The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector

Tamer Bani Amer[1], Mohammad Ibrahim Ahmed Al-Omar[2]
Assistant Professor, Department of Computer Science, Jadara University, Irbid, Jordan[1]
Assistant Professor, Department of Computer Networks and Cyber Security, Jadara University, Irbid, Jordan[2]

***Abstract*—As technology advances and cyber threats continue to evolve, cyber security professionals play a critical role in developing and implementing robust security measures, staying ahead of potential risks, and mitigating the impact of cyber incidents. Many studies have examined the impact of cyber security on banks, without focusing on electronic crimes. Despite its importance, to the best of our knowledge, there are no studies on the impact of cyber security on mitigating electronic crimes in the banking sector. Therefore, the purpose of this study is to ascertain how cyber security affects electronic crimes in the Jordanian banking industry. The study sample consisted of 270 senior Jordanian managers and employees who understand the importance of cyber security in the banking sector in 14 Jordanian commercial banks, listed on the Amman stock exchange. The study used SPSS to evaluate how banks can enhance network security infrastructure to prevent unauthorized access and data breaches and also to find out the role of cybersecurity in granting competitive advantage to banks. A relative importance index (RII) was conducted to rank the importance of variables' statements and test the hypotheses. The results found the most important method through which banks can effectively mitigate the risk of electronic crimes and ensure the security of customers' financial data is that banks utilize robust encryption technologies to ensure the protection of customer financial data while it is being transmitted and when it is stored (RII=0.740). About 81.5 % of the sample agree, also, banks that have a strong cyber security system provide a secure platform for digital financial services which increases the competitive advantage as they were ranked first for their relative importance at both the category level and overall ranking with (RII=0.754). The study recommended that the banking industry, must consistently educate its customers on information security techniques and how to avoid hacking into their accounts, and develop an alert system that can raise awareness for both banks and bank customers if there is any possible entry or access to the customer's account or organization confidential information.**

Keywords—Cyber security*; *electronic crime; Jordanian banks; banking sector

I. Introduction

As technology advances and cyber threats continue to evolve, cyber security professionals play a critical role in developing and implementing robust security measures, staying ahead of potential risks, and mitigating the impact of cyber incidents. Moreover, cyber security refers to the practice of protecting computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. With the increasing reliance on technology and the interconnectedness of digital systems, cyber threats have become a significant concern for individuals, organizations, and governments worldwide [2]. The field of cyber security encompasses various measures, technologies, and practices designed to defend against cyber threats and ensure the confidentiality, integrity, and availability of information [3]. It involves protecting not only computers and servers, but also other devices connected to networks, such as smartphones, tablets, and the Internet.

Electronic crimes refer to illegal activities that are carried out using electronic devices, networks, or the internet [4]. With the rapid advancement of technology and the increasing reliance on digital systems, electronic crimes have become a significant concern for individuals, businesses, and governments worldwide [5]. In addition, to combat electronic crimes, governments, law enforcement agencies, and cyber security professionals work together to develop stringent laws, improve cyber security measures, raise public awareness, and promote digital literacy [6]. It is crucial for individuals and organizations to take necessary precautions, such as using strong passwords, keeping software up to date, and practicing safe online behavior, to protect themselves from falling victim to electronic crimes.

According to Arcuri et al. [7], the median cost of electronic crimes has climbed by approximately 200 percent in the last five years. Electronic crime expenditures quadrupled between 2015 and 2019, and it appears that they will double again between 2019 and 2024 [8]. Nonetheless, a considerable fraction of electronic crimes go unnoticed, such as industrial espionage getting access to confidential information. According to Seete [9], cyber risk is a huge potential threat to public and private institutions because of its effects on organizational information systems, reputation, loss of stakeholders' confidence, and financial losses. According to Bonfanti [10], the daily operations of virtually every person and organization are impacted by cyber security. Therefore, we must try to protect ourselves, our customers, and the supply chain against the loss of personal or sensitive information as technology enhances the flexibility, agility, and global reach of day-to-day operations. Must also be on the lookout for intellectual property theft, brand or reputation damage, and of course, monetary and economic losses.

Accordingly, the current study questions can be represented as follows questions:

- How can banks effectively mitigate the risk of electronic crimes and ensure the security of customers' financial data?
- How banks can enhance network security infrastructure to prevent unauthorized access and data breaches?
- How strong cyber security can give banks a competitive advantage?
- How banks can effectively educate and train employees and customers to be aware of and prevent cyber threats?

Many studies have examined the impact of cyber security on banks, without focusing on electronic crimes. However, the results are mixed [11, 12, 13] with cyber security having both a positive and a negative impact. Despite its importance, to the best of our knowledge, there are no studies on the impact of cyber security on electronic crimes in the banking sector. Therefore, the purpose of this study is to ascertain how cyber security affects electronic crimes in the Jordanian banking industry. In the unique context of the Jordanian banking industry, the study offers actual proof of the link between cyber security measures and the prevention and mitigation of electronic crimes. This empirical finding adds to the body of knowledge already available in digital crime prevention and cyber security. The study may aid in the creation and improvement of theoretical frameworks that clarify the complex link between cyber security measures and the decline in electronic crimes. This could improve the theoretical underpinnings of studies in cyber security. By concentrating on the Jordanian banking sector, the study provides context-specific insights into a particular business. For researchers, policymakers, and practitioners looking to grasp the complexities of cyber security within financial institutions, these sector-specific results can be helpful. The research will be separated into sections. We present a literature review and hypothesis development in Section II. We describe the data and methodology in Section III. We review the findings in Section IV and offer our discussions in Section 5 and conclusions in Section 6.

II. Literature Review and Hypotheses Development

A large number of studies [14, 15, 16, 17, 18, 19, 20, 21] deal with information security breaches, but there is still a limited amount of literature related to the banking sector. Electronic crimes have an unknown economic impact. A breach in information security has a negative economic impact, including decreased sales revenues, more expenses, a loss in future profits and dividends, a deterioration in reputation, and a decrease in market value [22]. Market value symbolizes investor confidence in a bank, and evaluating it is one way to calculate the damage of electronic crimes. Furthermore, Arcuri et al. [7] claim that investor behavior is influenced by what they have seen in the past, i.e., investors make decisions based on the impact of security breaches on a bank's market value in the past.

