Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks

Emad Tariq[a*], Iman Akour[b], Najah Al-Shanableh[c], Enass Khalil Alquqa[d], Nidal Alzboun[e], Sulieman Ibraheem Shelash Al-Hawary[f], and Muhammad Turki Alshurideh[g,h]

[a]*Business and Marketing Department, Business School, Liverpool Hope University, United Kingdom*
[b]*Information Systems Department, College of Computing & Informatics, University of Sharjah, Sharjah, United Arab Emirates*
[c]*Department of Computer Science, Al al-Bayt University, Jordan*
[d]*Social Sciences and Humanities, College of art, University of Fujairah, United Arab Emirates*
[e]*The University of Jordan, Amman, Jordan*
[f]*Department of Business Administration, Business School, Al al-Bayt University, Jordan*
[g]*Department of Marketing, School of Business, The University of Jordan, Amman, Jordan*
[h]*Department of Management, College of Business Administration, University of Sharjah, Sharjah 27272, United Arab Emirates*

CHRONICLE

Article history:
Received: July 18, 2023
Received in revised format: September 3, 2023
Accepted: October 17, 2023
Available online: October 17, 2023

Keywords:
Cybersecurity
NIST Framework
Fraud Prevention
Commercial Banks
Jordan

ABSTRACT

In this digital age, fraudulent practices are among the most challenging that organizations must be aware of due to the increasing use of online transactions. This also applies to the banking sector whose business has become more complex with the recent developments in information and communication technology, which has changed the nature of bank fraud requiring advanced prevention measures. From this perspective, this paper aims to determine how cybersecurity affects fraud prevention for Jordanian commercial banks. A five-dimensional NIST cybersecurity framework was used. The research data was collected from 173 information technology managers in commercial banks listed on the Amman Stock Exchange. Structural equation modeling (SEM) was applied to investigate research hypotheses. The results of the research demonstrated the significant impact of cybersecurity in fraud prevention, especially detect function which had the largest impact among the dimensions of cybersecurity. Therefore, a set of recommendations were formulated for policymakers in Jordanian commercial banks, the most important of which is the adoption of multi-factor authentication (MFA) approaches for customer accounts, employee access, and biometric systems that add an additional layer of protection and make access to sensitive information to unauthorized individuals more difficult.

1. Introduction

Fraud has become a big problem for individuals, corporations, and governments alike in today's quickly expanding technological ecosystem (Othman et al., 2020). Fraud is defined as the deliberate distortion of facts with the aim of obtaining a disproportionate advantage or financial gain (Ni & Wang, 2022; Naim et al., 2023). It may occur in various ways, including identity theft, credit card fraud, online fraud, insurance fraud, and more, as described by Roszkowska (2021). Moreover, it may have serious repercussions, including financial losses, harm to the corporation's image, and a decline in confidence. Fraud prevention is a proactive strategy used by people and organizations to reduce the risk of becoming vulnerable to fraud (Cross, 2022; Abdulrahman, 2019). It entails using a variety of tactics, methods, and best practices to recognize, stop, and prevent fraudulent activity before it causes loss (Gale et al., 2022; Setyaningsih, 2020). According to Clyde and Hanifah (2022), the purpose of fraud prevention is to promote the integrity of financial systems and sustain consumer trust across a range of industries, in addition to safeguarding the interests of people and corporations.

* Corresponding author.
E-mail address: tariqe@hope.ac.uk (E. Tariq)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.10.016

The modern economic landscape and digital transformation initiatives depend heavily on cybersecurity. Companies must be watchful and aggressive in preserving their digital assets and information while they reap the benefits of technology (Corallo et al., 2022). To build a robust and secure cyber environment and guarantee a safer online experience for everyone, it is imperative that individuals, organizations, governments, and cybersecurity experts work together (Wang et al., 2022; Eaton et al., 2019). The area of cybersecurity is continually developing to meet the dangers and hazards that hackers and other bad actors are posing (Alqudhaibi et al., 2023). Confidentiality, integrity, and availability of information and computer resources are the main objectives of cybersecurity (Cram et al., 2023). Lee (2021) deemed that access to systems and services must be always available, and confidentiality, integrity, and availability all assure that only authorized people have access to sensitive information.

