Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 3, 2753-2760
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i3.5865

Building resilience: A strategic framework for managing information security risks

Blerton Abazi[1*]
[1]University for Business and Technology UBT, Prishtina, Kosovo; blerton.abazi@ubt-uni.net (B.A.).

Abstract: Information security risk management and its connection to incident handling play a crucial role in today's digital landscape, where threats to data integrity and confidentiality are widespread. This study explores the importance of information security risk management and its relationship with incident handling to enhance understanding and awareness in the field. Initially, existing literature on information security risk management and incident handling was reviewed to identify research gaps. The findings revealed that comprehensive risk assessments, evaluations of an organization's current security posture, and the deployment of advanced security technologies are key steps for building an effective information security risk management system. However, several challenges hinder successful implementation, such as organizational resistance to change, limited resources, lack of expertise, and regulatory compliance complexities. By examining how businesses handle information security incidents, this study offers valuable insights into integrating risk management with incident response. Beyond contributing to academic research, this work provides practical recommendations for organizations looking to bolster their information security in an ever-evolving environment.

Keywords: *Framework, Information security, Incident response, Risk assessment, Risk management.*

1. Introduction

In an increasingly digitized world, the protection of sensitive information has emerged as a paramount concern for organizations across all sectors. The escalating frequency and sophistication of cyber threats have underscored the critical need for robust information security risk management and effective incident handling. These two components are integral to safeguarding data integrity, confidentiality, and availability, yet their integration remains a challenge for many organizations. Despite widespread recognition of their importance, gaps persist in both academic understanding and practical implementation, particularly in aligning risk management strategies with incident response capabilities.

This study addresses these gaps by exploring the interplay between information security risk management and incident handling. Drawing on a comprehensive review of existing literature, the research identifies key areas requiring further investigation and employs Saunders' Research Onion model to guide its methodology. Adopting an interpretive research philosophy and an inductive approach, the study utilizes semi-structured interviews with nine security managers to gather qualitative data, which is then analyzed thematically. The findings reveal that effective information security risk management hinges on comprehensive risk assessments, evaluations of organizational security postures, and the deployment of advanced security technologies. However, significant challenges, including organizational resistance to change, resource limitations, expertise shortages, and regulatory complexities, often impede successful implementation.

By examining how organizations manage information security incidents, this research provides valuable insights into the integration of risk management and incident response frameworks. Beyond its academic contributions, the study offers practical recommendations for organizations seeking to

History: Received: 14 January 2025; Revised: 13 March 2025; Accepted: 17 March 2025; Published: 29 March 2025
* Correspondence: blerton.abazi@ubt-uni.net

enhance their information security resilience in the face of evolving threats. This work thus bridges the gap between theory and practice, providing a strategic framework that can inform both future research and organizational decision-making in the dynamic field of information security.

2. Literature Review

Businesses worldwide are increasingly recognizing the benefits of digitalization, as noted by Kraus, et al. [1]. However, despite its numerous advantages, digitalization also introduces significant risks, particularly the heightened threat of cyberattacks for companies adopting these technologies [2]. A "cyber-attack" is defined as an attempt to damage, disrupt, or gain unauthorized access to a device, computer system, or electronic communication channel. The primary motivation behind these attacks is often the theft of sensitive corporate information. The financial services sector is notably vulnerable, accounting for 96% of all hacker attacks [3]. To mitigate the impact of cyber threats, Information Security Risk Management (ISRM) is commonly employed. ISRM focuses on securing information in terms of privacy, reliability, and accessibility. Despite these efforts, the frequency of attacks on businesses and online services continues to rise [4]. New types of cyber threats reveal the inadequacy of current static risk management approaches, which typically only update periodically, a few times a year [5]. Risk management is fundamentally about estimating potential harm and risks. The International Organization for Standardization defines risk as the "effect of uncertainty on objectives," encompassing unauthorized use, disruption, modification, or destruction of information. While traditional data-driven risk assessments were effective when fewer devices were internet-connected, they are less suitable in today's rapidly changing environment [6]. Experts recommend that the information security risk management process should evolve into a more dynamic system, where actions are continuously adjusted to meet new organizational and social challenges [7]. Addressing these challenges requires not only solving social issues but also tackling technical aspects of information security, as highlighted by Lapke and Dhillon [8]. A holistic approach that integrates both technical and social dimensions is essential for managing cyber threats effectively, as suggested by. The term "social" refers to human-related risks that consider user behavior, while "technical" pertains to technological risks that exclude user behavior [9]. In this context, "static" denotes a fixed state, whereas "dynamic" implies an ongoing response to changes [10]. Initially focused on the financial sector, a dynamic risk management model can be adapted for any organization seeking to regularly assess risks, set priorities, and decide on protective measures. This model will be developed using Design Science Research Campbell, et al. [11] a methodology aimed at creating and validating innovative solutions for complex problems. Despite the current emphasis on either technological or social aspects of cyber threat prevention, there is a notable lack of literature on dynamic risk management. Related research explores the works of various scholars, including [12-14]. Highlighting the need for a combined social and technological approach to adaptive risk management in combating cybercrime.