In the same context, information security plays a crucial role in combating electronic crimes [23]. Electronic crimes, also known as electronic crimes, encompass a wide range of illegal activities that are carried out using digital technologies and the internet. According to Wang et al. [12], these crimes include hacking, identity theft, phishing, malware attacks, data breaches, online fraud, and more. According to Mughal [24], Information security measures such as strong passwords, encryption, access controls, and multifactor authentication help prevent unauthorized access to sensitive data and systems. In addition, information security ensures the integrity and confidentiality of data [25]. Encryption techniques, secure data transmission protocols, and secure storage mechanisms help safeguard data from unauthorized modification, interception, or disclosure. Maintaining data integrity and confidentiality is vital in protecting sensitive information from cybercriminals who exploit it for financial gain or other malicious purposes [26].

According to Burton-Howard [27], network security plays a crucial role in mitigating electronic crimes in firms. Furthermore, effective network security measures help protect an organization's digital assets, including sensitive data, intellectual property, and financial information, from unauthorized access, data breaches, and cyberattacks [28]. Network security measures, such as firewalls, intrusion detection systems (IDS), and access controls, help prevent unauthorized individuals from gaining access to a firm network and systems [29]. Network security plays a vital role in safeguarding sensitive data from unauthorized disclosure or manipulation [30]. According to Prasad et al. [31], network security tools and technologies, such as intrusion prevention systems (IPS), security information and event management (SIEM) systems, and advanced threat detection solutions, enable firms to detect and respond to electronic crimes more effectively. According to Rafea et al. [32], network security plays a critical role in mitigating electronic crimes in the banking sector. As technology has advanced, so have the methods and sophistication of cybercriminals. By implementing robust access controls and encryption protocols, banks significantly reduce the risk of cybercriminals gaining unauthorized access to sensitive financial information [6]. According to Zainal et al. [33], banks store vast amounts of personal and financial information about customers, including account details, social security numbers, and transaction records.

In the same context, operational security known as OPSEC, plays a crucial role in mitigating electronic crimes [34]. According to Bandari [35], operational security measures, such as strong access controls, authentication protocols, and encryption, help prevent unauthorized individuals from gaining access to critical sensitive customer data. Banks hold vast amounts of personal and financial information about customers, making them attractive targets for cybercriminals [36]. According to Ritchot [37], effective operational security measures safeguard this data, ensuring its confidentiality, integrity, and availability. By implementing robust data encryption, secure storage practices, and regular data backups, banks mitigate the risk of data breaches, identity theft, and financial fraud. Operational security encompasses advanced monitoring and detection systems that identify suspicious activities or anomalies within banking networks [38]. By deploying intrusion detection and prevention systems, security information and event management (SIEM) tools, and real-time monitoring solutions, banks promptly detect electronic crimes, such as malware infections, phishing attempts, or network intrusions [39]. Rapid detection allows for swift incident response, minimizing the potential damage caused by cybercriminals. According to Rivaldo et al. [40], maintaining a strong reputation and customer trust is vital for banks. Operational security measures, including robust cybersecurity frameworks and transparent communication about security practices, contribute to building customer confidence [41].

End-user education plays a crucial role in mitigating electronic crimes in the banking sector [42]. According to Catota et al. [43], end-user education, such as bank-customers and employees, about the risks, best practices, and preventive measures, the overall security posture of the banking sector be significantly improved. According to Alkhalil et al. [44], phishing attacks are a common method used by cybercriminals to trick users into revealing sensitive information like passwords, credit card numbers, or social security numbers. Through education, end-users learn to identify phishing attempts, recognize suspicious emails or websites, and avoid falling victim to such scams. This knowledge helps protect personal and financial information from being compromised. End-user education about safe online practices, such as keeping software and devices updated, avoiding suspicious downloads or attachments, and using secure networks, helps prevent malware infections and unauthorized access to sensitive information [45]. In the same context, end-user education and report suspicious activities promptly. Prompt reporting of potential electronic crimes to the bank security teams helps prevent further damage and enables the bank to take appropriate measures to investigate and mitigate the threat [46]. Reporting incidents also aids in the identification of emerging trends and the development of proactive security measures. Based on the aforementioned, the study develops the following hypotheses:

H1. Cybersecurity plays a crucial role in preventing and mitigating electronic crimes.

H2. Improving network security infrastructure contributes to preventing unauthorized access and data breaches.

H3. Strong cyber security practices give banks a competitive advantage.

H4. Training and educating employees and customers contribute effectively to preventing electronic crimes.

III. Research Methodology

A. Research Population and Sampling

The commercial banks listed on the Amman Stock Exchange will be the subject of the research. As the research sample, all 14 Jordan Commercial banks listed on the ASE were chosen. 270 personnel and managers who worked in various areas of the commercial banks listed on the ASE were the research participants. Due to the challenges in precisely identifying the research population, convenience sampling, a non-probability sample technique, was used. To ascertain the impact of cyber security on electronic crimes in the Jordanian banking sector, the research looks at a questionnaire.

B. Research Design

Based on feedback from bank managers, literature research, and pre-survey analysis, the questionnaire will be created. To make it simpler for the participants to understand, it will be divided into three sections. Demographic information about the participants, such as age, gender, years of experience, position, and educational background, was requested in the first section of the survey. The second half concentrated on cyber security in commercial banks. The dependent variable (Electronic Crimes) was the subject of the third section measurement. A five-point Likert scale, with a rating of 1 for least important and 5 for most important, was used in the questionnaire. The selected sample consisted of senior Jordanian managers and employees who understood the importance of cyber security in the banking sector.

C. Measurement of Research Variables

The current research included several variables that required careful measurement to test the hypotheses and produce useful results. Cybersecurity was used as an independent variable. The electronic crimes in Jordanian banks served as the dependent variable. A structured online questionnaire and key performance indicators will be used to measure the variables. Accordingly, the data was analyzed, and the mean and standard deviation were determined.