The banking industry in Jordan has benefited greatly from the rapid digital transformation and growing dependence on technology, allowing easy and effective customer services. However, increasing digitalization has raised the danger of fraud and cyber risks for Jordanian commercial banks. Cybersecurity's effect on fraud prevention in Jordanian commercial banks has grown to be a serious issue that needs careful consideration. Although cybersecurity measures are being put in place to safeguard banks and customers from cyberattacks and data breaches, it is still unknown how effective these measures are at preventing and mitigating fraud incidents unique to the Jordanian banking environment because there aren't any studies that have looked at this industry in the context of developing economies. This treatment will offer insightful information on how cybersecurity influences fraud prevention in Jordanian commercial banks. To safeguard banks and their customers from the rising danger of cyber fraud, the findings will assist pinpoint areas for improvement and serve as a roadmap for the creation of more effective and specialized cyber security initiatives. Additionally, it will help Jordanian commercial banks' decision- and policymakers create efficient defenses against fraud and cyber threats.

2. Theoretical background and research framework

2.1 Cybersecurity

Cybersecurity is a multidisciplinary area that incorporates ideas from several disciplines such as computer science, cryptography, information security, risk management, and human behavior (Li et al., 2022; Eaton et al., 2019). Its theoretical foundation revolves around understanding the nature of cyber threats, vulnerabilities, and strategies for protecting digital assets and information from malicious actors using theoretical frameworks from various theories such as the CIA Triad, vulnerabilities and exploits, and security and defense architecture in depth (Shah et al., 2023). Cybersecurity, additionally recognized as information security or computer security, is the activity of securing computer systems, networks, devices, and data from unauthorized access, electronic assaults, and damage (Shaikh & Siponen , 2023; Cram et al., 2023). Accordingly, it entails putting in place a set of procedures, technologies, and policies to prevent, identify, and respond to threats and vulnerabilities in the digital domain. Lee (2021) explained that cybersecurity is a multifaceted system that attempts to safeguard digital assets and information from cyber threats and assaults since it is a constant and dynamic process that involves collaboration, continual learning, and a proactive strategy to secure the digital ecosystem. Cybersecurity is a set of technological, organizational, and administrative means employed to avoid unauthorized use and misuse of electronic information and communication and information systems, as well as to restore them, with the goal of ensuring the availability and continuity of information systems and improving the protection, confidentiality, and privacy of private information in cyberspace (Kumar & Mallipeddi , 2022; Janvrin & Wang, 2022).

The Cybersecurity Framework offers a methodical way to deal with the many dimensions and components of cybersecurity. It provides a roadmap for enterprises to plan, implement, and manage their cybersecurity strategy efficiently. Organizations can increase their cybersecurity posture by implementing one of many well-established cybersecurity frameworks. The National Institute of Standards and Technology (NIST) cybersecurity framework is one of the most generally recognized frameworks. This framework divides cybersecurity into five functions (Wong et al., 2022; Alqudhaibi et al., 2023). (1) “Identify” entails comprehending an organization's assets, business environment, and risk management plan, as well as recognizing essential systems, data, and resources and analyzing cybersecurity threats. (2) “Protect” is concerned with putting protections in place to ensure the security of key assets and data, such as access restrictions, encryption, patch management, and secure settings. (3) “Detect” is defined as the constant monitoring and identification of cybersecurity events and incidents using intrusion detection systems, security monitoring tools, and threat intelligence. (4) "Respond" refers to steps conducted in reaction to cybersecurity issues, such as incident response planning, containment, elimination, and recovery. (5) "Recover" is concerned with returning services and operations to normal following a cyber security catastrophe, and involves disaster recovery planning, lessons learned, and enhancements to avoid such disasters from occurring in the future.

2.2 Fraud prevention

Fraud prevention has been characterized as a combination of techniques, procedures, and practices aimed at detecting, discouraging, and mitigating fraudulent activity before it causes harm to individuals, enterprises, or organizations (Roszkowska, 2021). According to Abdulrahman (2019), fraud prevention is the process of recognizing and evaluating anomalous patterns, activities, or behaviors in financial transactions, systems, or processes to detect possible cases of fraud or unauthorized activity. In a similar vein, it is composed of internal controls related to rules, processes, and systems put in place within a company to ensure accurate financial reporting, protect assets, and prevent fraud and misappropriation of resources (Kaur et al., 2022; Setyaningsih, 2020). Fraud prevention is a continuing and dynamic process that necessitates ongoing surveillance, adaptation, and collaboration among various stakeholders in order to reduce the impact of fraudulent activities and protect reputation, resources, and customer trust (Tarjo et al., 2022; Saputra et al., 2022).

