Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Examining the Impact of Cybersecurity Disclosure on Bank Profitability: The Moderating Role of FinTech in the Egyptian Banking Sector

Mohamed Abdelraouf

mohamedabdelraouf04@gmail.com

University of Hertfordshire

Mona Khalil

High Institute For Computers and Management Information Systems

Research Article

Keywords: Cybersecurity Disclosure, FinTech, Bank Profitability, Panel Data, Egypt, Resource-Based View

Posted Date: September 21st, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10785453/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Examining the Impact of Cybersecurity Disclosure on Bank Profitability: The Moderating Role of FinTech in the Egyptian Banking Sector

Abstract

This study examines the impact of cybersecurity disclosure on bank profitability and investigates the moderating role of financial technology (FinTech) in this relationship within the Egyptian banking sector. Using a longitudinal panel of 16 Egyptian commercial banks over the period 2016-2025 (160 bank-year observations), the study applies fixed- and random-effects panel regression to test three hypotheses linking cybersecurity disclosure, FinTech adoption, and bank profitability, the last measured through return on assets (ROA), return on equity (ROE), and net profit margin (NPM). The Hausman specification test supports the Fixed Effects estimator as the preferred model across all three profitability measures. The results show that cybersecurity disclosure alone does not have a statistically significant direct effect on bank profitability, whereas FinTech has a significant positive effect across all three models. Most notably, the interaction between cybersecurity disclosure and FinTech is positive and statistically significant in every model, indicating that FinTech substantially strengthens the relationship between cybersecurity disclosure and profitability. Interpreted through the Resource-Based View and Dynamic Capabilities Theory, these findings suggest that cybersecurity functions as a strategic capability whose financial value is realised only when complemented by adequate technological infrastructure. The study contributes to the literature by integrating cybersecurity, FinTech, and profitability within a single empirical framework in an emerging-market banking context, and offers practical and policy implications for Egyptian banks and regulators seeking to strengthen digital resilience and financial performance.

Keywords: Cybersecurity Disclosure; FinTech; Bank Profitability; Panel Data; Egypt; Resource-Based View

1. Introduction

The banking sector has undergone a profound digital transformation over the past decade, with electronic payments, mobile banking, and increasingly data-intensive service models replacing traditional branch-based operations. This shift has brought considerable gains in efficiency and customer reach, but it has also exposed banks to an expanding range of cyber threats, from data breaches and payment fraud to systemic operational disruption. Because banks are custodians

of highly sensitive financial data and are deeply interconnected within national and global payment systems, the financial and reputational consequences of inadequate cybersecurity can be severe and can extend well beyond the institution directly affected.

In response, banks worldwide have increased their disclosure of cybersecurity practices and investments, both to satisfy regulatory expectations and to signal resilience to customers, investors, and counterparties. This raises an important empirical question: does greater cybersecurity disclosure translate into improved financial performance, or does it represent a cost centre whose benefits are primarily defensive rather than value-generating? The literature offers no consensus. Some studies report a positive relationship between cybersecurity practices and profitability, others find no significant relationship, and still others suggest the relationship is indirect, operating through complementary organisational or technological capabilities.

Financial technology (FinTech) is one such capability, and it has itself become central to the competitiveness of modern banks. FinTech adoption, spanning digital payment infrastructure, automated services, and data-driven customer engagement, has been shown in prior research to affect bank profitability, although the direction and consistency of this effect vary across contexts. What has received comparatively little attention is whether FinTech and cybersecurity interact, that is, whether the financial return on cybersecurity disclosure depends on the extent to which a bank has also invested in the technological infrastructure needed to convert that disclosure into a genuine trust and efficiency advantage.

This question is particularly relevant to the Egyptian banking sector. Egypt's banking system has experienced rapid digitalisation since the Central Bank of Egypt's 2019 financial inclusion strategy, alongside a corresponding rise in cyber-risk exposure. Yet empirical research on cybersecurity and bank profitability has concentrated overwhelmingly on advanced economies and, to a lesser extent, other MENA markets, leaving the Egyptian context comparatively under-examined despite its distinct regulatory environment and pace of digital adoption.

This research addresses this gap by examining, within a single integrated framework: (i) the direct relationship between cybersecurity disclosure and bank profitability; (ii) the direct relationship between FinTech and bank profitability; and (iii) whether FinTech moderates the relationship between cybersecurity disclosure and profitability. The analysis draws on a panel of 16 Egyptian commercial banks observed between 2016 and 2025 (160 bank-year observations), with profitability measured through ROA, ROE, and NPM, and estimated using fixed- and random-effects panel regression.

The study contributes to the literature in three ways. First, it extends the cybersecurity-profitability literature to an emerging banking market that has been underrepresented in prior empirical work. Second, it treats FinTech not merely as an independent determinant of profitability but as a moderating variable, offering a more nuanced account of how cybersecurity investment translates into financial performance. Third, by integrating cybersecurity, FinTech, and profitability within a single model, it responds directly to calls in the literature for research that moves beyond isolated, bilateral relationships between pairs of variables.

The remainder of the paper is organised as follows. Section 2 reviews the theoretical framework and relevant literature and develops the research hypotheses. Section 3 outlines the research gap. Section 4 describes the research methodology, data, and empirical models, and presents the results of the statistical analysis. Section 5 discusses these results in relation to the hypotheses and prior literature. Sections 6 to 8 present the theoretical implications, practical implications, and policy recommendations, respectively. Section 9 concludes with the study's limitations and directions for future research.

2. Theoretical Framework and Literature Review

2.1 Cybersecurity in the Banking Sector

The banking sector's recent, substantial shift toward digital transformation, marked by increased reliance on electronic systems and digital financial services, has left banks increasingly exposed to cyberattacks and electronic breaches. Ensuring the continuity of banking operations, protecting financial data, and increasing customer confidence all depend heavily on cybersecurity. The development of digital financial services and artificial intelligence technology has also increased the complexity of cyber risks, leading banks to increase their investment in risk management and cyber-protection systems. The effectiveness of cybersecurity strategies contributes to the operational and financial stability of banking institutions and reduces losses from cybercrime, according to numerous recent studies (Saha et al., 2025).

