International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

Cyber security Risk Management: A Theoretical Study

https://www.doi.org/10.56830/IJAMS01202604

Noora A. Hassan
School of Government, University Utara Malysia, Kedah, Malysia
noora_ayoob_moham@gsgsg.uum.edu.my
Esam O. Elharon
School of Government, University Utara Malysia, Kedah, Malysia
Esam_Omar_Saleh@gsgsg.uum.edu.my
Ahmed Z. Metwally
Professor of Auditing, Faculty of Commerce, Suez Canal University, Ismailia, Egypt.
prof.ahmed.zaki@commerce.suez.edu.eg

Received: 25 Oct 2025. Accepted: 5 Dec. 2025. Published: 30 Jan. 2026

Abstract:

This paper explores the evolving landscape of cybersecurity risk management, emphasizing its critical importance for organizations handling vast amounts of sensitive data. With cyberattacks rising dramatically—from individual-targeted threats to complex assaults on businesses and nations—managing these risks has become a top priority for experts worldwide. The study outlines common cyber threats such as malware, ransomware, and distributed denial-of-service attacks, highlighting their severe consequences including data loss, reputational damage, and operational disruption. It presents a comprehensive cybersecurity risk management framework that involves five key steps: scoping the assessment, identifying risks, analyzing likelihood and impact, prioritizing and treating risks through avoidance, transfer, or mitigation, and documenting all findings in a risk register. The paper also discusses recognized standards like ISO 27001, and prominent frameworks including NIST CSF, DoD RMF, FAIR, and the AICPA reporting framework, each providing structured approaches to identify, evaluate, and mitigate cyber risks. The conclusion underscores the increasing complexity of cybersecurity risk management amid technological advances and regulatory pressures, particularly intensified by recent global challenges such as the COVID-19 pandemic. Continuous risk assessment, reassessment, and monitoring are advocated as essential practices to safeguard organizational assets and ensure resilience against emerging cyber threats.

Keywords: Cybersecurity - Risk Management - COVID-19 pandemic - Information Systems.

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

1. Introduction

Cyber security is an ongoing issue for businesses of all sizes. Increasingly, consumers provide a vast amount of their data to businesses, ranging from credit card information to sensitive data like social security numbers. While in the past cyberattacks against individuals were more commonplace, with the amount of data being stored by businesses, malicious actors now directly attack businesses to obtain vast amounts of personal and private data. Recent data from the (Alamri et al., 2024; Apsari & Khudri, 2025; Nelson et al., 2025) show that most risk management experts regard cyberattacks as one of their leading concerns when it comes to the business world. Almost half of all experts stated that it is a top concern. From 2010–2019, data breaches increased from 662 million to over 1,500 million with the number of records exposed increasing from a low 16 million in 2010 to 164 million exposed records in 2019.

The ISACA (originally known as the Information Systems Audit and Control Association) defines cybersecurity as "the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems. The scale of attacks, methods of attacks and objectives of the cyberattack vary greatly. Attacks can vary from single-user individual-level attacks to system-wide or network-wide attacks. These cyberattacks can seek to target individuals, organizations and even nations. At the individual level the attacks may want to obtain personal information or scam data for small amounts of money. At the corporate level the attacks may aim to steal proprietary information on vast caches of customer data, while at a national level the attacks may seek to compromise a nation's security. Recent data on the top five concerns individuals have when it comes to cyber threats shows that even at the individual level, the threat posed by cyberattacks includes identity theft, online fraud and virus attacks (Alahmari & Duncan, 2021; Klumpes, 2023).

1.1 Threats to Businesses

From a business standpoint though, the most common method of cyberattacks which businesses need to contend with are malware, ransomware and DDoS. Malware is the most common attack form and is essentially a malicious software type which includes viruses, worms, trojan horses, bots, etc. which are surreptitiously loaded onto a system and compromise it for the benefit of some other party. Other methods of cyberattacks that are a threat to businesses include ransomware which renders systems unusable until a ransom is paid and distributed denial of service (DDoS) attacks which prevent users from accessing a website until the threat is resolved. Ransomware attacks have increased in recent years with over 50% of surveyed US businesses subjected to a ransomware attack and paying the ransom and another 22% being attacked but not paying (Haque et al., 2025; Lee, 2021). Extensive consequences can arise from a cyberattack, ranging from loss of data, loss of reputation or market equity, internal investigations, regulatory investigations or even disruption of operations.

