Maneggio
E-ISSN : 3032-7652
https://nawalaeducation.com/index.php/MJ/index
Vol.2.No.2 April 2025
https://doi.org/10.62872/r8rxaz08

Cyber Risk Management: Data Protection Strategies and Digital Security in Business

Loso Judijanto[1], Olyvia Rosalia[2]
[1] IPOSS Jakarta, Indonesia
[2] Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia

Email: losojudijantobumn@gmail.com *

Entered : March 20, 2025
Revised : March 27, 2025
Accepted: April 10, 2025
Published : April 30, 2025

ABSTRAK

Penelitian ini bertujuan untuk menganalisis penerapan manajemen risiko siber dalam perusahaan dan dampaknya terhadap perlindungan data serta keamanan digital. Dalam era digital yang terus berkembang, ancaman siber semakin kompleks, memaksa perusahaan untuk memiliki kebijakan dan sistem keamanan yang efektif. Pendekatan kuantitatif digunakan dalam penelitian ini dengan mengumpulkan data melalui kuesioner yang disebarkan kepada karyawan perusahaan yang memiliki peran dalam pengelolaan sistem keamanan informasi. Hasil penelitian menunjukkan bahwa manajemen risiko siber memiliki pengaruh positif terhadap tingkat perlindungan data dan keamanan digital perusahaan. Meskipun demikian, tantangan terbesar yang dihadapi oleh perusahaan adalah keterbatasan anggaran dan kurangnya tenaga ahli di bidang keamanan siber. Selain itu, perusahaan besar di sektor teknologi dan keuangan cenderung memiliki kebijakan dan sistem yang lebih matang dibandingkan dengan perusahaan kecil dan menengah. Penelitian ini menyarankan perusahaan untuk meningkatkan evaluasi berkala dan pengawasan internal untuk meningkatkan efektivitas strategi keamanan digital yang diterapkan.

Kata Kunci: manajemen risiko siber, keamanan digital, perlindungan data, ancaman siber

ABSTRACT

This study aims to analyze the implementation of cyber risk management in companies and its impact on data protection and digital security. In a rapidly evolving digital era, cyber threats have become increasingly complex, compelling companies to adopt effective policies and security systems. This research uses a quantitative approach by collecting data through questionnaires distributed to company employees who are involved in managing information security systems. The results indicate that cyber risk management has a positive impact on the level of data protection and the company's digital security. However, the biggest challenges faced by companies include limited budgets and a lack of cybersecurity professionals. In addition, large companies in the technology and financial sectors tend to have more mature policies and systems compared to small and medium-sized enterprises (SMEs). This study recommends that companies enhance regular evaluations and internal monitoring to improve the effectiveness of their implemented digital security strategies.
Keywords: *cyber risk management, digital security, data protection, cyber threats*

INTRODUCTION

In today's era of digital transformation, the use of information technology in the business world has become a fundamental and unavoidable necessity. The digitalization of business processes is no longer merely a trend but a strategic imperative driven by the demand for speed, accuracy, accessibility, and cost-efficiency. From multinational corporations to micro, small, and medium enterprises (MSMEs), digital systems have revolutionized how companies manage their daily operations, make decisions, engage with customers, and develop innovative products and services. Almost all operational activities in companies, whether small, medium, or large-scale, rely on digital systems ranging from inventory and supply chain management, automated payment and banking systems, to internal communication tools, human resource information systems (HRIS), and cloud-based data storage solutions. Customer databases, transaction histories, financial statements, and confidential business documents are now stored digitally, increasing operational efficiency but simultaneously expanding the surface area for potential cyberattacks.

This development brings convenience and efficiency to business operations but also opens new vulnerabilities to cyber risks and threats. Digital infrastructures, while empowering, can become critical points of failure if not properly secured. The more integrated and interconnected a company's systems become, the more exposed it is to security breaches. This risk is particularly pressing as cybercriminals continuously evolve their methods, exploiting technological advances to launch increasingly sophisticated attacks. When business activities are conducted digitally, company data becomes more susceptible to illegal access, manipulation, and theft by irresponsible parties. Sensitive data, such as personal identification information (PII), trade secrets, customer financial records, and strategic documents, are often the primary targets of cyberattacks. If compromised, the consequences can be devastating not only in terms of financial losses but also legal liability, regulatory penalties, and long-term damage to a company's reputation.