Fraud prevention employs theories and techniques from criminology, economics, psychology, risk management, and financial accounting. The theoretical foundation of fraud prevention investigates the elements that drive fraudulent conduct as well as the tactics used to dissuade, identify, and reduce fraud episodes (Chen, 2022). According to Donald Cressy's fraud triangle, three major elements lead to fraudulent behavior: perceived pressure or financial necessity, perceived opportunity, and justification for the activity (Gupta, 2023). Hence, fraud prevention techniques target these elements by encouraging financial wellness, tightening controls, and fostering an ethical culture. Within the framework of rational choice theory, individuals are rational agents who assess costs and rewards before engaging in illicit behaviors such as fraud (Monteiro et al., 2023; Hermawan & Pramana, 2022). This idea of fraud prevention contends that increasing the perceived costs of committing fraud while diminishing the perceived advantages might dissuade potential offenders. Anyadufu and Uchechi (2023) considered that by establishing the theoretical groundwork for fraud prevention, businesses may establish comprehensive strategies to address the underlying causes of fraudulent activity, create a strong deterrent, and foster a culture of integrity and ethical behavior.

2.3 Cybersecurity and fraud prevention

Cybersecurity could support fraud prevention efforts in a variety of ways. As fraudsters increasingly use digital channels to attack weaknesses in computer systems and networks, having a strong cybersecurity framework in place to guard against various forms of fraud becomes increasingly important. Victory et al. (2022) evaluated the influence of cybersecurity on fraud prevention in Nigerian commercial banks through interviews with executives from relevant commercial institutions who are knowledgeable about this issue. According to the findings, cloud security improves fraud prevention prospects in Nigeria. The application's security also helps to avoid fraud in Nigerian commercial banks. Selvaraj (2021) conducted a literature study of numerous prior research to investigate the function of cybersecurity, aided by artificial intelligence (AI), in preventing and detecting financial fraud. According to the findings, cyber security is a must, which is why it was highlighted in this literature study to serve as a foundation for the complex IoT ecosystem in which users are involved.Buil et al. (2021) examined the influence of firms' online activities and cybersecurity measures on preventing fraud in the United Kingdom using the regular activity theory framework. The findings revealed that monitoring cyber security breaches is the most promising strategy to prevent cyber assaults and their consequences on financial fraud by investing in internal cyber security human resources and improving employees' online self-protection through cyber security training. As a result, the research hypotheses are as follows:

Hypotheses 1 (H1): *Identify has a positive impact on fraud prevention*.
Hypotheses 2 (H2): *Protect has a positive impact on fraud prevention.*
Hypotheses 3 (H3): *Detect has a positive impact on fraud prevention.*
Hypotheses 4 (H4): *Respond has a positive impact on fraud prevention.*
Hypotheses 5 (H5): *Recover has a positive impact on fraud prevention.*

Fig. 1 illustrates the research framework applied in this study, which elucidates the research hypotheses regarding the relationship between the dimensions of the NIST cybersecurity framework and fraud prevention.

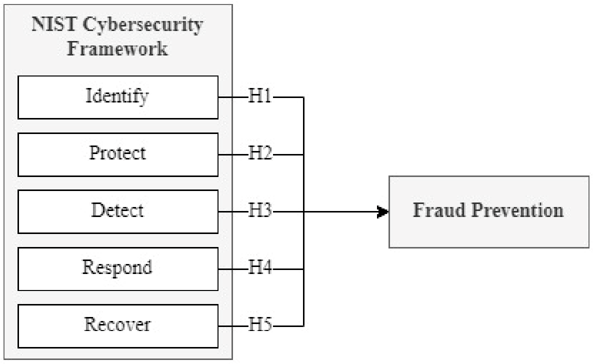

Fig. 1. Research framework.

