REVISTA MEXICANA DE ECONOMÍA Y FINANZAS Nueva Época REMEF (THE MEXICAN JOURNAL OF ECONOMICS AND FINANCE)

**Revista Mexicana de Economía y Finanzas, Nueva Época**

Volumen 21 Número 1, enero - marzo 2026, pp. 1-25, e1115

DOI: https://doi.org/10.21919/remef.v21i1.1115

*(Recibido: 31/agosto/2024, aceptado: 25/abril/2025, publicado: 1/enero/ 2026)*

imef fundación de investigación

# Credit and Cyber Risk Effects on Egyptian Bank Profitability

**Mohamed Abdelraouf**[1] - King Salman International University, Egypt

**Abstract**

In the ever-changing environment of banking and finance, it is important for both institutions and regulators to understand how one risk factor influences another and how these interactions affect profitability. This study investigates whether credit risk impacts Egyptian banks' profitability, with cyber risk acting as a moderator. A quantitative research design is adopted using panel data from 17 Egyptian commercial and public banks covering the period 2017–2022. The findings reveal that cyber risk significantly moderates the relationship between credit risk and profitability, mitigating the negative effect of credit risk on return on assets (ROA). Specifically, while an increase in credit risk typically reduces profitability, higher levels of cyber risk—often indicative of more robust risk management and digital infrastructure—appear to cushion this adverse effect. However, the study is limited by data availability, as it does not include observations beyond 2022, and by its focus on the Egyptian banking sector, which may limit generalizability. The practical implications suggest that strengthening cyber risk management systems can serve as a strategic tool for banks to buffer consequences of financial risk exposures, particularly credit risk.

*JEL Classification: G55, G32, G33, G41*

*Keywords: Credit risk, Fintech, Cybersecurity, Cyber risk, Banks profitability.*

# Efectos del riesgo de crédito y cibernético en la rentabilidad de los bancos egipcios

**Resumen**

En el entorno dinámico de la banca y las finanzas, es fundamental que tanto las instituciones como los reguladores comprendan cómo un factor de riesgo influye en otro y cómo estas interacciones afectan la rentabilidad. Este estudio tiene como objetivo investigar si el riesgo crediticio influye en la rentabilidad de los bancos egipcios, considerando el riesgo cibernético como una variable moderadora. Se adopta un diseño de investigación cuantitativo utilizando datos de panel de 17 bancos comerciales y públicos de Egipto durante el período 2017–2022. Los resultados revelan que el riesgo cibernético modera significativamente la relación entre el riesgo crediticio y la rentabilidad, atenuando el efecto negativo del primero sobre el rendimiento sobre activos (ROA). Específicamente, mientras que un aumento en el riesgo crediticio reduce normalmente la rentabilidad, niveles más altos de riesgo cibernético —frecuentemente indicativos de una infraestructura digital más sólida y de una mejor gestión de riesgos— parecen contrarrestar dicho efecto adverso. Se recomienda que los bancos refuercen sus sistemas de gestión del riesgo cibernético como una estrategia clave para enfrentar las consecuencias de los riesgos financieros, especialmente el riesgo crediticio. Entre las limitaciones del estudio se encuentran la disponibilidad de datos, que solo alcanzan hasta 2022, y su enfoque exclusivo en el sector bancario egipcio, lo que puede limitar la generalización de los resultados. La originalidad del estudio radica en su enfoque en la interacción entre el riesgo crediticio y el riesgo cibernético como determinantes conjuntos de la rentabilidad bancaria en un contexto emergente. En conclusión, el fortalecimiento de la infraestructura cibernética y la gestión del riesgo digital puede representar una herramienta estratégica efectiva para mejorar la resiliencia financiera de los bancos.

*Clasificación JEL: G55, G32, G33, G41*

*Palabras clave: Riesgo crediticio, Fintech, Ciberseguridad, Riesgo cibernético, Rentabilidad bancaria anormales, estudio de eventos, VIX, S&P 500, DJIA.*

[1] Corresponding Author. Email: mohamedabdelraouf04@gmail.com

* No funding source was received for the development of this research.

# 1. Introduction

The last few years have posed certain issues to the Egyptian banking structure, leading to internal inefficiencies and risks that can potentially harm its stability and profit. Annual reports for bank industries are among the documents most eagerly studied by investors striving to determine the health and performance of a company, as well as its attractiveness on the financial market in terms of profitability (Butt et al., 2022). While credit risk has long been a primary concern for banks, the rapid adoption of financial technology (fintech) in Egypt has introduced a new dimension of risk. Namely, it has become apparent that cyber risk complicates matters.

Originally, credit risk, or the risk involving loss as a result of borrowers' failure to meet their obligations, remained a key determinant of banks' profitability. Like the other banks in the global markets, banks in Egypt have astoundingly applied elaborate models and business strategies to address the issue of credit risk. However, the blending of fintech solutions is changing the ladder aggressively day by day.

Advanced digital banking has become common in Egypt due to the rise of fintechs, whereby payment systems, mobile apps or solutions, and online services have improved the consumer experience and business procedures (Elkmash, 2021). This digital transformation was supposed to enhance the banking industry's profits by enhancing products, services, and operations (Mavlutova et al., 2021). On the other hand, it has endangered banks with extra securities, considering cyber risks, affecting their profitability and stability.

With the recent increase in the use of net banking among the Egyptian population, banks find themselves handling large amounts of confidential information belonging to their clients. Due to the digital transformation, banks have become exposed to various cyber-risk factors that have a major tendency to lead to financial loss (Uddin et al., 2020). Threat actors target banking organisations' networks, which involve phishing, malware, ransomware, and data breaches, among others, in an attempt to breach the digital security layers (Alawida et al., 2022).

The interplay between credit risk, cyber risk, and bank profitability presents a complex challenge for the Egyptian banking sector. While credit risk remains a fundamental concern, the moderating effect of cyber risk on this relationship is becoming increasingly apparent. Cyber incidents can exacerbate credit risk by compromising loan approval processes, manipulating credit scores, or causing reputational damage that affects borrower behaviour.

Thereby, strong cybersecurity measures, protection of the financial institutions' structure, and clients' data security require significant investments from the financial institutions. To this effect, the various measures put in place have been realised at the expense of the banks, even though they are vital (Tao et al., 2019). The question arises: How does the interaction between credit risk and cyber risk affect bank profitability in Egypt, and what are the implications for investor confidence and financial stability?

In this era of technological disruption and digital revolution, understanding the intricate relationship between credit risk, cyber risk, and bank profitability is crucial. Investors rely on bank annual reports to evaluate financial stability, but the presence of cyber risks complicates this assessment and potentially erodes confidence (Buckley et al., 2019).

This study aims to investigate the effect of credit risk on bank profitability in Egypt, with a particular focus on how cyber risk moderates this relationship. By analysing financial data, conducting statistical studies, and examining institutional responses to these risks, we seek to provide insights into the true implications of both credit and cyber risks for the Egyptian banking industry.

The study observed that though Attijariwafa and the National Bank of Egypt had relatively lower and variable ROA compared to the highly and relatively stable ROA of HSBC, variation in ROA was widespread among most sampled banks, especially before the emergence of COVID-19. The heat map assessment showed that overall, banks' log debt ratios were moderate, and the Egyptian Gulf Bank exhibited the highest value in 2018. The cyber risk ratio was not fluctuating much between the banks, and the recent values were even higher than the previous ones, with the highest values in HSBC and CIB.

