Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180117

The Impact of Cybersecurity on the Quality of Financial Statements

Saad A. Kareem Alsakini[*], *Hanan Ali Alawawdeh and Saleh Alsayyed*

Accountig Department, Facutly of Business, Isra University, Amman, Jordan

Received: 10 Sep. 2023, Revised: 2 Dec. 2023, Accepted: 17 Dec. 2023
Published online: 1 Jan. 2024

Abstract: Banks and other financial institutions in Jordan are prone to continuous cybersecurity breaches on their financial accounting statements. The impact of cybersecurity breaches on financial statements is directly related to accounting information's susceptibility to cyber-hackers. Cybersecurity breaches affect the quality of financial accounting statements. Thus, this study aims to investigate the impact of cybersecurity on the quality of financial accounting statements among selected banks in Jordan. Two types of datasets and sampling approaches were used. The primary approach consists of 506 data points about cybersecurity breaches at three banks in Jordan from 2012 to 2022, while the secondary approach employs a survey to sample 170 participants. The finding revealed that the cybersecurity breaches had a significant impact on the quality of financial accounting statements. The cybersecurity breaches had positive and significant impacts on the balance sheet, cash flow, and profit and loss. These breaches include accidental information disclosure (ADID) and stealing the encryption key (STEK), which mostly target the balance sheet. In addition to mischievous internal opening access (MVIA), database breach (DTBB), and man-in-the-middle attacks (MITM) that mostly target the cash flow statement. Lastly, the malware with encryption (MWWE) and a malicious external attack (MVEA) are aimed at profit and loss accounting. These variables were found to have a significant impact on the quality of financial accounting statements, except MVIA, which had no significant impact. It is suggested that a rapid response to a cyberattack can aid in minimizing the breach's impact on the bank's financial statements and reputation.

Keywords: Balance Sheet; Banks; Cash Flow; Cybersecurity; Profit and Loss; Quality.

1 Introduction

Financial and banking institutions use account analysis to analyze the comprehensive economic structure of their businesses. The comprehensive financial accounts of the company are examined to ascertain its situation generally and for a number of decision-making rationales. For stakeholders, managers, investors, and other parties, the economic information contained in the financial statements that was assessed by account analysis is more valuable (Sun, 2020). The measurement and analysis of any financial institution's expenditure patterns are made possible by accounting statements (Schroeder, Clark, & Cathey, 2022). Account analysis facilitates the detection of potential cybersecurity assaults and enables banks and other financial organizations to spot unexpected and irregular financial transactions. In conjunction with banks and other financial institutions, account analysis is of interest to creditors, financiers, and potential shareholders (Kiradoo, 2020). A guarantee that the company can pay back a credit line or a loan is necessary. Prospective investors look at a company's financial information to assess its ability to generate revenue and meet the necessary growth expectations (Gao, 2022).

In the first place, accounting data needs cybersecurity. Protecting accounting data requires ensuring cybersecurity. The financial accounting information requires robust and comprehensive security procedures. Accounting experts must be involved in discussions about business cybersecurity (Ghelani, Hua, & Koduru, 2022). Information protection and the use of accounting procedures to prevent organizational, technological, public relations, and investment losses are important for cybersecurity. It is crucial to concentrate on the general concepts of protection, avoidance, and elimination of the effects of threats to the security of accounting information, regardless of the type of cyberattack (Shulha et al., 2022). Bank cybersecurity must be improved in order to ensure efficiency in theory, methodology, application, and organization.

However, banks are prone to security breaches when fundamental cybersecurity guidelines, or "cyber hygiene," are not strictly followed. According to a recent study, weak

[*]Corresponding author e-mail: Saad.alsakini@iu.edu.jo

or stolen passwords were used to access business networks in over 85% of breaches (Sharif & Mohammed, 2022). According to reports, 91 percent of all attacks begin when a target receives a phishing email (Sanusi, Rameli, & Isa, 2015; Buch & Goldberg, 2022; Janvrin & Wang, 2022). Additionally, phishing techniques are used in 35% of all successful intrusions. Despite years of concerted efforts by banks' security programs to inform customers about the risks of phishing emails and how to recognize them, these assaults continue to be quite effective. Cybersecurity breaches in financial statements are occurring more frequently through employee-owned devices, business-owned mobile devices, or applications. These breaches are caused by individuals' poor online safety practices, which directly affect financial or banking security (Alzoubi et al., 2022). Individuals are undoubtedly being used by the attackers as a point of entry to banking systems and data.

Banks and other financial institutions in Jordan are found to be prone to continuous cyberattacks on their financial accounting statements (Tawfik et al., 2021). Furthermore, the impact of cybersecurity breaches on financial statements is directly related to accounting information's susceptibility to cyber hackers in Jordan. Although no company can be 100% secure online, high-quality cybersecurity for bank accounting is a potent deterrent. The sophistication of hackers is rising, and there has been a huge increase in cyber breaches. In 2021, in Jordan, the General Intelligence Directorate (GID) revealed that it received daily reports of between 500 and 1,000 cyberattacks, with most targeting financial institutions like banks. According to reports, the GID is one of Jordan's most significant and capable intelligence organizations (Abulhaija, Hattab, & Qusef, 2022).

