Fairness

Vol 01 (1) 2025 p. 64-80

Corresponding author:
Jessy Juanda.
Email : jessyjuanda885@gmail.com

Received 30 April 2025;
Accepted 20 May 2025;
Published 28 May 2025.

Conflict of interest statement:
Author(s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-fr.2025.1(1)-05

A COMPREHENSIVE LITERATURE REVIEW ON THE IMPACT OF CYBERATTACKS ON ACCOUNTING PRACTICES AND SECURITY MEASURES

Jessy Juanda[1]

[1] STIE Bank BPD Jateng, Indonesia

ABSTRACT

Objective: This research aims to investigate the increasing cybersecurity threats to accounting information systems and assess the effectiveness of cybersecurity governance in mitigating these risks. This research emphasizes the importance of integrating cybersecurity measures into accounting practices to enhance resilience against cyberattacks.

Research Design & Methods: This study uses the Systematic Mapping Study method to comprehensively analyze the existing literature, identify research gaps, and provide a structured overview of cybersecurity governance in accounting. A total of 45 articles from the Scopus database were selected using Publish or Perish 8, covering publications from 2014 to 2024.

Findings: The study revealed that Cyberattacks on accounting systems pose a threat to financial, operational, and public trust. Effective mitigation requires the integration of AI, blockchain, encryption, and employee training, along with investments in regulatory compliance and security to maintain system integrity.

Implications & Recommendations: Practically, organizations should enhance cybersecurity awareness, adopt stricter security policies, and integrate predictive analytics to effectively mitigate cyber threats. Boards of directors play a crucial role in overseeing cybersecurity governance and ensuring the implementation of sustainable risk management strategies. The theoretical implications highlight the need for further empirical research to assess cybersecurity measures across diverse industries and regulatory frameworks.

Contribution & Value Added: This study contributes to the growing literature on cybersecurity in accounting, offering insights into emerging threats and effective mitigation strategies. The study also underscores the importance of a holistic, technology-based approach to cybersecurity management, ensuring long-term resilience in accounting information systems.

Keywords: Cyberattacks, Accounting, Financial Security, Cybersecurity.

JEL codes: M41, M15, G32
Article type: research paper

INTRODUCTION

Digitalization has resulted in many beneficial impacts, including increased accessibility and better flexibility in areas such as education, marketing, and public services (Hadi et al., 2022; Manuputty et al., 2024; Saputra, 2022). Nonetheless, it also has some drawbacks, especially regarding the rise of cyberattacks (Herdiana et al., 2021; Laksana and Mulyani, 2024; Syahputra et al., 2023). These cyber threats can severely compromise data and information security, resulting in significant financial losses. Therefore, it is imperative to raise cybersecurity awareness and implement strategies to mitigate the risks associated with cyberattacks (Suartana et al., 2022; Surya et al., 2024).

In recent years, Indonesia has become an increasingly targeted destination for cyberattacks originating from both within and outside the country. As a developing country experiencing rapid growth in internet access, cybersecurity issues have emerged as a pressing concern. In Indonesia, incidents of cyberattacks are increasing, such as ransomware attacks on government agencies in 2022 that disrupted public services and caused huge losses (BSSN, 2022). In response, the Indonesian government has intensified its efforts to improve cyber defense through international collaboration, increased cybersecurity awareness, and the formulation of stricter policies to address similar threats in the future (Laksana and Mulyani, 2024). Additionally, a 2021 data breach at a telecommunications company, which affected more than one million users, underscores the severity of cyber threats in the business world (Herdiana et al., 2021). To mitigate such risks, organizations should enhance their security protocols by implementing advanced encryption technologies and providing staff with training on effective data security practices (Muravskyi et al., 2021).

The accounting profession is increasingly becoming a target for cyber-attacks, necessitating stricter cybersecurity measures within organizations (Zadorozhnyi et al., 2020). Integration between accounting and cybersecurity is crucial to improve an organization's ability to detect, prevent, and respond effectively to cyber threats (Abrahams et al., 2023). A strong cybersecurity culture has been proven to play a crucial role in reducing the risk of cyberattacks and enhancing an organization's resilience to digital threats (Silva, 2023). Additionally, awareness of the risk of cyberattacks among corporate directors is increasing. This has led to a strengthened supervisory role in ensuring effective cybersecurity risk management (Alashi and Badi, 2020). The impact of cyberattacks on the accounting profession extends beyond the financial aspect to also affect organizational sustainability and trust in financial statements. Cybersecurity incidents can disrupt business operations, compromise sensitive financial data, and undermine stakeholder confidence in the integrity of reported financial information (Daoud and Serag, 2022). Professional accountants should, therefore, raise cybersecurity awareness and adopt proactive measures to protect accounting data from potential threats (Kafi and Akter, 2023).

The optimal implementation of cybersecurity measures, such as continuous monitoring and periodic training, is crucial in establishing a resilient security culture within the organization (Dornheim and Zarnekow, 2024). Integrating predictive analytics with cybersecurity systems can improve the effectiveness of threat detection and response, reduce incident costs, and strengthen operational resilience (Mathew, 2023). Research indicates that professionals with more experience tend to be more compliant in implementing security protocols, highlighting the importance of both training and experience in shaping effective cybersecurity behavior (Alhuwail et al., 2021). With the increasing risk of cyberattacks, organizations must strengthen their protective measures to prevent data breaches and digital threats (Nadeem et al., 2023). Given the evolving dynamics of threats, a comprehensive security strategy is necessary, encompassing both technological aspects and human behavioral factors (Gunawan et al., 2023). Through the implementation of a comprehensive cybersecurity framework, organizations can increase resilience to threats while building trust among stakeholders (Ramírez et al., 2022). Today, the role of organizational governance in ensuring the sustainability of cybersecurity practices is increasingly important. Corporate boards are now taking a more active role in overseeing cyber risk management and ensuring the effective implementation of security strategies (Alashi and Badi, 2020). This shift reflects a broader

understanding of the interconnections between corporate governance, cybersecurity, and business sustainability.

However, a gap remains in research regarding the specific approaches required by the accounting profession in response to evolving cyber threats. This study presents a new perspective by highlighting the integration between cybersecurity governance and the specific needs of the accounting profession. This aspect has not been widely explored in previous research. To address the threat of cyberattacks, the accounting profession requires a proactive approach to cybersecurity. Organizations should prioritize increasing awareness, training, and integrating advanced technologies into their security systems. By establishing a robust cybersecurity culture, implementing best practices, and leveraging predictive analytics, the accounting profession can enhance its cybersecurity posture and safeguard critical financial information against evolving cyber threats.