2.1. Information Security Risk Management

The International Organization for Standardization (ISO) defines risk as the "effect of uncertainty on objectives" and describes risk management as "coordinated activities to direct and control an organization with regard to risk." The risk management process involves systematically applying management policies, procedures, and practices to activities such as communication, consultation, context establishment, and risk identification, analysis, evaluation, treatment, monitoring, and review. In the context of information security, Information Security Risk Management (ISRM) encompasses handling all risks related to data usage in digital environments. This process focuses on maintaining integrity, availability, and security of information while managing threats that could compromise information security. The primary goal is to align risk management efforts with the organization's overall risk tolerance. The ISO standard provides guidelines for conducting risk assessments, managing and accepting risks, reporting and managing risks, and performing risk reviews to protect information assets. According to Lapke and Dhillon [8] the three main components of ISRM are risk assessment, mitigation strategies, and evaluation. These elements are essential for managing and reducing risks to an acceptable level, ensuring the organization's information security aligns with its risk management objectives. The literature highlights the challenges of current ISRM standards, which often rely on static principles that may not adequately address the dynamic nature of modern cyber threats [5, 7, 15]. Experts recommend adopting a more dynamic and emergent approach to risk management, integrating both technical and social aspects to effectively manage cyber threats [16].

2.2. Potential Issues and Obstacles in Applying Current ISRM Standards

The current suite of Information Security Risk Management (ISRM) standards aims to standardize the management of information security across various forms. These standards significantly contribute to an organization's ISRM processes, as noted by Al Harthi [17]. Despite the availability of numerous risk management standards and recommendations, organizations often face confusion regarding which ones to implement [18, 19]. This confusion has prompted scholars to compare and analyze existing ISRM techniques, as there is limited guidance on selecting the most appropriate one [17], [18]. Researchers hope that sharing their findings will assist businesses in selecting and utilizing an effective ISRM strategy. For example, Montesino and Fenz [20] and Montesino and Fenz [21] examined and contrasted several ISRM approaches and proposed a basic technique for assessing information security risks. Similarly, Bagheri [18] evaluated various ISRM strategies based on factors such as cost, scope, availability of implementation information, execution complexity, and required skills. They also proposed a methodology for businesses to choose the best ISRM strategy. Despite improvements in ISRM practices due to standards and recommendations, organizations encounter challenges when adopting an ISRM standard [22]. One significant challenge is the need for specialized knowledge and resources to implement ISRM standards effectively [23]. Consequently, the creators of these standards have designed a more formal and sophisticated implementation method, which can be particularly difficult for organizations lacking an ISRM system and with limited resources and knowledge. Christiansson and Hudson [23] conducted three comprehensive case studies of organizations purportedly compliant with best-practice information security standards to gain insights into their risk assessment processes. The study found that instead of performing the detailed evaluations required by the standards, the organizations adopted a more casual and straightforward approach. These findings align with those of Von Solms, et al. [24] and Wright [25] regarding the motivation to adopt standards. Siponen [26] and Siponen and Willison [27] noted that the mere existence of ISRM procedures is sufficient for standards compliance, without regulating the level of detail. Furthermore it is highlighted that some organizations view compliance as an end in itself rather than a means to enhance security measures. According to Tanriverdi [28] this leads to a compliance culture where individuals focus more on meeting organizational policies and standards than on actively improving security. The lack of consensus on terminology and meanings in ISRM literature can lead to misunderstandings and affect implementation. Different terms are used to describe similar processes, such as "risk assessment," which encompasses identifying, analyzing, and evaluating risks. This process can be broken down into more manageable components, including identifying threat sources, events, vulnerabilities, and predisposing conditions, and determining likelihood, impact, and risk. Brackney and Anderson [29] use the term "risk analysis" to encompass analyzing and assessing risks. Various terms are used to describe the process of rating hazards based on their impact and likelihood. Some sources use "assess risk," while others use "evaluate risk" [30, 31]. Additionally, the terms "response," "treat," and "mitigate" are used interchangeably to describe actions taken to reduce risks to a manageable level. The use of varying and contradictory language and semantics in current ISRM materials can confuse organizations and impact the guidance provided by standards and guidelines.