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

1.2 Cyber security Risk Management

Traditionally, risk management has focused on assessing what has been identified as significant challenges to an organization and its operations and then implementing a set of predetermined compliance-based risk responses. A cyber-RMF (risk management framework) assists the organization in selecting the appropriate and necessary security controls that would protect the organization's assets (information, process and people).

A cyber security risk assessment can be split into many parts, but the five main steps are scoping, risk identification, risk analysis, risk evaluation and documentation (Dioubate & Wan Daud, 2022; Kure et al., 2022).

Step 1: Determine the scope of the risk assessment

A risk assessment starts by deciding what is in scope of the assessment. It could be the entire organization, but this is usually too big an undertaking, so it is more likely to be a business unit, location or a specific aspect of the business, such as payment processing or a web application. It is vital to have the full support of all stakeholders whose activities are within the scope of the assessment as their input will be essential to understanding which assets and processes are the most important, identifying risks, assessing impacts and defining risk tolerance levels. A third-party specializing in risk assessments may be needed to help them through what is a resource-intensive exercise (Alamri et al., 2023; Salin & Lundgren, 2022).

Step 2: How to identify cybersecurity risks

You can't protect what you don't know, so the next task is to identify and create an inventory of all physical and logical assets that are within the scope of the risk assessment. Creating a network architecture diagram from the asset inventory list is a great way to visualize the interconnectivity and communication paths between assets and processes as well as entry points into the network, making the next task of identifying threats easier (Ampel et al., 2024; Thach et al., 2021).

Step 3: Analyze risks and determine potential impact

Now it is time to determine the likelihood of the risk scenarios documented in Step 2 occurring, and the impact on the organization if it did happen. In a cybersecurity risk assessment, risk likelihood -- the probability that a given threat can exploit a given vulnerability -- should be determined based on the discoverability, exploitability and reproducibility of threats and vulnerabilities rather than historical occurrences (Melaku, 2023; Mizrak, 2023).

Step 4: Determine and prioritize risks

Any scenario that is above the agreed-upon tolerance level should be prioritized for treatment to bring it within the organization's risk tolerance level. There are three ways of doing this:

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

1. **Avoid.** If the risk outweighs the benefits, discontinuing an activity may be the best course of action if it means no longer being exposed to it.
2. **Transfer.** Share a portion of the risk with other parties through cyber insurance or outsourcing certain operations to third parties.
3. **Mitigate.** Deploy security controls and other measures to reduce the Likelihood and/or Impact and therefore the risk level.

However, no system or environment can be made 100% secure, so there is always some risk left over. This is called residual risk and must be formally accepted by senior stakeholders as part of the organization's cybersecurity strategy.

Step 5: Document all risks

It's important to document all identified risk scenarios in a risk register. This should be regularly reviewed and updated to ensure that management always has an up-to-date account of its cybersecurity risks. It should include:

- Risk scenario
- Identification date
- Existing security controls
- Current risk level
- Treatment plan -- the planned activities and timeline to bring the risk within an acceptable risk tolerance level
- Progress status -- the status of implementing the treatment plan
- Residual risk -- the risk level after the treatment plan is implemented

A cybersecurity risk assessment is a large and ongoing undertaking, so time and resources need to be made available if it is going to improve the future security of the organization. It will need to be repeated as new threats arise, and new systems or activities are introduced, but done well first time around it will provide a repeatable process and template for future assessments, whilst reducing the chances of a cyber-attack adversely affecting business objectives.