LITERATURE REVIEW

Cyber threats pose a significant danger to accounting information systems, necessitating the implementation of a robust cybersecurity strategy to safeguard sensitive financial data. The dynamic nature of these threats demands continuous monitoring and customization of security measures to mitigate potential vulnerabilities (Muravskyi et al., 2021). The integrity and dependability of accounting information are crucial, particularly in light of the growing prevalence of cyber threats. The complex nature of information processes in accounting, combined with technological advancements, has led to a surge in cyber threats targeting accounting information systems (Muravskyi et al., 2021). Various forms of cyber threats, including Distributed Denial of Service (DDoS) attacks, ransomware, and Advanced Persistent Threats (APTs), can have a devastating impact on financial institutions, potentially resulting in data loss, financial loss, and operational disruption (Cha et al., 2020). These threats underscore the importance of implementing cybersecurity measures to safeguard accounting information systems against potential breaches (Herath et al., 2022). The increasing frequency of cyberattacks targeting cyber-physical systems further highlights the urgent need for robust security protocols to protect critical infrastructure (Yevseiev et al., 2021).

Cyberattacks on accounting information systems can lead to unauthorized access, data loss, and damage a company's reputation, requiring mitigations such as training and security investments (Surya et al., 2024). This threat highlights the importance of implementing effective cybersecurity policies, including access control, encryption, and firewalls, to safeguard the integrity of financial data (Lehenchuk et al., 2022). The integration of cybersecurity in accounting is key in improving organizational resilience. Blockchain has proven to be effective in maintaining data security and reducing the risk of financial statement manipulation (Zhou and Sun, 2022). Additionally, artificial intelligence-based encryption and threat detection strategies are becoming increasingly important in financial data protection (Dawodu et al., 2023). Innovative methodology linking economics and cybersecurity to minimize financial risks from cyberattacks (Zadorozhnyi et al., 2021). Hybrid threat models and risk analysis across technology sectors also receive attention in cybersecurity strategies (Valenza et al., 2023). Advanced technologies such as blockchain and artificial intelligence increase system resilience by accelerating responses to cyber threats (Gong and Lee, 2021; Preuveneers and Joosen, 2021). Explainable AI facilitates early threat detection and enhances accounting data protection, thereby increasing confidence in financial statements (Kumar et al., 2023). The review confirms that synergies between accounting and cybersecurity are essential in addressing digital threats and ensuring the financial stability of companies.

METHODS

This research employs the Systematic Mapping Study method, a structured methodology designed to provide a comprehensive overview and insight into a particular research domain by systematically organizing and evaluating the existing literature. This approach enables the identification of gaps in previous research and facilitates the development of future studies (Toftedahl, 2021). The articles in this study were sourced from the Scopus database using the Publish or Perish 8 tool. The search process was carried out using keywords such as 'cyberattack', 'accounting information system', 'data security', and 'cybersecurity governance', resulting in 45 selected articles published in the 2014-2024 time span. The selection of articles was considered relevant to the research topic, as well as their publication in highly reputable journals, to ensure the quality and credibility of the sources used.

The research stages were conducted systematically, including the process of searching, selecting, and analyzing relevant articles. This process aimed to categorize previously researched variables and identify inconsistencies in existing research findings. Details of the research stages are illustrated in Figure 1.