To measure the validity of the study, the questionnaire was presented to a group of experts and specialists in the field of cybercrime and cybersecurity to review the data and receive their comments to ensure the suitability of the items of the questionnaire. The questionnaire was written in both Arabic and English to ensure high participation in this work and to obtain diverse perceptions from the sample. The results were analyzed using the SPSS statistical package for social sciences, descriptive analysis, which mainly used the factors of frequency, percentage of the study, and relative importance. After confirming the validity of the study tool and obtaining permission from the sample. A total of 300 questionnaires were distributed and 270 correct answers were received with a response rate of 90%. Responses with missing data or that did not meet serious data were excluded from the analysis.

The study examined the reliability of significant variables widely used in social studies. The main objective of this test is to verify the reliability of the items measuring variables to measure the target factors, also called internal consistency [47]. Cronbach Alpha is the most commonly used measure to perform a reliability analysis of the validity of measurement items [48], the reliability coefficient is rated between 0 to 1, although different assumptions have discussed this issue and suggest different acceptable values, the higher the value of the coefficient, the higher the degree of reliability of the measurements, the reliability analysis for this study was 0.885 which is high.

The feedback from the respondents has been analyzed and the Relative Importance Index technique was used for ranking.

The five-point Likert scale ranging from 1 (very low important) to 5 (very high important) was transformed into Relative Importance Index (RII) for each variable. The RII value has a range from 0 to 1 (0 not inclusive) and has been categorized into five levels of importance as shown in Table I.

TABLE I. RELATIVE IMPORTANCE INDEX VALUE

RII value	Importance level
From 0.8 to 1 From 0.6 to 0.8 From 0.4 to 0.6 From 0.2 to 0.4 From 0 to 0.2	High (H) High-Medium (H-M) Medium (M) Medium-Low (M-L) Low (L)

IV. RESULTS

A. Demographics Characteristics of Participant

The study includes 270 senior Jordanian managers and employees who understand the importance of cyber security in the banking sector, for gender distribution, the percentage of males 186 (68.9%) was higher than the percentage of females 84 (31.1%), and most of them were aged (31-40) while 94 (34.8%) of them more than 40 years old and 64 (23.7%) of them between (25 -30) About years of experience, the experience of the majority of the sample ranged from (1-5) years, at a rate of 37.4% and 78 (28.9%) from (6-15) years,61(22.6%) from (16-25) and 30 (11.1%) of them from 26-35 years. The majority of the sample was 57.8% of employees and 42.2% of managers. Table II summaries the demographic characteristics of the participants.

TABLE II. RESPONDENTS' DEMOGRAPHICS

Demographic	Frequency	Percent
Gender		
Male	186	68.9
Female	84	31.1
Age		
25-30	64	23.7
31-40	112	41.5
More than 40	94	34.8
Years of experience		
1-5	101	37.4
6-15	78	28.9
16-25	61	22.6
26-35	30	11.1
Nature of work		
Manager	114	42.2
Employee	156	57.8

The results about the normality distribution of the data showed a normally distributed dataset with a range of ±1.00 to ± 2.00 of the normality distribution measure of skewness and kurtosis respectively. Related to the first question of the study, which states “How can banks effectively mitigate the risk of electronic crimes and ensure the security of customers’ financial data?” To answer this question, we analyze the results of cyber security in commercial banks as the independent variable and ensuring network security infrastructure and mitigating risks of electronic crimes in banks, SPSS was used to calculate the mean of distribution and the standard deviation of each statement. Table III summarizes the results.

TABLE III. ARITHMETIC MEANS AND STANDARD DEVIATIONS ARE THE ESTIMATES OF THE STUDY SAMPLE ON ENSURING NETWORK SECURITY INFRASTRUCTURE AND MITIGATING RISKS OF ELECTRONIC CRIMES IN BANKS

No.	Statement	Mean	SD
1	Banks regularly provide comprehensive training programs to their employees on electronic crimes and protocols for cybersecurity.	3.04	1.113
2	Banks educate their customers on the risks of electronic crimes, cybersecurity, and the best practices for safeguarding their financial information.	3.23	0.964
3	Banks employ multi-factor authentication methods, such as hardware tokens and SMS-based verification, for customer logins.	3.23	0.925
4	Banks embrace biometric authentication techniques like fingerprint and facial recognition to verify the identity of customers.	3.32	1.136
5	Banks utilize robust encryption technologies to ensure the protection of customer financial data while it is being transmitted and stored.	3.70	0.806
6	Banks enforce strong password policies for both employees and customers.	3.30	0.647
7	Banks conduct regular security audits and vulnerability assessments of their IT systems.	3.49	0.865
8	Banks employ real-time fraud detection and prevention systems.	3.43	1.028
9	Banks have well-defined incident response plans and robust systems in place to recover from electronic crimes.	3.43	1.195
10	Banks implement systems that continuously monitor network traffic and utilize threat intelligence to identify suspicious activities.	3.67	0.798
11	Banks collaborate with cybersecurity firms and share threat intelligence.	3.42	0.656
12	Banks maintain stringent physical security measures at their data centers and server locations.	3.48	0.683
13	Banks keep their systems up to date with the latest security patches and software updates.	3.31	0.990
14	Banks maintain a strong and properly configured firewall infrastructure to prevent unauthorized access to the network.	3.40	1.043
15	Banks utilize secure protocols, such as HTTPS and SSL/TLS, for online transactions and implement disk encryption.	3.47	0.927
16	Banks segment their network into multiple zones and restrict access between them to minimize the impact of unauthorized access.	3.41	1.044
17	Banks employ Data Loss Prevention (DLP) solutions to monitor and prevent the unauthorized transmission or storage of sensitive data.	3.52	0.817
Ensuring Network Security Infrastructure and Mitigating Risks of Electronic Crimes in Banks		3.40	0.442