Cybersecurity involves principles and frameworks that protect digital systems, networks, and data from unauthorised access, damage, or theft. At its core, this field depends on a combination of technology, standardised policies, and human awareness to effectively prevent, detect, and respond to risks (Herrmann & Pridöhl, 2020).

In the same context, Chanda, Vafaei-Zadeh, Hanifah, and Nikbin (2024) examine cybersecurity awareness among bank employees in Bangladesh, using a multi-stage analytical approach, PLS-SEM, artificial neural networks, and fuzzy-set qualitative comparative analysis, on 355 responses collected from bank employees. The findings show that response cost, information security awareness, and employees' perceived threat and vulnerability to cyber risk are all significant drivers of cybersecurity awareness, reinforcing the role of human factors alongside technical safeguards.

Saha et al. (2025) investigate cybersecurity risk-assessment procedures in the banking industry, examining existing approaches, implementation challenges, and how well they address evolving threats. Drawing on survey data from 128 financial institutions across 17 countries together with in-depth case studies of six banks, the findings reveal significant differences in implementation maturity across institutions of different sizes, with larger banks consistently more mature across all assessment areas.

Oyewole et al. (2024) examine the various facets of cybersecurity in the banking sector in light of the growing use of online banking services and the corresponding rise in cybercrime, combining a literature review with an analysis of recent cybersecurity incidents to explore the nature of cyber threats, the financial consequences of breaches, and the strength of existing safeguards; the study concludes that the banking industry needs a thorough and flexible approach to cybersecurity, backed by strategic investment in technology, cooperation, and education.

Amer and Al-Omar (2023) examine the relationship between cybersecurity and cybercrime in the Jordanian banking sector, using a sample of 270 senior managers and staff from 14 Jordanian commercial banks listed on the Amman Stock Exchange. Using SPSS, the study evaluates how banks strengthen their network-security architecture to prevent unauthorised access and data breaches; the findings show that robust encryption of customers' financial data during transmission and storage is the most crucial strategy for reducing cybercrime threats and safeguarding customer data.

Most of these studies (Chanda et al., 2024; Oyewole et al., 2024) confirm that strengthening electronic-protection systems contributes to reducing cyber risk, protecting financial data, and improving the effectiveness of banking operations, and prior research broadly agrees that cybersecurity has emerged as an essential pillar of banking-sector stability given the growth of digital services and electronic transactions. Saha et al. (2024) similarly indicate that inadequate cyber infrastructure raises the probability of exposure to cyberattacks and to operational and financial losses.

The focus of these studies nonetheless varies: some concentrate on the technical elements of cybersecurity (Saha et al., 2025), while others examine organisational and administrative aspects of digital protection in banks (Amer & Al-Omar, 2023). Conclusions about the readiness of banks in emerging economies to adopt effective cybersecurity policies also differ from those concerning banks in advanced economies. Taken together, this literature suggests that cybersecurity is no longer simply a technical safeguard; it has become a strategic issue that shapes the stability and operational effectiveness of banking institutions.

A separate but related literature has examined the determinants of bank profitability more broadly. Bank profitability is one of the most important indicators of financial performance and banking stability, reflecting a bank's ability to generate returns and strengthen its competitiveness in financial markets. Prior studies have focused on a range of factors, including bank size, capital adequacy, liquidity, credit risk, and operational efficiency, as well as macroeconomic factors such as inflation, economic growth, and interest rates, and recent work confirms that technological advancement and digital transformation increasingly shape financial performance and bank profitability as well.

Return on equity (ROE), return on assets (ROA), and net interest margin (NIM) are common measures of bank profitability and can be expressed as functions of both internal and external variables, where internal determinants are characteristics specific to each bank and external variables reflect macroeconomic conditions.

Internal factors include bank size, diversification, various financial ratios (asset quality, liquidity, capital strength, leverage, and efficiency), a bank's risk appetite as reflected in risk-adjusted measures, and the level of competition it faces. Macroeconomic variables, by contrast, include the business cycle, inflation, interest rates, economic growth, industry concentration, and income diversity (See. Table 1.).

Table 1. Major Studies on Bank Profitability Determinants

Author	Period	Goals	Sample	Method	Variables	Key Results
Lamothe-López et al., 2024	2018-2021	Analyses the factors explaining bank profitability globally and by region.	2,091 commercial banks in 110 countries	Random-effects regression	Profitability; NPL; NPM; ROA; ROE	Listed status, impaired loans, efficiency, gross interest margin, and capitalisation explain much of bank profitability.
Mirović et al., 2024	2015-2020	Analyses the factors affecting bank profitability in the	18 Eurozone countries	Random- and fixed-effects	NPL; capital-to-interest	Cost-to-income ratio negatively

		Eurozone and offers recommendations for improving profitability.		models; GMM	ratio; NPM; ROE	affects profitability; net interest income, trading income, and fee income to operating income are positively related.

Source: Table created by authors.

The literature review as a whole indicates that bank profitability is shaped by a combination of internal and external factors, including liquidity, capital adequacy, operational efficiency, credit risk, and macroeconomic conditions, and that technological development and digital transformation have become important contemporary drivers of financial performance and bank profitability.

The literature nonetheless differs in identifying the single most influential determinant of profitability. Some studies focus on traditional financial factors, while others emphasise financial technology and digital innovation as key drivers of profitability in the modern banking environment. Studies also vary in their choice of profitability measure: some use return on assets while others rely on return on equity or net interest margin (Lamothe-López et al., 2024; Mirović et al., 2024). Taken together, these studies suggest that bank profitability is increasingly tied to banks' capacity to manage contemporary risks, such as cyber risk, and to adapt to technological change.

2.2 Cybersecurity Disclosure and Bank Profitability

The rising incidence of cyberattacks, and their direct effect on the financial performance of the banking sector, has made the relationship between cybersecurity and bank profitability an important subject of study. Inadequate cybersecurity measures can result in significant financial losses, declining customer trust, and higher operating and regulatory costs, all of which harm profitability. Conversely, investment in cybersecurity can enhance banks' long-term financial performance by strengthening financial stability, reducing operational risk, and improving the efficiency of banking operations. Recent studies suggest that cybersecurity has become a strategic element of banks' pursuit of financial sustainability (Bruno et al., 2025; Abdelraouf et al., 2024).

