical perspectives for a broader range of stakeholders, encompassing policymakers, tech enterprises, and financial institutions, covering both the robust prevention methods and present vulnerabilities in FinTech. Moreover, this research underscored the emergency requirement for adaptive and intellectual cybersecurity models and recommends further study directions in reinforcing digital finance resilience.

Magnusson et al. (2025) reviewed 41 chosen research studies that investigated information security governance within the context of the public sector. This paper concentrated on major areas including strategic alignment, regulatory obedience, responsibility, and risk management. Some organizations continue to suffer from a lack of proper governance practices, which leads to cybersecurity susceptibility despite the accessibility of developed governance standards such as the EU NIS Directive, GDPR, and ISO/IEC 27001. This research determined certain gaps in the application of risk assessment tools, maturity models, and performance indicators, along with the inadequate application of compliance audits. The researcher reported that robust governance implementation frequently correlates with accessible financial resources, emphasizing a difference in application capacity throughout institutions. Moreover, this research facilitates a primary reference for further practice and study intended to reinforce public sector cybersecurity via optimized governance frameworks.

Current Industry Practices

Metin et al. (2024) explored the connection between cybersecurity and digitalization, concentrating on success criteria, adoption factors, and assessment tools for cybersecurity applications. This research presented cybersecurity governance process groups to categorize fostering factors and underscored the requirement for personalized models, especially for SMEs. Outcomes showed that prior data security standards are highly complex and top-down in nature, making them complex for SMEs to incorporate, particularly when adopting new technologies such as blockchain, AI, and IoT. Therefore, this research offered an emerging bottom-up cybersecurity governance model dependent on the PDC ("Plan-Do-Check") framework, organized around the supports of standards, culture, and governance. Moreover, this model seeks to facilitate SME-friendly and scalable solutions and presents as both a basis for further study and operational support.

Oyeniyi et al. (2024) is an inclusive SLR that evaluated the changing cybersecurity fields in the financial industry, concentrating on the interplay between human factors, technological innovation, and regulatory models. Incorporating a qualitative method, this research emphasized enhancing the insufficiency of prior cybersecurity frameworks in covering the standard of advanced cyber threats. This study showed that while primary frameworks provide an initial point, they need to change toward more collaborative, technology-based, and adaptive frameworks. The research highlighted the requirement for a tripartite alliance, worldwide cooperation, and regulatory agility between technology facilitators, regulators, and financial institutions. Finally, this research is summarized by supporting an associated cybersecurity method that upholds resilience, innovation, and compliance, presenting a strategic pathway for policymakers and practitioners.

Modi et al. (2023) investigated how cybersecurity governance assists strategic decision-making by BoDs ("Board of Directors"). Certain board members possess insufficient actionable metrics, decision-support tools, and technical assessments required to regulate cybersecurity robustly. This study evaluated previous risk measurement mechanisms, governance frameworks, and cybersecurity metrics, determining seven conceptual themes that foster board-level error. Outcomes suggested that while optimized cybersecurity tools are accessible, there is an essential gap in converting technical perspectives into board-relevant models and language. Moreover, this research prioritized future accessible advancement, theory-based frameworks to effectively integrate BoDs in stimulating cyber elasticity at the strategic level.

Brezavšček & Baggia (2025) addressed 96 papers within the years range of 2012-2024. This research investigated the development of cybersecurity maturity and information assessments. The researcher employed a qualitative amalgamation of 36 core studies with a quantitative examination of field trends. Therefore, three foundational themes appeared, such as the improvement of methodologies assisting maturity understanding, the application of developed models, and the establishment of new maturity frameworks. The findings emphasized remarkable advances, encompassing the association of new technologies, the increase of slide frameworks for SMEs, and sector-specific customization. This research offered actionable perspectives for both practitioners and researchers, facilitating practical suggestions to boost cybersecurity flexibility via more personalized and scalable maturity measurement frameworks.

