FBA | Future of Business Administration

ISSN: 2783-5936
Volume **3**, Issue **2**

"The Effect of Cyber Risk on Banks Profitability in Egypt": An Empirical Analysis

Mohamed Abdelraouf[1*], Samira M. Allam[2], Farid Moharram[2]

[1] Faculty of Management, Arab Academy for Science and Technology and Maritime Transport-AAST, Egypt
[2] Faculty of Business, Ain Shams University- ASU, Egypt
mohamedabdelraouf04@gmail.com

ABSTRACT

Recent years have seen an impressive increase in the integration of financial technology or fintech in the global banking industry, resulting in product, service, and operational developments. Nowhere has this shift in focus been more pronounced than in fintech, a sector that has seen remarkable growth in Egypt. Nevertheless, this is not without its difficulties since integrating technology means that their banks are more susceptible to cyber risk, which could decrease its profitability. This research aims to assess whether cyber risk exerts a statistically significant negative impact on the profitability of banks in Egypt, utilizing a sample of 16 banks spanning the years 2017 to 2022. The study employs panel data analysis through STATA 14 for its investigation. The findings demonstrated that cyber risk has a negative significant effect on bank profitability, and this assumption was supported by the study's findings. According to the findings, cyber risk has a significant and negative impact on both ROA and GPM. As a consequence of this, it is necessary to incorporate preventative measures in order to deal with the constantly shifting cyber threat landscape. It is also essential to highlight the significant role that technology and data security play in ensuring that the banking industry remains robust and profitable in the digital era.

Keywords: Fintech, Cybersecurity, Cyber risk, Banks profitability

Cite this article as: Abdelraouf, M., Allam, S. M., & Moharram, F. (2024). "The Effect of Cyber Risk on Banks Profitability in Egypt": An Empirical Analysis. *Future of Business Administration, 3*(2), 1-16. https://doi.org/10.33422/fba.v3i2.693

1. Introduction

Inefficiency has plagued the Egyptian banking market recently. Investors have been attentively studying bank annual reports to assess their stability and financial well-being, particularly profitability. Investors expected financial technology, or fintech, to boost banking industry profits by improving goods, services, and operations (Mavlutova et al., 2021). However, the increased adoption of financial technology (fintech) has caused an unexpected issue: rising cyber risk.

Fintech adoption in Egypt has skyrocketed, transforming banking practices. Digital payment systems, mobile banking apps, and online financial solutions have made banking easier for customers (Elkmash, 2021). Nevertheless, this change has its risks. Technology dependence has made banks increasingly vulnerable to cybersecurity dangers, which may hurt their finances (Uddin et al., 2020).

Due to this transition, more people are using online banking, requiring financial institutions to protect large amounts of sensitive client data. Cybercriminals exploit banking network weaknesses to profit from the large amount of information available. Online adversaries use

phishing assaults, malware, ransomware, and data breaches to breach banking industry digital defences (Alawida et al., 2022).

The motivations of cybercriminals might vary, encompassing objectives such as financial profit and involvement in political espionage. The ramifications of their activities can be substantial. The interdependent association between the thriving fintech sector and the persistent menace of cybercrime has generated noteworthy apprehensions, specifically pertaining to the security and profitability of Egypt's banking business. The banking sector, traditionally seen as a bastion of reliability and confidence, presently faces an ever-changing cyber threat environment (Brewster et al., 2017; Abdel Megeid, 2015).

As a result, financial institutions must allocate significant resources to implement robust cybersecurity protocols, strengthening their operational infrastructure and safeguarding sensitive client information, which leads to significant financial burdens (Tao et al., 2019). Nevertheless, it is imperative to address the lingering query: Can cyber risk potentially exert an adverse influence on the profitability of banks, thereby dissuading investors and precipitating financial instability?

In light of the contemporary period characterised by technological disruption and the advent of the digital revolution, it is imperative to grasp the intricate relationship between cyber threats and the financial performance of banks. Investors depend on the annual reports of banks to evaluate their financial stability and overall condition, where profitability plays a crucial role as a performance metric and a factor that attracts investment. The existence of cyber hazards raises concerns over the potential of fintech to enhance profitability and has the potential to erode investor confidence (Buckley et al., 2019).

The objective of this study is to ascertain the potential negative impact of cyber risk on the profitability of banks operating in Egypt and to provide insight into the true ramifications of cyber risk for the Egyptian banking industry through the examination of financial data, statistical studies, and a careful examination of institutional responses to such risks.

The findings of this study have substantial consequences not only in the current context but also for policymakers, financial institutions, and consumers and can yield useful insights into the risks and strengths of Egypt's banking system when confronted with cyber threats and contribute to formulating policies that mitigate risks and safeguard Egypt's financial well-being.

At the end, this research is to understand the potential adverse effects of cyber risk on the profitability of banks in Egypt. In addition, the study provides professional recommendations to enhance cybersecurity measures and maintain investor confidence, establishing it as the pioneering research of its kind conducted in the country. Thus, there will be an academic contribution and a research gateway for future studies. These proposals have the potential to increase the cybersecurity measures of banks, safeguarding their profitability and maintaining investor confidence. Implementing these proposals can mitigate the risk of financial instability and bankruptcy.

