Borneo International Journal eISSN 2636-9826; Vol. 7 (2); 2024; 77-81
Published by *Majmuah Enterprise*
www.majmuah.com

The Role of Risk Management in Cybersecurity Protocols

[1] MUHAMMAD LOKMAN BIN SABIDI, [2] MOHAMAD FADLI BIN ZOLKIPLI

[1] *University Utara Malaysia, School Of Computing, Sintok, 06010 Bukit Kayu Hitam, Kedah, Malaysia,* [2]*University Utara Malaysia, School Of Computing, Sintok, 06010 Bukit Kayu Hitam, Kedah, MALAYSIA*

Email: [1]lokmansabidi4@gmail.com | Tel: +60199680051 | [2]m.fadli.zolkipli@uum.edu.my |

Received: June 15, 2024
Accepted: June 20, 2024
Online Published: July 8, 2024

Abstract

In today's rapidly evolving digital landscape, cybersecurity risk assessment and management are fundamental to safeguarding organizations against an array of increasingly sophisticated cyber threats. These processes play critical roles in fortifying cybersecurity measures, ensuring operational continuity, and maintaining trust in digital environments, which are essential for the smooth functioning of modern businesses and institutions. Cybersecurity risk assessment involves a systematic process of identifying, analysing, and evaluating potential threats and vulnerabilities that could compromise an organization's digital assets and data integrity. This comprehensive process includes activities such as threat modelling, vulnerability assessments, risk scoring, and the prioritization of mitigation efforts. By conducting thorough assessments, organizations gain valuable insights into their risk landscape, enabling them to prioritize security measures based on the severity and likelihood of potential threats, efficiently allocate resources, and implement targeted security controls that address the most critical risks first. Consequently, cybersecurity risk assessment and management are indispensable pillars of a holistic cybersecurity strategy. Integrating these processes into organizational practices bolsters cyber defences, protects sensitive data, and effectively mitigates evolving cyber threats. This proactive approach enhances an organization’s security posture and builds trust with customers, partners, and stakeholders by demonstrating a commitment to robust cybersecurity practices. Future research may explore emerging risk assessment methodologies leveraging advanced technologies such as artificial intelligence (AI) and machine learning (ML) to predict and counter cyber threats more effectively, as well as innovative risk management techniques incorporating real-time threat intelligence and automated response mechanisms. Additionally, understanding the dynamic relationship between regulatory compliance and cybersecurity resilience can help organizations navigate the complex regulatory landscape while maintaining a strong security posture. Continuous advancements in these areas are essential for staying ahead of cyber threats and maintaining a resilient cybersecurity posture in an increasingly digital and interconnected world.

Keywords: cybersecurity risk assessment, cyber strategy, cybersecurity resilience, cyber posture, threat modelling

1. Introduction

In today's digital landscape, cybersecurity risk assessment and management have become indispensable practices for organizations navigating the complex realm of cyber threats. As technology evolves and cyber threats grow in sophistication, the need to proactively identify, analyse, and mitigate risks to digital assets and sensitive information has never been more crucial. Cybersecurity risk assessment involves a systematic process of evaluating potential threats and vulnerabilities, while risk management encompasses the implementation of strategies and controls to mitigate these risks effectively. This paper delves into the vital role of cybersecurity risk assessment and management in fortifying organizational defences, ensuring data integrity, and maintaining operational resilience amidst evolving cyber threats. Early standalone SCADA systems were not particularly concerned with cybersecurity or security in general (Patel et al., 2005). The main method of achieving security was to limit physical access to system components, each of which had its own communication protocol and was unique. For a long time, security in SCADA systems was considered an afterthought related to safety. But in the last ten years, things have evolved, and a variety of guidelines and regulations pertaining to SCADA system cyber security have been developed. With the increasing interconnectedness of systems and the proliferation of digital platforms, cybersecurity risk assessment and management have transcended mere technical considerations to become integral components of overall business strategy. Organizations must now navigate a complex landscape of cyber threats that target not only technical

vulnerabilities but also exploit human behaviour and organizational processes. This shift underscores the need for a holistic approach to cybersecurity, where risk assessment and management extend beyond IT departments to involve stakeholders across the organization. This collaborative effort ensures that cybersecurity measures align with business goals, regulatory requirements, and industry best practices.

