METHODS AND ALGORITHMS OF PROTECTION AGAINST INFORMATION ATTACKS IN DIGITAL TRANSFORMATION

1st **Durdona Irgasheva**
Tashkent University of Information Technologies
Tashkent, Uzbekistan
durdona.ya@gmail.com

2nd **Dilnoza Sodiqova**
Tashkent University of Information Technologies
Tashkent, Uzbekistan
dilnoza_9517@mail.ru

Abstract: *This systematic literature review explores the digital transformation (DT) and cybersecurity implications for achieving business resilience. DT involves transitioning organizational processes to IT solutions, which can result in significant changes across various aspects of an organization. However, emerging technologies such as artificial intelligence, big data and analytics, blockchain, and cloud computing drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. This literature survey article highlights the importance of comprehensive knowledge of cybersecurity threats during DT implementation to prevent interruptions due to malicious activities or unauthorized access by attackers aiming at sensitive information alteration, destruction, or extortion from users. Cybersecurity is essential to DT as it protects digital assets from cyber threats. We conducted a systematic literature review using the PRISMA methodology in this research. Our literature review found that DT has increased efficiency and productivity but poses new challenges related to cybersecurity risks, such as data breaches and cyber-attacks. We conclude by discussing future vulnerabilities associated with DT implementation and provide recommendations on how organizations can mitigate these risks through effective cybersecurity measures. The paper recommends a staged cybersecurity readiness framework for business organizations to be prepared to pursue digital transformation.*

Keywords: *digital transformation; cybersecurity; information technology*

1.Introduction

Digital transformation refers to adopting digital solutions in the business processes of organizations, which can result in significant changes in their business operations. Such modification can impact various aspects of an organization, for instance, user experience, business processes, target markets, customers, customer relationships, and even diverse cultural implications. The accelerated technology adoption by business organizations during the COVID-19 pandemic also resulted in many abrupt challenges [1]. Emerging technologies such as artificial intelligence, big data and analytics, blockchain, cloud computing, the Internet of Things, and the industrial Internet of Things are critical enablers for digital transformation. Due to extensive benefits, businesses are accelerating the digital transformation drive. Still, cybersecurity has grown into a significant challenge for companies, and to gain business continuity, organizations need to secure their digital transformation tools and artifacts. Therefore, it is crucial for organizations undergoing DT adoption to prioritize cybersecurity measures and ensure that their systems are secure from potential threats [2,3].

Cybercriminals may take advantage of vulnerabilities in digital technologies; therefore, organizations must ensure that technological solutions are secure from digital attacks. Cybersecurity can be achieved by implementing encryption, authentication, and access control measures to protect data and networks from unauthorized access or malicious activities. Additionally, organizations should consider investing in cyber insurance policies that can provide financial protection against losses due to a successful attack on their systems. Another critical issue is to raise awareness among employees regarding cybersecurity attacks, as higher awareness results in dependable information security behavior [4,5]. Cyber-attacks have drastically escalated; therefore, business organizations must understand cybersecurity threats and how best to mitigate them comprehensively. These attacks usually aim to assess, change, or destroy sensitive information; extort monetary benefits from users; or interrupt normal business processes. Cybersecurity involves techniques to protect computers and networks from unauthorized access and malicious activities such as data theft and destruction.

Cybersecurity costs and cybercrimes are exhibiting an increasing trend globally [6]. Haislip et al. [7] highlighted that the economic cost of cybersecurity breaches is underestimated, as it is not only limited to the targeted form; they spill over to the industry concerned through negative returns and higher insurance costs. Garg [8] has highlighted seven critical benefits of investing in cybersecurity to motivate organizations in making cybersecurity investments. These include protecting intellectual property, better meeting customer requirements, minimizing customer turnover, branding secure products, joining secure vendors in an integrated network, company reputation, and minimizing collateral damage in the industry. Lee [9] has presented a risk management framework focusing on continuously improving cybersecurity practices and cost–benefit analysis for cybersecurity investments. Many organizations use the National Institute for Standards and Technology (NIST) Cybersecurity Framework for cybersecurity risk management; however, the standard lacks a cost–benefit analysis. The Gordon–Loeb model has been proposed to identify which tier of NIST is more effective for a particular organization in terms of cost–benefit study [10]. Krutilla et al. [11] enhanced the Gordon–Loeb model by considering the depreciation cost of cybersecurity assets, which can impact the cost–benefit analysis of cybersecurity initiatives. Simon and Omar [12] highlighted that companies may be affected by cybersecurity risks via cybersecurity attacks on their supply chain partners, so they maintain that cybersecurity investments need to consider both coordinated and uncoordinated attacks. Uddin et al. [13] highlighted that cybersecurity weaknesses impact organizational growth and performance, and, especially for the banking sector, operational risks have increased due to cybersecurity threats. Curti et al. [14] highlighted that cybersecurity attacks are on the rise in the governmental sector, and to mitigate these threats, governments are increasing governmental operating costs and overall financing costs.