Cybersecurity comprises the technologies, procedures, and controls used to protect digital systems, networks, and data from internal and external threats (Herrmann & Pridöhl, 2020).

Growing dependence on technology across many facets of life has made cybersecurity more critical: it protects private data, prevents identity theft and account intrusion, limits financial losses, safeguards national security, and strengthens customer confidence (Oyewole et al., 2024; Saha et al., 2025).

Shehadeh et al. (2026) examine how cybersecurity disclosure affects the relationship between the proportion of women on bank boards and earnings per share in Jordanian banks between 2010 and 2022. The results reveal a positive interaction between board gender diversity and cybersecurity disclosure with respect to earnings per share, suggesting that strong cybersecurity practices moderate how board gender diversity relates to financial performance.

Al-Nimer et al. (2025) examine the non-linear impact of corporate governance on bank performance, exploring the moderating role of cybersecurity policy across a sample of commercial banks operating in the Middle East and North Africa (MENA) region between 2016 and 2024, using a least-squares approach; the results demonstrate a non-linear interaction effect of cybersecurity policy on the relationship between corporate governance and bank performance.

Abdelraouf (2025) hypothesises that cyber risk significantly reduces the profitability of Egyptian banks during 2017-2023, using a sample of 16 banks analysed in STATA with a pooled-effects model; the findings support a negative relationship between cyber risk and bank profitability, with both return on assets and gross profit margin negatively affected.

Relatedly, Opuni-Frimpong, Adefunso Dzorka, and Boadi (2025) examine the impact of the Bank of Ghana's mandate to establish a Cybersecurity and Information Security Governance Committee on bank financial performance and efficiency, measuring performance through ROE and ROA and efficiency through the operating cost-to-income ratio. Using data from 20 Ghanaian banks for 2019-2022 with generalised linear regression and robustness testing, the findings indicate that the Committee's experience positively affects ROA, but not ROE or the cost-to-income ratio.

Bruno, Pistolesi, and Teti (2025) examine the relationship between cybersecurity policy, environmental, social, and governance (ESG) performance, operational risk, and bank profitability, using 1,673 annual banking observations across multiple economic regions between 2009 and 2023 and discrete time-series regression. The results show that banks adopting cybersecurity policies experience improved financial resilience, with cybersecurity policy adoption having a statistically significant positive impact on both ROA and ROE.

Elsayed, Ismail, and Ahmed (2024) examine the impact of cybersecurity disclosure on bank performance and whether the presence of a Chief Risk Officer (CRO), an Information Technology Committee, or board size moderates this relationship, using manual text analysis to measure cybersecurity disclosure in a sample of MENA-listed banks between 2019 and 2021 and a random-effects regression model. The results show that MENA banks are increasingly disclosing cybersecurity information, that this disclosure has a significant positive impact on bank performance, and that the presence of a Chief Risk Officer moderates the relationship.

Al-Nimer et al. (2025) and Bruno, Pistolesi, and Teti (2025) both find that cybersecurity improves banks' profitability and financial performance by reducing financial losses, increasing consumer confidence, and improving operational stability, whereas Abdelraouf (2025) reports a more direct, negative effect of cyber risk on profitability, underscoring that the strength, and even the direction, of this relationship remain contested in the literature.

These mixed results suggest that further investigation is needed to explain more precisely how cybersecurity affects bank profitability. We therefore propose:

H1: Cybersecurity disclosure positively impacts Bank Profitability.

2.3 Financial Technology and Bank Profitability

Financial technology (FinTech) is one of the most significant innovations to have transformed the banking sector, contributing to the development of financial services, improving operational efficiency, and expanding banks' customer base. This transformation has prompted researchers to examine how FinTech affects banks' profitability and financial performance, particularly given intensifying competition between traditional and digital financial institutions; consequently, numerous studies have assessed how FinTech applications affect different indicators of bank profitability (Tarawneh et al., 2024).

Hijazin and Badwan (2026) examine the impact of FinTech development on the profitability of conventional and Islamic banks listed on the Palestine Exchange between 2015 and 2022, using panel data regression with a fixed-effects model for 13 banks and testing the results with two-stage least squares. The findings indicate a strong relationship between bank performance and FinTech development, suggesting that FinTech development is associated with a significant deterioration in bank profitability. The paper also suggests that the absence of accommodative monetary policy support mitigates the negative effects of FinTech on bank profitability.

Yuan, Puah, and Marikan (2025) select 50 commercial banks listed on Chinese stock exchanges between 2012 and 2023 and use a fixed-effects model together with Hansen's threshold

regression to examine how FinTech development, and its non-linear characteristics, affect bank profitability. The main findings are, first, that FinTech significantly weakens the overall profitability of commercial banks by reshaping the sector's competitive landscape and intensifying technology-driven substitution effects; and second, that large state-owned and joint-stock banks experience more pronounced negative effects than small and medium-sized banks.

Berisha and Rayfield (2025) investigate the relationship between the adoption of internal FinTech solutions and bank profitability in Kosovo, examining the impact of mobile banking, e-banking, electronic payment systems, and data analytics on profitability using net interest margin and ROA as key indicators, based on data from 10 commercial banks. The results show that FinTech adoption positively affects profitability and improves ROA, even though investment in operational-efficiency initiatives has a negative effect on ROA on its own.

Chand et al. (2025) examine the impact of FinTech on banking risk and profitability in Fiji's small-island economy between 2000 and 2024, using a fixed-effects model with robustness tests based on random effects, pooled OLS, and generalised method of moments. The results indicate that FinTech development reduces banking risk and enhances profitability, showing a significant positive effect on both performance and financial stability.

Nguyen (2025) examines the impact of FinTech on the operations of Vietnamese commercial banks, particularly their profitability and stability, using panel data from 14 publicly listed banks between 2013 and 2022 and a panel regression model estimated via generalised least squares. The study finds that bank equity is positively correlated with both stability and profitability.