Cybersecurity breaches can affect the quality of financial accounting statements. The two main characteristics that make accounting statements such as the cash flow statement, balance sheet, and profit and loss statement valuable for decision-making are relevance and reliability, which define the quality of financial reporting. A lack of dependability is defined as a lack of information breach or loss to unauthorized individuals (Kohlbeck & Warfield, 2010). The assumption that financial reporting is intended to provide financial information that is both relevant and accurately portrays a bank's current financial state based on accounting quality without information loss to unauthorized individuals (Achim & Chiș, 2014; Nikolaev, 2018). Consequently, those involved in financial reporting or statements are very interested in accounting quality. High-quality financial statements will be impacted by low-quality financial data due to cybersecurity breaches. Internal security breaches due to negligence and poor handling of highly sensitive accounting information have an impact on the reliability of financial statements. Financial statement breaches include issues with information loss due to cyberattacks during recording, storage on personal or private devices, a lack of comparability in accounting information, and accidental information disclosure (Azar, Zakaria, & Sulaiman, 2019). In addition to the cybersecurity issues facing banks and financial institutions in Jordan discussed above, there is currently a paucity of research on the impact of cybersecurity on the quality of financial accounting statements in Jordan. Therefore, this study aims to investigate the impact of cybersecurity on the quality of financial accounting statements among selected banks in Jordan.

2 Literature Review

2.1 Accounting and Banking System

Accounting has an impact on every part of bank operations and necessitates recordkeeping systems that produce accurate and trustworthy data and reports required to satisfy the demands of clients, stakeholders, oversight organizations, tax institutions, and legal authorities (Bushman, 2014; Okab & Al-Oqool, 2014). Banks are required to prepare statutory accounts each year that reveal all of their assets. The preparation of financial statements for external spectators, including shareholders, creditors, tax agencies, and others, is the primary goal of financial accounting (Razafiarivony & Hosna-Janeta, 2022).

The banking systems are cloud-based and offer limitless storage for account information in the form of accounting reports or statements. The online banking system often connects to or is a component of the main banking system run by a bank to give clients access to financial services and make information available to stakeholders and financial authorities (Shulha et al., 2022). Financial organizations have implemented a number of security procedures to lower the possibility of illegal internet access to clients and bank details, but the various strategies used vary widely (Alzoubi et al., 2022; Buch & Goldberg, 2022). A growing problem is cybersecurity in the accounting and banking systems. It is traumatic for accountants and financial institutions because financial information is a key target for hackers and information breach attempts (Gao, 2022; Peng & Li, 2022).

2.2 Cybersecurity

The practice of safeguarding systems, networks, applications, and databases from online threats is known as cybersecurity (Craigen, Diakun-Thibault, & Purse, 2014). In the financial industry, cybersecurity means protecting sensitive financial data and important systems from online threats (Hasham, Joshi, & Mikkelsen, 2019). Combining the functional capabilities of blockchain technology with the advantageous aspects of "Internet Bank" and "Client-Bank" interactions allows for the creation of a hybrid non-cash payment system. Accounting data is gathered without the usual payment filing and bank statement creation. Electronic information from the hybrid communication system serves as the foundation for non-cash transfer management, completely automated documenting, accounting record compilation, and informing accountants (Alzoubi et al.,

2022). Due to timely and remote information exchange, the automation of accounting for cash transactions aids in enhancing the level of cyber defense control over the execution of financial operations.

The reliability of records is related to the concepts of secrecy, integrity, and accessibility. Following these guidelines makes sure that valuable accounting information reaches both internal and external shareholders without jeopardizing the confidentiality of the bank's trade secrets. The concepts of completeness, sanction, addresses, reliability, and comparability are added to the theoretical underpinnings of accounting information cybersecurity (Janvrin & Wang, 2019). The establishment of cybersecurity standards for businesses is based on these principles in order to prevent, mitigate, and ultimately eradicate the effects of risks to the security of accounting data. Adherence to the theoretical concepts of accounting and computer science is crucial for getting accurate accounting information (Smith, 2020). The list of core guidelines for the protection of accounting and banking technologies continues to grow, and cyber dangers to the operation of bank businesses become more complex.

Financial accounting is viewed as a cutting-edge method of assuring the interplay between the enterprise's economics and cybersecurity. Accounting connections are present at five aggregate levels and help to explain how increased dangers to the financial statement security are impacted as a result of cyber risk activities (Couce-Vieira, Insua, & Kosgodagan, 2020; Ghelani, Hua, & Koduru, 2022). (i) The cybersecurity breach at the organizational level impacts accounting principles and roles. (ii) At quality level, the accuracy of the accounting information is impacted. (iii) At the systematic level, the accounting statements, records, and stored data are impacted. (iv) At the communication level, the quality of accounting information provided to shareholders suffers, and (v) at the reputation level, the bank's business image causes financial losses.

Banks are facing the growing ties between cybersecurity breaches and the majority of financial crimes as they start to adapt their operations to the evolving profile of financial crime. The cybersecurity component is not particularly new. For instance, up until recently, the majority of fraud was transaction-based and financial statement-based, with fraudsters preying on control flaws in financial statements or information (Sun, 2020). Banks combat such fraud with a relatively simple focus on transaction-based, point-based, control-specific safeguards, while the opening through financial statements (cash flow statement, balance sheet, profit and loss) remains weak (Peng & Li, 2022).However, financial statement-based fraud has become more prevalent recently as a result of fraudsters using software to exploit actual or financial data (Stein, 2018; Shulha et al., 2022). As a result of more pervasive and aggressive cyber-aided attacks, personal data and internal security shield precautions alone are becoming less valuable (Vincent & Trussel, 2019).

2.3 Bank Financial Accounting are gateways

There is a surge in cyberattacks on all forms of accounting practices. Year-end and the deadlines for filing tax returns are the most typical times for the cyberattack. While cybersecurity poses a threat to most organizations, it is becoming more of an issue for accountants because of the vast volumes of sensitive customer data and confidential information that their systems store (Negrea, 2022). These typically consist of financial information, a cash flow statement, a balance sheet, tax identification numbers, bank account information, payroll information, future plans, and intellectual property (Al-Alawi & Al-Bassam, 2020). Cyber fraudsters are highly encouraged to access this important information.