Although specific methodologies vary, a risk management programmer typically follows these steps:

1. Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

2. Analyze the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
3. Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. Priorities the risks.
5. Decide how to respond to each risk. There are generally four options:
    - Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.
    - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).
    - Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
    - Transfer – share the risk with another party, usually by outsourcing or taking out insurance.
6. Since cyber risk management is a continual process, monitor your risks to make sure they are still acceptable, review your controls to make sure they are still fit for purpose, and make changes as required. Remember that your risks are continually changing as the cyber threat landscape evolves, and your systems and activities change.

The international standard for information security management.

Clause 6.1.2 of ISO 27001 states that an information security risk assessment must:

- Establish and maintain information security risk criteria.
- Ensure that repeated risk assessments produce "consistent, valid and comparable results";
- "identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the information security management system";
- Identify the owners of those risks; and
- Analyze and evaluate information security risks according to the criteria established earlier.

Defines five major pillars that are needed for managing Cybersecurity Risk and seven steps that must be followed in carrying out a Risk Assessment:

- Risk identification
- Vulnerability reduction

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

- Threat reduction
- Consequence mitigation
- Enable cybersecurity outcome

NIST CSF: The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) stands as one of the most popular cybersecurity risk management frameworks in the industry. NIST CSF provides an end-to-end map of the activities and outcomes involved in the five core functions of cybersecurity risk management: identify, protect, detect, respond, and recover. NIST Cybersecurity Framework (CSF) contains a set of 108 recommended security actions across five critical security functions identifies, protect, detect, respond and recover. It is designed to help organizations better manage and reduce cyber risk of all types – including malware, password theft, phishing attacks, DDoS, traffic interception, social engineering, and others. Within the documents first pillar Identify -> Risk Assessment -> it states that "the organization understands the cybersecurity risk to organizational operations (including mission, function, image, or reputation), organizational assets, and individuals." Specifically, it recommends organizations take the following steps: (Ambreen et al., 2023; Nkambule & Jansen van Vuuren, 2024; Yang et al., 2020)

- Identify and document asset vulnerabilities
- Tune into the latest cyber threat intelligence from information-sharing forums
- Identify and document threats, both internal and external
- Identify the potential business impacts and likelihood of risk events
- Utilize threats, vulnerabilities, likelihood, and impacts to determine risk
- Identify and prioritize risk responses

DoD RMF: The Department of Defense (DoD) Risk Management Framework (RMF) is the set of standards that DoD agencies use to assess and manage cybersecurity risks across their IT assets. RMF breaks down the development of a cyber-risk management strategy into six distinct steps of categorize, select, implement, assess, authorize, and monitor (Ambreen et al., 2023; Song et al., 2024).

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

FAIR: The Factor Analysis of Information Risk (FAIRTM) is a cyber-risk framework developed by The Open Group for the purpose of helping enterprises understand, measure, and analyze information frisk to help business leaders, cybersecurity experts, and risk professionals make well-informed decisions about their cybersecurity practices (Perols & Murthy, 2021; Yang et al., 2020).

AICPA: The American Institute of Certified Public Accountants (AICPA, 2017) developed an entity-level cybersecurity reporting framework that firms can use to disclose useful information to stakeholders about their cybersecurity risk management program and its effectiveness. The framework consists of the following three components that aim to assist stakeholders in monitoring a firm's cybersecurity risk management program (Demek & Kaplan, 2023; Perols & Murthy, 2021; Prakesh et al., 2025):

1. Management's description of the program.
2. Management's assertion that the program description is in accordance with the AICPA's description criteria and measures of effectiveness in terms of achieving the entity's cybersecurity objectives; and
3. The AICPA's opinion on the description and effectiveness of the controls put in place.

2. Conclusion

Managing risk across the enterprise is harder than ever today. Modern security landscapes change frequently and the explosion of third-party vendors, evolving technologies, and a continually expanding mine-field of regulations challenge organizations. The COVID-19 pandemic and recession have further raised the bar for security and compliance teams by creating more responsibility while diminishing resources. With this backdrop, it's become critically important for your organization to employ a Risk Management Process. Identify and assess to create your risk determination, then choose a mitigation strategy and continually monitor your internal controls to align with risk. Keep in mind, re-assessment, new testing, and ongoing mitigation should always play a prominent role in any risk management initiative.