2. Literature Review

2.1. Cyber Risk

Böhme et al. (2019) categorise cyber risk into two main types: digital damage stemming from physical assets and physical harm arising from digital assets. Additionally, cyber risk can be delineated by three key parameters: (i) impact, signifying the potential severity of the damage

resulting from a specific risk; (ii) threat, gauging the probability of the occurrence of a given risk; and (iii) vulnerability, assessing the effectiveness of existing information security measures (Biener et al., 2015, p. 134).

The discourse surrounding the subject of cyber risk has relatively recently gained prominence in academic circles, particularly considering the multifaceted nature of cyber risks and the swift evolution of cyber threats and corresponding cybersecurity measures. The concept of cyber risk encompasses two primary dimensions: technological and economic (Cavelty & Wenger, 2020).

From a technical standpoint, this phenomenon is distinguished by its intricate design complexity, capacity to alter component behaviour, and pervasive and constantly evolving landscape of hazards. On an economic front, cyber risk is characterised by imperfect information, externalities, and correlations stemming from shared risk variables (Böhme et al., 2018, p. 181).

2.2. Banks Profitability

Country-level economic resource allocation relies on commercial banks. They regularly transfer depositor funds to investors. For sustainable intermediation, banks must be profitable by creating enough income to cover their operational costs over time. For sustainable intermediation, banks must be profitable. Banks' financial performance affects economic growth beyond intermediation (Mugyenyi, 2018).

Good financial performance rewards shareholders' investments. This spurs investment and economic growth. Although bad banking performance can cause bank failure and crises, which hurt economic growth, Since the Great Depression in the 1940s, academics have studied commercial bank financial performance. For two decades, research has shown that commercial banks in Sub-Saharan Africa (SSA) have a greater return on assets (ROA) than their worldwide counterparts (Dzombo et al., 2017; Flamini et al., 2009).

Banks assume a crucial function within the financial system and the broader economy. Evaluating profitability has significant relevance for a range of stakeholders, encompassing investors, regulators, and policymakers. Two primary metrics used to assess a bank's profitability are return on assets (ROA) and gross profit margin (GPM). Assessing a bank's profitability, Return on Assets (ROA) serves as a crucial indicator. This analysis offers valuable insights into the efficacy with which a financial institution employs its assets to produce profits (Jhoansyah et al., 2023; Alshehadeh et al., 2022).

2.3. Cyber Risk and Banks Profitability

Najaf and Mostafiz (2021) investigated how fintech startups affect partner banks' cybersecurity risk. They used 50 banks from 10 countries that had worked with fintech businesses to create a composite index to assess their cybersecurity risk.

The study found that banks' cybersecurity risk increased significantly after partnering with fintech businesses. The survey suggests that fintech companies lack the resources and awareness to tackle cybersecurity concerns. The research also found that fintech regulatory sandboxes may encourage cyberattacks. The authors recommend banks and regulatory bodies build cybersecurity defences and update the fintech sandbox framework to reduce these risks. The authors recommend these steps to institutions.

Aldasoro et al., (2020) examined financial sector operating and cyber vulnerabilities. The authors used a dataset of operational loss events from 100 large worldwide banks from 2002

to 2018 to achieve this goal. The data were separated into macro-regions and sub-regions for densely populated areas. Each loss event was marked for bank size; however, the authors could not identify a financial institution.

The authors calculated operational value-at-risk using analytic and loss distribution methods and recorded loss event occurrence, discovery, and recognition times. They also examined the relationship between operational losses and the macroeconomic climate and estimated cyber threats, a major financial sector risk.

Moreover, Erkan-Barlow et al. (2023) examined the effects of cyber risks on the bank's profits in the USA and controlled such variables as the kind of breach, the size, and the kind of ownership of the bank involved. It was established that data breaches negatively affect the profitability of banks, and larger banks are better placed to manage cyber threats because of their capacity than small, medium, and private banks. The study found that data breaches affect the profitability of commercial banks through the following intermediary variables bank deposits, lending, and liquidity.

In addition, Alsakini et al. (2024) explored the effect of cybersecurity threat incidents on the quality of financial accounting in Jordanian financial organizations. The researchers gathered information regarding 506 cybersecurity events at Jordanian banks from 2012 to 2022, and they used descriptive analysis. Breach attempts were significantly higher at Jordan Kuwait Bank, which takes the lead and is followed by Arab Jordan Investment Bank and the Bank of Jordan in equal order. The results showed that all the variables analysed in the research displayed a normal distribution across all the financial institutions investigated, and the distribution of the cybersecurity incidents of the last decade was evenly distributed.

2.4. Previous Studies in Egypt

Alber and Nabil (2015) conducted a study focusing on the impact of information security on the performance of Egyptian banks, analysing a sample of 13 banks in 2013. The assessment of information security involved the scrutiny of ISO 27001 and the application of PCI-DSS, while bank performance was evaluated based on profitability and asset quality. The study revealed that ISO 27001 could influence return on capital (ROC), whereas PCI-DSS might have an impact on non-performing loans. The authors recommended that Egyptian banks prioritise information security to maintain competitiveness.