All variables were checked for stationarity using the stationarity test, and all of them passed the test. Diagnostic tests justified the use of a feasible GELS regression model so that there was a significant relationship between ROA and numerous variables such as cyber risk ratio, CAR, debt ratio, and NPLR. Similarly, the products of cyber risk ratio and debt ratio were also significant, which suggests cyber risk acts as a moderator of the association between debt ratio and ROA. grouped, it was established that the size of the bank had a significantly positive effect on ROA and that the CAR only had an insignificant effect once the moderator was included in the model.

Besides contributing to the academic field, this study is the first extensive investigation in Egypt; it paves the way for subsequent studies. This one offer advice in both credit risk management and the measures to take to avoid cyber threats, which are all meant to keep the banks profitable and investors satisfied. Adoption of these recommendations may help in reducing the probability of financial vulnerability as well as the insolvent position of the sector in Egypt.

Therefore, understanding the relationship between credit risk, cyber risk, and bank profitability is the main objective of this study in an attempt to shed light on the challenges facing Egypt's banking industry and possible recommendations towards a more resilient financial system.

The recent years have been marked by the substantial transformation and issues generated in the Egyptian banking sector, mainly because of the domestic inefficiencies, the increase in the credit risk, and emergence of the financial technology (fintech), which posed multi-dimensional financial risks through cyber risks. Although risk management, i.e., the probability of a borrower defaulting on his loan, used to be the major target of risk management in banks, the digital revolution has transformed this situation. The introduction of mobile banking, online payment systems, and other online platforms have led to the improvement of the delivery of services but at the same time contributed to the susceptibility to cyberattacks like phishing, ransomware attacks, and data leaks. These dangers not only jeopardize the profitability of the banks; they also endanger investor trust and financial stability of nations. With digital banking increasingly entering into the daily lives of Egyptians, their vulnerability to cyber risks increases and it is now time to invest in cybersecurity in a big way to counter such threats. A recent examination of the Egyptian banking systems entails empirical analysis that shows how much cyber risk has moderated the correlation between the traditional variables of risk, like the debt ratio and credit risk, and profitability among the Egyptian banks, that is, banks like the HSBC, CIB, Attijariwafa, and the National Bank of Egypt.

The paper demonstrates the initial comprehensive analysis of the interaction between cyber risk and credit risk in determining the return on assets (ROA) in the Egyptian banking system which employs such statistical methods as GELS regression and heat map rating. The results have important implications on policymakers and investors alike, and this is because it proves that credit risk has continued to be central to financial performance, but has been changing, identified as a new factor that investors and policymakers should consider given that it can either increase or reduce profitability levels. These two risks require well-orchestrated risk management approaches to ensure financial resilience in the Egyptian banking system that is becoming more and more digital, as well as to enhance stability in the MENA region as regional economies of the region undertake a similar transformation.

The absolute and relative contribution of the present study shall be to be among one of the first studies to empirically test the moderating mechanism of cyber risk on the correlation between the financial risks of credit risk and bank profitability within a setting in Egypt banking sector which has been largely unaddressed in the current literature. Although previous studies have mostly examined credit risk only or cyber risk only, the proposed research is different and unique in that both aspects are integrated into examining the effects of technological vulnerabilities on the traditional measures of financial performance such as ROA. Further, inclusion of the interaction terms, and feasible generalized least squares (FGLS) estimation makes the methodology rich in that it allows a more precise estimate under both panel-effects on heteroskedasticity and autocorrelation. In addition to improving the knowledge of risk interdependence in emerging markets, this treatment also gives, in a very practical way, learning to both the Egyptian banks and policymakers struggling with the issue of digital transformation.

Finally, in Section 2, the literature review of each variable of the study will be presented before the methodology in Section 3. Section 4 will provide the main findings of the study in response to the formulated hypothesis. Sections 5 and 6 will comprise discussion and, lastly, limitations, which will bring a conclusion to the whole research work.

# 2. Literature review

This section explores prior work on bank profitability, credit risk, and cyber risk, which together form the thematic structure of this study

## 2.1. Credit risk

Credit risk is simply the possibility of losing money through non-repayment of contractual debt, especially loans, by the debtor. Information on credit risk evaluation has grown over the years, particularly in light of financial crises that revealed that standard means of credit assessment were ineffective (Kanyambu, 2021). Credit Risk Transfer Theory is one of the first theories describing the possibility of credit risk shifting from lenders to other financial players with the help of credit derivatives. This theory also focusses on recognising the sources of risk and how one link in the financial market can transfer a risk to another, and if the latter does not cope with it, then such a risk becomes a systemic risk (Naili and Lahrichi, 2022).

Another important framework is the structural model of credit risk, which stems from the Black-Scholes model and Merton's view that equity can be thought of as a call option on firms assets. This model, which was developed around the 1970s by Merton, seeks to determine credit risk based on the probability that the value of a firm's asset will be below a set value (the default point) when the credit is due to mature (Aywak, 2022).

Some of the determinants include the level of volatility of the firms' assets and the economic conditions, which provide a more mathematical basis for calculating default probabilities. These theories, coupled with achievements in artificial intelligence and big data, have changed the methods of credit risk assessment and opened the possibilities of using more sophisticated techniques that consider the greater number of conditions and behaviors of borrowers (Åhman, 2024).

## 2.2. Cyber risk

Böhme et al., (2019) categories cyber risk into two main types: virtual loss resulting from tangible goods and vice versa tangible loss due to virtual commodities. Additionally, cyber risk can be delineated by three key parameters: This risk term is used to measure: (i) impact, which is the possible extent of damage Abdelraouf et al., (2024) that may be caused by or result from a certain risk; (ii) threat, which describes the likelihood of the occurrence of a certain risk; and (iii) vulnerability, which determines the adequacy of existing information security measures. Biener et al., 2015, p. 134). The problem of cyber risk as the subject of discourse has emerged only quite recently in the academic community, and this is quite logical, considering two factors: the complexity of cyber risks and the tendencies of the rapid development of cyber threats and corresponding protection mechanisms.

The concept of cyber risk encompasses two primary dimensions: technological-environmental, or technological and economical (Cavelty & Wenger, 2020). From a technical perspective, this phenomenon is characterized by design complexity, the ability to transform the parts' behavior, and a high, unfolding density of threats that are ubiquitous and evolving (Abdel Megeid, 2017). From an economic perspective, cyber risk is linked with features like information asymmetry, negative externalities, and jointly determined risks (Böhme et al., 2018, p. 181).

## 2.3. Banks Profitability

At the country level, economic resources are distributed through the use of commercial banks. They frequently remit the depositor's money to the investors. For sustainable intermediation, banks must be profitable, whereby some form of income is generated to cater for some of the basic operational costs in the long run. For sustainable intermediation, therefore, the banks have to be viable. This paper has found that there is more to banking and financial intermediation in determining economic growth in Uganda; banking firms' financial performance contributes to Ugandan economic growth regardless of the level of intermediation. If the financial performance is good, then shareholders are rewarded for the investments that they have made. This creates awareness, and as a result, the money that was idle in the banks circulates in the economy (Mugyenyi, 2018).