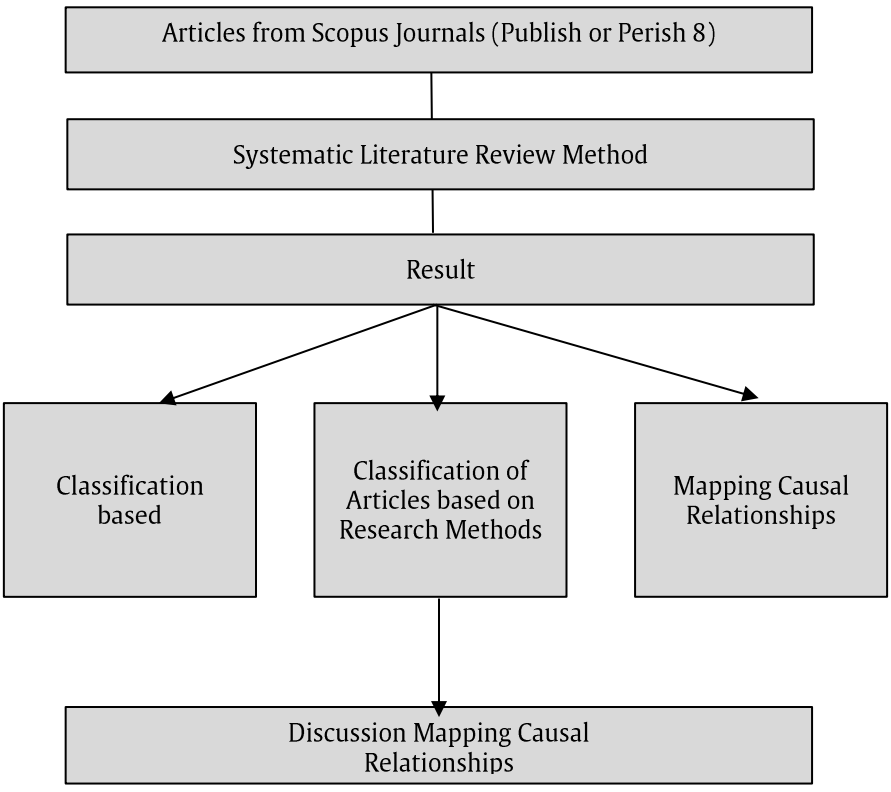

Figure 1. Research Framework

RESULT

Classification by Article

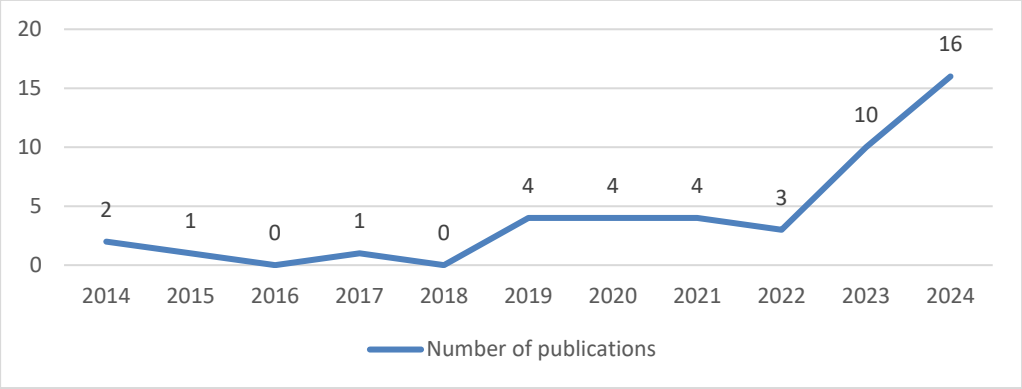

Figure 2. Distribution of Research Publications in 2014 - 2024

The distribution of research publications by year shows a significant upward trend in recent years. As shown in Figure 2, research in this field has increased significantly since 2019. The number of publications, which was initially low in the 2014-2017 period, began to increase in 2019 with four studies, then stabilized in 2020 and 2021 with the same number. In 2023, the number of studies more than doubled compared to the previous year, reaching 10 publications. This trend strengthened further in 2024, with the highest number of studies and 16 publications. This surge indicates an increase in academic interest in the topic, which may be influenced by technological advancements, rising cyber threats, and the need for stricter regulation and enhanced information security in accounting and information systems. This pattern of an increasing number of studies may also reflect the growing urgency of the topic in academia and industry, particularly with the rapid digital transformation and increasing complexity of cyber threats in financial and business systems.

Table 1. Categorization of Articles on Cyber Attack Disclosure

No	Journal	Publication Count
1	Lecture Notes in Networks and Systems	2
2	Computers, Materials, and Continua	2
3	IEEE Access	2
4	Contributions to Finance and Accounting	2
5	Salud, Ciencia y Tecnologia - Serie de Conferencias	1
6	Proceedings of the Annual Hawaii International Conference on System Sciences	1
7	AAAI Spring Symposium - Technical Report	1
8	International Journal of Software Engineering and Knowledge Engineering	1
9	Communications in Computer and Information Science	1
10	Business and Information Systems Engineering	1
11	Journal of Ecohumanism	1
12	EuroMed Journal of Business	1
13	2023 International Conference on Digital Applications, Transformation, and Economy	1
14	2nd International Conference on Unmanned Vehicle Systems	1
15	2023 International Conference on Data Science, Machine Learning, and Security	1
16	2023 IEEE Industry Applications Society Annual Meeting	1
17	Applied Mathematics and Information Sciences	1
18	Financial and Credit Activity: Problems of Theory and Practice	1

No	Journal	Publication Count
19	2023 IEEE Guwahati Subsection Conference, GCON	1
20	Proceedings of the 30th European Safety and Reliability Conference	1
21	Lecture Notes on Data Engineering and Communications Technologies	1
22	International Journal of Control, Automation and Systems	1
23	CEUR Workshop Proceedings	1
24	2022 IEEE International Conference on Communications	1
25	Procedia Computer Science	1
26	Journal of Cybersecurity and Privacy	1
27	Journal of Cases on Information Technology	1
28	ACM International Conference Proceeding Series	1
29	International Journal of Emerging Markets	1
30	Journal of Computer Security	1
31	Jisuanji Yanjiu yu Fazhan/Computer Research and Development	1
32	Baltic Journal of European Studies	1
33	Sustainability (Switzerland)	1
34	Computers and Security	1
35	Journal of Safety Science and Resilience	1
36	Intelligent Automation and Soft Computing	1
37	IEEE Transactions on Dependable and Secure Computing	1
38	2022 IEEE 8th International Conference on Computing, Communication, and Automation	1
39	Zidonghua Xuebao/Acta Automatica Sinica	1
40	Advances in Cybersecurity Management	1
41	International Journal of Recent Technology and Engineering	1
	Total	45

The distribution of research publications indicates that the topic of cybersecurity in accounting and finance is still dispersed across various journals, with no single journal dominating. Of the total 41 journals identified, only four journals have more than one publication, namely Lecture Notes in Networks and Systems, Computers, Materials and Continua, IEEE Access, and Contributions to Finance and Accounting, each accounting for 4.88% of the total publications. This indicates that these journals have a broad scope and serve as the primary reference in the fields of information systems, cybersecurity, and accounting and finance. Meanwhile, 37 other journals have only one publication, indicating that research in this field is still dispersed across various disciplines, including information security, finance, accounting, and business sustainability.

The existence of publications in journals such as the Journal of Cybersecurity and Privacy, the Journal of Computer Security, and IEEE Transactions on Dependable and Secure Computing indicates that aspects of data security and information systems are a major concern in this research. Additionally, journals such as Sustainability (Switzerland) highlight the connection between cybersecurity and business sustainability. The publications found also reflect the important role of conferences in research dissemination, as evident in proceedings-based journals such as the Proceedings of the Annual Hawaii International Conference on System Sciences and the ACM International Conference Proceedings Series.

Based on this publication pattern, it can be concluded that research on cyberattacks, data security, and their impact on accounting and finance is still in its exploratory stage. Academics seem to be still looking for the right platform to publish their work, given that there is no one journal that is the main center in this field. Moreover, this trend also indicates that the field of cybersecurity in

accounting is multidisciplinary, meaning that various disciplines contribute to its development. Going forward, with the increasing number of cyber threats in the financial sector, there will likely be a consolidation of publications in specialized journals that are more relevant to the theme of cybersecurity in accounting and financial systems.

Classification of Articles Based on Research

Based on the analysis of the research methods used in the observed studies, it was found that the literature review approach was the most widely employed method, accounting for a total of 12 articles, or approximately 26.67% of the overall research. This shows that many researchers rely more on reviewing previous research to understand and develop their studies. Furthermore, the case study method ranked second, with 10 articles, or 22.22%. This method is often employed to delve deeper into specific phenomena in real-world contexts, particularly in accounting and cybersecurity. Then, quantitative methods are also quite widely used, with a total of 8 articles or about 17.78%. The use of this method demonstrates that numerical data-based analysis remains a prevalent approach in research related to cybersecurity and accounting.