Subsequently, it was observed that there is a research gap in the existing literature concerning cyber risk and its association with bank profitability, particularly in the context of Egyptian banks. This current study aims to address this gap by investigating the relationship between cyber risk and the profitability of Egyptian banks. The research will utilise a sample of Egyptian banks to explore the effects of cyber risk on profitability. The insights gained from this investigation will be valuable for shaping risk mitigation strategies and promoting financial stability.

Therefore, to strengthen the hypothesis, relevant theories are mentioned to explain the relationship between cyber risk and bank profitability. The resource-based view (RBV) is one of the contemporary strategic management theories that anchors its analysis on a firm's internal resources and capabilities. The concept assumes that organisations can sustain high levels of business performance by mobilising resources that are valuable, rare, unique, and inimitable (Ferreira and Ferreira, 2024).

In contrast, agency theory deals with the issues that are realised because of the separation of ownership and control in organizations. The paper explores the roles and responsibilities of

principals (for example, shareholders) and studying agents (for instance, managers) and their conflicts of interest and issues of asymmetric information (Moloi et al. 2020).

Accordingly, the following is hypothesized:

H1: Cyber risk has a negative significant effect on Banks profitability.

H1a: Cyber risk has a negative significant effect on ROA of banks profitability.

H1b: Cyber risk has a negative significant effect on GPM of banks profitability.

3. Methods

The secondary source of the statistical data is annual reports covering the 6-year period from 2017 to 2022. Moreover, the official websites of various financial institutions provided the data used to demonstrate the reliability of the results.

The method chosen to collect is secondary data, mainly from historical data, which comes from the annual reports of 16 banks in Egypt, which are the Commercial International Bank (CIB), Hong Kong and mainly from historical data, which comes from the annual reports of 16 Banks in Egypt, which are commercial international bank (CIB), Hongkong and Shanghai Banking Corporation (HSBC), Egyptian Gulf Bank, Abu Dhabi Islamic Bank (ADIB), Arab International Bank (AIB), Qatar National Bank (QNB), Attijariwafa Bank, National Bank of Kuwait (NBK), Ahli United Bank of Kuwait (AUB), Arab African International Bank (AAIB), Alex bank, Al Baraka Bank, Suez Bank, Banke misr, Banque du caire and National Bank of Egypt (NBE). The sample did include national and private banks, as mentioned earlier.

3.1. Sampling Technique

Sharma (2017) stated that the random sampling method's primary objective is to guarantee that each person or thing in the population has an equal and independent chance of being chosen for the sample. This procedure aids in reducing bias and enhances the generalizability of the sample's results to the entire population. The sample size for the research paper was decided by Cochran (1963).

$$n = \frac{z^2 \times p \times (1-p)}{e^2} = \frac{(1.65)^2 \times (0.5)(0.5)}{0.1^2} \approx 68.0625 \approx 68 < 97 \quad (1)$$

Therefore, the sample needs to exceed 68 respondents to obtain a margin of error of 0.1.

The Egyptian banks were the target population of the study. The banks chosen stated that they had adapted fintech. In this study, secondary data in the form of financial statements were analysed using STATA 14. Samples are chosen where the target populations are:

1) The banks have released the full set of financial reports for the 2017–2022 fiscal year.
2) The banks that mentioned the cyber risks in their financial reports.
3) The banks provide all the necessary data, including the ratios of cyber risk as an independent variable, while the control variable is CAR and bank size and the dependent variable is ROA and GPM.
4) The key metrics of each variables as follows:

Independent variables:

i) Cyber risk ratio

- Key words of annual reports and interpreting it by using gunning fog index

$$0.4[\left(\frac{total\ words}{total\ sentences}\right) + 100\left(\frac{complex\ words}{total\ words}\right)] \quad (2)$$

According to Figure 2, the Gunning Fog Index (FOG) is utilised as a measure of the reading level of the cyber-risk text. The FOG index is calculated based on the number of words per sentence and the percentage of complex words in the text. Complex words are defined as words with at least three syllables (Loughran and McDonald, 2014).

In the context of the cyber risk ratio, a higher FOG index indicates a greater frequency and/or complexity of cyber risk disclosures in a bank's annual report. This suggests that the bank is facing more cyber threats (Swift et al. 2020). In this study, we measured the cyber risk ratio using the Fog Index approach, which assesses textual complexity and readability. The study applied this concept to analyze the prevalence and complexity of cyber risk disclosures in bank annual reports as we searched for key terms related to cyber threats in Table 1.

ii) ROA

$$\frac{\text{Net income}}{\text{Total assets}} \quad (3)$$

iii) GPM

$$\frac{\text{Gross income}}{\text{income received from sales of goods or services}} \quad (4)$$

Control variables:

In this study the, the following control variables are adopted by the researcher:

iv) CAR

$$\frac{Tier\ 1\ capital + Tier\ 2\ capital}{Risk - weighted\ Assets} \quad (5)$$

- Tier 1 Capital includes common equity and retained earnings.
- Tier 2 Capital includes items like subordinated debt.
- Risk-Weighted Assets are determined by applying the appropriate risk weights to various assets held by the bank.