Financial accounting is now seen as the entry point for gaining access to a wealth of sensitive data, allowing a cunning hacker to defraud the firm's clients (Hota & Hota, 2022). The bigger and better the picture they develop of the companies they wish to target, the more information they gather, which could result in the financial statements suffering a catastrophic financial loss and the bank suffering damage to its reputation (Vinciguerra, Cappellieri, & Pizzo, 2021). In addition to the unpleasant process of contacting stakeholders and customers and determining where and how the system was compromised, cyber-attacks hold businesses hostage and cost time and capital (Al-Alawi & Al-Bassam, 2020; Hota & Hota, 2022).

2.4 Quality of Financial Accounting

The accuracy of financial accounts is not an easily quantifiable indication because it depends on users' perceptions and is not directly observable. Each user group has its own standards and notions of what information is valuable and of high quality. The concept of financial accounting quality is being examined more and more in the fields of accounting and economics. Understanding what financial accounting quality means in the context of cybersecurity, as well as how it can be defined and measured, is critical in proposing solutions to financial accounting problems (Nikolaev, 2018).Financial accounting quality is secure and reliable accounting information of high accuracy and free for individual items of the financial statement through ICT that guarantees the cybersecurity of businesses (Muravskyi, 2021). The caliber of financial accounting determines its value (Hribar, Kravet& Wilson, 2014). The fundamental idea behind financial accounting quality is that some accounting information communicates what it is intended to communicate better and with greater accuracy than other accounting information (Azar, Zakaria, & Sulaiman, 2019). Because of this, different financial users that are involved in the financial statements are very interested in accounting quality.

2.5 Accounting Statements

The health and strength of a bank or financial institution can be hard to assess through other methods, but financial

statements provide a window into that health. Examples of accounting statements include the cash flow statement, balance sheet, profit and loss statement, etc. A statement on the cash that was received and spent is the cash flow statement (Muniroh & Yuliati, 2021). In addition to classifying the types of expenses incurred, such as payroll, taxes, loan payments, and equipment purchases, it also classifies the source and quantity of cash received, for instance from sales, interest income, and loan proceeds (Sayari & Mugan, 2013). Whether an expense or revenue is

1. The cybersecurity breach would impact the quality of cash flow.
2. The cybersecurity breach would impact the quality of balance sheet.
3. The cybersecurity breach would impact the quality of profit and loss.

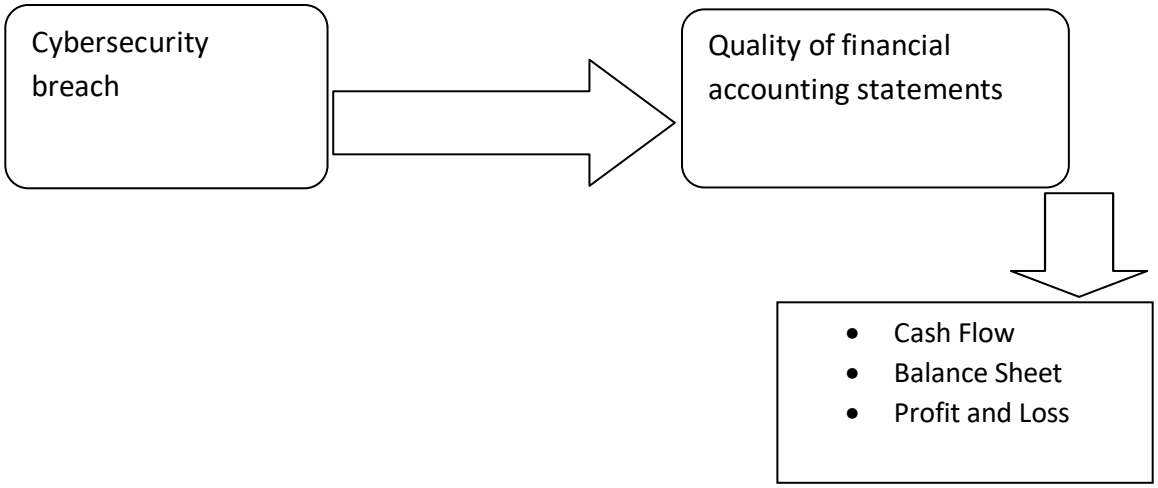


Fig. 1: Conceptual Framework.

2.6 Conceptual Framework

Figure 1 displays the conceptual framework of this study. Based on this framework, the cybersecurity breach is expected to impact the quality of financial accounting statements (cash flow statement, balance sheet, and profit and loss statement) obtained from the Bank of Jordan, Jordan Kuwait Bank, and Arab Jordan Investment Bank databases. The independent variable is a cybersecurity breach, while the dependent variables are the quality of financial accounting statements (cash flow, balance sheet, and profit and loss).

(https://www.ajib.com/download-center/annual-reports).

3 Materials and Methods

3.1 Research Desig

3.1.1 Primary Data Source and sampling

long-term or short-term has no bearing on the situation. The financial statements for the company, which are linked to the liabilities and equity on the balance sheet, are closely related to the other two sections of the cash flow statement, investment and financing (Nguyen & Nguyen, 2020).
Therefore, the following are the hypotheses formulated and tested by this study:

using primary and secondary data sources. The primary data sources were the selected banks and the intelligence agency database, while the secondary data source was the survey as supporting data. Using random probability sampling, three banks were chosen as financial institutions.The dataset were collected from Bank of Jordan (https://bankofjordan.com/en/financial-statements), Jordan Kuwait Bank (https://www.jkb.com/content/annual-reports-0), and Arab Jordan Investment Bank.
These banks have compiled an archive of cybersecurity events and their impacts, which are available on their databases. For further verifiable and supporting action, information for each incident was obtained from the General Intelligence Directorate (GID) database. Although this collection of information cannot be regarded as thorough because several organizations are unaware, they have been violated by cyber fraudsters or are not compelled to report it, it is representative of the entire set of incidents that occurred from 2012 to 2022 among the selected banks in Jordan.