Human-centric skills in IT Service Management

Uchendu et al. (2021) reviewed 58 papers within the years range of 2010-2020. This study explored the establishment and measurement of the cybersecurity environment within organizations. This research covered major questions regarding measurement methods, existing models, primary factors, and definitions for cybersecurity culture. The outcomes showed that despite changing terminologies, major aspects, including employee awareness, formal policies, and top management support, remain key to developing a robust security culture. The majority of models determined distributed components sourced from the wider organizational culture.

At the same time, the surveys and questionnaires were the most widely implemented assessment techniques. However, the issues were initiated regarding the requirement for more context-sensitive and effective metrics. Finally, this review facilitates valuable perspectives for practitioners intending to stimulate an effective security culture and highlights future study requirements, especially in the segment of change management and the role of national culture on cybersecurity patterns.

Figueroa et al. (2025) determined complex challenges in previous cybersecurity models for digital government facilities, especially in strategic governance, adaptive risk management, and interoperability. Therefore, this research offered the GAUCHO model, a comprehensive cybersecurity framework developed for e-governments. At the same time, GAUCHO associates an adaptive risk management methodology, an authentic data exchange guideline, and a strategic governance stage. Underscoring the framework, regulatory obedience, sustainability, and citizen-centric protection seek to cover intensifying cyber threats in the public industry by combining fragmented security operations. Moreover, the framework facilitates an effective blueprint for protecting digital governance frameworks in increasingly interconnected cultures.

Literature Gaps

After reviewing the articles, the systematic literature review found different major gaps. Initially, there is a lack of study associating IT management competence, particularly at the leadership standard, with robust cybersecurity preparedness, especially in financial institutions. Secondly, previous cybersecurity models often have insufficient personalization for SMEs, making the application complex due to resource limitations and top-down methods. At the same time, while human-centric skills in IT service management are determined, they are not effectively associated with the cybersecurity governance framework. Furthermore, certain offered frameworks possess inadequate empirical justification and are unable to cover regulatory and interoperability barriers in different financial fields. Finally, such gaps demand more associated, practice-based, and context-specific studies.

Methodology

Systematic Review Design

The research developed an SLR focused on the PRISMA ("Preferred Reporting Items for Systematic Reviews and Meta-Analyses") model. This review is intended to interpret previous studies on the association between cybersecurity preparedness and IT management, especially within the field of financial institutions. This research employed a clear and replicable system to confirm the inclusion of a significant and high-quality study.

Data Sources and Databases

Subsequent peer-reviewed and academic databases, such as Google Scholar, ScienceDirect, SpringerLink, IEEE Xplore, and the Web of Science, were examined to gather significant studies. Such databases were chosen for their inclusive coverage of IT governance studies, cybersecurity, and information systems.

Search Strategy and Keywords

An amalgamation of controlled vocabulary and Boolean operators was applied to confirm wide yet concentrated outcomes. The core search terms or phrases involved "IT service management" AND "human-centric skills", "information security" AND "IT governance", "banking sector" OR "financial institutions", "cybersecurity preparedness" OR "cybersecurity awareness", "cyber flexibility" OR "cyber resilience", and "IT leadership skills" OR "IT management competence".

Furthermore, the search strings were incorporated to connect the composition and filtering tools of all databases. Therefore, searches were restricted to peer-reviewed journal articles or studies published in English between the year range 2018 and 2025.

Inclusion and Exclusion Criteria

A transparent set of exclusion and inclusion criteria was followed to confirm the significance and quality of research involved in the systematic review. The inclusion criteria were research papers that followed conceptual, theoretical, and empirical methodologies associated with the review objectives; papers written in English; research concentrating on cybersecurity preparedness, IT management competence, or similar human-centric and governance aspects in digital or financial service sectors; research issues between 2018 to 2025; and conference proceedings or peer-reviewed journal articles.

On the contrary, the exclusion criteria removed studies that possess inadequate information to understand the association between cybersecurity preparedness and IT management competence; those were news articles, editorials, or opinion pieces without experimental support; were not directly connected to cybersecurity or IT management (for example, unrelated digital trends or causal technology incorporation); possessed inadequate full-text accessibility; and were redundant or duplicates publications.