v) Bank size

- Log to total assets

Table 1.
Measurement of variables

Variables	Measurement	Sources
Independent variables		
• Cyber risk ratio	• Checklist from annual report based on the following Keywords • "Cyber-attack, cyber security, cybercrime, cyber risk, hacking, swift attack, internet hacking or crimes)	• Thach et al. (2021); Alber and Nabil (2016)
Dependent variables		
• ROA • GPM	• Checklist from annual reports for each bank	• Rahmani (2020); Shakoor et al. (2014)
Control variables		
• CAR • Bank size	• Checklist from annual reports for each bank	• Fauziah and Fadhilah (2022)

To test the research hypotheses, the researcher identifies the following empirical models:

$$ROA = \beta 0 + \beta 1 Cyber\ risk\ ratio + \beta 2\ CAR + \beta 3 Bank\ Size + \varepsilon it \quad (6)$$

$$GPM = \alpha 0 + \alpha 1 Cyber\ risk\ ratio + \alpha 2 CAR + \alpha 3 Bank\ Size + \varepsilon it \quad (7)$$

The models included in the study were as mentioned in equations (2 and 3). They describe the impact of cyber risk ratio (CR), capital adequacy ratio (CAR), and bank size on bank profitability. The presence of CR in Eqs. (6 and 7) that may have a direct effect on ROA and GPM.

The appropriate statistical method is panel data analysis to tackle the issues with panel data. Panel data refers to a type of data that has two dimensions, namely the individual effect and the temporal effect. In contrast to cross-sectional data analysis, panel data captures the observations of each individual at distinct and specified time intervals (Hsiao, 2022). Several statistical techniques have been developed to address panel data, including the fixed effect model, random effect model, and pooled effect model (Arellano and Honoré, 2001).

Nevertheless, the prevailing models in academic research are fixed-effect models and random-effect models. The study used both fixed-effect and random-effect models. To compare the performance of both models and use the optimal model, the study will use the Hausman test (Zulfikar and STp, 2018).

4. Results

4.1. Descriptive Statistics

Table 2.
Descriptive Measure for the variables in phenomenon

Variable	Mean	Std. Dev.	Min	Max
ROA	0.015912	0.010456	0.001237	0.054207
GPM	0.439818	0.226437	0.035702	1.230364
Cyber Risk Ratio	0.35901	0.177204	0	1.2
Bank size	9.467151	1.357548	7.601597	11.67833
CAR	0.177715	0.039479	0.105	0.3107

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

It was found that the average ROA of banks was 1.6%. The ROA variation among the banks sampled was relatively high (CV = 65%). In terms of GPM, the sampled firms had an average of 44%. It is also found that there is a high variation between the banks (CV = 51.5%). The average cyber risk ratio was 0.36, where the minimum was 0 and the maximum was 1.2. If the cyber risk ratio is greater than one, it reflects the high cost of cyber risk to banks. The average bank size was approximately 9.47. The variation in terms of bank size is relatively low (CV = 14%). The CAR average was found to be 0.1777 in the sampled banks.

Table 3.
Descriptive Measure for the variables in phenomenon by year

Variable	Mean	Std. Dev.	Min	Max
2017				
ROA	0.016922	0.012901	0.001722	0.050377
GPM	0.435614	0.289743	0.035702	1.168173
Cyber Risk Ratio	0.380625	0.055913	0.2	0.44
Bank size	9.345414	1.3831	7.601597	11.34822
CAR	0.156799	0.022071	0.12324	0.193
2018				
ROA	0.018025	0.011848	0.002059	0.047042
GPM	0.386307	0.263331	0.073405	1.204923
Cyber Risk Ratio	0.434375	0.197327	0.2333	1.143
Bank size	9.4021	1.377226	7.675873	11.41037
CAR	0.162829	0.022357	0.1247	0.2123
2019				
ROA	0.018572	0.013426	0.003369	0.054207
GPM	0.4398	0.258633	0.209444	1.230364
Cyber Risk Ratio	0.335	0.147603	0.11	0.56
Bank size	9.424442	1.384295	7.674753	11.42962
CAR	0.184501	0.042955	0.1253	0.2764
2020				
ROA	0.013978	0.009471	0.001237	0.030961
GPM	0.482508	0.244209	0.18266	1.189927
Cyber Risk Ratio	0.295625	0.159163	0	0.64
Bank size	9.469226	1.386336	7.735499	11.45557
CAR	0.183344	0.042183	0.1193	0.26
2021				
ROA	0.014361	0.00704	0.004359	0.02663
GPM	0.451966	0.148668	0.204522	0.771247
Cyber Risk Ratio	0.286875	0.17895	0	0.64
Bank size	9.546505	1.397036	7.759148	11.54924
CAR	0.1948	0.050528	0.1177	0.3107
2022				
ROA	0.013611	0.006357	0.005064	0.025435
GPM	0.442712	0.132757	0.265469	0.777538
Cyber Risk Ratio	0.421563	0.237667	0.11	1.2
Bank size	9.615221	1.421243	7.618686	11.67833
CAR	0.184019	0.039583	0.105	0.2504

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Observing table (3), there was an increasing trend in the cyber risk ratio over the years from 2017 to 2018, reaching a value of 0.434. There was a sudden decline in 2019 with the news of the outbreak of the pandemic. The focus of the banks was shifted to dealing with COVID-19. This explained the gradual decline that went on until it reached 0.28 in 2021. Then, after lifting the regulations accompanied by COVID-19, life returned to normal, as did the focus on cyber risks, which showed a cyber-risk ratio of 0.42. The ROA, on the other hand, kept

declining until it reached its lowest in 2022, at an average value of 1.36%. The bank size and CAR had a nearly constant average throughout the years.