It is noted from Table III that the arithmetic mean of the estimates of the sample members for how can banks effectively mitigate the risk of electronic crimes and ensure the security of customers' financial data. The results found about 81.5% of the sample agreed that Banks utilize robust encryption technologies to ensure the protection of customer financial data while it is being transmitted and stored with a mean of 3.70 and standard deviation of 0.806 and 80.7% of them ensure their banks implement systems that continuously monitor network traffic and utilize threat intelligence to identify suspicious activities with mean 3.67 and standard deviation 0.798. The results also showed that 68.1% of participants ensure banks employ Data Loss Prevention (DLP) solutions to monitor and prevent the unauthorized transmission or storage of sensitive data and 64.1% agree that their banks maintain a strong and properly configured firewall infrastructure to prevent unauthorized access to the network with mean 3.52,3.40 and standard deviation 0.817, 1.043 respectively while 37.4% and 35.6% of respondent agree that Banks employ multi-factor authentication methods, such as hardware tokens and SMS-based verification, for customer logins and enforce strong password policies for both employees and customers.

The findings found a high agreement (agree) in 58.1% of the sample with a mean of 3.32 and standard deviation 1.136 which represent that biometric authentication techniques used in the banks like fingerprint and facial recognition to verify the identity of customers. On the other hand, the samples were asked about to which extent banks keep their systems up to date with the latest security patches and software updates and collaborate with cybersecurity firms and share threat intelligence, the results showed also a high agreement of 44% and 46.7%of the sample with a mean of 3.31 and 3.42 and standard deviation 0.990 and 0.656 accordingly. Regarding the second question of the study, which states "How strong is cyber security that can give banks a competitive advantage?" The arithmetic means and standard deviations of the sample's answers to the statements related to the competitive advantage of strong cybersecurity in banks were analyzed. Table IV summarizes the results.

The results in Table IV indicated the arithmetic mean of the estimates of the sample members for the degree of effects of strong cybersecurity on competitive advantage in banks ranged between (3.08) for paragraph No (6) and (3.77) for paragraph No (10). The results show that 83.3% of participants agree that banks with a strong cybersecurity system provide them with a secure platform for innovative digital banking services with a mean (of 3.77) and standard deviation of 0.752 and 66.3% of them believe banks with a strong cybersecurity system enhance the safeguarding of customer data and minimize the risk of data breaches with a mean (3.51) and standard deviation 0.895. Regarding reputation and loyalty, the results show 46.2% confirmed banks with a strong cybersecurity system can bolster reputation and foster customer loyalty with a mean (3.44) and a standard deviation of 0.791. Meanwhile, when the participants were asked if banks with a strong cybersecurity system are less susceptible to operational disruptions or downtime, the findings revealed a moderate agreement of 40.7% of the sample with a mean of 3.08 and a standard deviation of 0.921. Otherwise, 57.8% of the sample understand that Banks with a strong cybersecurity system mitigate financial losses resulting from cyber-attacks and 35.2% understand that banks with a strong cybersecurity system establish trust and confidence among bank-customers with 3.57 and 3.21 and standard deviation of 0.961 and 0.675. Accordingly. 50.3% of participants consider banks with a strong cybersecurity system to be better equipped to detect and respond to emerging threats w with a mean of 3.10 and a standard deviation of 1.178.

TABLE IV. ARITHMETIC MEANS AND STANDARD DEVIATIONS ARE THE ESTIMATES OF THE STUDY SAMPLE ON THE COMPETITIVE ADVANTAGE OF STRONG CYBERSECURITY IN BANKS

No.	Statement	Mean	SD
1	Banks with a strong cybersecurity system establish trust and confidence among bank-customers.	3.21	0.675
2	Banks with a strong cybersecurity system enhance the safeguarding of customer data and minimize the risk of data breaches.	3.51	0.895
3	Banks with a strong cybersecurity system attract and retain customers.	3.63	0.839
4	Banks with a strong cybersecurity system mitigate financial losses resulting from cyberattacks.	3.57	0.961
5	Banks with a strong cybersecurity system comply with regulatory requirements and avoid penalties.	3.47	0.839
6	Banks with a strong cybersecurity system are less susceptible to operational disruptions or downtime.	3.08	0.921
7	Banks with a strong cybersecurity system set them apart from their competitors by fostering trust and dependability.	3.24	0.835
8	Banks with a strong cybersecurity system can bolster their reputation and foster customer loyalty.	3.44	0.791
9	Banks with a strong cybersecurity system are better equipped to detect and respond to emerging threats.	3.10	1.178
10	Banks with a strong cybersecurity system provide them with a secure platform for innovative digital banking services.	3.77	0.752
The Competitive Advantage of Strong Cybersecurity in Banks		3.39	0.446

Related to the third question of the study, which states "How can banks effectively educate and train employees and customers to be aware of and prevent cyber threats?" The arithmetic means and standard deviations of the sample's answers to the statements related to effective strategies for educating and training bank employees and customers were analyzed. Table V summarizes the results.

The results in Table V indicated the arithmetic mean of the estimates of the sample members for the degree of effects strategies for educating and training bank employees and customers ranged between (3.73) for paragraph No (2) and between (3.20) for paragraph No (5). The results show that 78.1% of participants agree that Banks can administer simulated phishing exercises to assess employees' awareness and response with a mean (3.73) and standard deviation of 0.541 and 71.1% of them believe banks can encourage the reporting of suspicious activities or potential cyber threats with a mean (3.57) and standard deviation 1.010. Regarding regular updates, the results show 63.4% confirmed Banks can provide regular updates and reminders about emerging cyber threats and best practices with a mean (of 3.47) and a standard deviation of 0.923. Meanwhile, when the participants were asked if banks can offer frequent training sessions on cybersecurity to the employee, the findings revealed a moderate agreement of 36.3% of the sample with a mean of 3.24 and a standard deviation of 0.720. Otherwise, 48.9% of the sample understand that banks can collaborate with external cybersecurity experts to organize workshops and seminars for employees and customers and 50.8 % understand that banks can regularly assess the effectiveness of cybersecurity education and training programs with a mean of 3.20, 3.31, and standard deviation 1.078, 0.983. Accordingly, 54.8% of participants consider Banks can provide incentives or rewards for active participation in cybersecurity initiatives by employees and customers with a mean of 3.38 and a standard deviation of 0.920.