However, qualitative methods appeared in 7 articles, or around 15.56%. Although less frequent than quantitative methods, this approach still plays an important role in understanding more complex and subjective phenomena. Meanwhile, the Mixed Methods approach, which combines quantitative and qualitative methods, was used in 5 articles or around 11.11%. This reflects researchers' efforts to obtain more comprehensive results by combining the advantages of both approaches. Finally, simulation and experimentation methods are the least used approaches, appearing in only three articles, or around 6.67%. This method is usually applied in technology-based research or system models to test the effectiveness of a concept or solution.

Based on this analysis, it can be concluded that research in this field tends to rely more heavily on literature studies and case studies. At the same time, experimental and simulation-based approaches are still relatively rarely used. This suggests that, while theory development remains the primary focus, there is a growing trend toward empirical, data-driven research in cybersecurity and accounting studies.

Table 2. Categorization of Articles Based on Research Methodology

No	Research Methods	Total Articles	Percentage (%)
1	Literature Review	12	26.67%
2	Case Study	10	22.22%
3	Quantitative	8	17.78%
4	Qualitative	7	15.56%
5	Mixed Methods	5	11.11%
6	Simulations and Experiments	3	6.67%
	Total	45	100%

Causes of Cyber Attacks and Influencing Factors

Cyberattacks are caused by a variety of factors, including system vulnerabilities, malicious cyber activities, human error, limited security resources, and risks associated with new technologies. Lack of data encryption (Wang, 2020) and security gaps in networks, especially in cloud accounting (Daengsi, 2023), make systems vulnerable to exploitation. Malware and ransomware attacks are getting more sophisticated, even targeting blockchain systems (Hasanov, 2024) and critical infrastructure such as solar power (Zhang, 2021). Additionally, human factors, such as low security awareness among accountants (Alsakini, 2024) and errors in managing information systems (Garza, 2023), also increase the risk of attacks. On the other hand, limited organizational resources in cybersecurity (International Conference on Comprehensible Science, ICCS 2021) and difficulties in detecting threats further exacerbate the situation (Vinšalek, 2023). New technologies, such as large language model (LLM) security in cybersecurity (Kang, 2014) and

Markov Models in ship security risk analysis (Mamoon, 2024), also bring new challenges in cyber risk mitigation. Therefore, more adaptive security strategies are needed to address increasingly complex threats.

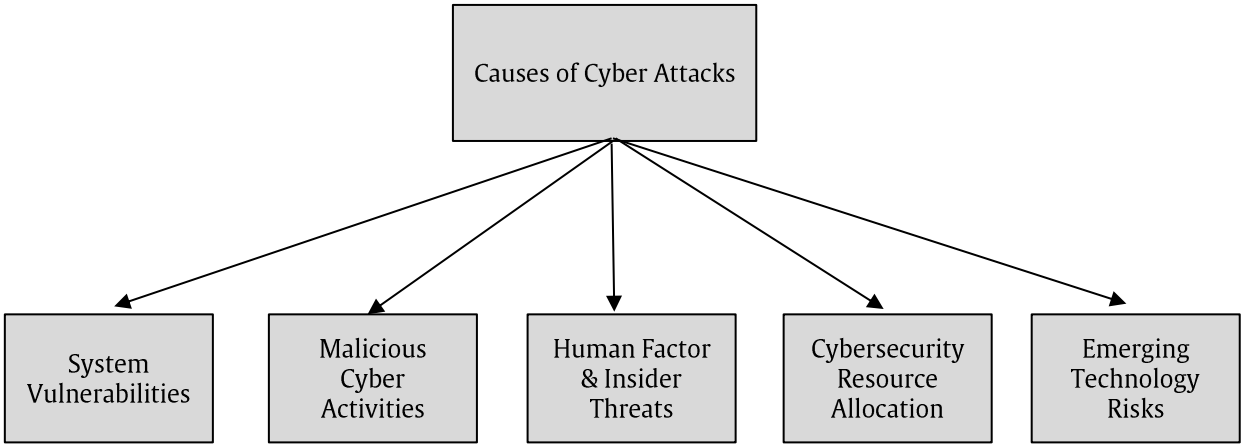

Figure 3. Causes of Cyber Attacks

The Impact of Cyber Attacks on Accounting Systems

Table 3. Impact of Cyber Attacks

Impact	Description	Relevant Articles
Financial Loss	Ransomware attacks and financial data theft result in significant financial losses for accounting firms and their clients.	(Alanazi, 2023; Hasanov, 2024; Hollman, 2017)
Data Manipulation & Fraud	Manipulation of accounting data through malware or exploitation of blockchain systems increases the risk of fraud in financial reporting.	(Al-Asady, 2024; Burton, 2019; Rubio, 2019)
Reputational Damage	Attacks on accounting information systems can lead to a loss of stakeholder trust due to the leakage of client data.	(Chen, 2024; Khan, 2024; Lee, 2023)
Operational Disruption	Disruptions to accounting information systems resulting from cyberattacks lead to delays in auditing and financial reporting.	(Daengsi, 2023; Laichuk, 2023; Mamoon, 2024)
Regulatory & Compliance Issues	Breaches of data security rules (e.g., GDPR or financial sector regulations) due to cyberattacks can lead to legal sanctions and fines for accounting firms.	(Almaiah, 2024; Chu, 2024; Kaminska, 2024)
Increase in Cybersecurity Costs	Accounting firms should increase cybersecurity budgets for technology investments such as encryption and AI-based fraud detection.	(Cranford, 2023; Jemima, 2024; Odularu, 2024)

Cyberattacks have a significant impact on accounting systems, ranging from financial losses and data manipulation to operational disruptions that can lead to legal risks and increased security costs. Data security is a crucial aspect of maintaining stakeholder trust and ensuring compliance with applicable regulations. Additionally, disruptions to accounting information systems can hinder the audit and financial reporting process, leading to operational instability. To further understand the impact of cyberattacks on accounting, please refer to the following table that summarizes the various aspects affected, including risk categories, impact descriptions, and relevant article references.

DISCUSSION

Factors Causing Cyber Attacks in Accounting Systems

1. Vulnerability of Technology Systems and Infrastructure

Vulnerabilities in technology systems and infrastructure are among the primary causes of cyberattacks in accounting. Lack of data encryption and security holes in cloud accounting-based systems make sensitive information vulnerable to unauthorized access (Daengsi, 2023; Wang, 2020). Cloud technology, while offering efficiency and flexibility, also presents significant security challenges, including man-in-the-middle attacks and the exploitation of user credentials, which can result in the leakage of financial data. Additionally, failing to update security systems and software also increases the risk of exploitation by cybercriminals. Organizations that fail to implement proactive security measures, such as multi-factor authentication and intrusion detection systems, are more susceptible to data breaches and cyberattacks.