The original dataset consisted of 5956 cybersecurity incidents disclosed by these banks in Jordan, and it is especially appropriate for events in the accounting and finance industries. This research focuses on three types of financial accounting statements: cash flow statements, balance sheets, and profit and loss statements. The primary target of the breached cybersecurity in this study is banks or

financial institutions. However, there are four key obstacles that the researchers of this study ran into while attempting to use the original dataset: (i) irrelevant information focusing on financial accounting statements; (ii) lack of links between cyberattacks and individual customers; (iii) the cyberattacks related to personal information disclosure from the customer to the cyber fraudsters; and (iv) the information does not match information found in the GID database.

We manually filtered information that did not match what was found in the GID database in order to get around these problems. We then manually collected indicators that are often utilized in various accounting and finance disciplines to enrich the dataset, namely: (1) the universal standard symbols used by the banks, which are common to all of them; and (2) the organization key, which is uniquely assigned to each financial institution in Jordan by the GID database. Additionally, we identified details like the fiscal year in which each occurrence took place (which may differ from a calendar one). This procedure finally improves the dataset's quality and reliability and enables researchers to combine the incidents with financial data gathered from databases.

The dataset used in this study is made up of 506 data breaches that Jordanian financial institutions (banks) experienced in the last ten years, from December 2012 to December 2022, and their characteristics.

3.1.2 Secondary Data Source

The study used a survey design approach to evaluate the views of accounting experts' understanding of cybersecurity breaches and information disclosure in their financial institutions (banks). The population for the study consists of forensic accountants, staff accountants, certified public accountants, investment accountants, project accountants, cost accountants, management accountants, auditors, security analysts, and managers from the Bank of Jordan, Jordan Kuwait Bank, and Arab Jordan Investment Bank. The survey consists of 170 samples. The survey was structured and randomly distributed, and it consisted of general questions from two groups of research questions: section (A) had six questions, and section (B) had seven questions. It was scored on a 5-point Likert scale, and the responses were limited to strongly agree (SA), agree (A), undecided (U), strongly disagree (SD), and disagree (D). Only 136 of the 170 copies of the questionnaires that were sent were used, for an overall response rate of 84%.

3.2 Data analysis method

The Statistical Package for Social Sciences (SPSS) version 28.0 software package was used. The significant level was considered to be 5%. To present the cybersecurity data characteristics from 2012 to 2022, descriptive statistics such as mean, median, maximum, minimum, range, and standard deviation were used. The results of Skewness, Kurtosis, Jarque-Bera, and Probability were also presented. The t-test statistic was used to evaluate the hypotheses. The result was that if the t-value is equal to or greater than the significant value, or, in other words, if the t-value > the significant value, then there is a large interaction effect or significant difference.

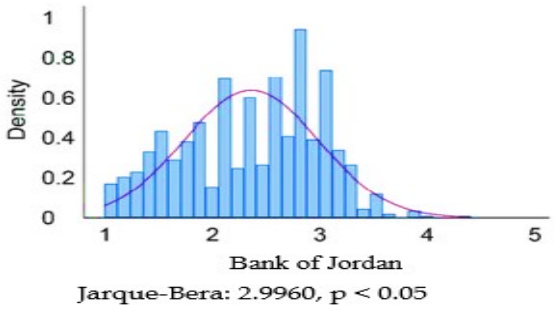
In order to determine the impact of independent variables on dependent variables, regression analysis was performed, which was done to estimate relationships between independent variables (cybersecurity breach) and dependent variables (quality of financial accounting statements). The R-square value (the coefficient of determination), the F statistic, and the p value were reported.

4 Results

The results of descriptive statistics are presented in Table 1. The mean value of incidents of cybersecurity among the financial institutions examined showed that Jordan Kuwait Bank had the highest breach attempts (M = 3.1381, SD = 0.4157), followed by Arab Jordan Investment Bank (M = 1.8406, SD = 0.6123), and Bank of Jordan (M = 1.0202, SD = 0.4157). The results also showed that the data distribution of all observations was normally distributed across all financial institutions examined, with the Bank of Jordan having 4.1545 kurtosis and 0.5578 skewness, the Jordan Kuwait Bank having 4.3775 kurtosis and -0.3069 skewness, and the Arab Jordan Investment Bank having 3.4258 kurtosis and 1.7511 skewness. The observed data distribution around a mean as described by kurtosis and skewness showed that the data were well distributed, with the kurtosis of a probability distribution found to be close to skewness. Compared to a normal distribution, a distribution with excessive kurtosis has more tails.

Table 1: The Descriptive Statistics.

Mean	1.0202	3.1381	1.8406
Median	1.0134	3.2653	1.7509
Maximum	2.1753	5.0181	2.5214
Minimum	1.0032	1.0666	1.0062
Range	1.1621	3.8680	2.9511
Standard Deviation	0.4157	0.9946	0.6123
Kurtosis	4.1545	4.3775	3.4258
Skewness	0.5578	-0.3069	1.7511
Jarque-Bera	2.9960	3.0778	3.0021
Probability	1.1055	3.2121	2.3548
Observations	506	506	506
Cross sections	10	10	10



In Jarque-Bera's test, the sample data in Table 1 was checked to see if the skewness and kurtosis matched a normal distribution. Normal distributions have a symmetrical box with the mean and median at the center, as shown in Figure 1. This indicated few outliers as the data met the assumption of normality, with the probability plotted. The Jarque-Bera results in Table 1 and their distributions in Figure 1 reaffirmed that the data obtained from the financial institutions were well distributed with regards to the incidents of cybersecurity breaches within the last decade.