While poor performance in banking precipitates either the failure of a bank or crises damaging the growth of an economy, since the Great Depression in the 1940s, scholars have embarked on analyzing commercial bank financial performance. The studies revealed that for the past twenty years, commercial banks in Sub-Saharan Africa (SSA) have been more profitable in terms

of return on assets (ROA) than the global commercial bench (Dzombo et al., 2017; Flamini et al., 2009). Banks play a very important role in the overall financial sector as well as in the whole economy of the country. Assessing profitability has immense significance for all types of stakeholders, including the investment community, the government, and policymakers. There are two key ratios that shed light on the ability of a bank to generate profits, and they are returned on assets (ROA). Therefore, in rating a bank's performance, the return on assets (ROA) test plays a significant role. This analysis provides the efficiency with which a financial institution uses its assets to generate revenues (Jhoansyah et al., 2023; Alshehadeh et al., 2022).

## 2.4. Credit risk and Banks profitability

Ekinci and Poyraz, (2019) analyzed the impact of credit risk on the financial performance of deposit banks in Turkey, specifically examining the relationship between credit risk management and profitability indicators such as return on assets (ROA) and return on equity (ROE) for the period from 2005 to 2017. It can be seen from the results that credit risk, which is proxied by the ratio of non-performing loans to total loans, negatively affects both ROA and ROE. This means that credit risks in Turkey have a negative effect on the deposit banks; therefore, they earn a lower amount of profit than those banks with fewer credit risks. The study therefore finds that credit risk management, especially in controlling and monitoring non-performing loans, is vital to increasing the profitability of the bill's. Whereas, Lawrence et al., (2024): The purpose of this study was to analyze and compare how credit risk indicators affected the financial performance of the big four commercial banks together with the small commercial banks of South Africa. The financial year under analysis was 2008–2017.

As the previous studies stressed, our results also showed that the credit risk variables, including the capital adequacy ratio (CAR), the non-performing loan-to-gross loan (NPLGL) ratio, and the board gender diversity (BGD), affected the performance measured by return on assets (ROA) and return on equity (ROE) for both big and small samples. In particular, credit risk indicators inflicted a comparatively bigger impact on the small banks as compared to the big banks.

## 2.5 Cyber risk an banks profitability

Najaf and Mostafiz (2021) studied how threat intensity varied between fintech startups and partner banks. To estimate the cybersecurity risk of the banks, they aggregated a set of composite indices using 50 banks from 10 countries that had previously collaborated with fintech companies. One observed that the underlined cybersecurity risk was more profound once the banks teamed up with fintech businesses. The survey shows that fintech firms are unable to address cybersecurity issues because they are understaffed and not well-informed enough. A report on the research also discovered that fintech regulatory sandboxes may provide incentives for cyberattacks. The authors suggest banks and regulators invest more resources in cybersecurity and modify the fintech sandbox framework further. These steps should therefore be followed by institutions, according to the authors. In their study, Aldasoro et al., (2020) explored operating and cyber financial sector risks. To do this, the authors analysed a sample of operational loss events in 100 large worldwide banks during 2002–2018. In larger macro-regions and densely populated sub-regions, the data were divided operationally into sub-regions or zones. Both the loss events were categorised with reference to the size of the bank; however, the authors failed to find out a bank name. The authors estimated

operational value-at-risk using quantitative and qualitative approaches, as well as loss distribution analysis, and documented loss event occurrence, discovery, and recognition periods. They also looked at how other operational losses might relate to the macroeconomic environment and tried to assess the number of cyber threats as one more significant challenge for the financial sector.

Furthermore, Erkan-Barlow et al., (2023) analyzed the impact of cyber risks and included USA bank profits, and the controlling variables included the breed of the cyber incident and the size and breed of the bank. As the study concluded, it was agreed that data breaches were detrimental to the performance of the banking industry and that large banks were in a better position to handle cyber threats given their resources compared to small, medium, and private banks. The study also discovered that data breaches have an impact on the profitability of commercial banks via bank deposits, lending, and liquidity as intermediary variables.

Similarly, Alsakini et al., (2024) investigated the impact of cybersecurity threats on the accuracy of financial accounting in organizations operating in Jordan. The researchers collected data about 506 cybersecurity incidents at Jordanian banks from 2012 to 2022, and the methodology that was employed for analysis was descriptive statistics. That means breaches' attempts were even more at Jordan Kuwait Bank, followed by Arab Jordan Investment Bank and Bank of Jordan, respectively, in turn of order. The results revealed that all the variables studied in the research were normally distributed in all the financial institutions in the sample, in addition to the distribution of the ten years of cybersecurity incidents being uniform.

## 2.6. Cyber risk and Credit risk

Cyber risk and credit risk can be correlated within the framework of the modern financial environment. Given the fact that technology has become more crucial in operating businesses and financial institutions and that a that a growing number of organisations retain critical information online, technology risk may directly impact credit risk. If the cyber attack is executed successfully, it can compromise customers' data, financial losses, company functions, and brand images of the organisation (Ossola et al., 2017).

Some of these consequences might erode the company's financial worth and capacity to pay the debt and could decline its credit rating. In addition, expenses that are incurred in responding to an event, for example, legal costs, fines imposed by the regulatory authorities, and cybersecurity enhancements, are expensive for a business. Speaking of credit risk, it is crucial for financial institutions to be able to evaluate it properly, and a cyber attack can hinder this process if the credit issuer's systems or data are violated. Therefore, modern lenders and credit rating agencies take into account cybersecurity measures as factors in their credit risk evaluations since information protection evidenced by the implementation of cybersecurity measures might be crucial for understanding the general level and quality of risk management and financial sustainability (Vučinić and Luburić, 2022).

The Basel III is a complete package of reform-measures formulated by the Basel Committee on banking supervision to enhance better regulation, supervision and risk-management of banks after the 2008 financial crisis (Birindelli et al., 2022). The framework establishes elevated capital provision, containing higher minimum capital proportions and the initiation of capital conservation and countercyclical capital buffers with the introduction of new liquidity arrangements, one of which contains the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR) to provide banks

with sufficient liquid resources during the time of stress. Basel III also proposes leverage ratio as a complement to the risk-based capital ratio, and introduces a systemic risk buffer in that capital surcharges rely on the classification of banks as systemically important (Baptista and Karmakar, 2017).

In a risk management context, the framework promotes good risk governance, stress testing, and future-looking risk assessment capacities and obligates banks to retain thorough risk managing units that will be in a position to recognise, measure, track and manage all kinds of risks such as the credit risks, market risks, operational risks, as well as liquidity risks (Van Greuning and Bratanovic, 2020). Network Requirements of Basel III has essentially changed the way of risk management adopted by financial institutions and encouraged more prudent forms of risk taking and created a stronger banking system with greater ability to absorb the shock of the economy and yet make a contribution to economic growth (Vousinas, 2015).

## 2.7. Previous studies in Egypt

Abdelraouf et al., (2024) pointed out that they examined the effect of cyber risk on the profits of several banks in Egypt. In particular, it aimed at identifying how cyberrisks influence financial performance indicators, including return on assets (ROA) and gross profit margin (GPM) for the bank. The findings showed that the level of cyber risk significantly affected the measured banks' profitability negatively. The empirical results suggested that when the level of cyber risk increases, it also decreases the ROA and GPM, meaning that the indicated threats pose significant financial risks to the banks. The study pointed out that much attention should be paid to the enforcement of effective risk management measures to fight against cyber threats and threats to reliability and financial performance.