In this paper, we have conducted a systematic literature review that documents how digital transformation has changed the business sector and the implications of cybersecurity for digital transformation. We have investigated the papers published during 2019–2023 using PRISMA guidelines for conducting a literature review. We have proposed a cybersecurity readiness framework for business organizations pursuing digital transformation. The findings of this paper will help business organizations, practitioners, and researchers to grasp the state of the art in this domain and will form the basis for further research.

This paper is organized as follows: Section 2 outlines the methodology adopted to conduct the survey, and Section 3 discusses the literature in detail. Section 4 provides a discussion, and a conclusion is offered in Section 5.

2.Materials and Methods

In this section, we explain the methodology. We did a systematic literature review using the PRISMA guidelines [15]. As shown in Figure1, we used the Google Scholar database. Primary studies were extracted using specific keywords in search criteria. Keywords were chosen to facilitate the generation of research articles relevant to our topic. The search terms used were (business transformation) AND (security), (digital transformation) AND (cybersecurity), (digital transformation) AND (cyber security), (digital transformation) AND (protection), and (digitization) AND (security). To refine our search results, we used the following inclusion criteria:

- The paper should be relevant to digital business and cybersecurity.
- The paper is published between 2019–2023.

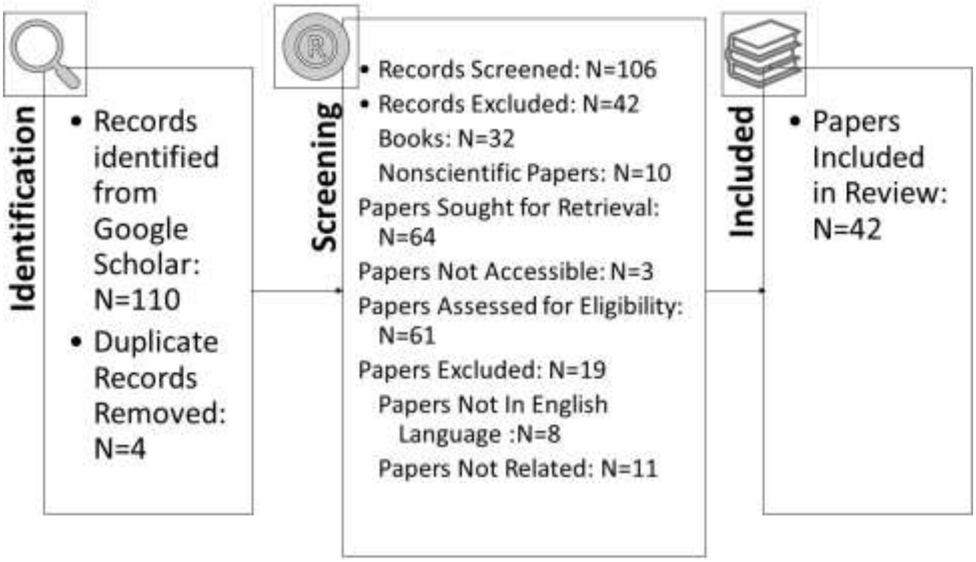
Identification
• Records identified from Google Scholar: N=110
• Duplicate Records Removed: N=4
Screening
• Records Screened: N=106
• Records Excluded: N=42
Books: N=32
Nonscientific Papers: N=10
Papers Sought for Retrieval: N=64
Papers Not Accessible: N=3
Papers Assessed for Eligibility: N=61
Papers Excluded: N=19
Papers Not In English Language :N=8
Papers Not Related: N=11
Included
• Papers Included in Review: N=42

Figure 1. Prisma diagram for our systematic literature review.