TABLE V. ARITHMETIC MEANS AND STANDARD DEVIATIONS ARE THE ESTIMATES OF THE STUDY SAMPLE ON EFFECTIVE STRATEGIES FOR EDUCATING AND TRAINING BANK EMPLOYEES AND CUSTOMERS

No.	Statement	Mean	SD
1	Banks can offer frequent training sessions on cybersecurity to employees.	3.24	0.720
2	Banks can administer simulated phishing exercises to assess employees' awareness and response.	3.73	0.541
3	Banks can provide regular updates and reminders about emerging cyber threats and best practices.	3.47	0.923
4	Banks can conduct cybersecurity awareness campaigns through email newsletters, social media, or other platforms.	3.38	0.817
5	Banks can collaborate with external cybersecurity experts to organize workshops and seminars for employees and customers.	3.20	1.078
6	Banks can encourage the reporting of suspicious activities or potential cyber threats.	3.57	1.010
7	Banks can provide incentives or rewards for active participation in cybersecurity initiatives by employees and customers.	3.38	0.920
8	Banks can regularly assess the effectiveness of cybersecurity education and training programs.	3.31	0.983
Effective Strategies for Educating and Training Bank Employees and Customers		3.41	0.509

To determine the importance of the role that cybersecurity plays in preventing and mitigating cybercrime, the ranking method was used to achieve this goal, and the importance was classified based on the relative importance index (RII). Table VI summaries the results.

TABLE VI. RANKING THE ROLE THAT CYBERSECURITY IN PREVENTING AND MITIGATING CYBERCRIME

Statements	RII	Rankingb y category	Overall ranking	Importance level
Banks regularly provide comprehensive training programs to their employees on electronic crimes and protocols for cybersecurity.	0.608	17	35	M
Banks educate their customers on the risks of electronic crimes, cybersecurity, and the best practices for safeguarding their financial information.	0.646	16	29	H-M
Banks employ multi-factor authentication methods, such as hardware tokens and SMS-based verification, for customer logins.	0.646	15	30	H-M
Banks embrace biometric authentication techniques like fingerprint and facial recognition to verify the identity of customers.	0.664	12	23	H-M
Banks utilize robust encryption technologies to ensure the protection of customer financial data while it is being transmitted and stored.	0.740	1	3	H-M
Banks enforce strong password policies for both employees and customers.	0.660	14	26	H-M
Banks conduct regular security audits and vulnerability assessments of their IT systems.	0.698	4	10	H-M
Banks employ real-time fraud detection and prevention systems.	0.686	7	16	H-M
Banks have well-defined incident response plans and robust systems in place to recover from electronic crimes.	.686	8	17	H-M
Banks implement systems that continuously monitor network traffic and utilize threat intelligence to identify suspicious activities.	.734	2	4	H-M
Banks collaborate with cybersecurity firms and share threat intelligence.	.684	9	18	H-M
Banks maintain stringent physical security measures at their data centers and server locations.	.696	5	11	H-M
Banks keep their systems up to date with the latest security patches and software updates.	.662	13	24	H-M
Banks maintain a strong and properly configured firewall infrastructure to prevent unauthorized access to the network.	.680	11	20	H-M

Banks utilize secure protocols, such as HTTPS and SSL/TLS, for online transactions and implement disk encryption.	0.694	6	12	H-M
Banks segment their network into multiple zones and restrict access between them to minimize the impact of unauthorized access.	.682	10	19	H-M
Banks employ Data Loss Prevention (DLP) solutions to monitor and prevent the unauthorized transmission or storage of sensitive data.	0.704	3	8	H-M

Based on the relative importance index, all methods related to cybersecurity methods in preventing and mitigating cybercrime were of medium to high importance, but the most important methods can banks effectively mitigate the risk of electronic crimes and ensure the security of customers' financial data that banks utilize robust encryption technologies to ensure the protection of customer financial data while it is being transmitted and stored (RII=0.740). Then banks implement systems that continuously monitor network traffic and utilize threat intelligence to identify suspicious activities (RII=0.734), banks employ Data Loss Prevention (DLP) solutions to monitor and prevent the unauthorized transmission or storage of sensitive data with (RII=0.704).

Educating customers about the dangers of cybercrime, cybersecurity, and best practices to protect their financial information was also ranked 16th in importance with (RII=0.646) and Banks regularly provide comprehensive training programs to their employees on electronic crimes and protocols for cybersecurity 17th in importance with (RII=0.608).

Related to how strong cyber security gives banks a competitive advantage, the ranking method was used to achieve this goal, and the importance was classified based on the relative importance index (RII). Table VII shows the results.

TABLE VII. RANKING THE ROLE OF CYBER SECURITY ON BANKS' COMPETITIVE ADVANTAGE

Statements	RII	Ranking by category	Overall ranking	Importance level
Banks with a strong cybersecurity system establish trust and confidence among bank-customers.	.642	8	31	H-M
Banks with a strong cybersecurity system enhance the safeguarding of customer data and minimizes the risk of data breaches.	0.702	4	9	H-M
Banks with a strong cybersecurity system attract and retain customers.	0.726	2	5	H-M
Banks with a strong cybersecurity system mitigate financial losses resulting from cyberattacks.	0.714	3	6	H-M
Banks with a strong cybersecurity system comply with regulatory requirements and avoid penalties.	0.694	5	13	H-M
Banks with a strong cybersecurity system are less susceptible to operational disruptions or downtime.	0.616	10	34	H-M
Banks with a strong cybersecurity system set them apart from their competitors by fostering trust and dependability.	0.648	7	27	H-M
Banks with a strong cybersecurity system can bolster their reputation and foster customer loyalty.	0.688	6	15	H-M
Banks with a strong cybersecurity system are better equipped to detect and respond to emerging threats.	0.620	9	33	H-M
Banks with a strong cybersecurity system provide them with a secure platform for innovative digital banking services.	0.754	1	1	H-M