As a result, to strengthen the hypothesis, there is a reference to concerns about theories to elucidate the connection between credit risk, cyber risk, and bank profitability. Among the more recent BCG frameworks, the resource-based view (RBV) is rooted in the organisation's internal resources and competence. The concept presumes that organisations must maintain high levels of business performance with valuable, rare, inedible, and the organisation's resources (Ferreira and Ferreira, 2024). On the other hand, agency theory focusses on the problems that appear due to the fact that possession and control of organisations are not united. While doing this, it examines various aspects such as conflicts of interest between principals (shareholders) and the studying agents (managers), as well as issues of asymmetrical information (Moloi et al., 2020). Therefore, the following hypothesis was made:

- *H1: Credit risk has a significant effect on Banks profitability*
- *H2: Cyber risk moderates the relationship between credit risk and Banks profitability*

## 2.8. Conceptual Model

Concerning the results of the experiment with regard to the dependent variable defined as bank profitability, it is noteworthy that the changes and manipulation of the independent variables may have an impact. The major focus of the research and the deriving basis of its results is the behaviour of this dependent variable.Therefore, in this research, credit risk remains the principal research focus, portraying it as the primary independent variable while the moderator variable is credit risk. It is in the model, together with a host of other factors, that will be used to invoke the model for an analysis of the given phenomenon. It was necessary to have more than one way to assess each variable based on people's perceptions. The effectiveness of each of these measures was computed by applying the pertinent statistical analyses.

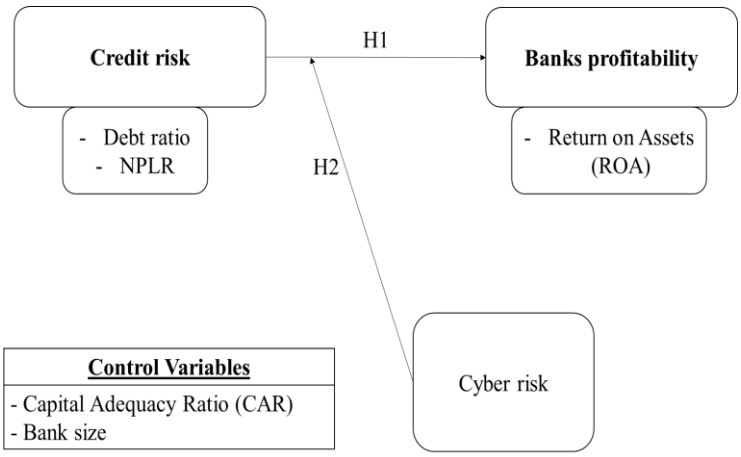


**Figure 1**. Conceptual Model
Source: Developed by the authors

In this study, credit risk is the primary independent variable, while the CAR ratio and bank size are kept as the control variables.Thus, by investigating the topic with the example of Egypt, It is important to note that the research design, as developed by this study, comprehensively seeks to empirically examine these theoretical associations in the Egyptian setting. Second, due to the usage of endogenous satisfactions and panel data, multiple forms are included, allowing you to consider the relationships implied by the I theory controlling certain variables for the influence of countries.
To estimate the impact of these variables, the analysis will use pooled and fixed effects models. The selection of these models and variables is based on the principles of cyber risk, credit risk, and bank profitability concepts.

# 3. Methodology

The research utilizes secondary data sources, primarily focusing on historical information extracted from annual reports spanning a six-year period from 2017 to 2022. To enhance the reliability of the results, additional data was sourced from the official websites of various financial institutions. The study's data collection method centers on secondary data, with a particular emphasis on historical records. These records are derived from the annual reports of 16 Egyptian banks, encompassing a diverse range of national and private institutions. The selected banks include:

| | |
|---|---|
| 1- Commercial International Bank (CIB) | 2- HSBC Bank Egypt |
| 3- Egyptian Gulf Bank | 4- Abu Dhabi Islamic Bank (ADIB) |
| 5- Arab International Bank (AIB) | 6- Qatar National Bank (QNB) |
| 7- Attijariwafa Bank Egypt | 8- National Bank of Kuwait - Egypt (NBK) |
| 9- Ahli United Bank Egypt (AUB) | 10- Arab African International Bank (AAIB) |
| 11- Bank of Alexandria (Alex Bank) | 12- Al Baraka Bank Egypt |
| 13- Suez Canal Bank | 14- Banque Misr |
| 15- Banque du Caire | 16- National Bank of Egypt (NBE) |

This diverse sample ensures a comprehensive representation of the Egyptian banking sector, incorporating both state-owned and private financial institutions.

## 3.1. Sampling technique

Sharma (2017) noted that the use of random sampling entails the probability that any person or thing being chosen in a sample is independent and equal to any other person or thing in the population. This procedure helps in eliminating bias and increases the possibility of transferring the overall results to the sample to the whole population. Cochran in 1963 specified the sample size for the research paper.

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

Therefore, the sample needs to exceed 68 respondents to obtain a margin of error of 0.1. The target population of this study consisted of Egyptian banks that had adapted financial technology (fintech). The sample selection was based on several criteria: banks that had released complete financial reports for the fiscal years 2017–2022, banks that had mentioned cyber risks in their financial reports, and banks that provided all the necessary data. Specifically, the data included ratios for credit risk (independent variable), cyber risk (control variable), capital adequacy ratio (CAR), and bank size (control variables), and return on assets (ROA) as the dependent variable.

Secondary data in the form of financial statements were analysed using STATA 17. The study aimed to understand the impact of credit and cyber risks on bank profitability, moderated by the control variables. The key metrics for each variable were carefully extracted from the financial reports to ensure a comprehensive analysis of the relationship between these factors. The study's rigorous data selection and analysis process ensured that the findings were robust and reflective of the current state of fintech adaptation and its implications on the profitability of Egyptian banks.

**Independent variable:**

i) Debt to asset

$$\frac{Total\ Debt}{Total\ Assets} \quad (2)$$

ii) NPL

$$\frac{Non\ Performing\ Loan}{Total\ Loan} \quad (3)$$

**Moderator variable:**

iii) Cyber risk ratio

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

$$0.4[\frac{Total\ Words}{Total\ Sentences} + 100(\frac{Complex\ Words}{Total\ Words})] \quad (4)$$

According to equation 3, 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 (See. Table 1). 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 by using www.gunning-fog-index.com website. The study applied this concept to analyze the prevalence and complexity of cyber risk disclosures in annual bank reports as we searched for key terms related to cyber threats in Table 1.

**Dependent variable:**

*i)* ROA

$$\frac{Net\ Income}{Total\ Assets} \quad (5)$$

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

*ii)* CAR

$$\frac{Tier\ 1\ Capital + Tier\ 2\ Capital}{Risk-Weighted\ Assets} \quad (6)$$

- 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.