References:

Alahmari, A. A., & Duncan, R. A. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021*. https://doi.org/10.1109/ECAI52376.2021.9515166

Alamri, B., Crowley, K., & Richardson, I. (2023). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. In *Sensors* (Vol. 23, Issue 1). https://doi.org/10.3390/s23010218

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

Alamri, B., Richardson, I., & Crowley, K. (2024). Cybersecuriy Risk Management and Evaluation Framework of Blockchain Identity Management Systems in HIoT: Experts Evaluation. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3468379

Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2023). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, *6*. https://doi.org/10.31893/multirev.2023ss080

Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Nunamaker, J. F. (2024). Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach. *Journal of Management Information Systems*, *41*(1). https://doi.org/10.1080/07421222.2023.2301178

Apsari, R. D., & Khudri, T. M. Y. (2025). An Evaluation of Cybersecurity Risk Management Implementation at Bank Pembangunan XYZ. *Greenation International Journal of Economics and Accounting*, *3*(1). https://doi.org/10.38035/gijea.v3i1.366

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems*, *49*. https://doi.org/10.1016/j.accinf.2023.100616

Dioubate, B. M., & Wan Daud, W. N. (2022). A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(5). https://doi.org/10.6007/ijarbss/v12-i5/12924

Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review. *The American Journal of Engineering and Technology*, *7*(08). https://doi.org/10.37547/tajet/volume07issue08-14

Klumpes, P. (2023). Coordination of cybersecurity risk management in the U.K. insurance sector. *Geneva Papers on Risk and Insurance: Issues and Practice*, *48*(2). https://doi.org/10.1057/s41288-023-00287-9

Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, *34*(1). https://doi.org/10.1007/s00521-021-06400-0

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5). https://doi.org/10.1016/j.bushor.2021.02.022

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6). https://doi.org/10.3390/risks11060101

Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Pressacademia*. https://doi.org/10.17261/pressacademia.2023.1807

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *NIST Special Publication 800 NIST SP 800-61r3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management A CSF 2.0 Community Profile*. NIST Special .

International Journal of Accounting and Management Sciences
Vol.5 No.1, Jan. 2026
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

Nkambule, M., & Jansen van Vuuren, J. (2024). Integrating Enterprise Architecture into Cybersecurity Risk Management in Higher Education. *International Conference on Cyber Warfare and Security*, *19*(1). https://doi.org/10.34190/iccws.19.1.2189

Perols, R. R., & Murthy, U. S. (2021). The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions. *Auditing*, *40*(1). https://doi.org/10.2308/AJPT-18-010

Prakesh, V., Khare, S., Talwandi, N. S., Surender, Lalar, S., & Thakur, P. (2025). Strategic Framework Form Cybersecurity Risk Management: Enhancing Resilience in an Evolving Threat Landscape. *Lecture Notes in Networks and Systems*, *1287 LNNS*. https://doi.org/10.1007/978-981-96-3284-8_13

Salin, H., & Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. *Journal of Cybersecurity and Privacy*, *2*(2). https://doi.org/10.3390/jcp2020015

Song, J. M., Wang, T., Yen, J. C., & Chen, Y. H. (2024). Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains? *International Journal of Accounting Information Systems*, *54*. https://doi.org/10.1016/j.accinf.2024.100695

Thach, N. N., Hanh, H. T., Huy, D. T. N., Gwoździewicz, S., Nga, L. T. V., Huong, L. T. T., & Nam, V. Q. (2021). TECHNOLOGY QUALITY MANAGEMENT OF THE INDUSTRY 4.0 AND CYBERSECURITY RISK MANAGEMENT ON CURRENT BANKING ACTIVITIES IN EMERGING MARKETS - THE CASE IN VIETNAM. *International Journal for Quality Research*, *15*(3). https://doi.org/10.24874/IJQR15.03-10

Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting and Information Management*, *28*(1). https://doi.org/10.1108/IJAIM-02-2019-0022