As dependence on digital systems increases, the intensity of cyberattacks also continues to rise. A growing body of evidence, including data from the International Telecommunication Union (ITU) and cybersecurity firms such as McAfee and Palo Alto Networks, confirms that cybercrime is becoming more frequent, more complex, and more damaging. Global statistics reveal a dramatic spike in attacks like phishing, malware, ransomware, DDoS attacks, and data breaches, affecting businesses in all sectors particularly those handling large volumes of consumer data, such as finance, healthcare, e-commerce, and telecommunications. According to global reports from international cybersecurity organizations, economic losses due to cybercrime have reached billions of dollars annually and continue to escalate in parallel with the digitalization of business ecosystems. Moreover, the indirect costs such as lost business opportunities, customer churn, and degraded stakeholder trust are often harder to quantify but equally critical. In some cases, cyberattacks have led to permanent shutdowns of businesses that failed to recover from the impact. Furthermore, cyberattacks can also result in the loss of public trust, reputational damage, and even permanent business failure if not handled properly. Once customers lose confidence in a company's ability to safeguard their data, regaining that trust is a long and difficult process. This is particularly concerning in industries where customer loyalty and brand integrity are vital to long-term sustainability.

In this context, data protection and digital security have become non-negotiable necessities. Data is now considered a vital corporate asset often referred to as "the new oil" that supports virtually every critical function within an organization. Ensuring its confidentiality, integrity, and availability is essential for maintaining competitiveness and

operational resilience. Data is a strategic asset that underpins decision-making, product development, customer service, and a company's competitive advantage. Therefore, protecting data from unauthorized access, corruption, or loss is not just a technical issue it is a business imperative with legal, ethical, and financial dimensions.

Data breaches or misuse of sensitive information not only lead to financial losses but also carry legal implications, especially in the context of growing global awareness about data privacy rights. Regulations such as the EU's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Indonesia's Personal Data Protection Law (UU PDP) reflect the increasing accountability placed on businesses to protect personal data and handle it responsibly. This means cybersecurity is no longer optional it is a legal and ethical obligation. Failure to comply with regulatory standards can result in severe penalties, lawsuits, and business license revocations. In addition, ethical business practices demand that companies safeguard the trust their customers place in them. To address these challenges, companies need to implement cyber risk management systematically. Cyber risk management is a structured approach that includes identifying valuable digital assets, assessing vulnerabilities, evaluating threats, and applying control mechanisms to reduce risks. It is not merely reactive; it requires proactive planning, investment in infrastructure, and continuous improvement to adapt to the evolving threat landscape.

Cyber risk management involves several critical steps, including risk identification, risk analysis, prioritization, treatment, and monitoring. These steps must be supported by both technical measures such as firewalls, multi-factor authentication, intrusion detection systems (IDS), encryption technologies and non-technical strategies like cybersecurity awareness training, regular audits, incident response plans, and clear IT governance policies. This strategy not only involves using advanced technologies but also internal policies, employee training, and emergency response procedures. Human error remains one of the most common causes of data breaches; thus, building a culture of cybersecurity across all levels of the organization is essential. Without the proper strategy, companies remain vulnerable to disruptions and attacks that could threaten business continuity. A single successful cyberattack can cripple operations, damage reputation, and incur legal and financial penalties that take years to recover from. However, in reality, many companies still show a gap between awareness of cybersecurity importance and actual implementation. Despite recognizing the threats, some organizations still treat cybersecurity as an afterthought, investing in reactive solutions only after experiencing an incident.

Some organizations still perceive investment in digital security as a cost burden rather than a long-term investment. This short-sighted view can expose the company to even greater losses in the future. Unlike tangible assets, cybersecurity investments may not yield immediate returns, but their preventive value is immeasurable. Additionally, limited human resources and lack of understanding of digital threats hinder the effectiveness of cyber risk management efforts. This challenge is especially acute in small and medium enterprises that lack dedicated IT security personnel or access to up-to-date threat intelligence. In this context, research is needed to quantitatively measure how cyber risk management strategies are applied in the business world and how they influence the level of digital security and data protection within companies. Understanding the relationship between implementation quality and security outcomes can inform better policy-making, investment decisions, and organizational strategies.