It is clear from Table VII that banks that have a strong cyber security system provide a secure platform for digital financial services, which increases the competitive advantage as they were ranked first for their relative importance both at the category level and overall ranking with (RII=0.754). The results also showed the high importance of a strong cybersecurity system in attracting and retaining customers and mitigating financial losses resulting from cybercrime. With (RII=0.726) and (RII=0.714) accordingly, the results also showed that there is a high importance of a strong cyber security system in banks to protect customer data, reduce risks and data breaches with (RII=0.702), and enhance the bank's reputation and loyalty with (RII=0.688), detect and respond to emerging threats with (RII=0.620)

Regarding training and educating employees and customers to contribute effectively to preventing electronic crimes, the ranking method was used, and the importance was classified based on the relative importance index (RII). Table VIII shows the results.

TABLE VIII. RANKING THE ROLE OF TRAINING AND EDUCATING EMPLOYEES AND CUSTOMERS TO PREVENT ELECTRONIC CRIMES

Statements	RII	Ranking by category	Overall ranking	Importance level
Banks can offer frequent training sessions on cybersecurity to employees.	0.648	7	28	H-M
Banks can administer simulated phishing exercises to assess employees' awareness and response.	0.746	1	2	H-M
Banks can provide regular updates and reminders about emerging cyber threats and best practices.	0.694	3	14	H-M
Banks can conduct cybersecurity awareness campaigns through email newsletters, social media, or other platforms.	0.676	5	21	H-M
Banks can collaborate with external cybersecurity experts to organize workshops and seminars for employees and customers.	0.640	8	32	H-M
Banks can encourage the reporting of suspicious activities or potential cyber threats.	0.714	2	7	H-M
Banks can provide incentives or rewards for active participation in cybersecurity initiatives by employees and customers.	0.676	4	22	H-M
Banks can regularly assess the effectiveness of cybersecurity education and training programs.	0.662	6	25	H-M

The results showed the importance of training and educating employees and customers to contribute effectively to preventing electronic crimes. The statement that Banks can administer simulated phishing exercises to assess employees' awareness and response came in the highest rank of importance (RII=0.746). The results also showed high importance for banks to encourage the reports of suspicious activities or potential cyber threats with (RII=0.714). The results also showed that there is a high importance on providing regular updates and reminders about emerging cyber threats and best practices with (RII= 0.694) providing incentives or rewards for active participation in cybersecurity initiatives by employees and customers with (RII=0.676), and conducting cybersecurity awareness campaigns through email newsletters, social media, or other platforms with (RII=0.676). Banks can offer frequent training sessions on cybersecurity to employees and assess the effectiveness of cybersecurity education and training programs also banks can collaborate with external cybersecurity experts to organize workshops and seminars for employees and customers all these methods have a highly important role in preventing electronic crimes.

V. DISCUSSION

The results showed that cybersecurity plays a crucial role in preventing and mitigating electronic crimes. Improving network security infrastructure contributes to preventing unauthorized access and data breaches like encryption technologies; employing data loss prevention (DLP) solutions to monitor and prevent the unauthorized transmission or storage of sensitive data; enforce strong password policies for both employees and customers, define incident response plans and robust systems to recover from electronic crimes; configured firewall infrastructure to prevent unauthorized access to the network; use biometric authentication techniques and employ real-time fraud detection and prevention systems. These results are consistent with study of Ghelani et al. [17], which recommended the establishment of a smart internet banking system and intruder detection through the use of biometric prints, fingerprints, passwords, OTPs, and other methods which reduces the number of threats.

The results also showed the importance of training and educating employees and customers to prevent electronic crimes banks can conduct cybersecurity awareness campaigns and banks can collaborate with external cybersecurity experts to organize workshops and seminars for employees and customers. These results agree with Sharma [49] who recommended the key to cyber security solutions is having well-trained staff and effective awareness campaigns to conduct a thorough analysis of risk management, an internal security task team should collaborate with a reliable security vendor. These study results also agreed with Al-Alawi & Al-Bassam's [50] study which shows mandating security awareness training is one of the most commonly used methods by boards of directors and executive managers to reduce cyber risks.

The finding shows that the knowledge and skills of the team of employees who deal with cyber attempts are important factors in determining the effectiveness of the cyber security method used. These results agreed with the study of Malik & Islam [51], which showed that cybercrime incidents harm organizational performance but awareness of information security reduces the negative impact of cybercrime and the roles of awareness related to information security in reducing cyber fraud and enhancing the security of customer information and the overall performance of financial institutions, also agreed with Khan [52] and Al-Daeef et al. [53] studies which emphasized the need to educate employees through programs aimed at educating employees about safe computing practices and the risks of human error that may lead to security breaches; for example, phishing simulations that provide in-depth worker training scenarios are a proven method for increasing security awareness.

The results ensure that cybersecurity can boost customer trust by preventing sensitive customer data from being leaked and allowing a company to deliver on its promises, so if a bank had no breaches, it would be highly regarded and retained by its customers. These findings agreed with Kosutic [54] which recommended that companies could achieve strategic value that will be challenging to imitate by developing specific cybersecurity dynamic capabilities, and thereby achieve sustainable competitive advantage. Another study by Vijayalakshmi et al. [55] also confirmed this result.

The study also confirmed that one source of competitive advantage for a bank is to have cybersecurity to evaluate the current security measures and protect crucial data which is consistent with Kosutic [54] which explores the elements needed for cybersecurity implementation and management in an organization, as well as how cybersecurity can contribute to the competitive advantage of a company.

The study confirms that cybercrime is an emerging threat to IT facilities, the ever-changing nature of cybercrime and the associated development makes it increasingly difficult for policymakers and government institutions to implement cybercrime laws and policies, as a result, the banking industry must consistently educate its customers on information security techniques and how to avoid hacking into their accounts.