Table 2 presents the results of the impact of the cybersecurity breaches on financial accounting statements. The types of cybersecurity breaches on financial accounting statements vary across the Jordanian banks examined (Bank of Jordan, Jordan Kuwait Bank, and Arab Jordan Investment Bank). These breaches include accidental information disclosure (ADID) and stealing the encryption key (STEK), which mostly impacted and targeted the balance sheet. in addition to mischievous internal opening access (MVIA), database breach (DTBB), and man-in-the-middle attacks (MITM), which mostly impacted and targeted the cash flow statement. Finally, cybersecurity breaches include malware with encryption (MWWE) and a malicious external attack (MVEA) aimed at profit and loss accounting. The recorded breach characteristics range from intercepted to encrypted to encryption hacked.

Table 2: The results of the impact of the cybersecurity breaches on financial accounting statements.

Type	**Description**	**Records Breached**	**Financial Accounting Statement**
ADID	Accidental Information Disclosure.	Unknown	Balance sheet
STEK	Steal the Encryption Key	Intercept the data	Balance sheet
MVIA	Mischievous Internal opening access	First attempt access to database	Cash flow
DTBB	Database breach	Unknown	Cash flow
MITM	Man-in-the-Middle Attacks	Intercepts communications	Cash flow
MWWE	Malware with encryption	Continuous breach attempt	Profit and loss
MVEA	Mischievous External Attack	Encrypted password hackers	Profit and loss

Table 3 provides a summary of the number of incidents per year across the financial institution. The highest number of incidents of a cybersecurity breach was observed in 2020 (N = 76), and the lowest number of incidents were noted in 2013 (N = 11), 2012 (N = 20), and 2017 (N = 20). It appeared that there was an increased trend from 2013 to 2016 and a

decreasing trend from 2020 to 2022. Table 4 presents a summary of the number of incidents per breach type. The MWWE breach type had the most incidents (N = 139) in cybersecurity, followed by the MVEA breach type (N = 118). The DTBB breach type had the lowest number of incidents (N = 25) across all financial institutions.

Table 3: Number of incidents per year across the financial institutions.

Year	Number of Incidents
2012	20
2013	11
2014	36
2015	65
2016	66
2017	20
2018	60
2019	48
2020	76
2021	61
2022	43
Total	506

Table 4: Number of incidents per breach type.

Breach Type	Number of Incidents
DTBB	25
ADID	80
MVEA	118
MVIA	83
STEK	30
MWWE	139
MITM	31
Total	506

The description for the variables (abbreviations) are display in table 2.

Table 5 displays the results of the regression analysis for cybersecurity breaches and the quality of financial accounting statements. The results in the Bank of Jordan indicate that cybersecurity incidents (breach) had a positive and significant impact on the quality of financial accounting statements, all else being equal. On average, the quality of financial accounting statements of this breached bank is 10% higher in each year in which a cybersecurity incident happens. This result is in line with our expectations (H1 to H3; Table 6). The regression results also indicate that cybersecurity breaches had positive and significant impacts on the quality of financial accounting statements, including the balance sheet (ADID and STEK), cash flow (DTBB and MITM), and profit and loss (MWWE and MVEA). The MVIA cybersecurity breach had no significant impact on the quality of financial accounting. Lastly, the results showed that the cyberattacks across the fiscal years had a significant effect on the quality of the accounting information reported over a 10-year period. Jordan Kuwait Bank's analysis revealed the consequences of various types of cybersecurity breaches. The results revealed that cybersecurity breaches because of ADID, STEK, MVIA, DTBB, MITM, MWWE, and MVEA had a highly significant impact on the quality of the balance sheet, cash flow, and profit and loss statement within the 10-year period. This result indicated that the bank's internal control measures were likely lax, encouraging cyber fraudsters to increase their activities. The last results of the Arab Jordan Investment Bank revealed that breaches had positive and significant impacts on the balance sheet (ADID and STEK), cash flow (DTBB and MITM), and profit and loss (MWWE and MVEA). Similarly, the MVIA activity had no significant effect on the quality of financial accounting statements.

The description for the variables (abbreviations) are display in table 2. Dependent is an indicator variable which is equal to 1 if a bank belongs to dependent sample (i.e., if it was breached), 0 elsewise. Independent is an indicator variable which is equal to 1 in cybersecurity breach event, 0 elsewise. Dependent x Independent is the intercept interaction. **Highly significant at <0.05, *Significant at <0.05. The dependent variable is the natural logarithm of quality of financial accounting statements (LQFAS).

while all the alternative hypotheses have been accepted at the 5% significance level. All the cybersecurity breaches had a significant and positive impact on cash flow, the balance sheet, and profit and loss. Table 7 displays the result of the test of differences on matched samples and the t-tests on differences between incident and non-incidental banks. The results showed some fascinating understandings with regards to dependent variables. The results further implied that breached banks had greater risk by default (ADID, STEK, and MVIA), continuous intercepts (MITM and MWWE), and using encryption strategies. This suggests that the banks faced more combined cybersecurity challenges than single or simple ones.