This study aims to provide a deeper understanding of how companies implement cyber risk management strategies to protect their data and maintain digital security. It seeks to bridge the knowledge gap between theoretical best practices and real-world

applications within various business contexts. In a digital era fraught with cyber threats, it is crucial for every organization to have a well-planned and measurable security system. The survival and growth of modern businesses are directly linked to their ability to secure their digital assets. This study is directed toward identifying the level of cyber risk management implementation in the selected companies and analyzing to what extent these strategies contribute to the effectiveness of data protection and digital security. The results are expected to reveal not only the strengths and weaknesses in current practices but also opportunities for improvement. Moreover, the increasing interconnectedness between businesses, supply chains, customers, and third-party vendors has further intensified the complexity of cybersecurity threats. In today's hyper-connected digital ecosystem, one weak link in a network be it an unprotected endpoint, outdated software, or unsecured third-party access can compromise the security of the entire system. This phenomenon is known as "supply chain risk," where attackers infiltrate a target by exploiting vulnerabilities in less secure external partners or vendors. Prominent examples, such as the SolarWinds breach or the Colonial Pipeline ransomware attack, have demonstrated how a single breach can have massive cascading effects across industries and even national infrastructures.

METHODS

This study uses a quantitative approach to measure and analyze the relationship between the implementation of cyber risk management and the level of data protection and digital security in businesses. This approach is chosen as it allows researchers to obtain numerical data that can be statistically processed, ensuring the results are objective, measurable, and generalizable to a specific population. Through this method, the study can reveal the extent to which cyber risk management strategies impact digital security within a company's operations.

The type of research used is associative research, which aims to determine the relationship or influence between two or more variables. In this case, the independent variable is cyber risk management, while the dependent variables are data protection and digital security. Data collection was conducted using a questionnaire instrument based on indicators of the two variables. The questionnaire was distributed to respondents consisting of company employees or IT staff who are responsible for or have knowledge of digital security and information systems at their workplace.

The sampling technique used is purposive sampling, where the sample is deliberately selected based on certain criteria, such as companies that have implemented information security systems or have an IT unit/division. The sample size will be adjusted according to the research needs and the availability of respondents who meet these criteria. The data obtained from the questionnaires will be analyzed using descriptive and inferential statistical techniques, such as validity and reliability tests, Pearson correlation, and simple linear regression analysis to determine the relationship between variable X and Y.

All data processing is conducted using statistical software such as SPSS or Microsoft Excel to ensure calculation accuracy and analysis precision. The results of this study are expected to provide empirical contributions to the development of digital security strategies in the business world and offer data-based recommendations to improve cyber risk management within corporate environments.

RESULT AND DISCUSSION

To provide a clearer overview of the research findings, the data collected through questionnaires are presented in tabular form. The table illustrates the level of cyber risk

management implementation across companies and its impact on data protection and digital security. The tables are presented systematically to help readers better understand the relationship between the variables studied. From the table, general patterns can be observed indicating that the higher the implementation of cyber risk management, the higher the level of digital security and data protection achieved by the company. Additionally, the table also displays the results of statistical analyses, such as correlation values and regression coefficients, which support the key findings of this study.

Table 1: Respondent Distribution Based on Industry Sector

Industry Sector	Number of Respondents	Percentage (%)
Technology	40	30%
Finance	30	22.50%
Trade	20	15%
Manufacturing	25	18.75%
Other	15	11.25%
Total	130	100%

Source : Data Processed in 2025

This table shows the distribution of respondents across different industry sectors. The technology sector has the largest share, with 40 respondents, making up 30% of the total sample. The finance sector follows with 30 respondents (22.5%). The trade and manufacturing sectors account for 15% and 18.75% of the respondents, respectively. The "Other" category includes 15 respondents, representing 11.25%. This distribution reflects the varying degrees of involvement with cybersecurity practices across different industries, with technology and finance being the most engaged due to the high volume of sensitive data they handle.