***iii)* Bank size**

- Log to total assets

**Table 1**. Measurement of variables

| Variables | Measurement | Sources |
|---|---|---|
| Independent variable<br>Credit risk ratio<br>Debt ratio<br>NPL | Checklist from annual reports for each bank | Akhter, S., & Roy, J. (2017) |

| | | |
|---|---|---|
| Moderator variable<br>Cyber risk ratio | Checklist from annual report based on the following Keywords<br><br>"Cyber-attack, cyber security, cybercrime, cyber risk, hacking, swift attack, internet hacking or crimes)2 | Thach et al., (2021); Alber and Nabil (2016) |
| Dependent variables<br>Banks Profitability<br>ROA | Checklist from annual reports for each bank | Rahmani (2020); Shakoor et al., (2014) |
| Control variables<br>CAR<br>Bank size | Checklist from annual reports for each bank | Fauziah and Fadhilah (2022) |

Source: Own elaboration

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

$$ROA = \beta 0 + \beta 1\ Debt\ to\ asset + \beta 2\ NPL + \beta 3\ Cyber\ risk\ ratio + \beta 4\ CAR + \beta 5\ Bank\ size + \varepsilon i \quad (7)$$

The models which were incorporated in the study were as presented in (2, 3 & 4) In order to estimate the parameters of the model, it was adjusted to fit to the data obtained from the survey. They describe the hierarchal relationship between Credit risk, CAR and the size of the bank, and how this affects profit of the bank. In particular, concerning the moderator variable, it is Cyber risk. The fact that Credit risk that may affect the ROA since it's on the direct line exists, "Extreme values in continuous variables such as the debt/asset ratio were assessed and treated using log transformation to reduce their impact on the regression outcomes." The CoIntegration results of Eqs kicks that although Cyber risk works as an intermediary affecting the relationship between credit risk and bank's profitability. In addition, in the context of Egypt, Return on Assets (ROA) was chosen as the sole proxy for bank profitability due to its widespread use by Egyptian financial institutions and regulatory bodies as a standard measure of operational efficiency and profitability relative to total assets, while other metrics like ROE or NIM are often less consistently reported or influenced by capital structure variations across banks. Since it is understood that panel data has limitations, the correct approach to the issues related to panel data is the use of panel data analysis. In other words, the panel data can be described as a kind of cross-sectional data possessing two properties: the specific individual characteristic, and temporal characteristic. There is however the panel data where the observation of each of the individuals is done at different incidences or a specific point in time (Hsiao, 2022). It is with concern to these methods that the following techniques have been developed to deal with panel data some of which includes the Fixed effect model, Random effect model and Pooled effect model (Arellano and Honoré 2001). But the two most conventional types of models

[2] "Complex words" in cyber risk are defined as ≥3 syllables.

utilized in the present context of academic research studies are the fixed effect models and the random effect models. In this paper, models were compounded by Fixed effect and Random effects. Therefore, there is a plan to employ the Hausman test whereby both the models will be compared before the utilization of the preferred model (Zulfikar & STp, 2018).

# 4. Results

**Table 2.** Descriptive Statistics for the variables in phenomenon

| Variable | Mean | Std. dev. | Min | Max | SW Test | P-value |
|---|---|---|---|---|---|---|
| ROA | 0.015912 | 0.010456 | 0.001237 | 0.054207 | 4.34 | 0.0000 |
| Cyber risk Ratio | 0.35901 | 0.177204 | 0 | 1.2 | 5.702 | 0.0000 |
| Bank size | 9.467151 | 1.357548 | 7.601597 | 11.67833 | 5.023 | 0.0000 |
| CAR | 0.177715 | 0.039479 | 0.105 | 0.3107 | 2.624 | 0.0043 |
| Debt ratio | 186.9336 | 1722.295 | 0.000918 | 16860.36 | 9.497 | 0.0000 |
| Non-Performing Loans Rate | 0.429282 | 0.385953 | 0.00497 | 1.23 | 5.05 | 0.0000 |

Source: STATA V.17 OUTPUT

**Table 3**. Pearson correlation coefficients for the variables in phenomenon

| | logROA | logCRR | logBS | logCAR | logDR | logNPLR |
|---|---|---|---|---|---|---|
| logROA | 1 | | | | | |
| logCRR | 0.2026 | 1 | | | | |
| | 0.0477 | | | | | |
| logBS | -0.0589 | -0.3097 | 1 | | | |
| | 0.5689 | 0.0021 | | | | |
| logCAR | 0.0915 | -0.0334 | 0.1403 | 1 | | |
| | 0.3751 | 0.7468 | 0.1729 | | | |
| logDR | -0.139 | 0.0514 | 0.1011 | -0.0809 | 1 | |
| | 0.1768 | 0.619 | 0.3269 | 0.4335 | | |
| logNPLR | -0.0421 | 0.0302 | 0.1041 | -0.0237 | -0.1175 | 1 |
| | 0.6836 | 0.7705 | 0.3126 | 0.8184 | 0.2541 | |

Source: STATA V.17 OUTPUT

Table 2 reveals that the sample's average return on assets was 1.6%. The ROA ranged from 0.1% to 5.4%. Apart from bank size, all other variables had high variation in the sample's values. This shows that banks have different natures in terms of cyber risk, debt, and non-performing loans. The p-value of less than 0.05 indicated a non-normal distribution for all variables. Thus, the log

transformation should be considered for further analysis. The Pearson correlation coefficient is a measure of the strength and direction of the linear relationship between the variables. The results of the Pearson correlation coefficient are crucial as they indicate the presence of a relationship between independent and dependent variables. At a 95% confidence level, the log ROA had a positive, weakly significant relationship with the log of the cyber risk ratio. We should further investigate this relationship with the inclusion of other control variables in the modelling process. Furthermore, there appears to be no multicollinearity, as the independent variables had no Pearson correlation coefficient greater than 0.7.

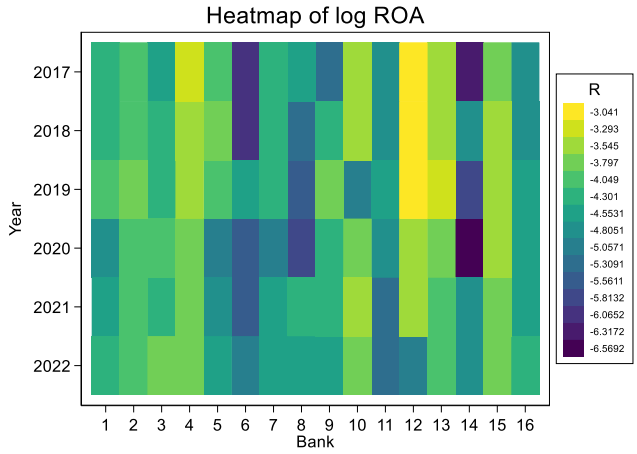


**Figure 2**. Heatmap of Log Return on Assets (ROA) Across 16 Egyptian Banks (2017–2022)
Source: STATA V.17 OUTPUT

As suggested by Figure 2, other banks including Attijariwafa and the National Bank of Egypt can be said to have registered low returns on assets as compared to other banks in Egypt. Conversely, the ROA of HSBC was better but less shifting over time.

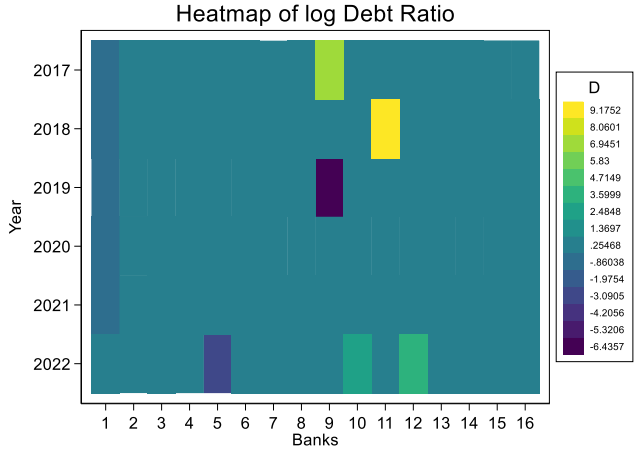


**Figure 3**. Heatmap of Log Debt Ratio Across 16 Egyptian Banks (2017–2022)
Source: STATA V.17 OUTPUT

As in figure 3, it shows the majority had almost close moderate values of log debt ratio. It is noticeable. Egyptian gulf bank had the highest log debt ratio in year 2018.