3. From Detection to Response: Strengthening Cybersecurity Through Effective Incident Handling

Cybersecurity incident response is an ongoing critical function for companies dealing with security threats. According to Van der Kleij, et al. [32] and Detection and Modeling [33] incident response encompasses preparation, detection, containment, investigation, recovery, and post-incident learning. Effective incident response requires organizations to develop robust response capabilities; without these, companies face significant risks, including potential operational shutdowns. Recent research highlights the severe financial impact of security breaches, with large enterprises experiencing an average global cost of $1.23 million and small to medium-sized businesses (SMBs) facing $120,000 in damages[34, 35]. This represents a notable increase of over 25% compared to figures from 2017.

Establishing a comprehensive incident response capability involves substantial effort, including communication with both internal and external stakeholders, developing policies and procedures, defining roles and responsibilities within the incident handling team, and implementing effective tools and services. Monitoring and measuring the maturity of the incident response process is crucial for its success.

Incident response is a vital component of information security management [36, 37]. This encompasses organizational processes for preventing, detecting, containing, mitigating, recovering from, and learning from incidents [22]. The objective is to minimize the impact of security incidents on systems and business operations. The increasing frequency and severity of information security events have heightened interest in incident response from both academic and practitioner perspectives. Researchers focus on enhancing organizational readiness and responsiveness to security breaches. International standards and guidelines, such as those from SANS, ISO/IEC 27035, and NIST SP 800-61, offer valuable frameworks for preparing and managing security incidents.

Recent literature explores various facets of the incident response cycle. For instance, studies have examined incident planning, preparation, and the integration of lessons learned into broader information security management practices. Additionally, research has investigated the structure, roles, effectiveness, and challenges faced by incident response teams. This paper will review and discuss the latest literature on incident response management and its implications.

4. Preparing for Effective Cybersecurity

Ezingeard and Bowen-Schrire [38] emphasize that the preparation and planning phase is critical for organizations to respond quickly and effectively to security incidents. During this phase, organizations develop an Information Security Incident Response (ISIR) strategy, secure executive support, design an ISIR management system, and update risk assessments and security policies as needed. Several sources, including [18, 39, 40]. Highlight that creating an Incident Security Incident Response Team (ISIRT) and conducting training and awareness sessions are also integral to this phase. Bagheri [18] note that setting up a comprehensive information security program involves developing security policies, implementing security measures, and conducting education and awareness activities.

Despite the recommendations from standards like ISO/IEC 27035, Jeong, et al. [40] found that many organizations lack adequate planning for ISIRs. A survey of 19 participants from six different companies revealed that these companies either lack an ISIR strategy or have an insufficient plan. This finding aligns with earlier research by Tanriverdi [28] which reported that many organizations fail to engage in adequate incident preparedness. Both academic and practitioner literature support the need for incident planning and preparation, yet actual implementation remains sparse, possibly due to a lack of practical guidance and a technical focus on the process [28].

The second phase of incident management, as outlined by Methods and tools for the development [41] involves responding to security incidents. This phase begins when a security event occurs and includes activities such as detecting, containing, eliminating, and recovering from the incident. These procedures are predominantly technical in nature.

DOI: 10.55214/25768484.v9i3.5865

The follow-up phase, described by Shinde and Kulkarni [42] is the final stage of the incident response process. It involves reviewing and analyzing the incident to determine necessary changes to the security program, such as adding additional controls. This phase is iterative, with insights from the follow-up phase informing the preparation and planning stage. This iterative process ensures organizations are continually prepared.

Recent research indicates that the ISIRT often focuses on technological aspects during the follow-up phase, with limited consideration of strategic management from a managerial perspective. Al-Ahmari, et al. [43] observe that incident-based learning tends to be informal and ad hoc, with insufficient opportunities to apply lessons learned broadly. Current ISIR methodologies primarily focus on recommending improvements to security systems, often neglecting a comprehensive evaluation of the entire ISIR process. Riadi and Prayudi [37] argue that the response and post-incident learning phases are undervalued.