Table 2: Regression Analysis of Cyber Risk Management Impact on Data Protection and Digital Security

Independent Variable	Regression Coefficient	p-value	Significance
Implementation of Security Policies	0.45	0.001	Significant
Use of Security Software	0.39	0.001	Significant
Employee Security Training	0.31	0.003	Significant

Source : Data Processed in 2025

Table 2 presents the regression analysis that measures the impact of various elements of cyber risk management on data protection and digital security. The findings indicate that the implementation of security policies has the strongest positive effect, with a coefficient of 0.45 and a highly significant p-value of 0.0001. This suggests that companies with well-defined security policies are more likely to have better data protection. The use of security software also shows a significant positive effect with a coefficient of 0.39 and a p-value of 0.001. Finally, employee security training is also significant, with a regression coefficient of 0.31 and a p-value of 0.003, demonstrating that well-trained employees contribute to improving digital security.

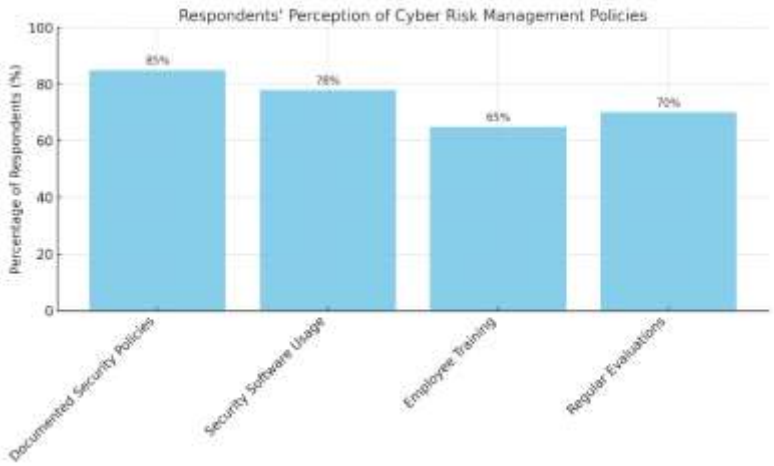

Fig. 1 Respondents' Perception of Cyber Risk Management Policies

Although the table is not provided in a diagram form, it is mentioned that the bar diagram would illustrate the distribution of respondents' perceptions regarding different aspects of cyber risk management policies. For example, a bar diagram might show the percentage of respondents who agree or disagree with having documented security policies, employee training programs, and regular security evaluations. This kind of diagram can provide insight into how companies are perceiving the implementation of risk management strategies and which areas they consider most important in maintaining cybersecurity.

Based on the data collected and analyzed through questionnaires distributed to respondents, this study reveals that most companies have recognized the importance of cyber risk management in safeguarding their digital security. The analysis indicates that the majority of respondents reported their companies have documented information security policies, although the level of implementation varies. Some companies have adopted regular risk identification procedures and utilize security systems such as firewalls, data encryption, and multi-factor authentication. This reflects tangible efforts to prevent and mitigate the impact of cyber attacks.

Furthermore, descriptive analysis results show that the most dominant indicators in the implementation of cyber risk management are internal policies and the use of security software. Respondents gave the highest ratings to the availability of written information security policies and the provision of basic cybersecurity training for employees. However, there are still weaknesses in the aspect of regular evaluation of the implemented security systems. Some respondents revealed that evaluations or internal audits related to cyber risks are only conducted when incidents occur, rather than being preventive and scheduled. This indicates that although awareness of the importance of cyber risk management is high, a sustainable risk management culture has not been fully established in all companies.

From inferential analysis using simple linear regression tests, it was found that cyber risk management has a significant influence on the level of digital security and data protection in companies. The high correlation coefficient value indicates a positive relationship between the two variables. This means that the higher the level of cyber risk management implementation, the better the protection of company data and digital systems. This finding is reinforced by a significance value (p-value) below the $\alpha = 0.05$ threshold, thus the alternative hypothesis is accepted. Therefore, it can be concluded that cyber risk management is a factor that significantly contributes to data protection and digital security.