Table 5: The results of regression analysis for cybersecurity breach

	Bank of Jordan			Jordan Ku
Variable	Coeff.	p-value		Coeff.
Intercept	8.422	0	**	10.781
Dependent	0.423	0.002	**	0.271
Independent	0.128	0.051	*	0.643
Dependent x Independent	0.285	0.026	*	0.252
DTBB	0.440	0.001	**	0.660
ADID	0.157	0.061		0.832
MVEA	0.167	0.044	*	0.941
MVIA	0.111	0.049	*	0.512
STEK	0.099	0.004	**	0.914

Table 7: The result of test of differences on matc

Variable	Overall	breached	Non- breached	Diff.
ADID	12.543	12.812	12.209	0.603
STEK	10.783	9.233	9.071	0.162
MVIA	3.64	0.467	0.256	0.211
DTBB	0.38	0.382	0.378	0.004
MITM	0.398	0.243	0.287	-0.044
MWWE	0.543	0.443	0.273	0.17

Table 8 displays the survey results about knowledge of cybersecurity and its impact on financial accounting statements. The survey results showed that on average, the forensic accountants, staff accountants, certified public accountants, investment accountants, project accountants, cost accountants, management accountants, auditors, security analysts, and managers of the Bank of Jordan, Jordan Kuwait Bank, and Arab Jordan Investment Bank had good knowledge about the cyber fraudsters' activities targeted at their banks. This is because the majority of them agreed (SA or A) on cybersecurity, its impact, and measures in relation to financial accounting statements.

Table 8: Knowledge of cybersecurity and its impact on financial accounting statements.

S/N	Statement	SA	A	U	D	SD
1	Cybersecurity and cybersecurity-related incidents are important knowledge for bank accountants.	35	60	14	8	8
2	Personality factors that influence cybersecurity and cybersecurity-related occurrences include the degree of knowledge possess and the	51	40	7	20	7
3	Daily measures are constantly put in place for route banking activities.	71	44	3	5	2
4	Aware that me or a colleague in the bank have been affected by cybersecurity, which affect financial accounting statements.	38	54	11	8	14
5	Professional accounting standards do not mandate the application of skepticism in financial statements in relation to cybersecurity breaches.	65	41	6	6	7
6	Aware that on a yearly basis, cyber-breach attempts have been targeted at my bank.	75	36	6	3	5

All results are in percentage (%). Strongly agree (SA), agree (A), undecided (U), Strongly disagree (SD), and disagreed (D).

Table 9 presents the results of banks and accidental financial information disclosures in relation to cybersecurity breaches. The results showed varied perceptions. Most of the accountants agreed (SA or A; 64%) that they had incidents of accidental financial information disclosure that resulted in fraud detection at the bank. Also, with many of them (A = 54%), noticed a few times some missing financial information from the bank accounting statement vaults. Accountants and auditors with special skills in cybersecurity have indicated that they have more quality and higher-level

Table 9: Banks and accidental financial information di

S/N	Statement

training on accidental financial information disclosure (A = 60%). In addition to the fact that the majority of the accountants (SA = 71%) also disagreed (D = 47) that the bank cybersecurity officers have identified weaknesses and areas susceptible to fraud.

5 Discussion

This article highlighted the impact of cybersecurity on the quality of financial accounting statements among banks in Jordan. Banks' primary concern in recent years has been cybersecurity, owing to their vulnerability to cyberattacks, which continue to employ new strategies based on modern technology. Opening of entry points, accidental disclosure, and malware attack strategies on financial accounting statements from financial institutions are all possible causes were also aware that banks that lose their financial data to cyberattacks must deal with the loss of assets, damage to their images, and possibly regulatory sanctions.

However, most of the accountants disagree (D = 60%) that there has been an incident of their bank disclosing its cybersecurity strategy, resulting in a bank cybersecurity breach. Also, most of the respondents disagreed (D = 70) that the cybersecurity system has affected stakeholder trust and confidence in the bank's financial statements. Similarly, they of increased cybersecurity incidents. The internal operations of financial institutions are a soft entry point for new accountants or employees with weak knowledge of cyberattack tactics. Evidence has shown that the MVIA, DTBB, MITM, etc. play a key role in cyberattack issues on financial accounting statements (Janvrin & Wang, 2019; Smith, 2020; Peng & Li, 2022), particularly in Jordan. Threats and attacks on financial statements have far-reaching consequences for Jordanian and global financial institutions.

Instead of viewing cybersecurity as a strategic risk, most banks in Jordan approach it from a threat-based perspective, which encourages the attackers more because this approach is like treating symptoms while leaving behind the root cause. Regular and incident-based financial reporting frequently fails to reach appropriate skilled experts or officers in time. Even when risks and weaknesses like DTBB, STEK, or sharing data with third parties are not frequently checked or reviewed (Alzoubi et al., 2022), this might result in a false sense of security.

In recent years, financial institutions or banks have reported a significantly higher volume of cybersecurity breaches (Peng & Li, 2022). Based on the findings of this study, the number of cybercrimes against financial institutions is still high per year, even though we noticed some decreasing trends from 2020 to 2022. These cybersecurity breaches indicate that the banks face more incidences on a yearly basis, maybe during the end-of-year accounting statement preparation. The duration of the breach is significant on a yearly basis, as few banks, such as the Bank of Jordan, were hacked in a month or two, while some banks (e.g., the Arab Jordan Investment Bank) reported cyber breach attempts to the GID on a quarterly basis. This may be because the cyber fraudsters could be highly active during a particular period of the year or in a selected month. The cybersecurity breaches analyzed in this study are just the ones that the banks have acknowledged; several other cyberattacks go unreported to the GID because of the reputation of the Jordanian banks and the seriousness of the matter. However, these occurrences show that there is a definite cybersecurity risk that the banks in Jordan pose that will adversely affect their financial accounting statements. In addition to causing a substantial financial loss, the cybersecurity risk also threatens investors' faith in Jordanian banks and the financial institutions that work with the banks (Abulhaija, Hattab, & Qusef, 2022). Additionally, financial institutions make major contributions to the global GDP (Vitolla et al., 2020). Therefore, a cybersecurity breach is more than just a technical concern for banks or other financial institutions; it also has the potential to lead to global financial uncertainty. These analyses of cybersecurity breaches show the effects that cyberfraud issues have on financial accounting statements. This is because the breached banks had greater risk by default (ADID, STEK, and MVIA) and continuous intercepts (MITM and MWWE).