In response to these challenges, Horne, et al. [44] conducted interviews and surveys with security and forensics professionals, recommending that ISIR practices incorporate formalized and structured learning processes. They highlight the need to integrate informal learning and tacit knowledge to enhance educational effectiveness. Horne, et al. [44] further explored issues within ISIRT and their impact on overall security functions, identifying inconsistent incident response methods, an unstructured information-sharing system, and an overemphasis on technical training at the expense of policy and risk considerations. To address these problems, Horne, et al. [44] propose a two-loop model for an event learning system designed to improve the efficiency and effectiveness of incident response practices.

3.1. Limitations of the Study and Future Directions

This research has significantly advanced the detailed examination of information security risk management and its connection to incident handling. However, it has certain limitations that may affect the study's generalizability. The primary limitation is that the qualitative approach used in the research might restrict the extent of quantitative analysis, making statistical inferences challenging. Consequently, future research should consider combining both quantitative and qualitative methods to achieve more comprehensive findings and address the potential limitations of each approach. Another limitation is the reliance on self-reported data collected through semi-structured interviews, which may introduce bias or inaccuracies. Therefore, future studies should employ alternative data collection methods to minimize potential bias and inaccuracies. These considerations should be considered in future research conducted on the same variables.

5. Conclusion

The research underscores the critical role of information security risk management in effective incident handling, examining its integration with incident response processes. The study evaluated whether current incident management practices align with industry standards. Findings indicate that developing a strong information security risk management system necessitates a comprehensive approach, following the Plan-Do-Check-Act cycle to enhance security posture and minimize business risks efficiently. The research highlights that integrating risk management with incident response is essential for a robust security framework, making these processes pivotal components of a broader cybersecurity program. Various organizational strategies for integration were identified, including combining risk assessment with incident response, fostering collaboration between security teams, and leveraging automation for swift detection and response to security incidents. These strategies ensure a seamless and consistent risk management and incident response process. The study also identified significant challenges in implementing information security risk management, such as organizational resistance to change, limited resources, lack of expertise, and regulatory compliance complexities. Overcoming these challenges requires leadership commitment, adequate budgeting for training, resource allocation, and fostering a security-conscious culture across the organization. Additionally, the research explored diverse incident management techniques used by organizations, ranging from detection and containment to response and recovery. Methods include establishing incident response teams, implementing incident response plans, utilizing threat intelligence, and conducting post-incident analysis for continuous improvement.

6. Recommendations

To strengthen information security, it is important to start by raising awareness and providing strong training programs that focus on current threats. Training helps employees learn how to identify, respond to, and prevent security problems. Topics like avoiding phishing, creating secure passwords, and safely handling data should be included. Companies need to invest time and money to make sure these training programs are updated regularly to keep up with new cyber threats. Without proper training, employees may unknowingly create security risks for the organization.

Another key step is creating and testing incident response plans. These plans guide how to act quickly and effectively during a security breach to reduce damage and recovery time. Regular testing, like practicing realistic attack scenarios, helps find weaknesses and improve response actions. For smaller companies, testing can take up valuable resources, but the benefits—like reduced downtime and financial losses during real incidents—make it worthwhile.

Good security management also means connecting incident response with risk management processes. This connection ensures that risk evaluations help improve response plans. For example, if a risk assessment shows weak points, the response plan can be updated to address those areas. However, making this work may require teams to work more closely together and even change how the organization is structured, which can be difficult but necessary.

Keeping an eye on threats in real time and using threat intelligence tools can help organizations act before risks turn into problems. Advanced systems, such as those using artificial intelligence, can monitor potential threats and provide early warnings. While these tools can be expensive and need trained staff to use them, they are essential for staying ahead of increasingly complex cyberattacks.

Finally, working together with other organizations and sharing knowledge is very important for improving cybersecurity. Companies can share information about threats and learn from each other to create stronger defenses. Groups like industry alliances and public-private partnerships make this possible. However, companies may hesitate to share information because of concerns about privacy, competition, or reputation. Building trust and clear rules for sharing can help overcome these challenges.

By focusing on these areas—training employees, preparing and testing response plans, connecting processes, monitoring threats, and collaborating with others—organizations can build a better and more flexible security system. This approach reduces risks and makes it easier to recover from future problems, protecting the company's important resources and gaining trust from stakeholders.