2. Malicious Cyber Activities

Malicious cyber activity includes a variety of attacks aimed at infecting accounting systems with malware, ransomware, or other exploitation methods. Malware and ransomware are evolving to target more sophisticated technologies, including blockchain-based systems (Hasanov, 2024). In addition, cyberattacks against critical infrastructure, such as solar power systems, target not only financial software but also the technical aspects that underpin overall business operations (Zhang, 2021). These attacks often use phishing techniques, outdated software exploits, and botnet-based attacks to access corporate data without authorization. According to McIntosh et al. (2022), the increase in ransomware attacks within the financial sector suggests that companies should adopt mitigation measures, such as periodic backups and faster incident response, to prevent a greater impact.

3. Human Factors and Insider Threats

The human factor is an element that cannot be ignored in cybersecurity. Lack of security awareness among accountants and human error in managing information systems are often the main causes of attacks (Alsakini, 2024; Garza, 2023). Employees who are not trained in detecting cyber threats can easily become targets of social engineering attacks, where hackers exploit individual negligence to gain unauthorized access. Additionally, insider threats pose a serious issue. Individuals within an organization, whether intentionally or unintentionally, can expose sensitive data or weaken security systems. A study by Greitzer (2019) reveals that more than 30% of data breaches in companies result from insider actions, whether due to malicious intent or negligence. Therefore, companies should implement regular security training and monitoring systems to minimize this risk.

4. Limited Cyber Security Resources

Many organizations face limitations in resource allocation for cybersecurity, which makes them more vulnerable to attacks. A lack of security resources within the organization, as well as uncertainty in detecting threats, are significant obstacles to maintaining secure accounting systems. Organizations with limited budgets often struggle to adopt the latest security technologies or hire competent cybersecurity experts. According to Price water house Coopers (2022), 60% of companies stated that budget constraints and lack of experts are the main obstacles to improving their cybersecurity resilience. Therefore, companies need to adopt a risk-based approach to allocate resources more effectively, including by utilizing artificial intelligence and automation-based security solutions to detect and respond to threats more quickly.

5. New Technology Risks in Cybersecurity

While new technologies bring innovations to accounting and financial systems, they also pose new cybersecurity challenges. The security of large language models (LLMs) in cybersecurity

is a major concern, as they can be used to create more complex attacks, such as deepfake phishing and AI-based data manipulation (Kang, 2014). Additionally, the Markov Model in ship security risk analysis reveals that analytic and predictive technologies are also susceptible to exploitation if not implemented with proper security measures (Mamoon, 2024). According to Brundage et al. (2018), while AI has great potential in improving cybersecurity, it can also be leveraged by malicious actors to increase the scale and sophistication of attacks. Therefore, companies should develop adaptive security strategies and invest in AI-based security technologies that can more effectively recognize attack patterns.

The Impact of Cyber Attacks on Accounting Systems

1) Financial Loss and Economic Risk

Cyberattacks on accounting systems can result in significant financial losses, both direct and indirect. Banking data theft, unauthorized transactions, and ransomware attacks can result in companies losing large amounts of funds. Laksana and Mulyani (2024) demonstrate that ransomware attacks in 2022 resulted in millions of dollars in losses due to encrypted financial data that could only be accessed again after a ransom payment. Additionally, companies must bear the costs of recovery, forensic investigations, and compensation to affected clients (Syahputra et al., 2023). A report by IBM (2023) states that the average loss due to data leakage is $4.45 million per incident, a figure that is increasing annually. To mitigate this risk, accounting firms need to implement data encryption, AI-based suspicious activity monitoring, and secure system backups to prevent further financial impact.

2) Data Manipulation and Fraud Threats in Financial Reporting

Cyberattacks also increase the risk of data manipulation in financial reports, potentially leading to financial fraud. Sophisticated malware can infiltrate accounting systems and alter figures surreptitiously, creating discrepancies between actual transactions and financial records (Silva, 2023). Daoud and Serag (2022) found that data manipulation-based cyberattacks have increased fraud cases in multinational companies, reduced transparency, and decreased investor confidence. In some cases, specially designed malware can infiltrate accounting systems and manipulate financial records without being detected, causing discrepancies between actual transactions and financial statements. A notable example is an American fintech company where hackers employed a cyberattack to alter transaction records before an audit was conducted, resulting in the company's financial statements showing inaccurate results (Boyens et al., 2022). A solution that is beginning to be implemented is blockchain technology, which offers a record-keeping system that is transparent, is difficult to manipulate, and simplifies financial audits. With blockchain, transaction data is stored in an immutable ledger, increasing the security of financial reporting and reducing the risk of cyber fraud (Allison, 2024).

3) Reputational Damage and Loss of Stakeholder Trust

Besides the financial impact, cyberattacks can also damage the reputation of accounting firms, especially in the event of a client data leak. Incidents such as the data leak at a major telecommunications company in Indonesia, which exposed the information of more than one million subscribers, demonstrate the serious impact of cyberattacks on public trust (Syahputra et al., 2023). Deloitte, one of the largest accounting firms, suffered a cyberattack in 2017 that resulted in the leak of its strategic client data, raising concerns about information security in the financial services industry (Bloomberg, 2017). To address this reputational risk, accounting firms should enhance employee awareness of cyber threats, implement robust security systems such as multi-factor authentication (MFA), and have an effective crisis communication strategy in place to respond to incidents transparently and promptly (Singh and Godugula, 2022). As cyber threats escalate, accounting firms must prioritize the security of their systems to safeguard their business data, finances, and reputation.

4) Operational Disruption and Implications for Audit and Financial Reporting

Cyberattacks can cause significant operational disruptions in the audit and financial reporting process. When a company's accounting system is compromised by a Distributed Denial of Service (DDoS) attack or malware, auditors may struggle to access critical documents required for transaction verification and financial statement preparation (Ramírez et al., 2022). DDoS attacks, in particular, can paralyze accounting servers, causing downtime that slows access to real-time financial data (FS-ISAC, 2024). In addition, cyberattacks also have the potential to disrupt data integrity, resulting in a mismatch between actual financial data and that recorded in the system. Ransomware, for example, can encrypt critical accounting files so that financial statements cannot be accessed or verified by auditors (Alashi and Badi, 2020). This can hinder the external audit process, slow down the company's compliance with financial regulations, and reduce the transparency of financial statements. Regulatory implications are also a concern, as delays in financial reporting can lead to sanctions from regulatory authorities, such as the Securities and Exchange Commission (SEC) or other financial regulators (Fierro, 2023). Therefore, companies should develop backup and disaster recovery systems that can operate in emergency conditions and ensure that auditors have alternative access to the data needed during the audit process.