In response to the evolving threat landscape, cybersecurity risk assessment methodologies have evolved to encompass a broader spectrum of risks. Beyond traditional IT risks such as malware and data breaches, organizations now face challenges related to supply chain vulnerabilities, insider threats, and geopolitical risks. Risk assessment frameworks such as the FAIR (Factor Analysis of Information Risk) model and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) provide structured approaches for quantifying and prioritizing these diverse risks. By adopting a risk-based approach, organizations can allocate resources effectively, focus on critical assets, and tailor security measures to specific risk profiles. Moreover, the role of cybersecurity risk management extends beyond mitigation efforts to include resilience-building strategies. This involves not only preventing cyber incidents but also preparing for and responding to them effectively. Incident response planning, business continuity management, and disaster recovery frameworks are essential components of cybersecurity risk management. These strategies ensure that organizations can withstand and recover from cyber incidents with minimal disruption to operations, thereby maintaining trust with stakeholders and customers alike.

2. Literature Review

Cybersecurity has emerged as a critical concern in the digital era, with organizations and individuals facing an ever-expanding range of cyber threats. This literature review aims to analyse and synthesize existing research and literature pertaining to cybersecurity risk assessment and management, providing insights into the current state of knowledge, key findings, challenges, and emerging trends. By examining various scholarly works and reports, this review seeks to contribute to the discourse surrounding cybersecurity risk assessment and management and offer implications for future research and practical applications in the field of cybersecurity. Cybersecurity risk assessments play a crucial role in helping public safety organizations detect and prevent cyber threats to their employees, organizational assets, and key services, among other operational components. According to the Cybersecurity and Infrastructure Security Agency (CISA, 28 October 2021), these assessments are vital for maintaining the integrity and security of critical infrastructure. SAFECOM has created a comprehensive handbook designed to assist managers, owners, and operators of public safety communications systems in understanding the procedures involved in conducting a cyber risk assessment. The goal of this handbook is to improve both operational and cyber security by providing clear guidelines and editable reference tables that help organizations identify and catalogue the staff and resources engaged in each phase of the assessment. Although the handbook includes sample entities and organizations, it recommends customizing the content to fit the specific needs and contexts of different organizations (NIST, CSF).

The literature on risk management extends beyond cybersecurity, encompassing a broad array of applications and techniques. Risk management has become a well-established discipline, with its own set of ISO/IEC standards for risk analysis (ISO, 2018) and managing information security (ISO/IEC, 2018). As the alignment between business objectives and IT strategies becomes more prevalent, managing cybersecurity risks has gained significant importance. For instance, The Open Group developed The Open Group Architecture Framework (TOGAF) to address the multifaceted challenges of business and IT alignment. This framework includes methodologies such as the Factor Analysis of Information Risk (FAIR), which provides a structured approach to risk analysis (Butterworth-Heinemann, Waltham, 2015). The application of such methodologies highlights the importance of systematic and quantitative risk assessment techniques in enhancing organizational resilience against cyber threats. The perspectives provided in these various works offer valuable insights into the different dimensions of cybersecurity risk assessment and management within organizational security. The first perspective emphasizes the critical role of cybersecurity risk assessments for public safety organizations, underscoring the need to protect critical assets and services from cyber threats. It highlights the practical utility of the SAFECOM handbook, which guides managers and operators through the assessment process to bolster both operational and cyber security. This practical approach ensures that organizations can tailor their risk assessment processes to their unique operational contexts and requirements. In contrast, the second perspective highlights the broader framework for risk management that extends beyond cybersecurity, referencing international standards for risk analysis and information security management. This perspective illustrates how established risk management principles and standards can be applied to the field of cybersecurity, providing a comprehensive approach to managing risks. The integration of methodologies such as FAIR within frameworks like TOGAF demonstrates how organizations can address the alignment challenges between business and IT strategies while conducting effective risk analysis.