The study recommends to develop an alert system that can raise awareness for both banks and bank-customers whenever there is any possible entry or access to the customer's account or organization's confidential information. Furthermore, the banking industry must take into account the concept of effectively implementing and integrating big data technology into its system mitigating the negative consequences of cybercrime. This will allow for the storage of large files, and the data would aid in the examination, monitoring, and detection of network irregularities.

VI. Conclusion

The study's conclusions may directly affect how the Jordanian banking industry develops its regulatory and policy frameworks for electronic crime prevention and cyber security. The study's findings can help policymakers as they create recommendations and legislation. The report might provide banks in Jordan and possibly elsewhere with useful advice for developing effective risk management plans to protect against cybercrime. Based on the study's recommendations, banks can modify their cyber security procedures. The study's findings may help banks to be better equipped to defend against online attacks. Banks can discover weaknesses and put preventative measures in place to stop electronic crimes using the study's insights.

VII. Limitation

This study has several limitations; one of the most important is the amount of survey feedback received such as this study would have benefited from more responses. Despite the limitation mentioned above the results obtained in this study is significant for Jordan's banking and financial institutions, which can use the findings to improve their employees' skills in detecting various cyber-attacks. Furthermore, these findings are critical in broadening the understanding of cybersecurity and its impact on financial matters for organizations. Also, the study was limited to cybersecurity with no examination of areas closely related to cybersecurity such as privacy, fraud, and physical security; these related areas may influence some cybersecurity models presented in this study.

References

[1] M. Lezzi and A. Corallo, “Cybersecurity for Industry 4.0 in the current literature: A reference framework,” Computers in Industry, vol. 103, pp. 97–110, Dec. 2018, doi: 10.1016/j.compind.2018.09.004.

[2] A. Ustundag, E. Cevikcan, B. C. Ervural, and B. Ervural, “Overview of cyber security in the industry 4.0 era,” *Industry 4.0: managing the digital transformation*, pp. 267–284, 2018.

[3] M. E. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.

[4] R. S. Deora and D. Chudasama, “Brief study of cybercrime on an internet,” *Journal of Communication Engineering & Systems*, vol. 11, no. 1, pp. 1–6, 2021.

[5] S. A. Afaq, M. S. Husain, A. Bello, and H. Sadia, “A critical analysis of cyber threats and their global impact,” in *Computational Intelligent Security in Wireless Communications*, Boca Raton: CRC Press, 2022, pp. 201–220.

[6] J. Telo, “Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis,” *Sage Science Review of Educational Technology*, vol. 6, no. 1, pp. 26–38, 2023.

[7] M. C. Arcuri, M. Brogi, and G. Gandolfi, “How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns,” in *ITASEC*, 2017, pp. 175–193.

[8] D. Margiansyah, “Revisiting Indonesia’s economic diplomacy in the age of disruption: Towards digital economy and innovation diplomacy,” *J. ASEAN Stud.*, vol. 8, no. 1, p. 15, 2020.

[9] M. Seete, “The digitisation of a firm process and its impact on corporate governance,” *Indian Journal of Corporate Governance*, vol. 15, no. 2, pp. 280–294, 2022.

[10] M. E. Bonfanti, “Artificial intelligence and the offence-defence balance in cyber security,” in *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge*, 2022, pp. 64–79.

[11] H. M. Alzoubi *et al.*, “Cyber security threats on digital banking,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022.

[12] V. Wang, H. Nnaji, and J. Jung, “Internet banking in Nigeria: Cyber security breaches, practices and capability,” *Int. J. Law Crime Justice*, vol. 62, no. 100415, p. 100415, 2020.

[13] T. M. Mbelli and B. Dwolatzky, “Cyber security, a threat to cyber banking in South Africa: An approach to network and application security,” in *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2016.

[14] A. L. Upashovna, “The Impact of Information Warfare on the Socio-Economic Development of Society and the Issue of Information Security,” *european journal of innovation in nonformal education*, vol. 2, pp. 245–248, 2022.

[15] N. M. Mallaboyev, Q. M. Sharifjanovna, Q. Muxammadjon, and C. Shukurullo, “Information Security Issues,” *In Conference Zone*, pp. 241–245, 2022.

[16] M. H. U. Sharif and M. A. Mohammed, “A literature review of financial losses statistics for cyber security and future trend,” World J. Adv. Res. Rev., vol. 15, no. 1, pp. 138–156, 2022.

[17] D. Ghelani, T. K. Hua, and S. K. R. Koduru, “Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking,” *Authorea Preprints*, 2022.

[18] I. Ashraf *et al.*, “A survey on cyber security threats in IoT-enabled maritime industry,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–14, 2022.

[19] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, “Threats and opportunities with AI-based cyber security intrusion detection: A review,” *Int. J. Softw. Eng. Appl.*, vol. 13, no. 5, pp. 13–21, 2022.

[20] R. Montasari, “Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. Countering Cyberterrorism: The Confluence of Artificial Intelligence,” in *Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, 2023, pp. 7–25.

[21] H. S. Lallie *et al.*, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” *Comput. Secur.*, vol. 105, no. 102248, p. 102248, 2021.

[22] S. E. A. Ali, F.-W. Lai, R. Hassan, and M. K. Shad, “The Long-Run impact of information security breach announcements on investors’ confidence: The context of efficient market hypothesis,” *Sustainability*, vol. 13, no. 3, p. 1066, 2021.

[23] M. R. Mphatheni and W. Maluleke, “Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions,” *International Journal of Research in Business and Social Science*, vol. 11, no. 4, pp. 384–396, 2022.

[24] A. A. Mughal, “Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment,” *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 35–48, 2021.

[25] F. Yan, Y. Jian-Wen, and C. Lin, “Computer network security and technology research,” in *Seventh International Conference on Measuring Technology and Mechatronics Automation*, IEEE, 2015, pp. 293–296.

[26] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[27] V. Burton-Howard, *Protecting small business information from cyber security criminals: A qualitative study, Doctoral dissertation,* Colorado Technical University, 2018.

[28] M. Shohoud, “Study the effectiveness of ISO 27001 to mitigate the cyber security threats in the Egyptian downstream oil and gas industry,” *J. Inf. Secur.*, vol. 14, no. 02, pp. 152–180, 2023.