4.2. Correlation Analysis

Table 4.
Pearson Correlation Coefficients for the phenomenon

	ROA	GPM	Cyber Risk Ratio	Bank size	CAR
ROA	1				
GPM	0.3057	1			
Cyber Risk Ratio	0.1036	0.0487	1		
Bank size	0.0435	-0.2343	-0.1704	1	
CAR	0.082	0.0856	-0.0378	0.1551	1

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Since ROA and GPM are different measures of the profitability of the banks, There is a weak significant relationship between ROA and GPM. It The analysis revealed no significant relationship between the variables. Therefore, the modelling will not exhibit multicollinearity (Shrestha, 2020).

4.3. Stationarity Test

Levin et al. (2002) provided the Levin Lin Chu test, which was used as a stationarity test. It presents the idea of applying an augmented dickey-fuller test to each panel. It assumes a common autoregressive parameter for all panels. Regarding the test, the hypotheses are as follows:

H0: Panel contain unit roots.
H1: Panel is stationary.

Table 5.
Levin Lin Chu stationarity test

Variables	Test Statistic	P-value	Decision
GPM	-3.2e02	0.0000	Stationary
ROA	-7.4351	0.0000	Stationary
Cyber Risk Ratio	-93.7157	0.0000	Stationary
CAR	-12.4466	0.0000	Stationary
Bank Size	-3.2766	0.0005	Stationary

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Table 5 found all the variables to be stationary at a 99% confidence level. This will require no difference or lag in the dataset to proceed with the analysis. Therefore, there is no need for a co-integration test (Levin et al., 2002).

4.4. Random and Fixed Model Building

4.4.1. 1st Model: Modelling the ROA of the Banks

Table (6) was computed to present the coefficients of the variables. The table shows that the cyber risk ratio had a significant negative impact on the ROA. This is justified by literature such as Ko & Dorantes (2006), Tweneboah-Kodua et al. (2018), and Allam & Abdelraouf (2023). The cyberattacks affect the stocks,, which in turn would lower the ROA (Tweneboah-Kodua et al., 2018). When the error was considered to have a fixed effect, the bank size had a significant negative significant impact on ROA at a 99% confidence level. However, there was not enough evidence that the rest of the variables had a significant impact on ROA.

Table 6.
Coefficients of the Random and Fixed Effect Model for ROA in banks

	Random Effect Model		Fixed Effect Model	
	Coefficient	***Standard Error***	***Coefficient***	***Standard Error***
Cyber risk Ratio	-0.00908**	0.004311	-0.01213***	0.003877
Bank size	-0.00034	0.001325	-0.01418***	0.005565
CAR	-0.02261	0.019322	-0.01933	0.018046
_cons	0.026412**	0.012954	0.157982***	0.05186
Test Statistic	Wald Chi square: 5.78*		F test statistic: 6.58**	
Rho	0.515		0.937	

*Sig Values: ***<0.01, **<0.05, *<0.1, *>0.1*
Source: Calculations based on 16 sampled banks along 6 years using Stata 14

51.5% of the variation in ROA was explained by the random effect model based on cyber risk, bank size, and CAR. On the other hand, 93.7% of the variation in ROA was explained by a fixed effect model based on cyber risk, bank size, and CAR. The models were found to be both significant at a 90% confidence level. Therefore, a Hausman test should be used to find the optimal model.

Table 7.
Hausman test for ROA of banks

	Test statistic	Degrees of freedom	P-value
Hausman Test	2.35	3	0.5036

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Observing table (7), the test statistic showed a p-value greater than significance level. Therefore, the random effect model was deemed better.

4.4.2. 2nd Model: Modelling the GPM of the Banks

Table 8.
Coefficients of the Random and Fixed Effect Model for n GPM in banks

	Random Effect Model		Fixed Effect Model	
	Coefficient	***Standard Error***	***Coefficient***	***Standard Error***
Cyber risk Ratio	-0.23024**	0.089047	-0.26325***	0.088839
Bank size	-0.03871	0.03329	0.069457	0.127537
CAR	0.211191	0.399432	0.048464	0.413552
_cons	0.851455***	0.321504	-0.13184	1.188467
Test Statistic	Wald Chi square: 7.96**		F test statistic: 3.06**	
Rho	0.633		0.787	

*Sig Values: ***<0.01, **<0.05, *<0.1, *>0.1*
Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Table (8) was computed to present the coefficients of the variables. The table shows that the cyber risk ratio had a significant negative impact on the GPM. That is logically explained as an occurrence of cyber-attacks would decrease the gross profit of the bank due to mistrust of customers. However, there was not enough evidence that the rest of the variables had a significant impact on GPM.

63.3% of the variation in GPM was explained by the random effect model based on cyber risk, bank size, and CAR. On the other hand, 78.7% of the variation in ROA was explained by a fixed effect model based on cyber risk, bank size, and CAR. The models were both

found to be significant at a 95% confidence level. Therefore, a Hausman test should be used to find the optimal model.