Together, these perspectives underscore the multidimensional approach required for effective cybersecurity risk assessment and management. Sector-specific guidelines, such as those provided for public safety organizations, offer targeted strategies to address specific operational needs. Meanwhile, broader risk management principles and standards provide a foundation for developing comprehensive security practices that can be applied across various organizational contexts. This holistic approach ensures that organizations can develop robust cybersecurity strategies that not only address immediate threats but also align with broader business and IT objectives, ultimately enhancing their overall security posture and resilience against an evolving threat landscape. In conclusion, the reviewed literature highlights the complexity and importance of cybersecurity risk assessment and management in today's digital environment. By incorporating both sector-specific guidelines and broader risk management frameworks, organizations can adopt a comprehensive approach to mitigating cyber threats. Future research should continue to explore innovative methodologies and technologies that can further enhance the effectiveness of cybersecurity risk management practices, ensuring that organizations remain resilient in the face of an increasingly sophisticated and dynamic cyber threat landscape.

3. Discussion

I. Cybersecurity Risk Assessment Methodologies and Techniques

Cybersecurity risk assessment methodologies encompass both quantitative and qualitative approaches. Quantitative methods involve assigning numerical values to risks, such as probability and impact, to calculate risk scores and prioritize mitigation efforts, often using tools like risk matrices and heat maps (NIST, 2011). Qualitative methods rely on expert judgment and scenario analysis, focusing on descriptive assessments of risk severity and likelihood (ISO, 2009). Both approaches have their strengths and limitations, and organizations should tailor their risk assessment processes accordingly (Chittester and Haimes, 2004). Techniques like threat modelling, which identifies potential threats and attack vectors (Leith, Piper, 2013), and vulnerability assessments, which scan for system weaknesses (Cheminod et al, 2013), are crucial for a comprehensive understanding of cyber risks. Supervisory Control and Data Acquisition (SCADA) systems, a type of Industrial Control System (ICS), are integral to Critical National Infrastructure (CNI) sectors such as energy, water, and transportation (NIST, 2011). These systems monitor and control assets over large geographical areas and were historically secured through physical access controls and proprietary communication protocols (Patel et al., 2005). However, the increasing sophistication, interconnectivity, and standardization of SCADA systems have heightened their vulnerability to cyber threats (Igure et al, 2006). Documented cyber-attacks, such as the 2010 Stuxnet worm that targeted Iranian nuclear facilities (Miller and Rowe, 2012), highlight the escalating risks and underscore the need for robust cybersecurity measures.

Modern SCADA systems face a growing number of cyber threats due to their complex and distributed architecture (Morgan, 2013). Effective cybersecurity risk management for these systems involves tailored risk assessment methodologies and proactive risk treatment plans, which include implementing security controls, updating policies, and establishing incident response measures (NIST, 2010; ISO/IEC, 2011). Historical incidents and expert analyses confirm that cyber threats to SCADA systems are real and expanding, necessitating continuous and adaptive risk management practices (Morgan, 2013).

II. Cybersecurity Risk Management Strategies and Frameworks

Effective cybersecurity risk management is crucial for protecting organizations from cyber threats, and several frameworks offer structured approaches to handle these risks. The NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT are some of the most recognized frameworks. The NIST Cybersecurity Framework consists of five main functions: Identify, Protect, Detect, Respond, and Recover, helping organizations assess their cybersecurity status, find gaps, prioritize actions, and set up risk management strategies that meet industry standards（ISO/IEC, 2012）. It emphasizes risk-based decision-making, continuous monitoring, and stakeholder collaboration to improve defences and response capabilities（Cusack & Ghazizadeh, 2016）.