[29] S. Maesaroh, L. Kusumaningrum, N. Sintawana, D. P. Lazirkha, and R. Dinda, “Wireless network security design and analysis using Wireless Intrusion Detection System,” *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 30–39, 2022.

[30] M. F. Nasution, “The Role of Civil Law in the Protection of Privacy and Personal Data,” *Innovative: Journal of Social Science Research*, vol. 3, no. 2, pp. 3669–3679, 2023.

[31] S. G. Prasad, M. K. Badrinarayanan, and V. C. Sharmila, A Study on the adoption of Threat Prevention and Proactive Threat Monitoring Technologies for Securing the Information Technology Assets in India. 2023.

[32] M. F. G. Rafea, A. Hamdan, R. Binsaddig, and E. Qasem, “The effects of cyber crime on E-banking,” in *Digitalisation: Opportunities and Challenges for Business*, Cham: Springer International Publishing, 2023, pp. 560–569.

[33] M. A. G. Zainal et al., “A decentralized autonomous personal data management system in banking sector,” Computers & Electrical Engineering, vol. 100, p. 108027, May 2022, doi: 10.1016/j.compeleceng.2022.108027.

[34] Singh, U. and Singh, P. (2022) ‘Managing cyber security’, *Journal of Management and Service Science (JMSS)*, 2(1), pp. 1–10. doi:10.54060/jmss/002.01.002.

[35] V. Bandari, “Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types,” *International Journal of Business Intelligence and Big Data Analytics*, vol. 6, no. 1, pp. 1–11, 2023.

[36] J. Wolff, “Trends in cybercrime during the COVID-19 pandemic,” in *Beyond the Pandemic? Exploring the Impact of COVID-19 on Telecommunications and the Internet*, Emerald Publishing Limited, 2023, pp. 215–227.

[37] B. Ritchot, “An enterprise security program and architecture to support business drivers,” *Technol. Innov. Manag. Rev.*, vol. 3, no. 8, pp. 25–33, 2013.

[38] M. Qasaimeh, R. A. Hammour, M. B. Yassein, R. S. Al-Qassas, J. A. L. Torralbo, and D. Lizcano, “Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions,” *J. Softw. (Malden)*, vol. 34, no. 11, 2022.

[39] Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Maddikunta, P. K. R., Yenduri, G., ... & Gadekallu, T. R. (2022). XAI for cybersecurity: state of the art, challenges, open issues and future directions. arXiv preprint arXiv:2206.03585.

[40] Y. Rivaldo, S. V. Kamanda, and E. Yusman, “The Influence Of Brand Image, Promotion And Trust On Customer Loyalty At Bank BSI Nagoya Batam Branch,” *Jurnal Mantik*, vol. 6, no. 2, pp. 2385–2392, 2022.

[41] A. Shukla, B. Katt, L. O. Nweke, P. K. Yeng, and G. K. Weldehawaryat, “System security assurance: A systematic literature review,” *Comput. Sci. Rev.*, vol. 45, no. 100496, p. 100496, 2022.

[42] M. Bidgoli, B. P. Knijnenburg, J. Grossklags, and B. Wardman, “Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting,” in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019.

[43] F. E. Catota, M. G. Morgan, and D. C. Sicker, “Cybersecurity incident response capabilities in the Ecuadorian financial sector,” *Journal of Cybersecurity*, vol. 4, no. 1, 2018.

[44] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing attacks: A recent comprehensive study and a new anatomy,” *Front. Comput. Sci.*, vol. 3, 2021.

[45] M. Alohali, N. Clarke, F. Li, and S. Furnell, “Identifying and predicting the factors affecting end-users’ risk-taking behavior,” Information *& Computer Security*, vol. 26, no. 3, pp. 306–326, 2018.

[46] N. C. Roy and S. Prabhakaran, “Sustainable response system building against insider-led cyber frauds in banking sector: A machine learning approach,” *Journal of Financial Crime*, 2022.

[47] A. C. de Souza, N. M. C. Alexandre, and E. de B. Guirardello, “Psychometric properties in instruments evaluation of reliability and validity,” *Epidemiologia e servicos de saude*, vol. 26, no. 3, pp. 649–659, 2017.

[48] J. J. Vaske, J. Beaman, and C. C. Sponarski, “Rethinking internal consistency in cronbach’s alpha,” *Leisure sciences*, vol. 39, no. 2, pp. 163–173, 2017.

[49] A. Sharma and P. Tandekar, “Cyber Security and Business Growth,” in *Advances in Business Information Systems and Analytics*, IGI Global, 2016, pp. 14–27.

[50] A. I. Al-Alawi and M. S. A. Bassam, “The significance of cybersecurity system in helping managing risk in banking and financial sector,” *Journal of Xidian University*, vol. 14, no. 7, pp. 1523–1536, 2020.

[51] Malik, M.S. and Islam, U. (2019), “Cybercrime: an emerging threat to the banking sector of Pakistan*”, Journal of Financial Crime, Vol. 26 No. 1, pp. 50-60.*

[52] M. J. Khan*, “Securing network infrastructure with cyber security,” World J. Adv. Res. Rev., vol. 17, no. 2, pp. 803–813, 2023.*

[53] M. M. Al-Daeef, N. Basir, and M. Saudi, “Security awareness training: A review,” *Proceedings of the World Congress on Engineering*, vol. 1, pp. 5–7, 2017.

[54] D. Kosutic and F. Pigni, “Cybersecurity: investing for competitive outcomes,” *J. Bus. Strategy*, vol. 43, no. 1, pp. 28–36, 2022.

[55] P. Vijayalakshmi and D. Karthika, “A COMPARATIVE STUDY ON CYBER SECURITY THREATS DETECTION IN INTERNET OF THINGS,” *A COMPARATIVE STUDY ON CYBER SECURITY THREATS DETECTION IN INTERNET OF THINGS. ICTACT Journal on Communication Technology*, vol. 12, no. 2, 2021.