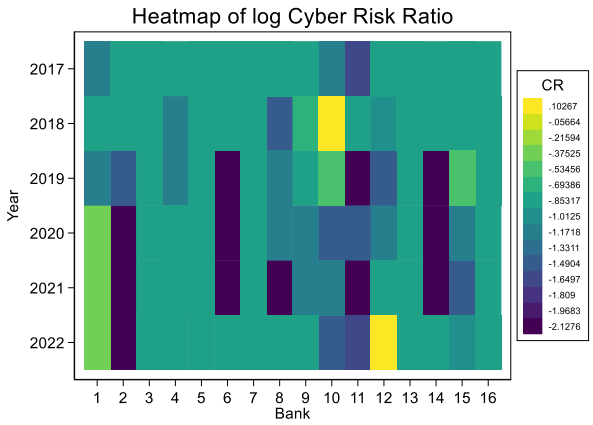


**Figure 4.** Heatmap of Log Cyber Risk Ratio Across 16 Egyptian Banks (2017–2022)

Source: STATA V.17 OUTPUT

In the figure, the heat map shows no much variation in cyber risk between banks, especially since 2020 until 2022. It seems HSBC and CIB witnessed the highest cyber risk ratios in 2022 and 2018, respectively. Some banks, like Suez Bank, NBK, El Baraka, and Arab African Bank in Egypt, had all witnessed no changes in the cyber risk ratio over the years.

**Table 4**. Stationarity test of the variables in phenomenon

| | **Test statistic** | **P-value** | **Decision** |
|---|---|---|---|
| Log ROA | -29.1556 | 0.0000 | Stationary |
| Log Cyber Risk Ratio | -48.6578 | 0.0000 | Stationary |
| Log Bank Size | -3.2826 | 0.0005 | Stationary |
| Log CAR | -160.0000 | 0.0000 | Stationary |
| Log Debt Ratio | -990.0000 | 0.0000 | Stationary |
| Log non-performing loans | -23.0015 | 0.0000 | Stationary |

Source: STATA V.17 OUTPUT

Before further analysis, some assumptions should be considered. To test stationarity of the variables, the Levin Lin Chu test statistic was calculated. It was found that all variables were stationarity since p-value was less than 0.05 thus rejecting the non-stationarity assumption of the variables. Table 5 provides various diagnostic test results and multicollinearity measures for a regression model, specifically the variance inflation factor (VIF) values for all variables. It was found to be below 5, indicating low multicollinearity, with the highest VIF being 1.17 for log bank size and the lowest being 1.03 for log CAR. The Breusch-Pagan test for heteroscedasticity shows significant results for log bank size with a value of 56.310 (p-value = 0.0419), suggesting the presence of heteroscedasticity.

**Table 5**. Model testing to determine the appropriate model

| Variables | VIF | 1/VIF | Breusch Pagan Test | Hausman Test | Wooldridge Test |
|---|---|---|---|---|---|
| Log Bank size | 1.17 | 0.853138 | | | |
| Log Cyber risk ratio | 1.12 | 0.891201 | 56.310 | 69.710 | 6.320 |
| Log Debt ratio | 1.05 | 0.953557 | (0.0419) | (0.0000) | (0.0000) |
| Log NPLR | 1.04 | 0.963831 | | | |
| Log CAR | 1.03 | 0.968028 | | | |

Source: STATA V.17 OUTPUT

The Hausman test, used to assess the consistency of the estimators, shows significant results for log bank size with a value of 69.710 (p-value = 0.0000), indicating that the fixed effects model should be more appropriate. Finally, the Wooldridge test for autocorrelation shows a significant result with a value of 6.320 (p-value = 0.0000), indicating the presence of autocorrelation in the model residuals. These diagnostics show that a feasible generalised least squares regression model with heteroscedasticity and autocorrelation taken into account will be the optimal modelling technique.

**Table 6**. Feasible generalized least square coefficient model in phenomenon

| Log ROA | Coefficient | Std. | z | P>z |
|---|---|---|---|---|
| Log CYBER | 0.226647 | 0.051895 | 4.37 | 0 |
| Log Bank size | 0.330606 | 0.254794 | 1.3 | 0.194 |
| Log CAR | 0.155792 | 0.052404 | 2.97 | 0.003 |
| Log Debt ratio | -0.08319 | 0.015496 | -5.37 | 0 |
| Log NPLR | 0.030169 | 0.006361 | 4.74 | 0 |
| _cons | -4.52008 | 0.599714 | -7.54 | 0 |
| | | | | |
| Coefficients | generalized least squares | | | |
| Panels | Heteroskedastic | | | |
| Correlation | panel-specific AR(1) | | | |
| Number of observations | 96 | | | |
| Number of groups | 16 | | | |
| Time periods | 6 | | | |
| Wald chi2(5) | 121.05 | | | |
| Prob > chi2 | 0 | | | |

Source: STATA V.17 OUTPUT

The model was found to be significant since the p-value is 0.000. The coefficients were calculated taking into consideration the heteroscedasticity and the autocorrelation issues in each panel. The coefficient for log cyber is 0.226647 with a standard error of 0.052, resulting in a highly significant p-value of 0.000. This suggests that a 1% increase in the cyber risk ratio is associated with an approximately 0.23% increase in ROA, holding other factors constant. Similarly, log CAR has a coefficient of 0.155792, a standard error of 0.052, and a p-value of 0.003, indicating that a 1% increase in the capital adequacy ratio is associated with an approximately 0.16% increase in ROA. Both effects are statistically significant at the 0.05 level.

Log DEBT RATIO and log NPLR show significant impacts on ROA. The coefficient for log DEBT RATIO is -0.08319 with a standard error of 0.015 and a p-value of 0.000, indicating that a 1% increase in the debt ratio is associated with an approximately 0.08% decrease in ROA. The coefficient for log NPLR is 0.030169 with a standard error of 0.006 and a p-value of 0.000, indicating that a 1% increase in the non-performing loan ratio is associated with an approximately 0.03% increase in ROA. Both variables are statistically significant at the 0.05 level. On the other hand, there was not enough evidence that bank size has a significant impact on ROA at the 0.05 level of significance.

**Table 7.** Feasible generalized least square coefficient model in phenomenon when moderator is added

| Log ROA | Coefficient | Std. | z | P>z |
|---|---|---|---|---|
| Log CYBER | 0.2288544 | 0.0695016 | 3.29 | 0.001 |
| Log Bank size | 0.4673696 | 0.2315971 | 2.02 | 0.044 |
| Log CAR | 0.0763851 | 0.0798219 | 0.96 | 0.339 |
| Log Debt ratio | -0.2791483 | 0.0737946 | -3.78 | 0 |
| Log NPLR | 0.0362701 | 0.0099009 | 3.66 | 0 |
| Log CYBER *Log Debt Ratio | -0.2355323 | 0.0820254 | -2.87 | 0.004 |
| _cons | -4.970786 | 0.583794 | -8.51 | 0 |
| | | | | |
| Coefficients | heteroskedastic | | | |
| Panels | panel-specific AR(1) | | | |
| Correlation | 96 | | | |
| Number of observations | 16 | | | |
| Number of groups | 6 | | | |
| Time periods | 66.48 | | | |
| Wald chi2(5) | 0 | | | |
| Prob > chi2 | 0.2288544 | | | |

Source: STATA V.17 OUTPUT

Observing the previous results, it shows that the cyber risk ratio can be considered a moderator in the relationship between the debt ratio and the ROA. Thus, it was inserted as an

interaction term between the debt ratio and the cyber risk ratio. If the term was found to be significant, then the cyber risk ratio significantly moderates the relationship between debt ratio and ROA.