Additionally, the following exclusion criteria were applied to search results:

- The papers are not written in the English language.
- The paper is not related to cybersecurity and digital transformation.
- The paper is a review paper.

All Google Scholar results were checked for compliance with these criteria. The process of identifying the extracted studies went through the quality assessment stage, starting with a quick scan of the title and the language of the paper (English or not). Secondly, it was also ensured that these papers are related to and relevant to our research. Figure1 shows the number of final papers that were selected after going through these stages.

As highlighted in Figure1, digital transformation and cybersecurity are widely researched, and our final analysis included forty-two papers. Figure2 highlights the year-wise publication history.

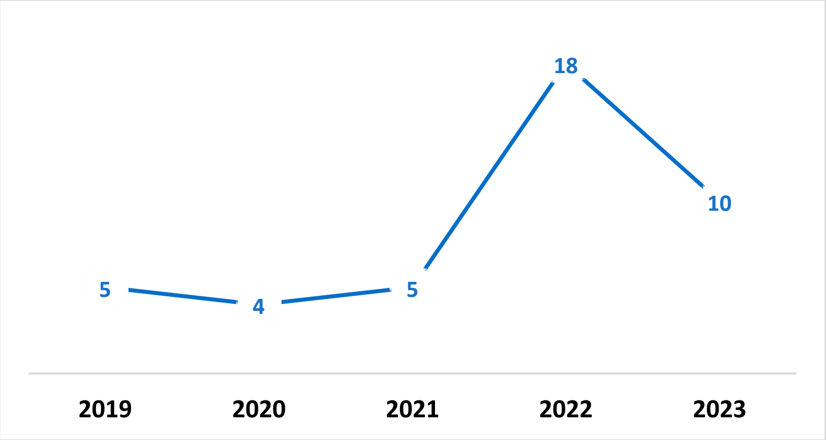

Figure 2. Year-wise publication history.

3.Results

In this section, we highlight the findings of downloaded papers.

3.1. Financial Sector

The financial sector is a critical component of an economy, and there have been many empirical studies in different geographical contexts. For example, Al-Alawi and Al-Bassam conducted empirical research in Bahrain and found that financial institutions are exposed to online identity theft, computer system damage, and hacking attempts resulting in operational disturbances [16]. Similarly, Hasan and Al-Ramadan [17] conducted an empirical study with bank customers in Iraq and found that although banks adopt significant security measures, some customers are still skeptical about online banking. In another study, Joveda et al. [18] investigated the banking sector in Bangladesh. They highlighted developing a cybersecurity system for identifying money laundering transactions that negatively impact economic development. There is a vast potential in modern technologies to support the financial sector. Almudaires and Almaiah [19] outlined major threats to credit card companies and associated solutions for credit card companies to improve their cybersecurity implementation. Smith and Dhillon [20] highlighted that blockchain is a crucial technology to minimize security threats in financial transactions; however, there is a need for rigorous analysis of blockchain implementation in the financial sector. Similarly, Kuzmenko et al. [21] used machine learning models to analyze large volumes of financial data to identify potential threats at an early stage.

Rodrigues et al. [22] developed a decision-support model for incorporating artificial intelligence (AI), digital transformation, and cybersecurity into the banking sector while ensuring data security is not compromised. The authors found that traditional banks are under pressure from their stakeholders to adapt to new technologies, and they also need to ensure that any potential data breaches or other security issues do not compromise their reputation. The authors used cognitive mapping and the decision-making trial and evaluation laboratory method to address this complex issue with an expert panel in group sessions. This resulted in a realistic framework for making decisions regarding AI implementation in the banking industry while ensuring data security is not compromised. The study developed a multi-stakeholder cognition-driven framework using cognitive mapping combined with DEMATEL methodology. This approach allowed them to identify critical factors affecting AI adoption within banks, such as customer trust toward technology- based services offered by banks; regulatory compliance requirements; and availability of a skilled workforce, which were then ranked based on their relative importance using DEMATEL analysis.