5) Regulatory Challenges and Compliance with Data Security Standards

From a regulatory perspective, cyberattacks also pose challenges in terms of compliance with data security regulations, especially in the accounting sector, which manages highly sensitive financial information. Many countries have adopted strict policies regarding data protection, such as the General Data Protection Regulation (GDPR) in Europe, which requires companies to protect their customers' personal information with adequate security measures (Nadeem et al., 2023). Breaches of this policy due to cyber-attacks can result in serious legal consequences, including substantial fines and lawsuits from aggrieved parties (Gunawan et al., 2023). For example, GDPR violations can lead to companies being fined up to 4% of their total global annual revenue (EDPB, 2022). Within the accounting sector, regulations such as the Sarbanes-Oxley Act (SOX) in the United States require companies to implement robust security systems for financial data to prevent manipulation of financial statements due to cyberattacks. Additionally, the Financial Action Task Force (FATF) provides guidelines on how companies should manage cybersecurity risks related to financial transactions to prevent money laundering and terrorist financing (Smith, 2024). Therefore, accounting firms should ensure that their security policies are compliant with applicable regulations and implement encryption-based security protocols and multi-factor authentication systems to protect financial data from potential exploitation.

6) Increased Cybersecurity Costs and Technology Investments

In response to rising cyber threats, accounting firms are now allocating larger budgets for investments in security technology. Artificial intelligence (AI)-based threat detection systems and predictive analytics are increasingly being used to identify attack patterns before they occur (Mathew, 2023). AI in cybersecurity enables anomaly detection in financial transactions, allowing for the identification of potential attacks before they cause widespread damage (Alhassan and Jin, 2023). However, while investments in cybersecurity can reduce the risk of attacks, the costs incurred are often an additional burden for companies, especially for small and medium-sized accounting firms (SMEs) that have limited financial resources (Taskin et al., 2025). Implementing security technologies, such as advanced firewalls, encryption systems, and 24/7 network monitoring, can be a challenging endeavor.

Therefore, efficient strategies are required that balance cybersecurity investments with the effectiveness of the protection provided. One solution is to adopt a risk-based approach in security budget allocation and utilize cloud-based security services, which are more flexible and cost-effective than traditional security solutions (Firmansyah and IRMAPA, 2024). Cloud security enables companies to obtain subscription-based protection without incurring significant expenses on physical infrastructure. In addition, the Zero Trust Architecture (ZTA) approach, which requires verification of every access to the financial system, has also begun to be implemented in various

financial institutions to mitigate the risk of increasingly complex cyberattacks (Rose et al., 2020). Therefore, while investments in cybersecurity are costly, the long-term benefits of reducing the risk of attacks and protecting the integrity of accounting data are crucial to a company's sustainability.

CONCLUSION

Cyber-attacks not only impact financial aspects but also threaten an organization's operational resilience and trust in financial reports. Disruptions in accounting systems due to attacks such as ransomware, DDoS, and malware can result in significant financial losses, increase the risk of data manipulation and fraud, and hinder the audit and financial reporting processes. In addition, cyberattacks can also damage a company's reputation, resulting in the loss of stakeholder trust and potential loss of business contracts. In the face of these threats, organizations must adopt a proactive cybersecurity strategy that includes implementing advanced technologies such as artificial intelligence and blockchain, enhancing security awareness through continuous training, and ensuring compliance with global regulations, including the GDPR and the Sarbanes-Oxley Act. In addition, companies must also balance investment in cybersecurity with the effectiveness of the protection provided, especially for small and medium-sized accounting firms that have limited budgets.

This research uses a Systematic Mapping Study to analyze 45 articles from the Scopus database (2014-2024) selected through Publish or Perish 8 to map the literature, identify gaps, and direct future studies. Limitations of the study include a limited scope of accounting systems, a temporal coverage that may not reflect the latest cyber threats, and reliance on secondary data, which risks bias. Therefore, further studies, including empirical research, are needed to explore more effective mitigation strategies. Practically, this study emphasizes the importance of cyber threat awareness and preparedness through the adoption of security technologies and strict protection policies. Theoretically, this research enriches the cybersecurity literature in accounting systems and encourages further studies related to threat mitigation. Protection against cyberattacks necessitates a technical approach and a holistic, sustainable risk management strategy to maintain organizational resilience.

REFERENCES

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews, 20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

Al-Asady, S. Y. (2024). Managing Cyber Security Costs for Sustainable Competitive Advantage. *Salud, Ciencia y Tecnologia - Serie de Conferencias*, 3. https://doi.org/10.56294/sctconf2024670

Alanazi, J. M. (2023). An Optimized Method for Information System Transactions Based on Blockchain. *Intelligent Automation and Soft Computing, 35*(2), 2289–2308. https://doi.org/10.32604/iasc.2023.029181

Alashi, S. A., & Badi, D. H. (2020). The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations. *Journal of Information Security and Cybercrimes Research, 3*(1), 97–112. https://doi.org/10.26735/EINT7997

Alhassan, Y., & Jin, H. (2023). Reducing Poverty Through Microfinance in Developing Economies (pp. 39–59). https://doi.org/10.4018/978-1-6684-5647-7.ch003

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. *Applied Clinical Informatics, 12*(04), 924–932. https://doi.org/10.1055/s-0041-1735527

Allison, D. (2024). How Blockchain Enhances Transparency and Security in Financial Transactions for CPAs.

Almaiah, M. A. (2024). Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems. *Computers, Materials and Continua, 81*(2), 3189–3220. https://doi.org/10.32604/cmc.2024.057673

Alsakini, S. A. K. (2024). The Impact of Cybersecurity on the Quality of Financial Statements. *Applied Mathematics and Information Sciences, 18*(1), 169–181. https://doi.org/10.18576/amis/180117

Badan Siber dan Sandi Negara (BSSN). (2022). Laporan Tahunan Keamanan Siber.