Table 7. shows that the model was found to be significant since the p-value is 0.000. The coefficients were calculated taking into consideration the heteroscedasticity and the autocorrelation issues in each panel. The results remained almost the same after adding the moderator; however, it was noticeable that the log debt ratio had a lower coefficient after the moderator.

This aligns with the interaction term being significant. Thus, the cyber risk ratio significantly moderates the relationship between debt ratio and ROA at a 99% confidence level. Regarding control variables, bank size is found to have a significant positive impact on ROA, as a 1% increase in bank size would result in an estimated increase in ROA of 0.47%. The CAR, on the other hand, became insignificantly influential on the ROA since the p-value was greater than 0.05 (See. Figure 5.).

Although the statistical analysis proves that cyber risk plays a huge moderate role in the connection between debt ratio and bank profitability, the economic consequences are also extremely important. The revealing that cyber risk decreases the adverse effects of debt measure on ROA indicates that put in the scheme of things, the investments in cybersecurity can be considered as a texture of financial risk absorption, which makes the banks rather resistant to ill effects of high leverage. In the context of the banks working in the environment of the developing Egyptian economy, it implies that active digital risk management may have a direct impact on profits and investor trust. Furthermore, bigger banks that have better cybersecurity systems might have competitive advantages in terms of stable returns and deposit mobilisation as well as sustaining creditworthiness under economic duress. The above-provided insights can be used practically by financial institutions that want to maximize the degree of capital distribution between credit risk management and IT security system.

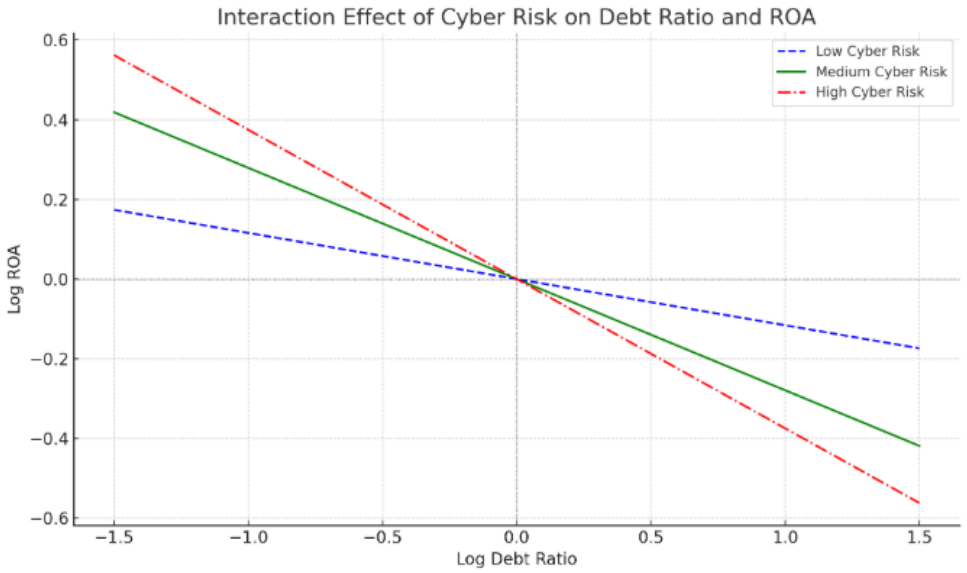


**Figure 5.** Graph visualizing how cyber risk moderates the relationship between debt ratio and ROA, based on the coefficients in Table 7. Source: STATA V.17 OUTPUT

The figure above illustrates that as cyber risk increases (from low to high), the negative impact of debt ratio on ROA becomes less severe. Specifically, the slope of the line flattens with higher levels of cyber risk, indicating a moderating (buffering) effect. This visual evidence supports the significant interaction term in Table 7 ($\beta = -0.235$, $p < 0.01$), confirming that cyber risk mitigates the adverse influence of debt ratio on profitability in Egyptian banks.

# 5. Discussion of Results

The findings of this study provide valuable insights into the complex relationships between credit risk, cyber risk, and bank profitability in the Egyptian banking sector, both supporting and extending previous research in this field. The study results indicate a significant relationship between cyber risk and bank profitability. Thus, the first hypothesis is accepted, as it also matches the findings of Abdelraouf et al., (2024) in their study of Egyptian banks. However, the positive coefficient for cyber risk in our model could be indicative of a more complex relationship, where banks with higher cyber risk exposure may be those that are more technologically advanced and thus potentially more profitable. This aligns with the observations of Najaf and Mostafiz (2021), who noted that banks partnering with fintech companies faced higher cybersecurity risks but potentially higher returns.

The significant negative relationship between debt ratio and ROA in our study supports the findings of Ekinci and Poyraz (2019) in their study of Turkish banks. They found that credit risk, as measured by the non-performing loans (NPL) ratio, negatively affected both ROA and ROE. Our results extend this understanding by demonstrating that cyber risk moderates this relationship, suggesting that the impact of credit risk on profitability is not uniform but varies with the level of cyber risk exposure. This unexpected result might be explained by the specific context of the Egyptian banking sector during the study period, possibly reflecting aggressive lending practices that resulted in higher short-term profits despite increased credit risk. This finding underscores the need for further investigation into the unique characteristics of the Egyptian banking environment.

The significant moderating effect of cyber risk on the relationship between debt ratio and ROA aligns with the theoretical framework proposed by Ossola et al., (2017) and Vučinić and Luburić (2022). They suggested that cyber risk could impact credit risk by affecting a company's financial position and creditworthiness. Our empirical results provide concrete evidence for this interaction in the context of bank profitability. So, the second hypothesis is also accepted. The varying impact of bank size on ROA in our models (initially insignificant, then significant when the moderator was added) echoes the findings of Lawrence et al., (2024) in South African banks. They noted that credit risk indicators had a comparatively bigger impact on smaller banks. Our results suggest that the relationship between bank size and profitability is complex and may be influenced by other factors, such as cyber risk exposure.

In conclusion, this research study's findings both support and extend previous research, highlighting the complex interplay between credit risk, cyber risk, and bank profitability in the Egyptian context. The moderating role of cyber risk in particular offers new insights into how technological factors are reshaping traditional banking risk-profit relationships. These results underscore the need for a nuanced approach to risk management in banks, considering both traditional credit risk factors and emerging cyber risks.

## 5.1. Recommendations

Banks should adopt a holistic risk management strategy that considers both credit and cyber risks simultaneously. Given the moderating effect of cyber risk on the relationship between debt ratio and profitability, financial institutions should develop integrated frameworks that assess these risks in tandem rather than in isolation. The positive relationship between cyber risk and ROA suggests that banks with higher cyber risk exposure may be more technologically advanced. However, this also implies greater vulnerability. Therefore, banks should invest significantly in robust cybersecurity measures to protect their digital assets and maintain customer trust.

Regulatory bodies should consider updating their guidelines to reflect the interplay between cyber and credit risks. This could include mandating regular cyber risk assessments as part of credit risk evaluations and incorporating cyber resilience into capital adequacy requirements. Additionally, banks should develop and implement performance metrics that account for both credit and cyber risks. This would provide a more accurate picture of a bank's true profitability when adjusted for its risk exposure.