Similarly, Fedorov et al. [23] highlighted how cognitive technologies could ensure data security when using biometric identification technology in remote banking transactions. The article discussed how digital transformation and biometric identification would impact financial services in Russia. It emphasized that advanced security measures are necessary for protecting sensitive customer data during these transactions. The proposed solution is through cognitive technologies focused on human intellectual abilities as one direction for ensuring information security within this context.

Another research study by Patil and Bharath [24] investigated technological advancements in the financial sector. The study's findings showed that Fintech has improved businesses, and investors have more confidence in the technology. They also presented new technologies adopted by Fintech and their associated issues. The effect of financial technology was positive on the factors of trust and business authorization. Traditional finance has noticed the most important critical issues, such as the risks of fraud and low performance, and differences and limitations have been encountered. The research was conducted on a limited sample of approximately 160.

Moreover, Rãƒdulescu et al. [25] explained the risks associated with digitalization regarding economic development and ensuring social and information security. They highlighted that digitalization significantly impacts economic growth, social inclusion, and sustainable development. However, it also introduces new vulnerabilities that can lead to cyber-attacks and require smart controls to prevent them. The authors suggested that technology experts and other stakeholders should be involved in assessing these risks as they can grow and become more complex over time. Risk managers must develop a comprehensive strategy that includes mitigation and risk transfer solutions, prioritizing which IT security options best mitigate the organization's risk.

Moreover, international cooperation is essential to combat cybercrime due to the evolving global crime and terrorist threats associated with digital transformation.

Finally, it highlighted the growing importance of information technology in business development, human relations, and communication between people and governments. Digital risk management should therefore be a priority for all involved stakeholders.

3.2. Health Sector

Cybersecurity in the health sector deals with patient data privacy [26] and the security of medical devices [27–30]. A secure digital transformation drive can help improve health organizations' organizational governance [31–33]. Garcia-Perez et al. [34] discussed how the digital transformation of healthcare systems must be managed effectively from a cybersecurity perspective. This paper analyzed data from higher management in the UK during the COVID-19 pandemic. According to their findings, a balanced foundation that considers cybersecurity knowledge development, uncertainty management, and the sector's high systematic and organizational interdependence that has implications for research and management practices is essential for digital resilience and sustainability efforts in the health sector.

On the other hand, Paul et al. [35] discussed the use of digital technology in the healthcare sector and highlighted privacy and security issues related to these technologies. This study examined how digitization is transforming the healthcare sector, its impact on patient care, and opportunities for new business models with Industry 4.0 and business intelligence approaches. The rise in chronic diseases and the current pandemic have increased the need for person-centered care that encourages individuals to be involved in their health care. Digital solutions such as biosensors and software are being introduced to meet the growing need for on-demand healthcare services. Big data analytics have also significantly impacted healthcare organizations by providing access to decades of stored data, which serves as evidence-based medicine for better decision-making when treating patients while ensuring patient privacy remains protected. There are many ways to address security and privacy concerns related to digitalization in healthcare. It covers various solutions such as mutual authentication, key agreement, lightweight cryptography, blockchain-based solutions, etc., which can help ensure the secure handling of medical data. The authors also suggest developing management programs for medical equipment and investigating how patient engagement can impact privacy and security measures. Finally, they recommend further research on regulations regarding privacy and security in the healthcare sector and exploring the role of artificial intelligence (AI) and blockchain technology in improving healthcare outcomes while maintaining data safety. The adoption of cloud-based technology is also discussed as a potential solution for better patient data archiving and usage, lower storage costs, quicker innovation cycles, more straightforward collaboration, and increased telemedicine possibilities.

Nwaiwu and Mbelu [36] highlighted that the General Data Protection Regulation GDPR is essential for businesses and governments to comply with to track and monitor people's health, develop business models, and discover market opportunities. Statistics show that Europe has recorded 1.92 million confirmed COVID-19 cases and contact tracing with personal data is necessary to limit and contain the spread of the virus.

Maleh and Mellal [37] provided insights into how digital transformation and cyber-security are impacted by COVID-19 proliferation. The author discussed how COVID-19 has accelerated digital transformation trends such as cloud computing, the IoTs explosion, and big data accumulation while also increasing cyber-attacks related to personal data protection. The three main categories of challenges faced by cybersecurity departments during and after the pandemic are resilience against cyber attackers exploiting crises such as phishing or ransomware; recovery by ensuring secure pre-COVID-19 working methods upon return to the office; and adapting a technology roadmap for new realities while meeting business needs and customer expectations in digital transformation projects.