Bloomberg. (2017). Deloitte Email Platform and Client Data Hit by Cyberattack.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management for systems and organizations. https://doi.org/10.6028/NIST.SP.800-161r1

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., HÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., … Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://doi.org/10.48550

Burton, J. (2019). Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation. *Baltic Journal of European Studies, 9*(3), 116–133. https://doi.org/10.1515/bjes-2019-0025

Cha, J., Singh, S. K., Pan, Y., & Park, J. H. (2020). Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. *Sustainability, 12*(16), 6401. https://doi.org/10.3390/su12166401

Chen, W. (2024). Gimmick or Revolution: Can Corporate Digital Transformation Improve Accounting Information Quality? *International Journal of Emerging Markets, 19*(10), 2966–2990. https://doi.org/10.1108/IJOEM-04-2022-0572

Chu, K. F. (2024). Multi-Agent Reinforcement Learning-Based Passenger Spoofing Attack on Mobility-as-a-Service. *IEEE Transactions on Dependable and Secure Computing, 21*(6), 5565–5581. https://doi.org/10.1109/TDSC.2024.3379283

Cranford, E. A. (2023). Accounting for Uncertainty in Deceptive Signaling for Cybersecurity. *In Proceedings of the Annual Hawaii International Conference on System Sciences* (Vol. 2023, pp. 876–885). https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85152134905&origin=inward

Daengsi, T. (2023). Analyzing Bank Account Information of Nominees and Scammers in Thailand: Insights from ChaladOhn Website Data. *In 2023 International Conference on Digital Applications, Transformation and Economy, ICDATE 2023*. https://doi.org/10.1109/ICDATE58146.2023.10248609

Daoud, M. M., & Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. *6th International Conference Tanta University Faculty of Commerce, 42*(1), 20–61. https://doi.org/10.21608/caf.2022.251730

Dawodu, S. O., Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., & Hassan, A. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews, 20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

Dornheim, P., & Zarnekow, R. (2024). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security, 32*(2), 179–196. https://doi.org/10.1108/ICS-07-2023-0116

European Data Protection Board (EDPB). (2022). Guidelines 04/2022 on the calculation of administrative fines under the GDPR (Issue May).

Fierro, A. M. (2023). Don't delay – avail of the SEC amnesty today. Pwc.

Firmansyah, H., & IRMAPA, S. (2024). Pendekatan Berbasis Risiko dalam Keamanan Siber: Mengurangi Risiko Gugatan Hukum. *IRMAPA*.

FS-ISAC. (2024). DDoS: Here to Stay. March.

Garza, L. (2023). Detection and Classification of False Data Injection Attacks in Power Grids Using Machine Learning and Hyperparameter Optimization Methods. *In 2023 IEEE Industry Applications Society Annual Meeting, IAS 2023*. https://doi.org/10.1109/IAS54024.2023.10406838

Gong, S., & Lee, C. (2021). Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. *Electronics, 10*(3), 239. https://doi.org/10.3390/electronics10030239

Greitzer, F. L. (2019). Insider Threats: It's the HUMAN, Stupid! Proceedings of the Northwest Cybersecurity Symposium, 1–8. https://doi.org/10.1145/3332448.3332458

Gunawan, B., Ratmono, B. M., & Abdullah, A. G. (2023). Cybersecurity and Strategic Management. *Foresight and STI Governance, 17*(3), 88–97. https://doi.org/10.17323/2500-2597.2023.3.88.97

Hadi, S., Satato, Y. R., & Ainan, M. (2022). Studi Strategi Pemasaran Selama Masa Pandemi Covid 19 Pada UMKM Olahan Tempe Semarang. *E-Bisnis : Jurnal Ilmiah Ekonomi Dan Bisnis, 15*(2), 375–381. https://doi.org/10.51903/e-bisnis.v15i2.882

Hasanov, I. (2024). Application of Large Language Models in Cybersecurity: A Systematic Literature Review. *IEEE Access, 12*, 176751–176778. https://doi.org/10.1109/ACCESS.2024.3505983

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 2*(1), 1–18. https://doi.org/10.3390/jcp2010001

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology, 20*(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Hollman, A. (2017). Cyber in security: A post-mortem attempt to assess cyber problems from it and business management perspectives. *Journal of Cases on Information Technology, 19*(3), 42–70. https://doi.org/10.4018/JCIT.2017070104

IBM. (2023). IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. *In ibm*.

International Conference on Comprehensible Science, ICCS 2021. (2022). In Lecture Notes in Networks and Systems (Vol. 315). https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85115194589&origin=inward

Jemima, P. P. (2024). Malicious Cyber Attacks on Blockchain Handled Using Machine Learning Algorithm. *In Communications in Computer and Information Science* (Vol. 1970, pp. 270–284). https://doi.org/10.1007/978-3-031-75957-4_23

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. https://doi.org/10.18034/ajtp.v10i1.659

Kaminska, N. (2024). Modeling ship cybersecurity using Markov chains: an educational approach. *In CEUR Workshop Proceedings* (Vol. 3679, pp. 22–35). https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85192725147&origin=inward

Kang, Y. S. (2014). A study of the airport model based on security risk. *International Journal of Software Engineering and Its Applications, 8*(11), 67–74. https://doi.org/10.14257/ijseia.2014.8.11.06

Khan, S. (2024). Formal Verification and Security Assessment of the Drone Remote Identification Protocol. *In 2nd International Conference on Unmanned Vehicle Systems-Oman, UVS 2024*. https://doi.org/10.1109/UVS59630.2024.10467159

Kumar, P., Wazid, M., Singh, D. P., Singh, J., Das, A. K., Park, Y., & Rodrigues, J. J. P. C. (2023). Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy, 6*(6). https://doi.org/10.1002/spy2.312

Laichuk, S. (2023). Ensuring Cybersecurity in Accounting in The Digital Economy Era. *Financial and Credit Activity: Problems of Theory and Practice, 6*(53), 145–157. https://doi.org/10.55643/fcaptp.6.53.2023.4254

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin, 3*(01), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Lee, J. H. (2023). Solar Power Plant Network Packet-Based Anomaly Detection System for Cybersecurity. *Computers, Materials and Continua, 77*(1), 757–779. https://doi.org/10.32604/cmc.2023.039461

Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security. *Problems of Theory and Methodology of Accounting, Control and Analysis, 2*(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46

Mamoon, M. (2024). Fully-distributed Consensus Control of Multi-agent Systems Under Stochastic Hybrid Attacks on a Directed Graph. *International Journal of Control, Automation and Systems, 22*(7), 2085–2094. https://doi.org/10.1007/s12555-023-0769-9