3. Methods

The research adopted a cross-sectional design to investigate the relationship between cybersecurity dimensions, as defined by the NIST framework, and the effectiveness of fraud prevention measures in Jordanian commercial banks. This design involved the collection of primary data through the distribution of a structured questionnaire to the study population over a specific time frame, as per the methodology outlined by Al-Abbadi et al. (2021). An electronic questionnaire was meticulously crafted and delivered via email to a target group comprising 208 information technology managers representing 13 commercial banks listed on the Amman Stock Exchange. The data collection period extended from June 11, 2023, to July 25, 2023. A total of 195 questionnaires were received, but upon scrutiny, 22 responses exhibited duplicative patterns and were subsequently excluded from the dataset. Consequently, the final sample for this research comprised 173 responses, representing 83.2% of the total questionnaires disseminated. The electronic questionnaire utilized in this study comprised an introductory section and two main parts. The introduction served to elucidate the overarching research objectives, namely, the examination of the relationship between cybersecurity dimensions and fraud prevention, and also affirmed the author's commitment to upholding research ethics standards. The subsequent research sections encompassed a total of 29 items, systematically designed to measure both exogenous and endogenous constructs integral to the research inquiry. The exogenous construct of cybersecurity consisted of 24 items, aligned with the framework proposed by Alqudhaibi et al. (2023). This construct encompassed five distinct dimensions: six items dedicated to identity (ID), six items focused on protection (PR), three items addressing detection (DE), five items pertaining to response (RS), and four items related to recovery (RC). In parallel, the exogenous construct of fraud prevention consisted of five items (FP) and was conceptually harmonized with the framework introduced by Clyde and Hanifah (2022).

4. Results

Confirmatory factor analysis (CFA) served as the statistical method employed in this study to assess the validity and reliability of the constructs pertaining to cybersecurity and fraud prevention. CFA is a specialized form of structural equation modeling (SEM) that is particularly useful when researchers possess a well-defined theoretical framework or prior understanding of latent constructs and their interrelationships. Furthermore, CFA plays a pivotal role in ascertaining whether the empirical data collected aligns with the theoretical assumptions underlying the constructs (Aityassine et al., 2021). Table 1 offers a comprehensive overview of the outcomes pertaining to the validity and reliability assessments associated with the measurement model encompassing cybersecurity and fraud prevention.

Table 1
Evaluation of the research measurement model

Constructs	Items	Loadings	AVE	MSV	√AVE	CR	VIF
Identify	ID1	0.782	0.575	0.415	0.759	0.890	1.884
	ID2	0.755					
	ID3	0.703					
	ID4	0.764					
	ID5	0.815					
	ID6	0.727					
Protect	PR1	0.671	0.567	0.371	0.753	0.887	1.562
	PR2	0.824					
	PR3	0.716					
	PR4	0.772					
	PR5	0.791					
	PR6	0.734					
Detect	DE1	0.851	0.652	0.437	0.808	0.849	1.706
	DE2	0.767					
	DE3	0.803					
Respond	RS1	0.662	0.570	0.442	0.755	0.868	1.225
	RS2	0.813					
	RS3	0.781					
	RS4	0.743					
	RS5	0.768					
Recover	RC1	0.742	0.558	0.348	0.747	0.834	1.672
	RC2	0.708					
	RC3	0.752					
	RC4	0.783					
Fraud Prevention	FP1	0.824	0.587	0.439	0.766	0.876	---
	FP2	0.764					
	FP3	0.717					
	FP4	0.807					
	FP5	0.711					

The outcomes presented in Table 1 underscore a robust and reliable relationship between the observed variables and their corresponding latent constructs within the context of cybersecurity and fraud prevention. The factor loadings for the observed variables fell within a range of 0.662 to 0.851. Importantly, all factor loadings exceeded the lower limit of 0.50, as prescribed by Hair et al. (2019).

The average variance extracted (AVE) values surpassed the minimum threshold of 0.50, thus confirming the achievement of convergent validity, in line with Hair et al.'s (2022) criteria. Convergent validity establishes that the measured variables effectively converge toward the same underlying construct, thereby reinforcing the construct's reliability. Similarly, The results demonstrated the attainment of discriminant validity within the measurement model. This was evident as the AVE values exceeded the values of Maximum Shared Variance (MSV), and the square root values of AVE exceeded the minimum benchmark of 0.70. This highlights the distinctiveness of the constructs under scrutiny and their capacity to provide unique contributions to the overall model.