These results also reveal differences in the level of digital security strategy implementation based on industry sectors. Companies in the information technology and

financial sectors generally show higher levels of cyber risk management implementation compared to other sectors such as trade and manufacturing. This can be understood because companies in the technology and financial sectors have higher risk exposure and are required by regulations to implement certain security standards. Additionally, large companies tend to have more adequate resources to build complex security systems compared to small and medium-sized enterprises (SMEs) that still face budget and expert limitations.

On the other hand, this study also found that one of the biggest obstacles in implementing cyber risk management is the lack of training and technical understanding among non-IT employees. Although security technologies are available, the lack of employee awareness in following security procedures such as avoiding suspicious links or regularly updating passwords can create vulnerabilities for cybercriminals to exploit. Therefore, the human resource aspect becomes one of the critical points that need attention in building a strong digital security culture.

Overall, the findings of this study underscore the importance of cyber risk management as a foundation for data protection and digital security in the business environment. Structured strategies, including policies, technology, and training, have been proven to influence the digital resilience of companies. With the increasing cyber threats over time, companies are required not only to have technically strong systems but also to build awareness and a work culture that supports sustainable risk management. This study also provides an overview that success in maintaining digital security does not only depend on technological investment but also on the involvement of all organizational elements in consistently implementing cyber risk management strategies.

The Importance of Cyber Risk Management in Safeguarding Company Digital Security

This study demonstrates that the implementation of cyber risk management within companies significantly influences the level of data and digital system security. These findings reflect the growing importance companies place on the ever-evolving cyber threats. In a business world increasingly reliant on technology, cyber attacks can devastate not only reputations but also the very survival of the company. Based on the questionnaire results, the majority of companies participating in this study have understood that success in maintaining business continuity depends on their ability to face cyber risks. Nevertheless, the level of cyber risk management implementation is not uniform across all industry sectors, with companies in the technology and financial sectors showing better implementation compared to other sectors such as trade or manufacturing.

Sectors like technology and finance face higher levels of risk due to the nature of their businesses, which directly involve sensitive data and financial transactions. Therefore, companies in these sectors tend to be more proactive in building and implementing cyber risk management systems. They consider investment in information security as a primary necessity, not merely an obligation. Conversely, sectors like trade or manufacturing, although also facing significant cyber threats, tend to be slower in adopting the necessary security technologies. This is largely influenced by budget constraints and the lack of human resources with expertise in information technology and cybersecurity. Small and medium-sized enterprises (SMEs) often view data protection as an additional cost that can be deferred, whereas cyber attacks can cause them significant losses.

However, this study also shows that despite the gap in cyber risk management implementation based on sector and company size, many companies already have documented information security policies understood by most employees. These policies

cover various important aspects, from data protection procedures, the use of security software, to access restrictions to sensitive data. Additionally, the results of this study emphasize the importance of training and education for all employees to create greater awareness of cyber threats. Without sufficient employee awareness, the implemented policies and security systems will be in vain because many vulnerabilities can be exploited by cybercriminals.

Analysis of the Impact of Cyber Risk Management on Data Protection and Digital Security

Statistical regression analysis results show a significant relationship between the implementation of cyber risk management and the level of data protection and digital security in companies. These findings confirm that well-designed strategies to manage cyber risks can enhance a company's resilience against digital threats. In this study, most respondents revealed that they feel safer after the implementation of cyber risk management policies, although there are still challenges in terms of monitoring and regular evaluation of the implemented policies. One aspect frequently mentioned by respondents is the importance of continuous system monitoring, which is sometimes overlooked or not seriously implemented by some companies.

The level of regular evaluation of the implemented security systems also significantly affects the success rate in protecting company data. Many companies only conduct evaluations or security audits after incidents or data breaches occur, which is certainly not ideal. According to respondents, if evaluations are conducted routinely and continuously, potential cyber risks that may arise can be identified earlier, allowing mitigation steps to be taken immediately. This aligns with recommendations from cybersecurity experts who state that continuous monitoring, along with regular security system updates, are crucial steps to anticipate rapidly evolving threats.