Table 9.
Hausman test for GPM of banks

	Test statistic	Degrees of freedom	P-value
Hausman Test	31.85	3	0.000

Source: Calculations based on 16 sampled banks along 6 years using Stata 14

Observing table (9), the test statistic showed a p-value less than significance level. Therefore, the fixed effect model was deemed better.

5. Discussion

In this empirical analysis, the study explored the effect of cyber risk on the profitability of banks in Egypt, with a particular focus on key financial indicators, including return on assets (ROA) and gross profit margin (GPM). The study's findings shed light on the intricate relationship between cyber risk and the financial health of the Egyptian banking sector. The research hypothesis (H1) posited that cyber risk exerts a negative significant influence on banks' profitability, and this assertion found support in the study's outcomes. The analysis revealed that, H1a and H1b are accepted, meaning that the cyber risk has a substantial and adverse effect on both ROA and GPM.

This observation is consistent with existing research, underscoring those cyberattacks can erode customer trust, leading to decreased gross profits and ultimately compromising the profitability of banks. Additionally, the study considered other variables, such as bank size and capital adequacy ratio (CAR), and discerned that bank size had a negative significant effect on ROA. However, the influence of these variables on GPM and ROA was not as pronounced as that of cyber risk. Furthermore, the study conducted a Hausman test to determine whether a random effect model or a fixed effect model is better suited for the data. The results of the test indicated that both models held significance. However, observing Table (8), the test statistic showed a p-value greater than significance level. Therefore, the fixed effect model was deemed better.

The findings of the research are discussed within the context of the international body of literature on cyber risk exposure affecting financial institutions. Thus, based on the literature like Levin et al. (2002) on unit root tests in panel data and Mugyenyi (2018) on the adoption of cloud computing services for sustainable development in commercial banks, the specificity of the processes occurring in the banking sector of Egypt is revealed.

Moreover, the discussion section provides an overview of possible explanations for the noted relationships between cyber risk and bank profitability. Carrying out an analysis based on the identified models and presenting variables like cyber risk ratio (CR), capital adequacy ratio (CAR), and the size of the bank, the research reveals the impact of the described factors on the level of profitability using such coefficients as Return on Assets (ROA) and Gross Profit Margin (GPM). Employing the recommendations of Hsiao (2022) and Arellano & Honoré (2001) on panel data analysis, the study develops a sound methodology to determine how the several factors of cyber risk affect or influence bank performance.

The implications of this study are of paramount importance to the banking industry in Egypt. The rapid proliferation of fintech and digital banking channels has introduced numerous opportunities and conveniences for customers and financial institutions. However, this expansion has also increased the vulnerability of banks to cyber threats, spanning from phishing attacks to data breaches. These threats pose a substantial risk to banks' profitability

and, more broadly, to the financial stability and reputation of the banking sector. The study underscores the critical need for banks to prioritise cybersecurity measures and implement effective risk management strategies.

As the banking landscape continues to evolve in the digital age, it becomes imperative for financial institutions to recognise and quantify the genuine effect of cyber risks on their profitability. By doing so, they can make informed decisions, allocate resources efficiently, and invest in robust cybersecurity to safeguard their operations and customer data. The research's significance extends beyond the banking industry; it has relevance for policymakers and customers alike. It provides valuable insights into the strengths and vulnerabilities of Egypt's banking system in the face of cyber threats.

All these insights can become a starting point for learning, as well as for establishing and furthering the elaboration of policies that would help to reduce the risks and guarantee the financial sustainability of the given nation. Moreover, it instructs the customers about secure banking options in order to prevent the chances of cyber threats in a technologically advanced society. Thus, by outlining the perspectives of the necessity of taking active measures to resist cyberrisks and underlining the critical role of technology and data protection to maintain a sufficiently strong and sustainable banking system, the study highlights the significance of cybersecurity in the context of the modern digital world.

Lastly, this empirical analysis helps to expand the number of papers and contributions within the field of cybersecurity and the relationship between it and banking profitability in Egypt. It gives emphasis to the need to address the important issue of implementing a preventive approach with regards to the emerging threats to cyber risk and underscores the importance of technology and data to sustain the banking industry in the new millennium.

6. Recommendation

For the academic implications, future research can build on this study by examining how specific types of cyber events like data breaches, service outages, and fraud affect profitability. Additionally, studying banks across multiple countries can reveal whether the impacts of cyber risks vary by region. As cyber threats continue to escalate globally, understanding their business impacts will only grow in importance. ARDL can be applied to further investigation by banks to search for or examine the short- and long-term impact on their profitability.

At the practical implications, The study underscores the critical need to prioritise cybersecurity measures for banks that operate in Egypt, given the potential impact of cyber risk on profitability. Investing in robust cyber defences and resilience measures is imperative to safeguard operations and customer data. By elaborating on specific strategies such as implementing advanced threat detection systems, conducting regular cybersecurity audits, and enhancing employee training on cybersecurity best practices, banks can strengthen their defences against evolving cyber threats. Additionally, the study could delve into the importance of establishing incident response protocols and crisis management strategies to mitigate the financial and reputational risks associated with cyber incidents. The Central Bank of Egypt may need to provide enhanced oversight and issue regulatory guidelines to ensure banks are adequately managing cyber risks.