Transparency:

The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] S. Kraus, S. Durst, J. J. Ferreira, P. Veiga, N. Kailer, and A. Weinmann, "Digital transformation in business and management research: An overview of the current status quo," *International Journal of Information Management*, vol. 63, p. 102466, 2022. https://doi.org/10.1016/J.IJINFOMGT.2021.102466

[2] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606-1616, 2018. https://doi.org/10.1109/JIOT.2018.2847733

[3] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014. https://doi.org/10.1016/J.JCSS.2014.02.005

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176-8186, 2021. https://doi.org/10.1016/J.EGYR.2021.08.126

[5] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Applied Computing and Informatics*, vol. 9, no. 2, pp. 107-118, 2011. https://doi.org/10.1016/J.ACI.2011.05.002

[6] M. A. Afonasova, E. E. Panfilova, M. A. Galichkina, and B. Ślusarczyk, "Digitalization in economy and innovation: The effect on social and economic processes," *Polish Journal of Management Studies*, vol. 19, no. 2, pp. 22-32, 2019. https://doi.org/10.17512/PJMS.2019.19.2.02

[7] Y.-C. Wei, W.-C. Wu, and Y.-C. Chu, "Performance evaluation of the recommendation mechanism of information security risk identification," *Neurocomputing*, vol. 279, pp. 48-53, 2018. https://doi.org/10.1016/j.neucom.2017.05.106

[8] M. Lapke and G. Dhillon, "A semantic analysis of security policy formulation and implementation: A case study," presented at the In Association for Information Systems - 12th Americas Conference On Information Systems, AMCIS, 2006.

[9] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023. https://doi.org/10.3390/SU151813369

[10] K. Bernsmed, G. Bour, M. Lundgren, and E. Bergström, "An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects," *Journal of Air Transport Management*, vol. 102, p. 102223, 2022. https://doi.org/10.1016/J.JAIRTRAMAN.2022.102223

[11] S. B. Campbell, C. A. Brownell, A. Hungerford, S. J. Spieker, R. Mohan, and J. S. Blessing, "The course of maternal depressive symptoms and maternal sensitivity as predictors of attachment security at 36 months," *Development and psychopathology*, vol. 16, no. 2, pp. 231-252, 2004.

[12] A. Flórez, L. Serrano, U. Gómez, L. Suárez, A. Villarraga, and H. Rodríguez, "Analysis of dynamic complexity of the cyber security Ecosystem of Colombia," *Future Internet*, vol. 8, no. 3, p. 33, 2016. https://doi.org/10.3390/fi8030033

[13] D. L. Nazareth and J. Choi, "A system dynamics model for information security management," *Information & Management*, vol. 52, no. 1, pp. 123-134, 2015. https://doi.org/10.1016/j.im.2014.10.009

[14] P. Cheimonidis and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic literature review," *Future Internet*, vol. 15, no. 10, p. 324, 2023. https://doi.org/10.3390/FI15100324

[15] X. Zhang, M. Xu, G. Da, and P. Zhao, "Ensuring confidentiality and availability of sensitive data over a network system under cyber threats," *Reliability Engineering & System Safety*, vol. 214, p. 107697, 2021. https://doi.org/10.1016/J.RESS.2021.107697

[16] I. Tariq, M. A. Sindhu, R. A. Abbasi, A. S. Khattak, O. Maqbool, and G. F. Siddiqui, "Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning," *Expert Systems with Applications*, vol. 168, p. 114386, 2021.

[17] A. N. Al Harthi, "Effective communication of information security risk," Doctoral Dissertation, Cardiff University, 2019.

[18] A. B. Bagheri, "Potential applications of artificial intelligence and machine learning on diagnosis, treatment, and outcome prediction to address health care disparities of chronic limb-threatening ischemia," *Semin Vasc Surg*, vol. 36, no. 3, pp. 454–459, 2023. https://doi.org/10.1053/J.SEMVASCSURG.2023.06.003

[19] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," *International Journal of Electrical Computer Sciences IJECSIJENS*, vol. 11, no. 5, pp. 23-29, 2011.

[20] R. Montesino and S. Fenz, "Automation possibilities in information security management," in *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011, pp. 259–262, 2011. https://doi.org/10.1109/EISIC.2011.39*, 2011.

[21] R. Montesino and S. Fenz, "Information security automation: How far can we go?," presented at the In 2011 Sixth International Conference on Availability, Reliability and Security (pp. 280-285). IEEE, 2011.