Regarding reliability, MacDonald's omega coefficients were employed to assess it, in line with Bader et al. (2022). The results showed that these coefficients ranged from 0.834 to 0.890, all of which exceeded the threshold of 0.70. This underscores the internal consistency and reliability of the measurement model, in accordance with the criteria established by Hair et al. (2012). On the other hand, an examination of multicollinearity among the exogenous constructs, specifically the cybersecurity constructs, indicated that they were devoid of multicollinearity issues. The Variance Inflation Factor (VIF) values for these constructs were significantly below the upper limit of 5, aligning with the criteria articulated by Aryan et al. (2022). Consequently, it can be inferred that the exogenous cybersecurity constructs do not suffer from undue collinearity concerns, thereby enhancing the model's overall robustness and interpretability.

Furthermore, structural Equation Modeling (SEM) was employed as the analytical approach in this study to investigate the influence of cybersecurity dimensions, as defined by the NIST framework, on fraud prevention within Jordanian commercial banks. SEM is a powerful statistical technique that facilitates the examination of hypotheses regarding direct effects among latent constructs (Qurah et al., 2023). Additionally, SEM offers various fit indicators that enable the assessment of the degree to which the assumed model aligns with the observed data. Fig. 2 provides a graphical representation of the structural model used to explore the impact of cybersecurity dimensions on fraud prevention.

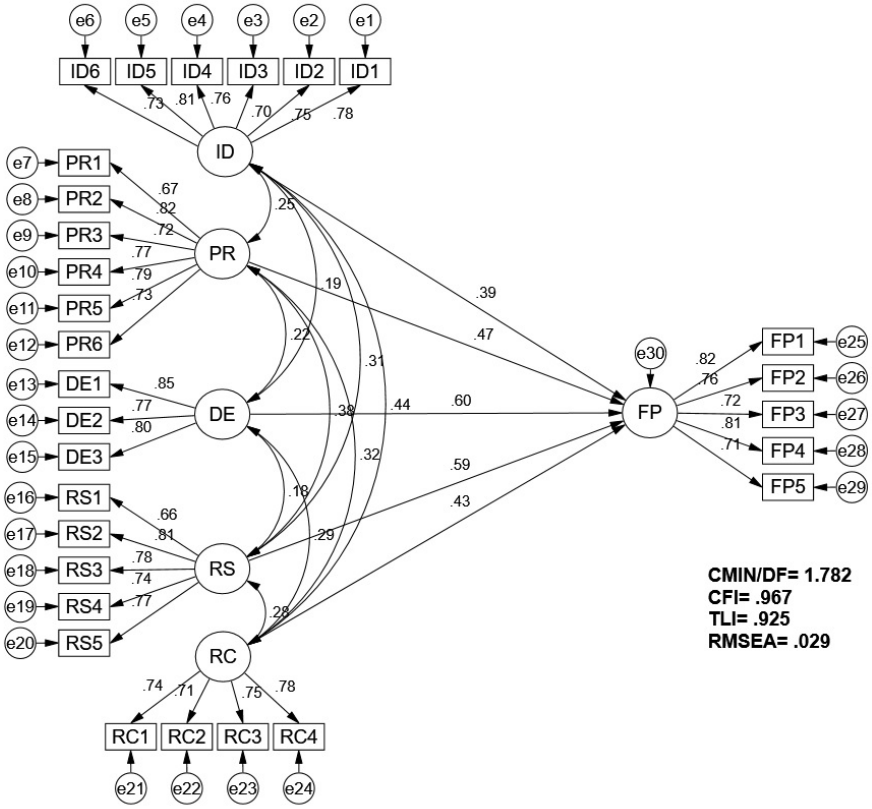

Fig. 2. Structural model to test the impact of cybersecurity on fraud prevention.