Moreover, the recommendations for policymakers can be further elaborated to provide guidance on enhancing regulatory oversight and issuing guidelines to ensure banks effectively manage cyber risks. Policymakers play a crucial role in setting standards for cybersecurity practices, promoting information sharing among financial institutions, and

fostering collaboration between the public and private sectors to combat cyber threats collectively. By expanding on recommendations such as developing cybersecurity frameworks tailored to the banking sector's specific needs, incentivizing investments in cybersecurity technologies, and establishing mechanisms for reporting and responding to cyber incidents, policymakers can create a more resilient and secure environment for banks to operate in.

Furthermore, the study could explore the potential benefits of public-private partnerships in addressing cyber risks, the role of regulatory sandboxes in fostering innovation while managing cybersecurity challenges, and the importance of international cooperation in combating cross-border cyber threats. ensure the long-term financial health and stability of the banking sector in Egypt.

Finally, by elaborating further on the practical implications and recommendations for banks and policymakers, the study can enhance the actionable insights derived from its findings. By offering specific strategies, best practices, and policy recommendations tailored to the Egyptian banking context, the research can empower stakeholders to proactively address cyber risks, strengthen their cybersecurity posture, and contribute to a more secure and resilient financial ecosystem.

7. Limitation

This study has some limitations that provide avenues for future research. First, the sample comprised only banks and did not include public or private firms, which face their own cyber-risk exposures. By restricting the analysis to a specific geographical region, the generalizability of the results to other countries or regions may be limited. This constraint raises questions about the transferability of the findings to different regulatory environments, market conditions, and technological landscapes. Future research could explore the cross-country variations in the impact of cyber risk on firms profitability to enhance the external validity of the results.

Second, the study restriction to the past six years limited the observations of major cyber incidents that occur sporadically. Cyber threats are dynamic and evolving, and their impact on bank profitability may vary over time. By extending the timeframe of the analysis, researchers could capture a more comprehensive picture of the long-term effects of cyber risk on banks' financial performance by applying the ARDL model. This expansion would provide a more robust foundation for understanding the persistence and magnitude of cyber risk challenges faced by banks in the short and long term.

Third, the study only considered ROA and GPM as measures of bank profitability, but it could overlook other dimensions of profitability that are influenced by cyber risk. Exploring a broader range of profitability indicators, such as Return on Equity (ROE) or Net Interest Margin (NIM), could provide a more holistic view of how cyber risk impacts different aspects of banks' financial health. Finally, the study focus on Egypt limits the generalizability of the results to other emerging or developed countries.

Future research could expand this study in several ways. One area to explore is the mediating role of factors such as bank capital adequacy and cyber insurance in the relationship between cyber risk and bank profitability. Applying the methodology to samples that include non-bank institutions and extending the time period studied could reveal additional insights. Evaluating multiple measures of profitability and conducting cross-country comparisons can help determine if the findings hold in other contexts. Despite its limitations, this initial study provides valuable evidence that the surging threat of cyber risks can undermine profitability

for banks as the financial sector embraces digitalization. Expanded samples, longer timeframes, more profitability indicators, and cross-country analyses can build on these findings in future cyber risk research.

Data availability: The data generated and/or analysed during the current study are available from the corresponding author on request.

Competing interests: The authors report no conflicts of interest.

References

Abdel Megeid, N. S. (2017). Liquidity risk management: conventional versus Islamic banking system in Egypt. *Journal of Islamic Accounting and Business Research*, *8*(1), 100-128. https://doi.org/10.1108/JIABR-05-2014-0018

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2022.08.003

Alber, N., & Nabil, M. (2015). The Impact of Information Security on Banks' Performance in Egypt. *International Journal of Economics and Finance*, *7*(9). https://doi.org/10.2139/ssrn.2752070

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. https://ssrn.com/abstract=3549526

Allam, S., & Abdelraouf, M. (2023). Role of Cyber-Risk on shaping the movement of stock returns: An event study on T-Mobile Company. *مجلة الدراسات التجارية المعاصرة*, *9*(15), 730-764. https://doi.org/10.21608/csj.2023.322077

Alsakini, S. A. K., Alawawdeh, H. A., & Alsayyed, S. (2024). The Impact of Cybersecurity on the Quality of Financial Statements. *Appl. Math*, *18*(1), 169-181. https://doi.org/10.18576/amis/180117

Alshehadeh, A. R., Elrefae, G., & Injadat, E. (2022). Influence of traditional performance indicators on economic added value: evidence from insurance companies. https://doi.org/10.22495/cgobrv6i4p2

Arellano, M., & Honoré, B. (2001). Panel data models: some recent developments. In *Handbook of econometrics* (Vol. 5, pp. 3229-3296). Elsevier. https://doi.org/10.1016/S1573-4412(01)05006-1

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158. https://doi.org/10.1057/gpp.2014.19

Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. Variance, 12(2), 161-185.