3.3. Governmental Sector

Digital transformation in governmental organizations is adopted all over the world, such as in Bahrain [38], the UK [39], and Saudi Arabia [40]; however, the adoption speed is not uniform. Al Shobaki et al. [41] investigated how digital transformation affects cybersecurity practices within the Ministry of Interior and National Security in Palestine. The researchers used a descriptive-analytical approach with a questionnaire as their primary research tool. They found a statistically significant correlation between all digital transformation dimensions and the ministry's cybersecurity practices. Additionally, certain organizational factors were found to have a powerful impact on these practices. For example, effective data exchange among different departments was identified as crucial for maintaining robust cybersecurity measures across all areas of operation. Overall results showed that there is indeed an impact of digital transformation on cybersecurity in this context, specifically in Gaza governorates, where it had an impact coefficient (0.897). Based on these findings, recommendations were made for improving electronic services offered by government agencies while also addressing gaps in worker performance related to technology use or knowledge gaps around best practices when dealing with sensitive information online. In conclusion: this paper provides valuable insights into how businesses can adapt their cybersecurity strategies when undergoing significant changes due to technological advancements such as those associated with "digital transformations", identifying key organizational factors impacting cybersecurity measures across organizations like ministries.

Another study by Al Najjar et al. [42] aimed to identify the reality of digital transformation in the Palestinian Ministry of Interior and National Security from the point of view of workers in computer and information technology units. The study used a comprehensive survey method, distributing questionnaires among workers, with 61 retrieved (representing an 87.1% response rate). Several dimensions related to digital transformation were measured through these questionnaires, including senior management support, strategic directions, technical infrastructure necessary for digital transformation, human resources coordination, data privacy and security, organizational structure, and job description. The results showed that most dimensions related to digital transformation are available within the ministry to a large extent. However, there is still room for improvement, such as providing more funds for electronic services development or innovation spending. Senior management support received a high approval degree along with strategic directions. At the same time, the technical infrastructure necessary for digital transformation also achieved a large approval degree, followed by human resources coordination, which scored lower than other dimensions but still had significant relative weight. In conclusion, this paper highlights how important it is for organizations seeking competitive advantage through improved efficiency or low-cost electronic service growth opportunities that exploit technological revolution possibilities offered at all levels, internally or externally, with various partner institutions, to consider investing in their efforts toward achieving successful digital transformation initiatives.

In another study, Fjord and Schmidt [43] examined the potential and challenges of using digital tools to simplify tax assessment and collection and enhance transparency. Practical experiences in Denmark showed that states had made progress in making tax processes more efficient but needed to take measures to ensure legality and transparency through cybersecurity.

Mijwil et al. [44] highlighted the importance of cybersecurity governance in digital transformation for public services provided by companies or institutions. The paper argued that changes in cybersecurity must be considered as it constitutes a large part of priorities for nations and companies undergoing digital transformation. The conclusion summarizes the importance of establishing straightforward programs and strategies to develop trustworthy cybersecurity governance without hacking or tampering with data/information while undergoing digital transformation. It also provided recommendations on how businesses can ensure secure operations while improving efficiency and effectiveness when providing public services through electronic means.

Maglaras et al. [45] focused on protecting critical infrastructure vital for public safety and national security. They proposed a methodology to protect critical national infrastruc- ture based on fileless attacks versus Advanced Persistent Threat (APT) group techniques used in such attacks. The study using this methodology aimed to quantify and score cyber-attacks from an offensive cybersecurity perspective.

3.4. Diverse Organizational Contexts

In a study, Dietal. [64] proposed a networked organizational structure for enterprise information security management based on genetic algorithms and analyzed its benefits compared to traditional approaches. The authors identified the challenges enterprises face in managing their information security during digital transformation efforts, such as risks from cyber-attacks and data breaches. They proposed a new genetic algorithm approach to improve work efficiency, reduce costs, and maintain strong information security. Their experiments comparing traditional network organization structures with those based on genetic algorithms found that the latter was much more efficient in terms of work efficiency. Additionally, they provided data showing advantages such as cost savings and room for growth when implementing this approach within enterprises. Overall, the results suggested that using a networked organizational structure for enterprise information security management based on digital transformation and genetic algorithms can effectively maintain strong information security while improving work efficiency within businesses undergoing technological change.