Selection Process

The studies' selection employed the PRISMA guidelines, as demonstrated in the supplementary flow diagram. The research determined 55 articles via database searches, with more than 3 records collected from other sources, resulting in 58 records. Therefore, 37 studies were left for screening after eliminating 21 duplicate accesses.

Furthermore, 25 articles were screened based on their abstracts and titles, and 10 articles were removed because they did not address the required standards. Furthermore, the remaining 15 full-text studies were measured for eligibility. At the same time, 5 articles were also excluded after thorough analysis due to inadequate data or being unable to address methodological standards. Moreover, 10 studies were included in the review, developing the foundation for the thematic amalgamation and evaluation of IT management competence regarding cybersecurity preparedness in certain financial institutions.

Data Extraction and Quality Assessment

This research used a data extraction form to gather continuous data from all the included research, encompassing journal, publication year, author, research methods, and objectives, key outcomes, and implemented models or frameworks. At the same time, quality assessment was designed applying a structured appraisal checklist incorporated from the CASP ("Critical Appraisal Skills Programme"), analysing all the papers for application of instruments or frameworks, significance to research questions, consistency of analysis, and transparency of aims and methods. Therefore, only studies addressing at least three among these four quality standards were included in the final amalgamation.

Thematic Alignment of Review Findings

Theme 1: Technical adaptability and mastery

Financial institutions highly depend on adaptive technical competencies to respond to changing digital transformation stress and cyber threats. A study on cybersecurity leadership emphasizes that robust leaders are efficient in legacy systems and also competent in analysing and organizing emerging technologies such as identity-based access, blockchain, and AI control effectively, directing different threats and integrating technical remedies with strategic objectives (Gilbert & Gilbert, 2024).

Theme 2: Purpose-driven IT leadership

In cyber risk governance, strategic leadership needs transparency of aim and association with organizational goals. Research emphasized that fragmented leadership models weaken cyber resilience. At the same time, coordinated and intentional leadership, especially at executive standards, assists in aligning cybersecurity intent throughout disparate roles, regulating organizational transparency and trust in mission (Lehto & Limnéll, 2021).

Theme 3: Empathy and communication as core skills

Robust communication and empathy play essential roles in IT-based cultures. Experimental research has illustrated that leaders who design security measures in a way that mirrors non-technical stakeholders encourage compliance and buy-in. Empathy in a software engineering environment was associated with optimized stakeholder involvement, while communication models (such as SACCIA) facilitate high-stakes frameworks for transparency under pressure (Gunatilake et al., 2025; Tejay & Winkfield, 2025).

Theme 4: Balancing people, projects, and operations

IT service management calls for a continuous balancing performance, upholding operational stability, project delivery, and user expectations simultaneously. At the same time, leadership study underscores that decision-makers with communication adaptability and agility can effectively transform priorities and reduce disruption, particularly during rapid change cycles or cybersecurity incidents (Umpain et al., 2024).

Theme 5: Business value and strategic alignment

Robust cybersecurity leadership addresses the gap between business value and technical implementation. Research on strategic cybersecurity governance reveals that leaders who introduce risk prevention in terms of business effect, compared to technical jargon, are effectively competent to protect board buy-in, integrate security investments with organizational objectives, and support ROI-based cybersecurity measures (Mızrak, 2023).