Data disclosure or gateway is another cybersecurity concern banks confront in addition to malware attacks directed at the financial statements, which thereby impact the quality of the accounting statements. There is evidence that the number of data seepage attacks among financial institutions has increased due to cyber breaches since the advancement of modern technology in big data management (Gao, 2022).Data leaking is a persistent and frequent problem that banks deal with (Shulha et al., 2022; Talha et al., 2022). Due to the fact that 90% of bank services in Jordan are digital, it appears that they are more susceptible to data leaks (Abulhaija, Hattab, & Qusef, 2022). This is likely the reason why this study found that cybersecurity breaches had positive and significant impacts on the quality of the balance sheet (ADID and STEK), cash flow (DTBB and MITM), and profit and loss (MWWE and MVEA).

Breached banks were more likely to have internal weaknesses or poor measures used as entry points by the cyber fraudsters to gain access to these financial statements. This suggests that banks with breaches experience less stringent regulatory oversight than banks without breaches. There is little difference between banks that have been breached and those that have not, contradicting this association, which is not supported by other variables. It had an effect on the quality of financial accounting statements by increasing the probability of reporting low profits or low income, getting a going concern report, or issuing a restatement. According to the Bank of Jordan's most recent report on cybersecurity, hackers recently used sophisticated malware to attack bank databases, and the susceptibility of malware attacks has grown in recent years. According to a recent survey report, hackers target financial institutions to exploit their weaknesses (Ghelani, Hua, & Koduru, 2022). According to research, hackers are increasingly targeting Jordanian banks as a result of cybersecurity vulnerabilities (Tawfik et al., 2021).

The acceptance of alternative hypotheses showed cybersecurity breaches had a significant and positive impact on cash flow, the balance sheet, and profit and loss. The results of the hypotheses showed that banks in Jordan revealed their MVIA exposure to cybersecurity incidents within the last decade. These results are consistent with the research by Negrea (2022), which revealed that organizations must share information about internal controls for cybersecurity. Moreover, the nature and impact of the cybersecurity breach are not fully known by various financial accountants in the banks in Jordan, as revealed by the survey findings. This showed that they lack the knowledge and skills necessary to evaluate the firm's position when it comes to questions about whether information users have the necessary knowledge and abilities to enhance the quality of the financial statements.

The acceptance of alternative hypotheses may be explained in another way. Based on the findings, the security breach was impacted by cyberattack activities targeting the financial statements through bank employee risk windows. Once a security manager chooses to implement a zero-trust architecture, they may grow overconfident, which can expose the financial statement's security to risks, which also support our hypotheses. The possibility that cyberattacks can assess options across banks through this overconfident window This can increase cyberattack optional activities by continuously attacking and intercepting overuse of passwords and gadgets or software by the manager to protect the system that creates the window for MWWE and ADID. Quantifying risks may also provide one with a fictitious sense of security; managers may feel that the circumstances are more under control by lowering risks to make bank officers or staff more accessible to the financial statements, but the uncertainty may still exist and can only be discovered during actual operations when actual events take place. Even outside the context of cybersecurity, this is true. non-fully in control of 100% of the security domain with the least amount of friction and documenting the resulting security requirements. This may become another set of functional requirements in software usage, which can produce a higher risk of financial statement exposure to third parties than

common security "toil" that yields only marginal value. MVEA that encourage security events can impact financial losses during the process of analysing the probability of a security breach on financial statements. According to Alzoubi et al. (2022), risk assessment can be helpful, but the most significant and impactful breach can affect subsequent choices of information disclosure among security officers, bank managers, and accountants. It is sufficient to guide effort priority if one has a reasonable idea of what is simplest for the attacker, that is, the things they are most likely to do first in their operations.

6 Conclusion, recommendations, and limitations

The findings of this study showed that the cybersecurity breaches or incidents among banks in Jordan had a significant impact on the quality of financial accounting statements. The cybersecurity breaches had positive and significant impacts on the balance sheet (ADID and STEK), cash flow (DTBB and MITM), and profit and loss (MWWE and MVEA). The MVIA cybersecurity breach had no significant impact on the quality of financial accounting. Bank managers, accountants, stakeholders, and policymakers could find these outcomes relevant and interesting. A deeper knowledge of the possible effects of cybersecurity issues beyond only the immediate, observable costs like lost financial records, lost income, etc. may be helpful to accountants and bank managers.

As cyber-attacks have progressed from isolated to widespread, banks and financial institutions must reconsider their strategy and shift their focus from prevention to resistance. Rapid response time can aid in minimizing the cyber breach's impact on the bank's financial statements and reputation. Financial institutions should focus on improving the accounting team's and managers' knowledge through training on the latest cybersecurity threats. To increase professional expertise, banks should work more closely with reliable training centres to organize training programs. The cash flow, balance sheet, and profit and loss statements are very helpful records for accountants and managers but require extreme protection from unauthorized individuals. Making financial statements is a difficult operation that takes a lot of work, but users today demand information that is of high quality. Accounting software should also be constantly updated, renewed, and checked daily. Large financial institutions with a lot of financial information may have a greater chance of being the target of the recent cyber breach.

Various research limitations apply to this study, some of which may open up new research directions. To start with, our selection of data breaches is not all-inclusive. It only includes a sampling of three banks in Jordan. It is difficult to generalize the finding that cybersecurity breaches at significant Jordanian banks do not result in a noticeable decline in the quality of financial accounting statements.

References

[1] Abulhaija, S., Hattab, S., & Qusef, A. (2022, June). Cyber Security Awareness, Knowledge and Behavior in the Banking Sector in Jordan. In 2022 13th International Conference on Information and Communication Systems (ICICS) (pp. 48-53). IEEE.