Tarawneh et al. (2024) provide a systematic review of the contemporary literature on FinTech indicators that affect bank profitability, presenting a methodology for quantitatively assessing emerging FinTech indicators and their interaction with profitability determinants. Following PRISMA guidelines, the review evaluates 28 articles from the Web of Science and Scopus databases published between August 2019 and August 2023, identifying FinTech metrics at both bank and country level alongside bank-specific and country-specific profitability determinants.

Berisha and Rayfield (2025) and Chand et al. (2025) agree that financial technology plays a significant role in improving bank profitability by reducing operating costs, developing banking services, and increasing performance efficiency, although the studies differ in their assessment of the magnitude of this effect. Hijazin and Badwan (2026) find that the positive impact of financial technology is more pronounced in banks with advanced digital

infrastructure, while also noting that the high costs of technological investment may reduce profits in the short term. Taken together, these studies underscore financial technology's importance as a tool that helps banks strengthen their competitiveness and achieve financial sustainability. We therefore propose:

H2: Financial Technology positively impacts Bank Profitability.

2.4 The Moderating Role of Financial Technology

The literature reviewed above shows that interest in cybersecurity in the banking sector has grown significantly in recent years, driven by the expansion of digital banking services and the corresponding rise in cyber threats. This literature emphasises the importance of developing cybersecurity infrastructure to safeguard data, reduce operational risk, and ensure business continuity (Amer & Al-Omar, 2023).

Other studies have examined the determinants of bank profitability more broadly, including Lamothe-López et al. (2024) and Mirović et al. (2024), who show that a range of internal and external factors, including capital adequacy, liquidity, operational efficiency, and credit risk, all affect profitability.

According to Shehadeh et al. (2026) and Elsayed, Ismail, and Ahmed (2024), investment in cybersecurity contributes to reduced financial losses, increased customer confidence, and improved operational stability, all of which support financial performance. However, most of these studies focus on quantifying the direct effect of cybersecurity on performance rather than on exploring the mechanisms through which this effect converts into profitability.

The relationship between cybersecurity and FinTech is itself important: a secure digital infrastructure is a prerequisite for the sustainability of FinTech applications, and operational vulnerabilities represent one of the most significant obstacles to the wider adoption of digital financial services (Elsayed, Ismail & Ahmed, 2024). Studies of the relationship between FinTech and bank profitability consistently show that digital financial services improve operational efficiency, reduce costs, and enhance service quality, thereby improving profitability indicators (Berisha & Rayfield, 2025; Chand et al., 2025). Despite this research momentum, most previous studies address cybersecurity, FinTech, and the determinants of profitability in isolation from one another, without developing an integrated model that links all three variables within a single framework. We therefore propose:

H3: Financial Technology positively moderates the relationship between Cybersecurity and Bank Profitability.

3. Research Gap

Despite numerous studies addressing cybersecurity and bank profitability, and others exploring the role of FinTech in improving banking performance, there remains a shortage of research examining FinTech's moderating role in the relationship between cybersecurity and bank profitability within a single, comprehensive framework. Most previous studies have focused on bilateral relationships between pairs of variables, without analysing the mechanisms through which cybersecurity might contribute to profitability via FinTech.

Furthermore, despite the substantial expansion of digital transformation and electronic financial services within the Egyptian banking sector, most of the existing literature has centred on advanced economies, while applied research on the Egyptian and wider Arab banking sectors remains scarce. Given recent economic and technological developments, these relationships warrant re-examination in light of advances in financial technology and the rise in cyberattacks.

This research addresses this gap by developing a model that examines the impact of cybersecurity on bank profitability while highlighting the moderating role of FinTech in this relationship. The research focuses on the Egyptian banking sector, which is undergoing significant expansion in FinTech applications and digital banking services, making cybersecurity increasingly important for banking sustainability and financial performance.

This research is distinctive in integrating three main variables, cybersecurity, financial technology, and bank profitability, within a single framework, contributing to a more comprehensive understanding of their interaction. In doing so, the research aims to provide bank decision-makers with useful evidence to support cybersecurity investment and FinTech development decisions intended to enhance bank profitability and competitiveness.

4. Research Methodology and Design

This research examines the theoretical structure of the research variables and reviews the relevant literature to identify a research gap concerning the impact of financial technology on the relationship between cybersecurity and the profitability of Egyptian banks. By presenting the research variables and their measurement, testing the research hypotheses using appropriate statistical methods, and reporting the results of the statistical analysis, the research applies this framework empirically to a sample of Egyptian banks. The following subsections describe this process in detail.

4.1 Data and Sample

This research adopts a positivist epistemological approach, based on the assumption that the relationship between cybersecurity disclosure, FinTech, and bank profitability constitutes an objective, quantifiable reality that can be examined through empirical observation and statistical inference. A deductive methodology is employed, whereby theoretical propositions derived from the Resource-Based View, signalling theory, and agency theory are translated into testable hypotheses, which are then evaluated using bank-level financial data. This quantitative design is appropriate given the research's objective of establishing systematic relationships across a multi-year, multi-institution longitudinal dataset, and it aligns with the prevailing methodology in banking empirical research (Ozili & Ndah, 2024).

The research uses a longitudinal panel structure covering 16 Egyptian banks over the period 2016-2025, yielding 160 bank-year observations. Panel data offer several advantages over purely cross-sectional or time-series approaches: they capture variation across banks as well as within banks over time, they provide greater variability and degrees of freedom, and they allow dynamic effects to be tracked that might not be visible in a single-period snapshot (Hsiao, 2003). The ten-year period was chosen deliberately, as it spans both the pre-digital-transformation period in the Egyptian banking sector and the accelerated digitisation phase that followed the Central Bank of Egypt's 2019 financial inclusion strategy, allowing temporal changes in both cybersecurity disclosure and profitability to be tracked.