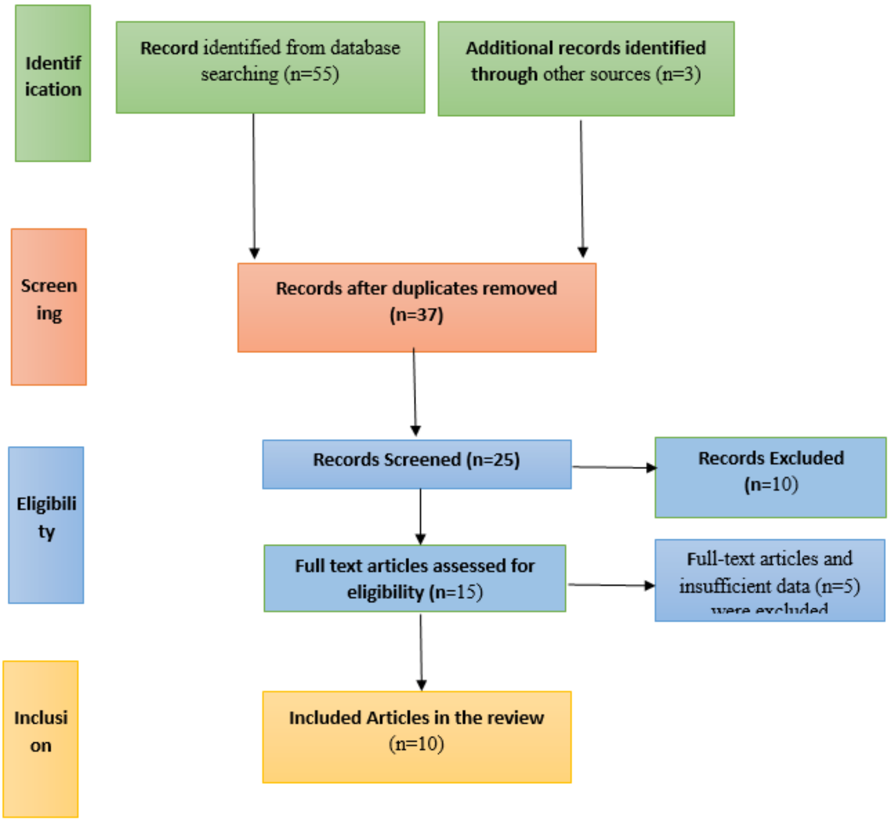
Theme 6: Continuous learning culture in IT

Consistent professional growth is increasingly identified as a crucial aspect for supporting adaptive cybersecurity readiness. Adaptive and agile learning models assist fast-paced upskilling, particularly for IT staff and developers, dynamically shifting learning into an embedded and consistent portion of professional activities rather than an interrupted circumstance (Tariq, 2025).

Theme 7: Meta-skills for decision-making and resilience

Decision-making and resilience under ambiguity are meta-skills that differentiate well-performing IT leaders in cybersecurity fields. Organizational research emphasizes situational awareness, executive amalgamation, and resilience training as essential for directing cyber events. Therefore, leaders with meta-skills are effectively incorporated to uphold calm, make fast and informed decisions, and support teams through emergencies (Virtanen & Yli-Viikari, 2023).

PRISMA Model


Identif ication
Record identified from database searching (n=55)
Additional records identified through other sources (n=3)
Screen ing
Records after duplicates removed (n=37)
Records Screened (n=25)
Records Excluded (n=10)
Eligibili ty
Full text articles assessed for eligibility (n=15)
Full-text articles and insufficient data (n=5) were excluded
Inclusi on
Included Articles in the review (n=10)

Results and Discussion

Summary of Key Findings

The amalgamation of chosen research papers emphasizes different key competencies that reinforce cybersecurity preparedness in financial institutions.

Mastery and technical adaptability is found as important as banks adopts advanced behavioural analytics, machine learning, and AI to determine and prevent standard threats or challenges in real time (for example, OCR-based fraud detection, AI-enabled cloud monitoring) (van de Wetering et al., 2018).

Purpose-based IT leadership is essential for associating cyber risks with organizational risk strategy rather than considering them only an IT concern. In the present scenario, some institutions uphold a superficial association between technical risk realities and board-level risk interpretations (Adeniran et al., 2024).

“Communication” and “empathy” support in addressing the distance between non-technical stakeholders and technical experts. Leadership that constructs cybersecurity principles as fair and practical enhances employee compliance and buy-in (Tejay & Winkfield, 2025).

Robust maintaining of operations, projects, and people allows institutions to uphold incident response and operational continuity without interruption, particularly among increasing third-party risks and resource limitations. At the same time, business value and strategic alignment are making a hike in cybersecurity from a compliance expense to a performance-enhancing and trust-building discipline, assisting executive-level decision-making and investment (McCoy, 2025).

Furthermore, continuous upskilling and learning culture, such as ML/AI, security automation, and data analytics, assist in mitigating the skills gap and continue resilience in the long term (Manikanta & Time, 2024). On the contrary, meta-skills of resilience and decision-making, including upholding composure under stress, stimulating crisis teamwork, and implementing clear recovery planning, are highly essential in high-stakes financial cyber culture (Mulgund et al., 2023).