The outcomes depicted in Fig. 2 offer significant insights into the adequacy of the structural model utilized to investigate the influence of cybersecurity dimensions on fraud prevention within Jordanian commercial banks. The chi-squared test statistic yielded a value of 1.782. Importantly, this value falls below the upper limit of 3, which is widely accepted as an indicator of good model fit. Both the Comparative Fit Index (CFI) and the Tucker-Lewis Index (TLI) exceeded the minimum threshold of 0.90. In this case, their values exceeding 0.90 indicate a strong correspondence between the model and the observed data, reinforcing the model's suitability for assessing the impact of cybersecurity dimensions on fraud prevention. The analysis indicated that the Root Mean Square Error of Approximation (RMSEA) was computed at 0.029. Importantly, this value does not surpass the upper limit of 0.80. Collectively, these results provide compelling evidence in favor of the structural model's fitness for evaluating the hypothesized impact of cybersecurity dimensions on fraud prevention within the context of Jordanian commercial banks, as mentioned by AL-Zyadat et al. (2022). Table 2, which presents the results of the path coefficients, offers a more detailed insight into the specific impacts under investigation, shedding light on the direct relationships between the variables of interest.

Table 2
Path coefficients for the impact of cybersecurity on fraud prevention

Paths			B	S.E	Beta	t-value	P
Identify	→	Fraud Prevention	0.443	0.066	0.391	6.71	0.03
Protect	→	Fraud Prevention	0.516	0.063	0.472	8.19	0.000
Detect	→	Fraud Prevention	0.712	0.062	0.605	11.48	0.000
Respond	→	Fraud Prevention	0.665	0.064	0.588	10.39	0.000
Recover	→	Fraud Prevention	0.482	0.067	0.426	7.19	0.007

The findings presented in Table 2 offer substantial support for all of the research hypotheses pertaining to the impact of cybersecurity constructs on fraud prevention within Jordanian commercial banks. Moreover, these results provide valuable insights into the varying magnitudes of effect among these dimensions. The detect dimension exhibited the most substantial effect, with a path coefficient (β) of 0.605. This noteworthy coefficient indicates a strong and positive relationship between the detect dimension of cybersecurity and fraud prevention within Jordanian commercial banks. The associated t-value of 11.48 and a p-value of 0.000 further underscore the statistical significance of this effect, emphasizing its paramount importance in the context of fraud prevention. The response dimension demonstrated a significant effect with a path coefficient (β) of 0.588. This coefficient suggests a robust and positive relationship between the response dimension of cybersecurity and fraud prevention. The associated t-value of 10.39 and a p-value of 0.000 reaffirm the statistical significance of this relationship, highlighting the substantial impact of the response dimension in mitigating fraud risks.

The protected dimension also exhibited a notable effect, with a path coefficient (β) of 0.472. This coefficient indicates a meaningful and positive relationship between the protected dimension of cybersecurity and fraud prevention. The associated t-value of 8.19 and a p-value of 0.000 underscore the statistical significance of this effect, emphasizing the protective role of this dimension in preventing fraud. Moreover, the recovery dimension showcased a significant effect with a path coefficient (β) of 0.426. Although slightly lower than the aforementioned dimensions, this coefficient still underscores the importance of the recovery dimension in the context of fraud prevention. The associated t-value of 7.19 and a p-value of 0.007 confirm the statistical significance of this relationship. Lastly, the identity dimension exhibited a significant effect, with a path coefficient (β) of 0.391. This coefficient signifies a meaningful and positive relationship between the identity dimension of cybersecurity and fraud prevention. The associated t-value of 6.71 and a p-value of 0.03 reinforce the statistical significance of this effect, highlighting the role of this dimension in identifying and preventing fraud.

5. Discussion

The purpose of this article was to investigate the role of cybersecurity in fraud prevention in Jordanian commercial banks. The investigation's findings revealed a complex beneficial influence of cybersecurity on fraud prevention in Jordanian commercial banks. According to Janvrin and Wang (2022), digital transformation and technology adoption continues to influence the financial industry, and cybersecurity measures are becoming increasingly important in protecting financial institutions from cyber threats and fraudulent activities. Consequently, the risk of fraudulent actions could be decreased by implementing cybersecurity measures such as data encryption and access restrictions that safeguard critical customer information such as personal and financial information. Through email filtering and security awareness training, cybersecurity helps Jordanian commercial banks mitigate phishing and social engineering assaults. Teaching employees about potential cyber hazards and methods for screening hazardous information minimizes their vulnerability to fraud schemes based on Victory et al. (2022).