The target population comprises all licensed commercial banks operating in Egypt and registered with the Central Bank of Egypt during the research period. Because the data are secondary and archival in nature, the sample of 16 banks was constructed through purposive rather than random selection. A bank was included if it met all of the following conditions:

- Complete annual reports were publicly available for each of the ten fiscal years, 2016-2025;
- The bank's financial statements were prepared in accordance with Egyptian Accounting Standards or IFRS, ensuring comparability;
- The bank was classified as a commercial bank, excluding investment banks, mortgage finance companies, and microfinance institutions.

The resulting sample includes both state-owned and privately-owned banks, and both domestic and foreign-owned institutions, together covering most of the Egyptian banking sector by total assets. Table 2. lists the banks included in the research sample.

Table 2. Banks in the Research Sample

No.	Bank	No.	Bank
1	National Bank of Egypt — nbe.com.eg	9	Banque Misr — banquemisr.com
2	Banque du Caire — bdc.com.eg	10	HSBC Bank Egypt S.A.E. — hsbc.com.eg
3	Commercial International Bank (CIB) — cibeg.com	11	Attijariwafa Bank Egypt — attijariwafabank.com.eg
4	Egyptian Gulf Bank — eg-bank.com	12	National Bank of Kuwait – Egypt — nbk.com/ar/egypt.html
5	Arab African International Bank — aaib.com	13	Qatar National Bank Al Ahli (QNB) — qnb.com.eg
6	Al Baraka Bank Egypt — albaraka.com.eg	14	Suez Canal Bank — scbank.com.eg
7	Alex Bank — alexbank.com	15	Abu Dhabi Commercial Bank — ca-egypt.com
8	Arab International Banking Corporation (SAIB) — saib.com.eg	16	Abu Dhabi Islamic Bank — adib.eg

Source: Table created by authors.

All profitability and control-variable data were hand-collected from audited annual reports and cross-validated against disclosures on individual bank websites and the Central Bank of Egypt's database of banking statistics. No imputation was applied to missing values; three observations with incomplete financial disclosures were excluded, and these exclusions are noted in the descriptive statistics.

4.2 Research Variables

Based on the literature reviewed above, the research variables are grouped into four categories (See. Table 3.):

- Independent Variable: Cybersecurity Disclosure
- Dependent Variable: ROA, ROE, NPM
- Moderating Variable: Financial Technology (FinTech)
- Control Variables: CAR, Bank Size, Bank Age

Table 3. Measurement of Variables

Variable Type	Variable	Measurement (Operationalisation)	Reference
Independent	Cybersecurity Disclosure (CS)	Checklist of annual-report disclosures. Dummy: 1 = bank discloses cybersecurity practices/checklist items, 0 = otherwise.	Elsayed, Ismail & Ahmed (2024)
Dependent	ROA (return on assets)	Net income ÷ total assets, from financial statements/annual reports.	Heikal et al. (2014)
Dependent	ROE (return on equity)	Net income ÷ shareholders' equity, from financial statements/annual reports.	Heikal et al. (2014)
Dependent	NPM (net profit margin)	Net profit ÷ net sales, from financial statements/annual reports.	Heikal et al. (2014)
Moderating	FinTech – Cost	Sum of automated systems, devices/equipment, and computer software, divided by total assets.	Tarawneh et al. (2024)

Moderating	FinTech – ATM	Number of ATMs.	Tarawneh et al. (2024)
Moderating	FinTech – Card credit	Value of the bank's credit-card lending ÷ total customer loans and facilities.	Tarawneh et al. (2024)
Moderating	FinTech – Branches	Number of branches per bank.	Tarawneh et al. (2024)
Control	CAR	Regulatory capital ÷ risk-weighted assets, from annual reports.	Mirović et al. (2024)
Control	BS (bank size)	Natural log of total assets.	Mirović et al. (2024)
Control	BA (bank age)	Natural log of years since bank establishment.	Mirović et al. (2024)

Source: Table created by authors.

4.3 Empirical Model and Measures of Variables

4.3.1 Empirical Model

Following the formulation of the hypotheses and identification of the relationships among the research variables, these relationships are tested using panel data that combine cross-sectional variation across banks with time-series variation for each bank, drawing on data from 16 Egyptian banks between 2016 and 2025. The general form of the model is:

$$Profitability_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 CAR_{it} + \beta_3 BS_{it} + \beta_4 BA_{it} + \varepsilon_{it}$$

To test the research hypotheses, the following empirical models are estimated:

$$ROA_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 CAR_{it} + \beta_3 BS_{it} + \beta_4 BA_{it} + \varepsilon_{it} \quad (1)$$

$$ROE_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 CAR_{it} + \beta_3 BS_{it} + \beta_4 BA_{it} + \varepsilon_{it} \quad (2)$$

$$NPM_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 CAR_{it} + \beta_3 BS_{it} + \beta_4 BA_{it} + \varepsilon_{it} \quad (3)$$

To test the moderating effect, the regression equation is extended as follows:

$$Profitability_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 FinTech_{it} + \beta_3 (CS \times FinTech)_{it} + \beta_4 CAR_{it} + \beta_5 BS_{it} + \beta_6 BA_{it} + \varepsilon_{it}$$

$$ROA_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 FinTech_{it} + \beta_3 (CS \times FinTech)_{it} + \beta_4 CAR_{it} + \beta_5 BS_{it} + \beta_6 BA_{it} + \varepsilon_{it} \quad (4)$$

$$ROE_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 FinTech_{it} + \beta_3 (CS \times FinTech)_{it} + \beta_4 CAR_{it} + \beta_5 BS_{it} + \beta_6 BA_{it} + \varepsilon_{it} \quad (5)$$

$$NPM_{it} = \beta_0 + \beta_1 CS_{it} + \beta_2 FinTech_{it} + \beta_3 (CS \times FinTech)_{it} + \beta_4 CAR_{it} + \beta_5 BS_{it} + \beta_6 BA_{it} + \varepsilon_{it} \quad (6)$$

Equations (1)-(3) estimate the effect of cybersecurity, capital adequacy, bank size, and bank age on bank profitability, measured through ROA, ROE, and NPM. Equations (4)-(6) extend this specification to examine the same relationships while treating financial technology (FinTech) as a moderating variable.