ISO/IEC 27001 provides a structured approach to managing sensitive data and cybersecurity risks through policies, procedures, and controls that address risks comprehensively, including ongoing monitoring, audits, and continuous improvement （Luiijf, 2013）. COBIT, developed by ISACA, focuses on managing and governing enterprise IT, aligning IT goals with business objectives, assessing risks, and setting up monitoring mechanisms. It emphasizes transparency, accountability, and effective decision-making. Together, these frameworks help organizations strengthen their cybersecurity defences, protect sensitive data, and respond to cyber threats effectively, ensuring smooth operations and maintaining trust with stakeholders （ISO/IEC, 2012；Gartner, 2020）. By adopting and integrating these frameworks, organizations can systematically identify, analyse, and mitigate risks, allocate resources efficiently, and implement targeted security controls. This proactive approach enhances their ability to defend against cyber threats, ensures compliance with regulations and industry standards, and continuously improves their cybersecurity posture in a more digital and interconnected world（Accenture,2019；Kerner,2019）.

III. Challenges and Innovations in Cybersecurity Risk Management

Cybersecurity risk management faces significant challenges due to the rapid evolution of cyber threats, resource limitations, and the complexity of modern IT environments. Organizations often struggle to keep pace with emerging risks, address skill shortages in cybersecurity, and manage the complexities of cloud integration and regulatory compliance (Cheminod et al., 2013;Igure et al., 2006). The fast-changing landscape requires continuous vigilance and adaptation, while the shortage of skilled professionals makes building strong security teams difficult (Nicholson et al., 2012). Additionally, integrating cloud services and adhering to regulatory requirements add complexity to risk management (Luiijf, 2013). However, innovative technologies like artificial intelligence (AI), machine learning (ML), and automation are transforming cybersecurity risk management by enhancing threat detection, anomaly analysis, and proactive risk mitigation (Larkin et al., 2014). Automation tools streamline risk assessment and incident response workflows, and blockchain technology enhances data integrity and supply chain security (Park and Lee, 2014). Integrating risk management with real-time threat intelligence provides actionable insights into potential threats, improves risk mitigation strategies, and facilitates informed decision-making, allowing for prioritized security controls based on threat severity (McQueen et al., 2006).

Integrated risk management platforms offer comprehensive visibility, aiding proactive risk management and strengthening overall cybersecurity resilience (Chittester and Haimes, 2004). These technological advancements enable organizations to better navigate the complex threat landscape, efficiently allocate resources, and maintain robust defences against cyber threats (Gold, 2009). The ongoing development and adoption of these innovations are crucial for addressing the dynamic challenges in cybersecurity risk management (Morgan, 2013).

4. Conclusions

In conclusion, cybersecurity risk assessment and management play pivotal roles in today's digital landscape, offering vital defence mechanisms against evolving cyber threats. As organizations increasingly rely on digital technologies and interconnected systems, the potential for cyberattacks grows, making robust risk assessment and management strategies essential. By systematically identifying, analysing, and mitigating risks, organizations can bolster their resilience and safeguard sensitive data from malicious actors. These processes enable a comprehensive understanding of the threat landscape, allowing for the development of tailored security measures that address specific vulnerabilities and potential attack vectors. Adopting established frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 provides structured guidelines for effective risk management, ensuring that organizations adhere to best practices and maintain compliance with regulatory requirements. Moreover, integrating innovative technologies like AI and automation enhances the efficacy of risk mitigation strategies. AI-driven threat detection systems can analyse vast amounts of data in real-time, identifying anomalies and potential threats with greater accuracy and speed than traditional methods, while automation streamlines incident response processes, reducing the time and effort required to address security incidents and minimizing operational impact. Despite challenges such as resource constraints and regulatory complexities, organizations must maintain a proactive stance in risk management, which includes continuous adaptation to emerging threats, investment in cutting-edge cybersecurity technologies, and fostering a culture of cybersecurity awareness throughout the organization. Employee training programs and awareness campaigns are crucial in mitigating human-related risks, as employees often represent the first line of defence against cyber threats.