Real-time fraud detection is enabled by advanced cybersecurity techniques such as behavioral analytics and machine learning algorithms. These tools examine transaction data, identify strange trends, and notify banks of any fraudulent activity as soon as they are identified. Furthermore, cybersecurity measures are critical in protecting online banking systems and payment channels. Selvaraj (2021) noticed that strong authentication procedures, encryption, and secure communication channels safeguard customers' online transactions from fraudsters who try to intercept or modify data. On the other hand, cybersecurity aids in the prevention of data breaches, which might result in huge fraud risks for banks and their consumers. Banks decrease the risk of insider threats and unauthorized access to critical information by adopting network security measures, monitoring access to sensitive data, and performing regular security audits. A well-established cybersecurity incident response strategy helps banks to respond to fraud occurrences swiftly and efficiently. This comprises mechanisms for containing, investigating, and recovering financial losses and restoring consumer confidence. Overall, cybersecurity is critical to Jordanian commercial banks' ability to operate in a flexible and safe environment. Banks may improve their fraud prevention skills, defend their reputations, and maintain their customers' confidence by proactively addressing cyber risks and vulnerabilities.

6. Recommendations

A variety of recommendations may be made to bank decisions and policymakers based on the favorable findings of the influence of cybersecurity in avoiding fraud in Jordanian commercial banks. First, all personnel, from frontline workers to top executives, should get regular cybersecurity awareness training. To improve their capacity to detect and prevent bank fraud, educate them on the newest cyber risks, phishing efforts, and social engineering strategies. Second, establishing multi-factor authentication (MFA) for customer accounts, staff access, and vital systems adds an extra layer of protection and makes unauthorized persons more difficult to access sensitive information. Third, employ powerful analytics and machine learning algorithms to monitor transactions in real time, allowing for instant action to prevent fraudulent transactions. Fourth, ensure that all endpoints, including computers and mobile devices used by employees, are protected against cyber-attacks by robust security measures like firewalls, antivirus software, and frequent upgrades. Finally, it encrypts important client data and financial transactions to prevent thieves from gaining illegal access or intercepting them.

In conclusion, Jordanian commercial banks may strengthen their cybersecurity operations and reduce fraud by adopting these guidelines. A proactive and comprehensive cybersecurity approach is critical to preserving consumer confidence, securing financial assets, and ensuring the banking sector's resilience in the face of ever-changing cyber threats.

References

Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review, 4*(2), 13-21.

Al-Alwan, M., Al-Nawafah, S., Al-Shorman, H., Khrisat, F., Alathamneh, F., &Al-Hawary, S. (2022). The effect of big data on decision quality: Evidence from telecommunication industry. *International Journal of Data and Network Science, 6*(3), 693-702.

Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, Available online 21 July 2023.https://doi.org/10.1108/TECHS-05-2023-0022.

AL-Zyadat, A., Alsaraireh, J., Al-Husban, D., Al-Shorman, H., Mohammad, A., Alathamneh, F., & Al-Hawary, S. (2022). The effect of industry 4.0 on sustainability of industrial organizations in Jordan. *International Journal of Data and Network Science, 6*(4),1437-1446.

Anyadufu, A., & Uchechi, O. G. (2023). Forensic Accounting Services and its effect on Fraud Prevention in Manufacturing Firms in Anambra State. *Journal of Accounting and Financial Management, 9*(3), 106-117.

Aryan, L., Owais, W., Dahiyat, A., Rahamneh, A., Saraireh, S., Haija, A., & Al-Hawary, S. (2022). The effectiveness of corporate governance on corporate social responsibilities performance and financial reporting quality in Saudi Arabia's manufacturing sector. *Uncertain Supply Chain Management, 10*(4), 1141-1146.

Bader, D.M., Aityassine, F., Khalayleh , M., Al- Quran, A. Z., Mohammad, A., Al-Hawary, S.S., & Alkhawaldah, RA. (2022). The Impact of E-marketing on Marketing Performance as Perceived by Customers in Jordan. *Information Science Letters, 11*(6), 1897-1903.

Buil, G.D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders, 16*(3), 286-315.

Chen, T. (2022). Blockchain and accounting fraud prevention: A case study on Luckin coffee. In 7th International Conference on Social Sciences and Economic Development (pp. 44-49). Atlantis Press, Netherlands.