Panel data analysis is the appropriate statistical approach for the structure of the data. The research uses EViews 13 and estimates both fixed-effects and random-effects models for each equation, applying the Hausman test to determine the preferred specification (Zulfikar & STp, 2018).

4.3.2 Descriptive Statistics

Table 4. presents descriptive statistics for cybersecurity, FinTech, and the three bank-profitability indicators across the sample of 16 banks over 2016-2025 (160 observations).

Table 4. Descriptive Statistics for Research Variables

Variable	Obs	Min	Max	Mean	Std. Dev.	Skewness	Kurtosis	Jarque-Bera
ROA	160	-0.0192	0.1741	0.0208	0.0191	3.553	25.087	426.826
ROE	160	-0.1787	3.8716	0.3044	0.5936	4.643	24.893	447.034
NPM	160	-0.0723	2.1739	0.2667	0.2656	4.495	27.516	541.624
Cybersecurity	160	0	1	0.6300	0.4840	-0.543	1.277	34.034
FinTech	160	1.5775	7.1731	3.7203	1.0597	-0.019	2.513	2.133
Bank Size	160	3.0072	11.7734	5.8494	2.2502	1.462	4.112	79.482
CAR	160	0.0614	0.6388	0.2223	0.1038	1.558	5.611	132.461
Bank Age	160	0.0935	2.1288	1.4563	0.3628	-0.504	3.846	13.615

Source: Outputs of data processing using EViews 13.

Table 4 shows that the mean return on assets (ROA) was 0.0208, with a standard deviation of 0.0191. The minimum value, -0.0192, indicates relatively small differences in asset-management efficiency among the least profitable banks, while the maximum was 0.1741, indicating that most sample banks are profitable and able to use their assets efficiently; skewness was 3.553, kurtosis 25.087, and the Jarque-Bera statistic 426.826.

Return on equity (ROE) had a mean of 0.3044, a relatively high rate reflecting the ability of many banks to generate good returns for shareholders, and a standard deviation of 0.5936 indicating a clear divergence in financial performance among banks, with a maximum of 3.8716 and a minimum of -0.1787; skewness was 4.643, kurtosis 24.893, and the Jarque-Bera statistic 447.034.

Net profit margin (NPM) had a mean of 0.2667, indicating banks' ability to retain a good share of revenue as net profit, and a standard deviation of 0.2656 reflecting differences in cost and revenue management across banks, with a maximum of 2.1739 and a minimum of -0.0723; skewness was 4.495, kurtosis 27.516, and the Jarque-Bera statistic 541.624.

For the independent variable, the mean cybersecurity score was 0.63, meaning that 63% of sample observations show cybersecurity disclosure or implementation, with a standard deviation of 0.484 indicating clear variation among banks. The FinTech indicator had a mean of 3.7203 and a standard deviation of 1.0597, ranging from 1.5775 to 7.1731, reflecting moderate variation in FinTech adoption across banks; this variable exhibits the most favourable statistical properties among all the research variables.

For the control variables: mean bank size was 5.849 with a standard deviation of 2.250, and a range from 3.007 to 11.773, indicating significant differences in bank size within the sample; the positive skewness (1.462) reflects a limited number of large banks relative to the rest of the sample, consistent with the nature of the banking sector. Mean capital adequacy was 22.23%, well above minimum regulatory requirements under Basel, indicating that sample banks generally hold healthy capital buffers; the positive skewness (1.558) suggests that some banks maintain markedly higher capital ratios than the rest of the sample. Mean bank age was 1.4563 (log years) with a standard deviation of 0.3628, indicating a relatively similar age range across banks, and the slight negative skewness (-0.504) suggests that most banks have a long operating history.

The Jarque-Bera test was used to examine whether the research variables follow a normal distribution. The results indicate that all variables except FinTech deviate significantly from normality ($p < 0.05$); this does not affect the validity of the panel regression estimates, because panel data techniques are robust to violations of the normality assumption, particularly when robust standard errors are used (Baltagi, 2021).

4.3.3 Correlation Matrix

In table 5. Correlation analysis was conducted to examine the strength and direction of the bivariate relationships among the research variables before estimating the panel regression models. Pearson's correlation coefficient, the most widely used measure of linear association for continuous data, was used. The correlation matrix offers a preliminary indication of potential multicollinearity among the explanatory variables, in addition to identifying preliminary associations.

Table 5. Pearson Correlation Coefficients

	ROA	ROE	NPM	CS	FinTech	Bank Size	CAR	Bank Age
ROA	1							
ROE	0.578	1						
NPM	-0.070	-0.093	1					
CS	0.012	0.012	0.035	1				
FinTech	-0.045	0.136	0.010	0.032	1			
Bank Size	-0.048	-0.187	-0.011	0.060	-0.042	1		
CAR	0.093	0.218	0.080	0.035	0.002	-0.181	1	
Bank Age	-0.282	-0.150	-0.155	0.061	-0.023	0.336	0.171	1

Source: Outputs of data processing using EViews 13. The Bank Age–CAR cell (originally printed as "09.171") is shown here as 0.171; please verify the sign and value against the EViews output.

Table 5 shows that the pairwise correlations among the explanatory variables are generally weak to moderate. The strongest correlation is between ROA and ROE (r = 0.578), reflecting that both variables capture different dimensions of bank profitability; this remains well below the generally recognised cut-off of 0.80, so multicollinearity is unlikely to bias the regression estimates.

Cybersecurity shows positive correlations with FinTech (r = 0.032), Bank Size (r = 0.060), Bank Age (r = 0.061), and CAR (r = 0.035). Correlations between cybersecurity and the profitability measures are similarly limited, suggesting that a multivariate panel regression is needed to capture the direct relationships adequately. Financial technology also shows modest correlations with the other explanatory variables, with ROE showing the highest coefficient at 0.136.

Overall, none of the correlation coefficients exceeds the critical threshold of 0.80, providing preliminary evidence that multicollinearity is unlikely to affect the regression estimates (Gujarati & Porter, 2009; Hair et al., 2018).