Furthermore, establishing robust incident response plans and conducting regular simulations ensure preparedness in the event of a cyberattack, while collaboration with industry peers, government agencies, and cybersecurity experts enhances threat detection and response capabilities. By prioritizing these efforts, organizations can navigate the dynamic cybersecurity landscape more effectively, ensuring the protection of critical assets and maintaining trust with stakeholders in an increasingly digital world. Ultimately, a comprehensive and proactive approach to cybersecurity risk assessment and management not only safeguards the organization's digital assets but also strengthens its reputation and competitive advantage in the marketplace.

Acknowledgments

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the System Network Security Project. This work was supported by Universiti Utara Malaysia.

References

A.Mario, M. Marisa, G. Ricardo, P. Daniel (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Information Management. Volume 1 , (219-238).

B. Venansius, T. Florence (2004). The Enhanced Digital Investigation Process Model. Digital Investigation.(253-260)

B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page(1 April 1993). Towards Operational Measures of Computer Security. Journal of Computer Security. Volume 2, no. 2-3, (211-229).

B. Richard (1 December 1993). Information systems security design methods: implications for information systems development. Information Systems Security. Volume 25, Issue 4, (375-414).

C. Liqun, C. Z, S. N(25 Jun 2007). International Journal of Information Security. International Journal of Information Security, Volume 6, (40-57).

D.Dzung, M. Naedele, T.P. Von Hoff, M. Crevatin(31 May 2005). Security for Industrial Communication Systems. Security and Communication Networks, Volume: 93, Issue 6, (1152-117).

Danda B. Rawat(1 March 2021). Journal of Cybersecurity and Privacy: A new Open Access Journal. Journal of Cybersecurity and Privacy, Volume 1, Issue 1, (195-198).

G. Abdoul Karim, B. Julien, B. Renaud, S. Francois(1 December 2006). A global security architecture for intrusion detection on computer networks. Computer & Security, Volume 27, Issues 1-2, (30-47).

H. Harry, P. Marta (2017). Introduction to Security and Privacy on the Blockchain. IEEE Symposium on Security and Privacy.

K.Hamdi, P. Jose J, V. Daniele, D. Saikou, G. Ross, S. Sachin(2021). Simulation for Cybersecurity:state of the art and future directions. Journal of Cybersecurity, (1-13).

K. Robert Osei, T. Vivian, M. Mingxue, M. Fidelis (15 June 2021). Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Critical Infrastructure Protection. Volume 60.

L. Jianwei, Z. Xiang, Z. Leqi, T. Yusheng, H. Sideng, H. Jinsong(March-April 2024). Neural Networks and Privacy-preserving protocols. IEEE Transactions on Dependable and Secure Computing, Volume 21, Issue 2.

Richard, Szapranski(1 January 1995). A theory of Information Warfare; Preparing for 2020. Journal of Information Warfare. (12).

M. Fabian, D. March, B. Gregory, A. G. Joaquin (19-21 September 2016). Research in Attack, Instrusions, and Defenses. International Symposium on Research in Attacks, Intrusions, and Defences (RAID).

N. N. Tu, L. H. Bing, N. P. Nam, C. T. Jung(June 2020). Cyber Security of Smart Grid: Attack and Defenses. International Conference on Cybersecurity(ICCS)

R. Khairur, S. Benfano (September 2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal. Volume 23, Issue 3, (383-404).

R. Eric(2003). Security Holes… Who cares?. UNISEX Security Symposium.

S. Reza, T. George, T. Carmela (16 December 2016). Privacy Games Along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy. ACM Transaction on Privacy and Security. Volume 19, Issue 4, Article No..11, (1-31)

S.Khalil (2006). A Backpropagation Neural Network for Computer Network Security. Journal of Network and Computer Applications. (710-715)

S. R. Ahmad, Z. Shaza (2016). ACM CCS 2016 Interviews, Part 2. ACM Conference on Computer and Communication Security (CCS)