Alenezi [65] examined the role of software engineering in digital transformation and its importance for secure development practices. The authors argued that software engineering has become essential in ensuring efficient functioning as organizations increasingly adopt digital solutions to improve their operations. They also highlighted that security concerns are critical during this process due to increased cyber threats. Analyzing trends in software engineering and examining case studies from various industries, such as healthcare and finance, they conclude that all digital systems rely on software for efficient performance while emphasizing how secure development practices can mitigate risks associated with adopting new technologies.

Moreover, in another paper, Marelli [66] discussed how digitization and new technolo- gies are becoming increasingly crucial in humanitarian operations, making organizations vulnerable to cyber-attacks that can impact their ability to protect and assist those affected by armed conflict and violence.

In another study, Dvojmocˇ and Verboten [67] emphasized that employers have certain obligations to ensure employee information security, such as using appropriate hardware and software, configuring firewalls, and implementing antivirus programs. Furthermore, they highlighted the need for companies to comply with international instruments such as the GDPR when dealing with personal data protection issues related to new technologies being implemented.

On the other hand, in the environmental sector, Mukhlynina et al. [68] examined the problem of introducing digital technologies into the system of environmental safety and protection in Russia. The authors focused on the role and specific steps currently being taken by state authorities at the federal level. They also highlighted legal problems that exist in this context. The detailed findings suggested several challenges associated with implementing digital transformation efforts related to environmental safety in Russia. These included a lack of clear regulatory frameworks, insufficient funding for research and development activities, inadequate infrastructure support, and limited public awareness about these issues. In terms of results, based on their analysis using the factor analysis method, they identified vital factors affecting digitization efforts, such as technological readiness, availability of a skilled workforce, government policies and regulations, etc., which can be used by policymakers while designing strategies toward achieving sustainable environmental goals through digitization. Furthermore, Halabi et al. advocated for green cybersecurity practices to save energy consumption [69].

Voskresenskaya [70] investigated the current state of digital transformation in governance, economy, and social sectors as a factor for development and security. The researchers found that digitalization has become an integral part of modern society. They identified vital attributes such as the mechanism for transforming economic cooperation into information/telecommunication space, active introduction/application of e-money/smart contracts into civil transactions, and development of e-governance. They also noted that problems within these areas could affect compatibility with other economies due to lagging data processing capabilities or the inability to use digital resources effectively. Based on their analysis using both qualitative (laws/regulations) and quantitative (statisti- cal/comparative) methods at national/international levels, they concluded that there are significant benefits associated with embracing digitization across various sectors, including increased efficiency/productivity in service delivery processes, which ultimately leads toward sustainable growth/security.

In conclusion, it was recommended that governments prioritize investment in infrastructure necessary for the effective implementation/adoption of new technologies while ensuring that adequate regulation/policy frameworks exist to support innovation without compromising citizens' privacy/data protection rights. Additionally, given the rapid pace of change, businesses must adapt quickly to remain competitive. In another study, Kuchumov et al. [71] suggested that while there are potential benefits from digitization initiatives, such as increased efficiency and productivity gains, significant risks are involved, such as cybersecurity threats or job displacement due to automation. Furthermore, the impact of these initiatives varies depending on regional policies toward digitization. In conclusion, this paper highlighted that it is essential that policymakers in Russia's regions consider potential benefits and carefully evaluate possible negative impacts when implementing digital transformation strategies. By doing so, they can develop adequate public policies based on systemic analyses that take into account both positive effects along with serious risk factors affecting further development within each region individually rather than applying one-size-fits-all solutions across all areas indiscriminately without considering local conditions or needs specificities, which could lead to unintended consequences if not adequately addressed beforehand through careful planning processes involving stakeholders at different levels (local communities/businesses/government agencies).

Alahmadi et al. [72] highlighted that digital agriculture has helped automate laborintensive jobs. However, many threats and vulnerabilities are associated with digital agriculture. They highlighted the potential side-channel attacks relevant to digital transformation. Similarly, Song et al. [73] highlighted that the Internet of Things and 5G networks have resulted in massive growth of digital agriculture. However, publishing a large volume of data is prone to security concerns. As a result, the authors have proposed a privacy- preserving data aggregation scheme that is more secure and flexible.