Practical Implications for Financial Institutions

Such findings indicate different strategic necessities for financial organizations, such as accelerating technical adaptability, implementing cyber risk in organizational governance, boosting human involvement and communication, encouraging a resilience culture and continuous learning, and validating incident practices and recovery. Institutions need to spend on scalable security automation platforms (such as identity governance, XDR, and ML/AI-driven threat analytics) matched to both smaller and large organizations (Devi, 2025). Boards need to raise cybersecurity to certain strategic risk settings, associating threat intelligence with operational resilience and scenario planning frameworks (Mishchenko et al., 2021). Design communication practices and leadership methods that construct policies in availability, suitable contexts to promote security culture and employee assessment (Tejay & Winkfield, 2025). Secure continuous investment in organized training schemes and certifications that underscore both scenario-based and technical response skills (Angafor et al., 2023). Develop response planning, crisis communication, and reproduction practices similar to national schemes (for example, SIMEX, CBEST) as appropriate benchmarks (Keys & Shapiro, 2018).

Findings integrate with the expert perspectives of Smedberg

Such empirical outcomes effectively address the professional perspectives of Smedberg about IT service management quality. Smedberg’s stress on purpose-based leadership reflects the requirement to link cyber processes with wider organizational effect and value. The support of Smedberg for technical control, composed with complex questioning, is echoed in the sector’s transformation toward automation-aware skills in new technologies. The expert’s concentration on empathy and communication associates with the study’s summary that security leadership needs to involve stakeholders. His determination to balance operations, projects, and people integrates with outcomes that continuity and resilience break in human-centered and agile management. Moreover, his demand for meta-skills, resilience, and continuous learning echoes with the determined requirement for a comprehensive security culture and adaptive leadership.

Moreover, the study outcomes justify and improve practitioner-based observation of Smedberg, emphasizing the authoritative of associated competence, technical, strategic, learning-focused, and human-centered to boost cybersecurity preparedness in the financial industry.

Conclusion

The review emphasizes the essential role of IT management competence in promoting cybersecurity preparedness in the financial context. The outcomes showed that beyond technical efficiency, success depends on a continuous learning culture, robust communication, human-centric leadership, and strategic alignment. Associating the practitioner perspectives of Smedberg with experimental data, this research highlights that cybersecurity is a technical role and a trust-making enabler. Financial institutions need to establish purpose-based and adaptable IT leadership assisted by meta-skills, continuous upskilling, and strong governance for decision-making under pressure.

Acknowledgement

The researcher thankfully acknowledges the actionable contributions of the research team and the main researcher for their expertise, insight, and dedication in constructing this research. Their promise to improve knowledge in cybersecurity preparedness and IT management becomes instrumental in the successful accomplishment of this systematic review.

References

[1] Adejumo, A. P., & Ogburie, C. P. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(3), 1542-1556. http://dx.doi.org/10.30574/wjarr.2025.25.3.0909

[2] Adeniran, I. A., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Efunniyi, C. P. (2024). Strategic risk management in financial institutions: Ensuring robust regulatory compliance. *Finance & Accounting Research Journal*, *6*(8), 1582-1596. https://doi.org/10.51594/farj.v6i8.1508

[3] Angafor, G. N., Yevseyeva, I., & Maglaras, L. (2023). Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, *31*(4), 404-426. https://doi.org/10.1108/ICS-05-2022-0085

[4] Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, 1-20. https://doi.org/10.1007/s42786-025-00056-3

[5] Brezavšček, A., & Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052

[6] Devi, Y. (2025). The Future of Cybersecurity: Predicting Trends and Preparing for Emerging Threats. *International Journal of Emerging Research in Engineering and Technology*, 263-275. https://doi.org/10.63282/3050-922X.ICRCEDA25-128

[7] Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919

[8] Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security*, *24*(3), 1-19. https://doi.org/10.1007/s10207-025-01024-0