[2] Achim, A. M., & Chiş, A. O. (2014). Financial Accounting Quality and Its Defining Characteristics. SEA: Practical Application of Science., **2(3)**, (2014).

[3] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber Security Threats on Digital Banking. In 2022 1st International Conference on AI in Cybersecurity (ICAIC) (pp. 1-4). IEEE.

[4] Azar, N., Zakaria, Z., & Sulaiman, N. A. (2019). The Quality of Accounting Information: Relevance or Value-Relevance?. Asian Journal of Accounting Perspectives., **12(1)**, 1-21(2019).

[5] Buch, C. M., & Goldberg, L. S. (2022). Complexity and riskiness of banking organizations: Evidence from the International Banking Research Network. Journal of Banking & Finance., **134**, 106244(2022).

[6] Bushman, R. M. (2014). Thoughts on financial accounting and the banking industry. Journal of Accounting and Economics., **58(2-3)**, 384-395(2014).

[7] Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis., **17(4)**, 356-374(2020).

[8] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review., **4(10),** (2014).

[9] Gao, J. (2022). Analysis of enterprise financial accounting information management from the perspective of big data. International Journal of Science and Research (IJSR)., **11(5)**, 1272-1276(2022).

[10] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.

[11] Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. McKinsey & Company, (October), 1-11.

[12] Hribar, P., Kravet, T., & Wilson, R. (2014). A new measure of accounting quality. Review of Accounting Studies., **19(1)**, 506-538(2014).

[13] Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. Journal of Information Systems., **33(3)**, A1-A2(2019).

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

[15] Kiradoo, G. (2020). Ethics in accounting: Analysis of

current financial failures and role of accountants. International Journal of Management (IJM)., **11(2)**, 241-2472020).

[16] Kohlbeck, M., & Warfield, T. (2010). Accounting standard attributes and accounting quality: Discussion and analysis. Research in Accounting Regulation., 22(2), 59-70(2010).

[17] Muniroh, I., & Yuliati, A. (2021). Do cash flow and accounting profit information affect stock prices?. Journal of Accounting and Strategic Finance., **4(1)**, 108-121(2021).

[18] Muravskyi, V. (2021). Accounting and Cybersecurity. Monograph, Scientific Editor – Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA.

[19] Negrea, C. I. (2022). Can Cyber Risk Affect Financial Stability?. Ovidius University Annals, Economic Sciences Series., **22(1)**, 368-376(2022).

[20] Nguyen, D. D., & Nguyen, A. H. (2020). The impact of cash flow statement on lending decision of commercial banks: evidence from Vietnam. The Journal of Asian Finance, Economics and Business., **7(6)**, 85-93(2020).

[21] Nikolaev, V. V. (2018). Identifying accounting quality. Chicago Booth Research Paper., (14-28).

[22] Okab, R., & Al-Oqool, M. A. (2014). The Role of Accountants in E-accounting Information Systems' Lifecycle at the Jordanian Banking Sector. International Journal of Business and Social Science., **5(4)**, (2014).

[23] Peng, J., & Li, C. W. (2022). Security breaches and modifications on cybersecurity disclosures. Journal of Accounting and Management Information Systems., **21(3)**, 452-470(2022).

[24] Razafiarivony, M. A., & Hosna-Janeta, M. (2022). Effects of Financial Statements Quality and Users' Knowledge on Decision Considerations and the Role of Satisfaction as a Potential Mediator. East African Journal of Business and Economics., **5(1)**, 35-47(2022).

[25] Sanusi, Z. M., Rameli, M. N. F., & Isa, Y. M. (2015). Fraud schemes in the banking institutions: prevention measures to avoid severe financial loss. Procedia Economics and Finance., **28**, 107-113(2015).

[26] Sayari, N., & Mugan, F. N. C. S. (2013). Cash flow statement as an evidence for financial distress. Universal Journal of Accounting and Finance., **1(3)**, 95-103(2013).

[27] Schroeder, R. G., Clark, M. W., & Cathey, J. M. (2022). Financial accounting theory and analysis: text and cases. John Wiley & Sons.

[28] Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews., **15(1)**, 138-156(2022).

[29] Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. Journal of Open Innovation: Technology, Market, and Complexity., **8(2)**, 80.

[30] Smith, S. S. (2020). Emerging Technologies and Implications for Financial Cybersecurity. International Journal of Economics and Financial Issues., **10(1)**, 27.

[31] Stein, K. (2018). Statement on commission statement and guidance on public company cybersecurity disclosures. International Journal of Management (IJM)., **11(2)**, 241-247(2018).

[32] Sun, G. (2020). Banking institutions and banking regulations. The Handbook of China's Financial System, 9-37.

[33] Talha, M., Wang, F., Maia, D., & Marra, G. (2022). Impact of information technology on accounting and finance in the digital health sector. Journal of Commercial Biotechnology., **27(2)**, (2022).

[34] Tawfik, O. I., Al Tahat, S., Jasim, A. L., & Abd Almonem, O. (2021). Intellectual Impact Of Cyber Governance In The Correct Application Of Cloud Accounting In Jordanian Commercial Banks-From The Point Of View Of Jordanian Auditors. Journal of Management Information and Decision Sciences., **24(5)**, 1-14(2021).

[35] Vincent, N. E., & Trussel, J. (2019). Predicting Reported Cybersecurity Breaches Using Financial Measures. Journal of Forensic and Investigative Accounting., **11(3)**, (2019).

[36] Vitolla, F., Raimo, N., Rubino, M., & Garzoni, A. (2020). The determinants of integrated reporting quality in financial institutions. Corporate Governance: The International Journal of Business in Society., **37(3)**, 73-89(2020).