Gonçalves [74] highlighted that digital transformation in the accounting sector of small- and medium-scale enterprises is in its early stages; however, the benefits are widely recognized. Data protection and cybersecurity threats are vital challenges that need to be handled by accounting professionals. In another study, Tiron-Tudor et al. [75] highlighted that artificial intelligence, blockchain, and GPS technologies can help companies' accounting departments implement real-time auditing systems. However, companies must allocate substantial resources to mitigate cybersecurity risks associated with advanced technologies.

Rodríguez-Abitia and Bribiesca-Correa [76] highlighted the fact that technological advancements, such as artificial intelligence, the Internet of Things, blockchain, 3D printing, and secure technical infrastructure, will also change universities. Everyone may adopt a new role, such as content producer, influencer, etc., to contribute to the education sector. Similarly, Pavlova [77] highlighted that the culture is typically based on free and open knowledge sharing in an educational setting. However, security threats demand a balance between openness and security mechanisms. Table1provides a summary of all the literature discussed.

Power systems are complex infrastructures in modern society and are vulnerable to cybersecurity threats [78,79]. Dagoumas [80] has used IEEE RTS 96 power system, and the author highlighted that a combination of operating conditions and cyber-attacks should be used to evaluate system stability. Diaba et al. [81] highlighted that power system communication protocols are prone to cyber-attacks by hackers. The authors have proposed an algorithm outperforming conventional deep learning approaches using SVM, ANN, and CNN. Similarly, Presekal et al. [82] developed a hybrid machine learning model using Graph Convolutional Long Short-Term Memory (GC-LSTM) and a deep convolutional network for anomaly detection in electrical power grids.

Kechagias et al. [83] highlighted that cybersecurity in the maritime industry has become very important. The authors have presented a detailed case of how a maritime company adopted a systematic approach to review its cybersecurity strategic policies, found loopholes, and subsequently performed risk mitigation.

4. Conclusions

This systematic literature review has shed light on the critical role of cybersecurity in digital transformation (DT). Digital transformation has transformed the business sector by transitioning organizational processes to IT solutions, resulting in significant changes across various aspects of an organization. It impacts multiple elements, such as user experience, operations, markets, customers, relationships, and cultural differences. Emerg- ing technologies, including artificial intelligence (AI), big data and analytics, blockchain technology, cloud computing, and services, drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. And the implications of cybersecurity for digital transformation are significant. As enterprises undergo the process of digital transformation, they become more vulnerable to cyber-attacks and security breaches. Cybersecurity is an essential component of digital transformation as it helps prevent interruptions due to malicious activities or unauthorized access by attackers aiming at sensitive information alteration, destruction, or extortion from users. The COVID-19 pandemic has further highlighted the importance of cybersecurity in DT implementation, as cybercriminals have taken advantage of vulnerabilities created by this rapid shift toward digitalization. Therefore, organizations undergoing DT adoption must prioritize cybersecu- rity measures to ensure a successful transition without any disruptions caused by security breaches. The study highlights that DT is a complex and ongoing process that requires organizations to be aware of emerging technologies and their associated security risks. As businesses transition their primary operations to IT solutions, they must ensure appropriate measures are in place to protect data and networks from unauthorized access or malicious activities. The findings suggest that implementing encryption or cyber insurance policies can help mitigate these risks during DT implementation. For future studies, we recommend the importance of organizations having comprehensive knowledge of cybersecurity threats throughout the entire process. This includes identifying potential vulnerabilities early on and proactively addressing them.