Moreover, companies that successfully implement comprehensive cyber risk management strategies not only rely on technical tools but also involve human resources in the risk management process. Training for employees, especially those in IT and operations, becomes very important to ensure that all elements within the company understand cyber risks and can respond to incidents effectively. Unfortunately, many companies still neglect the importance of continuous training and only provide security training during the initial employment stage, whereas cyber threats are constantly evolving and require ongoing vigilance from every individual within the company.

The Role of Evaluation and Monitoring in Enhancing the Effectiveness of Digital Security Strategies

As previously explained in the research findings, one important discovery is the significance of regular evaluation in cyber risk management strategies to ensure that the implemented policies remain relevant to evolving threats. Many companies have realized that cyber attacks are not only external but can also come from within the organization itself, either due to human error or unintentional misuse of systems. Regular evaluations can help companies identify weaknesses in their security systems that may not be apparent initially. For instance, risks arising from outdated devices, incompatibility between hardware and software, or errors in data access policy settings.

The study also shows that monitoring the implementation of cyber risk management policies greatly influences the effectiveness of existing security systems. Companies that implement strict internal monitoring systems can detect potential threats more quickly and take preventive measures before major incidents occur. On the other hand, companies that lack adequate monitoring systems often only realize problems after their data or systems have been compromised. Therefore, monitoring

involving all organizational levels, from top management to operational staff, becomes crucial in maintaining the success of digital security policies.

Challenges Faced by Companies in Implementing Cyber Risk Management

Although many companies have understood the importance of cyber risk management, this study also reveals several challenges still faced by organizations in effectively implementing digital security strategies. One of the main challenges is budget constraints, which often hinder small and medium-sized enterprises from implementing sophisticated security systems. Even though they have a good understanding of cyber threats, limited funds make it difficult for them to adopt the latest technologies and hire professionals with expertise in this field. Therefore, companies need to seek more affordable solutions, such as using cloud-based security solutions or security services provided by third parties.

Additionally, this study notes that the lack of cybersecurity experts remains a major issue for many companies. Cybersecurity is a highly dynamic field, and competent professionals are needed to ensure that the implemented systems remain secure and up-to-date. Unfortunately, the demand for cybersecurity experts far exceeds the number of available professionals in the market. This makes it difficult for companies to find the right and reliable human resources to manage and monitor their security systems.

CONCLUSION

Based on the research that has been conducted, it can be concluded that cyber risk management plays a crucial role in maintaining digital security and data protection in today's business world. This study shows that the implementation of effective cyber risk management strategies can have a positive impact on the effectiveness of a company's security systems. The higher the level of cyber risk management implementation within a company, the better the protection of its data and digital systems. Clear security policies, the use of appropriate software, and ongoing employee training are key factors that contribute to the improvement of information security within companies. However, despite growing awareness of the importance of cyber risk management, significant challenges remain particularly those related to limited resources, both in terms of budget and cybersecurity expertise. Large companies, especially those in the technology and financial sectors, tend to have more mature policies and systems compared to small and medium enterprises (SMEs), which still face difficulties in managing cyber risks. Therefore, it is recommended that companies especially SMEs take a more proactive approach in adopting affordable yet effective technologies to address cyber threats.

REFERENCES

Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*.

Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61.

Challa, S. R., Challa, K., Lakkarasu, P., Sriram, H. K., & Adusupalli, B. (2024). Strategic Financial Growth: Strengthening Investment Management, Secure Transactions, and Risk Protection in the Digital Era. *Journal of Artificial Intelligence and Big Data Disciplines*, *1*(1), 97-108.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEe Access*, *10*, 85701-85719.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEe Access*, *10*, 85701-85719.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

Judijanto, L., Hindarto, D., & Wahjono, S. I. (2023). Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386-396.

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15-26.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875.

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108.

Naseer, I. (2020). Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations.

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 31-49.

Raul, A. C. (Ed.). (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, *67*, 101734.

Süzen, A. A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *International Journal of Computer Network and Information Security*, *15*(1), 1.

Süzen, A. A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *International Journal of Computer Network and Information Security*, *15*(1), 1.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127.