[22] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Computers & security*, vol. 44, pp. 1-15, 2014. https://doi.org/10.1016/j.cose.2014.04.005

[23] R. Christiansson and J. Hudson, "ISRM suggested methods for rock stress estimation—part 4: Quality control of rock stress estimation," *International Journal of Rock Mechanics and Mining Sciences*, vol. 40, no. 7-8, pp. 1021-1025, 2003. https://doi.org/10.1016/J.IJRMMS.2003.07.004

[24] R. Von Solms, H. Van Der Haar, S. H. von Solms, and W. J. Caelli, "A framework for information security evaluation," *Information & Management*, vol. 26, no. 3, pp. 143-153, 1994. https://doi.org/10.1016/0378-7206(94)90038-8

[25] C. S. Wright, *The IT regulatory and standards compliance handbook: How to survive information systems audit and assessments*. Elsevier. https://doi.org/10.1016/B978-1-59749-266-9.00005-9, 2008.

[26] M. Siponen, "Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria," *Information Management & Computer Security*, vol. 10, no. 5, pp. 210-224, 2002. https://doi.org/10.1108/09685220210446560

[27] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, no. 5, pp. 267-270, 2009. https://doi.org/10.1016/j.im.2008.12.007

[28] H. Tanriverdi, "Performance effects of information technology synergies in multibusiness firms," *MIS Quarterly*, pp. 57-77, 2006. https://doi.org/10.2307/25148717

[29] R. Brackney and R. Anderson, "Understanding the insider threat," in *Proceedings of a March 2004 Workshop*, 2004.

[30] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special Publication*, vol. 800, no. 30, pp. 800-30, 2002.

[31] B. Von Solms, "Information security—the third wave?," *Computers & Security*, vol. 19, no. 7, pp. 615-620, 2000. https://doi.org/10.1016/S0167-4048(00)07021-8

[32] R. Van der Kleij, G. Kleinhuis, and H. Young, "Computer security incident response team effectiveness: A needs assessment," *Frontiers in Psychology*, vol. 8, p. 2179, 2017. https://doi.org/10.3389/FPSYG.2017.02179

[33] I. Detection and S. M. Modeling, "Interested in learning SANS institute infosec reading room improving detection , prevention and response with improving detection," *Prevention and Response with Security Maturity Modeling*, n.d.

[34] R. Angraini, A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Procedia Computer Science*, vol. 161, pp. 1216-1224, 2019. https://doi.org/10.1016/J.PROCS.2019.11.235

[35] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers & Security*, vol. 56, pp. 70-82, 2016. https://doi.org/10.1016/j.cose.2015.10.006

[36] S. Ahmad, M. R. Beg, Q. Abbas, J. Ahmad, and S. Atif, "Comparative study between stream cipher and block cipher using RC4 and Hill Cipher," *International Journal of Computer Applications*, vol. 1, no. 25, pp. 0975-8887, 2010. https://doi.org/10.5120/465-770

[37] I. Riadi and Y. Prayudi, "A maturity level framework for measurement of information security performance," *International Journal of Computer Applications*, vol. 141, no. 8, pp. 975-8887, 2016. https://doi.org/10.5120/ijca2016907930

[38] J.-N. Ezingeard and M. Bowen-Schrire, "Triggers of change in information security management practices," *Journal of General Management*, vol. 32, no. 4, pp. 53-72, 2007. https://doi.org/10.1177/030630700703200404

[39] K. Teh, V. Suhendra, S. C. Lim, and A. Roychoudhury, "Singapore's cybersecurity ecosystem," *Communications of the ACM*, vol. 63, no. 4, pp. 55-57, 2020. https://doi.org/10.1145/3378552

[40] C. Y. Jeong, S.-Y. T. Lee, and J.-H. Lim, "Information security breaches and IT security investments: Impacts on competitors," *Information & Management*, vol. 56, no. 5, pp. 681-695, 2019. https://doi.org/10.1016/j.im.2018.11.003

[41] Methods and tools for the development, "“Methods and tools for the development of information security policy — A comparative literature review | I," presented at the EEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/5967304, n.d.

[42] N. Shinde and P. Kulkarni, "Cyber incident response and planning: a flexible approach," *Computer Fraud & Security*, vol. 2021, no. 1, pp. 14-19, 2021. https://doi.org/10.1016/S1361-3723(21)00009-9

[43] S. Al-Ahmari, K. Renaud, and I. Omoronyia, "A systematic review of information security knowledge-sharing research," *HAISA*, pp. 101-110, 2018.

[44] C. A. Horne, A. Ahmad, and S. B. Maynard, "Australasian conference on information systems information security strategy in organisations: Review," *Discussion and Future Research Directions*, 2015.