Manuputty, C. Z. D., Dorebia, H., & Tafonao, T. (2024). Mentorship Gereja dalam Membentuk Karakter Remaja yang Religius di Era Digitalisasi. *Jurnal Ilmiah Multidisiplin, 1*(1), 74–86. https://doi.org/10.62282/juilmu.v1i1.74-86

Mathew, A. (2023). The 5 Cs of Cybersecurity and its Integration with Predictive Analytics. *International Journal of Computer Science and Mobile Computing, 12*(1), 47–50. https://doi.org/10.47760/ijcsmc.2022.v12i01.006

McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., & Watters, P. (2022). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys, 54*(9), 1–36. https://doi.org/10.1145/3479393

Muravskyi, V., Farion, V., & Hrytsyshyn, A. (2021). Quality of Accounting Information and Principles of its Cyber Protection. *Scientific Notes of Ostroh Academy National University, "Economics" Series, 1(23*(51)), 103–109. https://doi.org/10.25264/2311-5149-2021-23(51)-103-109

Nadeem, M. A., Hashmi, S., & Khan, M. A. (2023). Exploring the Interplay of Cybersecurity and cybercrime in Pakistan's Digital Landscape. *Contemporary Issues in Social Sciences and Management Practices, 4*(4), 207–222. https://doi.org/10.61503/cissmp.v2i4.94

Odularu, O. I. O. (2024). Data Security in Accounting and Information Management During the COVID-19 Pandemic. *In Contributions to Finance and Accounting* (pp. 85–109). https://doi.org/10.1007/978-3-031-64869-4_5

Preuveneers, D., & Joosen, W. (2021). Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. *Journal of Cybersecurity and Privacy, 1*(1), 140–163. https://doi.org/10.3390/jcp1010008

Price water house Coopers. (2022). Global Digital Trust Insights Survey. https://www.pwc.com/dti

Ramírez, M., Ariza, L. R., Miranda, M. E. G., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America–Proposal for a Cybersecurity Disclosure Index. *Sustainability, 14*(3), 1390. https://doi.org/10.3390/su14031390

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *In Controlling Privacy and the Use of Data Assets*. https://doi.org/10.6028/NIST.SP.800-207

Rubio, J. E. (2019). Tracking APTs in industrial ecosystems: A proof of concept. *Journal of Computer Security, 27*(5), 521–546. https://doi.org/10.3233/JCS-191293

Saputra, M. (2022). Integrasi Kewarganegaraan Digital dalam Mata Kuliah Pendidikan Kewarganegaraan untuk Menumbuhkan Etika Berinternet (Netiket) di Kalangan Mahasiswa. *Jurnal Pendidikan Kewarganegaraan, 12*(01), 6. https://doi.org/10.20527/kewarganegaraan.v12i01.13635

Silva, B. De. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime, 12*(1), 23–29. https://doi.org/10.19107/IJISC.2023.01.03

Singh, A., & Godugula, H. (2022). How security risks are impacting hybrid work models.

Smith, D. (2024). Virtual Assets. *In FATF* (pp. 191–219). https://doi.org/10.1007/978-3-031-59842-5_13

Suartana, I. M., Putra, R. E., Bisma, R., & Prapanca, A. (2022). Pengenalan Pentingnya Cyber Security Awareness pada UMKM. *Jurnal Abadimas Adi Buana, 5*(02), 197–204. https://doi.org/10.36456/abadimas.v5.i02.a4560

Surya, D., Doddy Setiawan, Y. Anni Aryani, & Taufiq Arifin. (2024). Cyberattacks on the Accounting Profession :a Literatur Review. *Media Riset Akuntansi, Auditing & Informasi, 24*(2), 255–272. https://doi.org/10.25105/v24i2.19953

Syahputra, A., Junaidi, J., Sukmawati, E., Deprizon, D., & Syafitri, R. (2023). Dampak Buruk Era Teknologi Informasi dan Komunikasi pada Remaja Usia Sekolah (dalam Perspektif Pendidikan Islam). *Journal of Education Research, 4*(3), 1265–1271. https://doi.org/10.37985/jer.v4i3.402

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. *Information (Switzerland), 16*(1). https://doi.org/10.3390/info16010066

Toftedahl, M. (2021). Localization Tools in General Purpose Game Engines: A Systematic Mapping Study. *International Journal of Computer Games Technology,* 1–15. https://doi.org/10.1155/2021/9979657

Valenza, F., Karafili, E., Steiner, R. V., & Lupu, E. C. (2023). A Hybrid Threat Model for Smart Systems. *IEEE Transactions on Dependable and Secure Computing, 20*(5), 4403–4417. https://doi.org/10.1109/TDSC.2022.3213577

Vinšalek, V. S. (2023). Effects of Protection Cloud Accounting and Connection with the Frequency of Cyber Attacks. *In Lecture Notes in Networks and Systems* (Vol. 644, pp. 441–452). https://doi.org/10.1007/978-3-031-43056-5_32

Wang, W. (2020). Allocation of Defense Resources Against Cyber Attacks to Cyber-Physical Systems. *In Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference* (pp. 1331–1337). https://doi.org/10.3850/978-981-14-8593-0_5255-cd

Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., Berestov, D., Fedorenko, R., & Kurchenko, O. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. *Eastern-European Journal of Enterprise Technologies, 5*(9 (113)), 30–47. https://doi.org/10.15587/1729-4061.2021.241638

Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. *Marketing and Management of Innovations, 5*(4), 36–46. https://doi.org/10.21272/mmi.2021.4-03

Zadorozhnyi, Z.-M., Muravskyi, V. V., Shevchuk, O., & Muravskyi, V. (2020). The Accounting System as the Basis for Organising Enterprise Cybersecurity. *Financial and Credit Activity Problems of Theory and Practice, 3*(34), 149–157. https://doi.org/10.18371/fcaptp.v3i34.215462

Zhang, D. F. (2021). Secure State Estimation Based on Distributed Sparse Optimization Under Malicious Attacks. *Zidonghua Xuebao/Acta Automatica Sinica, 47*(4), 813–824. https://doi.org/10.16383/j.aas.c200276

Zhou, W., & Sun, M. (2022). Accounting Cyber Security Based on Blockchain. *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC),* 1254–1257. https://doi.org/10.1109/IPEC54454.2022.9777549