[9] Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A systematic literature review. *arXiv preprint arXiv:2503.11659*. https://doi.org/10.48550/arXiv.2503.11659

[10] Gilbert, C., & Gilbert, M. A. (2024). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5*(12), 1174-1191. http://dx.doi.org/10.55248/gengpi.5.1224.3429

[11] Gunatilake, H., Grundy, J., Hoda, R., & Mueller, I. (2025). The Role of Empathy in Software Engineering--A Socio-Technical Grounded Theory. *arXiv preprint arXiv:2504.13002*. https://doi.org/10.48550/arXiv.2504.13002

[12] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/j.eswa.2023.122697

[13] Keys, B., & Shapiro, S. (2018). Frameworks and best practices. In *Cyber Resilience of Systems and Networks* (pp. 69-92). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_4

[14] Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

[15] Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4), 177. https://doi.org/10.1007/s10207-025-01097-x

[16] Manikanta, S., & Time, R. (2024). AI and Automation in Cybersecurity: Future Skilling for Efficient Defense. *ISACA Journal*, (3).

[17] McCoy, E. (2025). Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis. *Law, Economics and Society*, *1*(1), p115-p115. https://doi.org/10.30560/les.v1n1p115

[18] Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics*, *13*(21), 4226. https://doi.org/10.3390/electronics13214226

[19] Mishchenko, S., Naumenkova, S., Mishchenko, V., & Dorofeiev, D. (2021). Innovation risk management in financial institutions. *Investment Management and Financial Innovations*, *18*(1), 191-203. http://dx.doi.org/10.21511/imfi.18(1).2021.16

[20] Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. http://dx.doi.org/10.17261/Pressacademia.2023.1807

[21] Modi, A., Kuzminykh, I., & Ghita, B. (2023). Data Driven Approaches to Cybersecurity Governance for Board Decision-Making--A Systematic Review. *arXiv preprint arXiv:2311.17578*. https://doi.org/10.48550/arXiv.2311.17578

[22] Mulgund, P., Higgins, K., Singh, R., Li, Y., & Chew, S. L. (2023). A qualitative exploration of stressors influencing CISO burnout.

[23] Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal*, *5*(4), 903-925. https://doi.org/10.51594/csitrj.v5i4.1049

[24] Shaker, A. S., Al Shiblawi, G. A. K., Union, A. H., & Hameedi, K. S. (2023). The role of information technology governance on enhancing cybersecurity and its reflection on investor confidence. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(6), 7. http://dx.doi.org/10.26668/businessreview/2023.v8i6.1605

[25] Singh, C. (2023). The european approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (nis2) directive 2022/2555. *International Company and Commercial Law Review*, *5*, 251-261.

[26] Tariq, M. U. (2025). Enhancing Cyber Resilience in Software Development: Integrating Secure Coding Practices and Cybersecurity Frameworks. In *Navigating Cyber Threats and Cybersecurity in the Software Industry* (pp. 35-64). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6250-1.ch003

[27] Tejay, G. P., & Winkfield, M. (2025). Does Leadership Approach Matter? Examining Behavioral Influences of Leaders on Employees' Information Security Compliance. *Information Systems Frontiers*, 1-21. https://doi.org/10.1007/s10796-025-10592-4

[28] Tran, T. N. (2025). Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice. *arXiv preprint arXiv:2503.00070*. https://doi.org/10.48550/arXiv.2503.00070

[29] Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

[30] Umpain, S. H., Herachwati, N., Setiadi, Y., & Hanorsian, A. E. (2024). A systematic literature review of interpersonal communication strategies for optimizing government employee performance in the digital era. *F1000Research*, *13*, 979. https://doi.org/10.12688/f1000research.149729.1

[31] van de Wetering, R., Mikalef, P., & Pateli, A. (2018). Strategic alignment between IT flexibility and dynamic capabilities: An empirical investigation. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *9*(1), 1-20. https://doi.org/10.4018/IJITBAG.2018010101

[32] Virtanen, P., & Yli-Viikari, T. (2023). Exogenous Shocks, Resilience, and the Evolution of Public Governance, the Case of Finland. In *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 4590-4604). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-66252-3_4180