Brewster, B., Kemp, B., Galehbakhtiari, S., & Akhgar, B. (2015). Cybercrime: attack motivations and implications for big data and national security. In *Application of big data for national security* (pp. 108-127). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-801967-2.00008-2

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of fintech and the rise of techrisk. *UNSW Law Research Paper*, (19-89). https://doi.org/10.2139/ssrn.3478640

Cochran, W. G. (1963). *Sampling Techniques*, 2nd Ed., New York: John Wiley and Sons, Inc.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855

Dzombo, G. K., Kilika, J. M., & Maingi, J. (2017). The effect of branchless banking strategy on the financial performance of commercial banks in Kenya. *International Journal of Financial Research*, *8*(4), 167-183. https://doi.org/10.5430/ijfr.v8n4p167

Elkmash, M. R. M. A. (2022). The impact of financial technology on banking sector: evidence from Egypt. *International Journal of Finance, Insurance and Risk Management*, *12*(1), 100-118. https://doi.org/10.35808/ijfirm/280

Erkan-Barlow, A., Ngo, T., Goel, R., & Streeter, D. W. (2023). An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States. *Journal of Global Business Insights*, *8*(2), 120-135. https://doi.org/10.5038/2640-6489.8.2.1246

Fauziah, R. S., & Fadhilah, N. H. K. (2022). The Impact of Credit Risk on The Profitability With Characteristics Bank as Control Variables. *JAK (Jurnal Akuntansi) Kajian Ilmiah Akuntansi*, *9*(2), 145-158. https://doi.org/10.30656/jak.v9i2.4346

Ferreira, N. C., & Ferreira, J. J. (2024). The field of resource-based view research: mapping past, present and future trends. *Management Decision*. https://doi.org/10.1108/MD-10-2023-1908

Flamini, V., McDonald, C. A., & Schumacher, L. B. (2009). The determinants of commercial bank profitability in Sub-Saharan Africa. https://doi.org/10.5089/9781451871623.001

Hsiao, C. (2022). *Analysis of panel data* (No. 64). Cambridge university press. United Kingdom. https://doi.org/10.1017/9781009057745

Irfan Shakoor, M., Nawaz, M., Zulqarnain Asab, M., & Khan, W. A. (2014). Do mergers and acquisitions vacillate the banks performance?(Evidence from Pakistan banking sector). *Research Journal of Finance and Accounting*, *5*(6), 123-137.

Jhoansyah, D., Suryanto, S., Kostini, N., & Hermanto, B. (2023). Financial Indicators And Its Implications On Profitability Of Soe Banks In Indonesia. *Central European Management Journal*, *31*(3), 279-291.

Ko, M. and Dorantes, C. (2006), "The impact of information security breaches on financial performance of the breached firms: an empirical investigation", Information Resources Management Journal, Vol. 22 No. 2, pp. 13-22.

Levin, A., Lin, C. F., & Chu, C. S. J. (2002). Unit root tests in panel data: asymptotic and finite-sample properties. *Journal of econometrics*, *108*(1), 1-24. https://doi.org/10.1016/S0304-4076(01)00098-7

Loughran, T., & McDonald, B. (2014). Measuring readability in financial disclosures. *the Journal of Finance*, *69*(4), 1643-1671. https://doi.org/10.1111/jofi.12162

Mavlutova, I., Fomins, A., Spilbergs, A., Atstaja, D., & Brizga, J. (2021). Opportunities to increase financial well-being by investing in environmental, social and governance with respect to improving financial literacy under covid-19: The case of Latvia. *Sustainability*, *14*(1), 339. https://doi.org/10.3390/su14010339

Moloi, T., Marwala, T., Moloi, T., & Marwala, T. (2020). The agency theory. *Artificial Intelligence in Economics and Finance Theories*, 95-102. https://doi.org/10.1007/978-3-030-42962-1_11

Mugyenyi, R. (2018). Adoption of cloud computing services for sustainable development of commercial banks in Uganda. https://nru.uncst.go.ug/handle/123456789/4547

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. *International Journal of Financial Engineering*, *8*(02), 2150019. https://doi.org/10.1142/S2424786321500195

Rahmani, N. A. B. (2020). Pengaruh Return On Assets (ROA), Return On Equity (ROE), Net Profit Margin (NPM), Dan Gross Profit Margin (GPM) Terhadap Harga Saham Perbankan Syariah Periode Tahun 2014-2018. *HUMAN FALAH: Jurnal Ekonomi Dan Bisnis Islam*, *7*(1). https://doi.org/10.30829/hf.v7i1.6944

Sharma, G. (2017). Pros and cons of different sampling techniques. *International journal of applied research*, *3*(7), 749-752.

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. *American Journal of Applied Mathematics and Statistics*, *8*(2), 39-42. https://doi.org/10.12691/ajams-8-2-1

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. *Journal of Forensic and Investigative Accounting*, *12*(2), 197-212.

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671. https://doi.org/10.1016/j.future.2019.03.042

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845. https://doi.org/10.24874/IJQR15.03-10

Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. *Information & Computer Security*, *26*(5), 637-652. https://doi.org/10.1108/ICS-05-2018-0060

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability?. *International Review of Financial Analysis*, *72*, 101587. https://doi.org/10.1016/j.irfa.2020.101587

Zulfikar, R., & STp, M. M. (2018). Estimation model and selection method of panel data regression: an overview of common effect, fixed effect, and random effect model. *JEMA: Jurnal Ilmiah Bidang Akuntansi*, 1-10. https://doi.org/10.31106/jema.v15i2.838