4.4 Experimental Results and Analysis

4.4.1 Multicollinearity Test

In table 6. Although the correlation matrix provides an initial indication of the relationships among the variables, it cannot definitively establish the presence of multicollinearity. The Variance Inflation Factor (VIF) was therefore calculated. According to Hair et al. (2018), VIF values below 5 indicate the absence of significant multicollinearity, and values below 10 are generally regarded as acceptable.

Table 6. Variance Inflation Factor (VIF) Analysis

Variable	VIF	Tolerance (1/VIF)
CS	1.003	0.991
FinTech	1.000	0.997
Bank Size	1.151	0.867
CAR	1.053	0.872
Bank Age	1.140	0.951
Mean VIF	1.073	

Source: Outputs of data processing using EViews 13.

The VIF results show that all explanatory variables have remarkably low values, ranging from 1.003 to 1.151, well below the critical threshold of 5, indicating the absence of multicollinearity among the explanatory variables. Likewise, every tolerance value exceeds 0.80, considerably higher than the 0.20 minimum acceptable threshold. Consequently, each explanatory variable

contributes unique information to the regression model, and the independent, moderating, and control variables can be treated as statistically independent, supporting consistent coefficient estimates.

4.4.2 Panel Unit Root Tests

To avoid spurious regression results and ensure the validity of the estimated coefficients, it is essential to examine the stationarity properties of the panel variables before estimating the panel regression models. Panel unit root tests were therefore conducted to determine whether the variables are stationary at their levels or require first differencing (Levin et al., 2002).

To strengthen the robustness of the findings, both first-generation and second-generation panel unit root tests were used. The Levin–Lin–Chu (LLC), Im–Pesaran–Shin (IPS), and Breitung tests are first-generation tests; Pesaran's CIPS test, which accounts for potential cross-sectional dependence among panel units, is a second-generation test (Breitung, 2000). For all tests, the null hypothesis is that the variable has a unit root (is non-stationary), against the alternative that it is stationary (See. Table 7.).

Table 7. Panel Unit Root Tests — First-Generation

Variable	LLC – Level	LLC – 1st Diff.	IPS – Level	IPS – 1st Diff.	Breitung – Level	Breitung – 1st Diff.
ROA	0.0010	0.0000	0.0060	0.0000	0.0000	0.0000
ROE	0.0000	0.0000	0.0390	0.0000	0.0060	0.0000
NPM	0.0000	0.0000	0.0000	0.0000	0.0730	0.0000
Cybersecurity*	0.0000	0.0000	0.0000	0.0000	0.0190	0.0000
FinTech	0.0000	0.0000	0.0030	0.0000	0.3710	0.0000
Bank Size	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
CAR	0.0000	0.0030	0.0000	0.0000	0.0000	0.0000
Bank Age	0.0000	0.0000	0.0270	0.0000	0.0000	0.0000

Source: Outputs of data processing using EViews 13.

Most of the research variables are stationary at their level values according to the first-generation tests: the LLC test rejects the unit-root null for every variable at the 5% level, and the IPS test likewise finds every variable significant in level form. The Breitung test confirms stationarity at levels for most variables, but indicates that NPM and FinTech are non-stationary at the level form, given their insignificant p-values (0.0730 and 0.3710, respectively); both become highly significant after first differencing, indicating that they are integrated of order one, I(1). Overall, the consistency across the three first-generation tests provides strong evidence that the panel variables satisfy the stationarity assumption required for panel regression analysis.

Table 8. Panel Unit Root Tests — Second-Generation

Variable	Pesaran – Level	Pesaran – 1st Diff.	CIPS – Level	CIPS – 1st Diff.
ROA	0.0040	0.0000	0.2140	0.0000
ROE	0.0030	0.0000	0.0000	0.0000
NPM	0.0050	0.0000	0.0010	0.0000
Cybersecurity	0.0000	0.0000	0.5050	0.0000
FinTech	0.0930	0.0000	0.2480	0.0000
Bank Size	0.0000	0.0000	0.0000	0.0000
CAR	0.0000	0.0030	0.0000	0.0000
Bank Age	0.7670	0.0000	0.1250	0.0000

Source: Outputs of data processing using EViews 13.

In table 8. Most variables are stationary at their levels according to Pesaran's test; however, FinTech and Bank Age show insignificant p-values in level form (0.0930 and 0.7670), suggesting the presence of unit roots at level, and both become highly significant after first differencing. Similarly, the CIPS test shows that ROA, Cybersecurity, FinTech, and Bank Age are non-stationary at the level form, whereas all variables become stationary after first differencing. These second-generation results are broadly consistent with the first-generation tests, confirming that the panel variables satisfy the stationarity requirement needed to estimate the panel regression models.

4.4.3 Heteroscedasticity Test

Homogeneity of the error variance across observations is one of the fundamental assumptions of panel regression analysis; violating this assumption can produce inefficient standard errors and unreliable statistical inference. The Breusch-Pagan heteroscedasticity test was applied to each profitability model to assess whether heteroscedasticity is present. The null hypothesis states that residuals have constant variance (homoscedasticity), against the alternative that heteroscedasticity is present.

Table 9. Breusch–Pagan Heteroscedasticity Test Results

Model	p-value
ROA	0.2844
ROE	0.1614
NPM	0.3282

Source: Outputs of data processing using EViews 13.

In table 9. the results show no evidence of heteroscedasticity in any model: the ROA model ($p = 0.2844$), ROE model ($p = 0.1614$), and NPM model ($p = 0.3282$) all have p-values above the 0.05 significance level, so the null of homoscedasticity cannot be rejected. The error variance is therefore constant across banks, and heteroscedasticity does not affect the estimated standard errors or the statistical findings (Halunga et al., 2017).

4.5 Random- and Fixed-Effects Model Building

4.5.1 Model 1: ROA

Table 10. presents the estimation results for the ROA model using both Random- and Fixed-Effects estimators; the Fixed Effects model is used for interpretation, based on the Hausman specification test reported in Table 13.