REFERENCES

1. Hai, T.N.; Van, Q.N.; Thi Tuyet, M.N. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. *Emerg. Sci. J.* **2021**, *5*, 21–36. [CrossRef]
2. Möller, D. *Cybersecurity in Digital Transformation: Scope and Applications*; Springer: Berlin/Heidelberg, Germany, 2020.
3. Matt, C.; Hess, T.; Benlian, A. Digital transformation strategies. *Bus. Inf. Syst. Eng.* **2015**, *57*, 339–343. [CrossRef]
4. Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability* **2023**, *15*, 6019. [CrossRef]
5. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]
6. Sharif, M.H.U.; Mohammed, M.A. A literature review of financial losses statistics for cyber security and future trend. *World J. Adv. Res. Rev.* **2022**, *15*, 138–156. [CrossRef]
7. Haislip, J.; Kolev, K.; Pinsker, R.; Steffen, T. The economic cost of cybersecurity breaches: A broad-based analysis. In Proceedings of the Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019; Volume 1, p. 37.
8. Garg, V. Covenants without the Sword: Market Incentives for Cybersecurity Investment. In Proceedings of the TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Virtual, 22–24 September 2021.
9. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. *Bus. Horiz.* **2021**, *64*, 659–671. [CrossRef]

10. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *J. Cybersecur*. **2020**, *6*, tyaa005. [CrossRef]

11. Krutilla, K.; Alexeev, A.; Jardine, E.; Good, D. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. *Risk Anal*. **2021**, *41*, 1795–1808. [CrossRef]

12. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* **2020**, *282*, 161–171. [CrossRef]

13. Uddin, M.H.; Ali, M.H.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Manag*. **2020**, *22*, 239–309. [CrossRef]

14. Curti, F.; Ivanov, I.; Macchiavelli, M.; Zimmermann, T. City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. The Financial Costs of Lax Cybersecurity. Available online:https://ssrn.com/abstract=4465071(accessed on 15 June 2023).

15. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]

16. Al-Alawi, A.I.; Al-Bassam MS, A. The significance of cybersecurity system in helping managing risk in banking and financial sector. *J. Xidian Univ*. **2020**, *14*, 1523–1536.

17. Hasan, M.F.; Al-Ramadan, N.S. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Soc. Sci. Humanit. J.* **2021**, *5*, 2312–2323.

18. Joveda, N.; Khan, M.T.; Pathak, A.; Chattogram, B. Cyber laundering: A threat to banking industries in Bangladesh: In quest of effective legal framework and cyber security of financial information. *Int. J. Econ. Financ*. **2019**, *11*, 54–65. [CrossRef]

19. Almudaires, F.; Almaiah, M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 732–738.

20. Smith, K.J.; Dhillon, G. Assessing blockchain potential for improving the cybersecurity of financial transactions. *Manag. Financ*. **2020**, *46*, 833–848. [CrossRef]

21. Kuzmenko, O.; Kubálek, J.; Bozhenko, V.; Kushneryov, O.; Vida, I. An approach to managing innovation to protect financial sector against cybercrime. *Pol. J. Manag. Stud*. **2021**, *24*, 276–291. [CrossRef]

22. Rodrigues, A.R.D.; Ferreira, F.A.; Teixeira, F.J.; Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Res. Int. Bus. Financ.* **2022**, *60*, 101616. [CrossRef]

23. Fedorov, B.M.; Fedorova, S.V.; Zhang, H.; Mamedova, N.A. Using Cognitive Technologies to Ensure the Information Security of Banks in the Conditions of Digital Transformation and Development of Biometrical Identification. *WSEAS Trans. Bus. Econ.* **2023**, *20*, 382–387. [CrossRef]

24. Patil, R.; Bharathi, S.V. A Study on the Business Transformation, Security issues and Investors Trust in Fintech Innovation. *Cardiometry* **2022**, *24*, 918–932.

25. Rã*f*dulescu, C.V.; Bodislav, D.A.; Negescu, M.D.O. The Risks of Digitization in the Context of Economic Development and of Ensuring Social and Informational Security. In Proceedings of the International Management Conference, Poznan, Poland, 27–29 June 2019; Faculty of Management, Academy of Economic Studies: Bucharest, Romania, 2019; Volume 13, pp. 1040–1050.

26. Mijwil, M.; Aljanabi, M.; Ali, A.H. Chatgpt: Exploring the role of cybersecurity in the protection of medical information. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 18–21. [CrossRef]

27. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber attacks on healthcare devices using unmanned aerial vehicles. *J. Med. Syst.* **2020**, *44*, 29. [CrossRef]

28. Buzdugan, A. Integration of cyber security in healthcare equipment. In Proceedings of the 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, Chisinau, Moldova, 18–21 September 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 681–684.

29. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of medical things. *Health Policy Technol.* **2021**, *10*, 100549. [CrossRef]