Clyde, C., &Hanifah, I. A. (2022). The Effect of Whistle bowing System toward Fraud Prevention: Mediation of Forensic and Investigative Audit. *AFRE Accounting and Financial Review, 5*(2), 97-105.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614.

Cram, W. A., Wang, T., &Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting, 20*(1), 15-38.

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety, 24*(1), 30-41.

Eaton, T. V., Grenier, J. H., &Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing, 13*(2), 1-9.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840.

Gupta, C. M. (2023). Models to Study the New Age Financial Crimes. In Financial Crimes: A Guide to Financial Exploitation in a Digital Age (pp. 191-213). Cham: Springer International Publishing.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, *40*, 414-433.

Hermawan, A. W., &Pramana, Y. (2022). Addressing the Financial Reporting Fraud: A Rational Choice Theory Perspective. *The Scientia Journal of Social and Legal Studies, 1*(2), 77-104.

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons, 36*(4), 67-112.

Kaur, B., Sood, K., & Grima, S. (2022). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance, 31*(1), 60-95.

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management, 31*(12), 4488-4500.

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

Li, Y., Yang, J., Zhang, Z., Wen, J., & Kumar, P. (2022). Healthcare data quality assessment for cybersecurity intelligence. *IEEE Transactions on Industrial Informatics, 19*(1), 841-848.

Monteiro, R. S., Ribeiro, M. C., Viana, C. A., Moreira, M. W., Araúo, G. S., & Rodrigues, J. J. (2023). Fish recognition model for fraud prevention using convolutional neural networks. *Advances in Computational Intelligence, 3*(1), 2.

Naim, A., Malik, P. K., & Zaidi, F. A. (2023). *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses*. IGI Global, United States.

Ni, P., & Wang, Q. (2022). Internet and Telecommunication Fraud Prevention Analysis based on Deep Learning. *Applied Artificial Intelligence, 36*(1), 2137630.

Othman, Z., Nordin, M. F. F., &Sadiq, M. (2020). GST fraud prevention to ensure business sustainability: a Malaysian case study. *Journal of Asian Business and Economic Studies, 27*(3), 245-265.

Qurah, R. A., Al-Husban, N. A., Mohammad, A. A. S., Aldaihani, F. M. F., Al-Hawary, S. I. S., Abazeed, R. A. M., &Al Kurdi, B. (2023). The Impact of Brand Loyalty Determinants on the Tourists' Choice of Five Stars Hotels in Jordan. In The Effect of Information Technology on Business and Marketing Intelligence Systems (pp. 2193-2214). Cham: Springer International Publishing.

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change, 17*(2), 164-196.

Saputra, K. A. K., Mu'ah, M., Jurana, J., Korompis, C. W. M., & Manurung, D. T. (2022). Fraud Prevention Determinants: A Balinese Cultural Overview. *Australasian Accounting, Business and Finance Journal, 16*(3), 167-181.

Selvaraj, N.A. (2021). The Essence of Cybersecurity Through Fintech 3.5 In Preventing and Detecting Financial Fraud: A Literature Review. *Electronic Journal of Business and Management, 6*(2), 18-29.

Setyaningsih, P. R. (2020). Internal Control, Organizational Culture, and Quality of Information Accounting to Prevent Fraud: Case Study from Indonesia's Agriculture Industry. *International Journal of Financial Research, 11*(4), 316-328.

Shah, I. A., Jhanjhi, N. Z., &Laraib, A. (2023). *Cybersecurity and Blockchain Usage in Contemporary Business. In Handbook of Research on Cybersecurity Issues and Challenges for Business and Fintech Applications* (pp. 49-64). IGI Global, United States.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security, 124*, 102974.

Tarjo, T., Vidyantha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. *Cogent Economics & Finance, 10*(1), 2101222.

Victory, C. O., Promise, E., &Mike, C. N. (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan, dan Manajemen, 4*(1), 15-27.

Wang, C. N., Yang, F. C., Vo, N. T., & Nguyen, V. T. T. (2022). Wireless communications for data security: Efficiency assessment of cybersecurity industry—A promising application for UAVs. *Drones*, *6*(11), 363.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520.