Given the significance of cyber risk, banks should prioritise regular training programs for all staff levels to enhance cybersecurity awareness and skills. This should include both technical training for IT staff and general awareness programs for all employees. The varying impact of bank size on profitability suggests that one-size-fits-all approaches may not be effective. Smaller banks may need to develop specific strategies to manage cyber and credit risks, given their potentially higher vulnerability. The banking sector should implement systems for continuous monitoring of both cyber and credit risks, allowing for rapid adaptation to changing risk landscapes. This could involve the use of advanced analytics and AI-driven risk assessment tools.

Finally, since Egypt belongs to the category of an emerging market economy and the structural issues with the economy are inflation, currency fluctuations, banking sector liberalization, etc., it could be interesting to continue this study to Latin American states that also have similar economic situation, including Brazil, Argentina, Mexico, or Colombia. Such markets possess common characteristics such as growth in financial digitalization, regulatory change, and risk to sovereign exposure and thus they form a good basis of comparative analysis. It may be possible to find universal or regional patterns in the interaction of cyber risk and credit risk, which influence profitability, in a cross-regional study. It would not only enhance the robustness of generalizability but also facilitate the harmonization of policies in different developing financial systems amidst similar risk environments.

## 5.2. Limitations

The study was limited to 16 banks in Egypt over a six-year period. A larger sample size, including more banks or a longer time frame, could provide more robust and generalisable results. The focus on Egyptian banks limits the generalisability of the findings to other countries or regions, which may have different regulatory environments, technological landscapes, or economic conditions. The study relied on available data for measuring cyber risk. However, given the complex and evolving nature of cyber threats, the metrics used may not capture all aspects of cyber risk faced by banks. Additionally,

the study may not fully capture the time-lag effects between risk exposure and profitability impacts. Some cyber or credit risks might have delayed effects on bank performance that extend beyond the study's time frame.

While the study controlled for several variables, it may not account for all external factors that could influence bank profitability, such as macroeconomic conditions, political stability, or global financial trends. The study relied on publicly available data, which may have limitations in terms of completeness or accuracy, particularly regarding sensitive information like cyber-risk incidents.

While the chosen statistical models were appropriate for the data, alternative model specifications might yield additional insights or reveal different relationships among the variables. Furthermore, the quantitative nature of the study may not capture qualitative factors that influence risk management and profitability, such as corporate culture, management quality, or strategic decisions. These limitations suggest avenues for future research, including expanding the geographical scope, refining cyber risk measurements, and incorporating qualitative research methods to complement the quantitative findings.

In conclusion, the research contributes immensely in the study on credible risk and its management because it shows that credit risk does not affect the profitability of banks in isolation. The research is helpful because it recognizes cyber risk as an explaining factor and base on these explanations, it offers new knowledge on how credit risk can be dealt with strategically by the financial institutions in a digital banking environment. Based on the results, it is possible to find that banks that are exposed to increased cyber risk levels, which are usually related to more progressive digital services and protection systems, can better absorb the adverse impact of credit risk on profitability. This emphasizes why cyber risk management should be part of the wider risk governance structures and procedures and provide insights into the practical advice that may help bank managers, regulators, and policymakers improve financial stability and operational resilience in the emerging markets and Egypt in particular.

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

[1] 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

[2] 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

[3] Åhman, M. (2024). Markov Model for Credit Risk Spreads. https://urn.fi/URN:NBN:fi-fe2024051732333

[4] Akhter, S., & Roy, J. (2017). Analysis of credit risk, efficiency, liquidity, and profitability of selected non-bank financial institution: An empirical study. Journal of Business, 2(02), 16-23. https://ssrn.com/abstract=2951678

[5] 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

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

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

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

[9] 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. http://dx.doi.org/10.18576/amis/180117

[10] Alshehadeh, A. R., Elrefae, G., & Injadat, E. (2022). Influence of traditional performance indicators on economic added value: evidence from insurance companies.

[11] 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

[12] Aywak, B. O. (2022). Structural Credit Risk Modelling and Valuation Based on the Merton Model (Doctoral dissertation, University of Nairobi). http://erepository.uonbi.ac.ke/handle/11295/163299

[13] Baptista, D., & Karmakar, S. (2017). Understanding the Basel III Leverage Ratio Requirement. Economic Bulletin and Financial Stability Report Articles and Banco de Portugal Economic Studies.

[14] 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

[15] Birindelli, G., Ferretti, P., Ferri, G., & Savioli, M. (2022). Regulatory reform and banking diversity: reassessing Basel 3. Annals of Finance, 18(4), 429-456. https://doi.org/10.1007/s10436-021-00406-3

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

[17] 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

[18] 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://dx.doi.org/10.2139/ssrn.3478640

[19] Butt, M. A., Ayub, H., Latif, B., Asif, F., Shabbir, M. S., & Raja, A. A. (2022). Financial risks and performance of conventional and Islamic banks: do reputational risk matters?. Journal of Islamic Accounting and Business Research, 13(4), 581-595. https://doi.org/10.1108/JIABR-10-2020-0336

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

[21] 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

[22] 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

[23] Ekinci, R., & Poyraz, G. (2019). The effect of credit risk on financial performance of deposit banks in Turkey. Procedia computer science, 158, 979-987. https://doi.org/10.1016/j.procs.2019.09.139

[24] 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.

[25] 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. http://dx.doi.org/10.5038/2640-6489.8.2.1246

[26] 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

[27] 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

[28] Flamini, V., McDonald, C. A., & Schumacher, L. B. (2009). The determinants of commercial bank profitability in Sub-Saharan Africa. https://ssrn.com/abstract=1356442

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

[30] 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.

[31] 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.

[32] Kanyambu, F. M. (2021). A System Dynamics Model For Credit Risk Modelling And Simulation: The Case Of Licensed Credit Reference Bureaus In Kenya (Doctoral dissertation, KCA University). http://repository.kca.ac.ke/handle/123456789/826

[33] 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.

[34] Lawrence, B., Doorasamy, M., & Sarpong, P. (2024). The Impact of Credit Risk on Performance: A Case of South African Commercial Banks. Global Business Review, 25(2_suppl), S151-S164. https://doi.org/10.1177/0972150920969927

[35] 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

[36] 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

[37] 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

[38] 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

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

[40] Naili, M., & Lahrichi, Y. (2022). The determinants of banks' credit risk: Review of the literature and future research agenda. International Journal of Finance & Economics, 27(1), 334-360. https://doi.org/10.1002/ijfe.2156

[41] 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

[42] Ossola, G., Giovando, G., & Crovini, C. (2017). Cyber risk management in credit cooperative banks: A case study. In Global and national business theories and practice: bridging the past with the future (pp. 1239-1250). EuroMed Press. https://hdl.handle.net/2318/1648064

[43] 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

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

[45] 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

[46] 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.

[47] 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

[48] 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

[49] 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

[50] 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

[51] 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

[52] Van Greuning, H., & Bratanovic, S. B. (2020). Analyzing banking risk: a framework for assessing corporate governance and risk management. World Bank Publications. https://doi.org/10.1596/978-1-4648-1446-4

[53] Vousinas, G. L. (2015). Supervision of financial institutions: The transition from Basel I to Basel III. A critical appraisal of the newly established regulatory framework. Journal of Financial Regulation and Compliance, 23(4), 383-402. https://doi.org/10.1108/JFRC-02-2015-0011

[54] Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. Journal of Central Banking Theory and Practice, 11(2), 27-53. https://doi.org/10.2478/jcbtp-2022-0012

[55] 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