Table 10. Random- and Fixed-Effects Models for ROA

	RE Model (1)	RE Model (2)	FE Model (1)	FE Model (2)
CS	0.0425 (0.0017)	0.0455 (0.0028)	0.0646 (0.0021)	0.0654 (0.0032)
FinTech	0.1888** (0.1065)	0.2644* (0.1380)	0.3234** (0.1310)	0.4247** (0.2032)
CS × FinTech	—	0.6725** (0.5611)	—	0.8422** (0.6616)
Bank size	0.0225 (0.0162)	0.0226 (0.0191)	-0.0859 (0.0602)	0.0822 (0.0603)
CAR	0.3112 (0.1452)	0.3125 (0.1460)	0.3853 (0.1741)	0.3872 (0.1752)
Bank age	-0.0335 (0.0024)	-0.0226 (0.0043)	0.0046 (0.0043)	0.0052 (0.0056)
Constant	-0.1238 (0.5210)	-0.1182 (0.5431)	3.479** (1.513)	3.433** (1.515)
Year FE	Yes	Yes	Yes	Yes
Adjusted R^2	0.503	0.526	0.652	0.704
Prob > F	0.000	0.000	0.000	0.000
Observations	160	160	160	160

*Source: Outputs of data processing using EViews 13. Standard errors in parentheses; ** $p < 0.05$, * $p < 0.10$.*

Cybersecurity (CS) has a positive coefficient ($\beta = 0.0654$) in the Fixed Effects Model (2), but the relationship is statistically insignificant. This finding indicates that cybersecurity practices alone do not directly improve banks' ROA once other bank-specific variables are controlled for. One possible explanation is that cybersecurity investment is primarily aimed at reducing operational and cyber risk rather than generating quick financial returns, so its direct impact on profitability may take time to become evident. By contrast, ROA is positively and significantly affected by Financial Technology (FinTech) ($\beta = 0.4247$, $p < 0.05$), indicating that greater FinTech adoption improves asset utilisation and operational efficiency in banks.

Notably, CS × FinTech is a positive and statistically significant interaction term ($\beta = 0.8422$, $p < 0.05$), confirming that financial technology positively moderates the relationship between cybersecurity and ROA: as banks adopt more financial technology, the positive effect of cybersecurity on profitability strengthens. Among the control variables, Bank Size, CAR, and Bank Age show no statistically significant effect on ROA, suggesting that changes in profitability over the research period are more closely tied to technological capability than to structural bank characteristics. The Adjusted R^2 rises from 0.652 in Model (1) to 0.704 in Model (2), indicating that adding the interaction term meaningfully improves the model's explanatory power.

This positive effect of FinTech on bank profitability is consistent with Lee and Shin (2018), Frame, Wall and White (2019), and Ozili (2018). The moderating role of FinTech is also consistent with the Resource-Based View and Dynamic Capabilities Theory, both of which suggest that technological capability enhances the effectiveness of strategic organisational resources such as cybersecurity investment. By contrast, the insignificant direct effect of cybersecurity contrasts with Aldasoro et al. (2022), who report a direct relationship between cybersecurity investment and financial performance; this disparity may reflect differences in how cybersecurity is measured, institutional context, and sample characteristics.

4.5.2 Model 2: ROE

Table 11. Random- and Fixed-Effects Models for ROE

	RE Model (1)	RE Model (2)	FE Model (1)	FE Model (2)
CS	0.0646 (0.0127)	0.0745 (0.0221)	0.0666 (0.0128)	0.0743 (0.0134)
FinTech	0.2433 (0.1288)	0.3752* (0.1456)	0.4645** (0.1531)	0.5847** (0.1568)
CS × FinTech	—	0.7140** (0.6132)	—	0.8653** (0.7266)
Bank size	0.0272 (0.0171)	0.0277 (0.0181)	0.0449 (0.0182)	0.0548 (0.0188)
CAR	0.3511 (0.1464)	0.5525 (0.1583)	0.5478 (0.1824)	0.7872 (0.1832)
Bank age	-0.0236 (0.0026)	-0.0223 (0.0041)	0.0055 (0.0047)	0.0066 (0.0059)
Constant	-0.1112 (0.5377)	-0.1031 (0.5528)	3.634** (1.525)	3.833** (1.527)
Year FE	Yes	Yes	Yes	Yes
Adjusted R^2	0.514	0.537	0.662	0.715
Prob > F	0.000	0.000	0.000	0.000
Observations	160	160	160	160

*Source: Outputs of data processing using EViews 13. Standard errors in parentheses; ** $p < 0.05$, * $p < 0.10$.*

In table 11. The Fixed Effects results for Return on Equity (ROE) show that Cybersecurity continues to have a positive but statistically insignificant coefficient ($\beta = 0.0743$), while Financial Technology has a significant positive effect on ROE ($\beta = 0.5847$, $p < 0.05$), indicating that technological innovation improves banks' ability to generate higher returns for shareholders.

The interaction between cybersecurity and financial technology remains positive and statistically significant ($\beta = 0.8653$, $p < 0.05$), indicating that FinTech strengthens the effect of cybersecurity on ROE: banks with more advanced technological capability are better able to convert cybersecurity investment into higher financial returns. The Adjusted R^2 rises from 0.662 to 0.715 after the interaction term is added. These findings are broadly consistent with Lee and Shin (2018) and Frame, Wall and White (2019), who document how FinTech infrastructure strengthens strategic capability and operational efficiency in financial institutions.

4.5.3 Model 3: NPM

Table 12. Random- and Fixed-Effects Models for Net Profit Margin (NPM)

	RE Model (1)	RE Model (2)	FE Model (1)	FE Model (2)
CS	0.0704 (0.0153)	0.0818 (0.0238)	0.0736 (0.0185)	0.0820 (0.0243)
FinTech	0.2675** (0.1403)	0.3944* (0.1556)	0.4856** (0.1562)	0.5913** (0.1571)
CS × FinTech	—	0.8465** (0.6477)	—	0.9435** (0.8046)
Bank size	0.0331 (0.0184)	0.0382 (0.0193)	0.0492 (0.0189)	0.0572 (0.0980)
CAR	0.3699 (0.1489)	0.6463 (0.1603)	0.6126 (0.1833)	0.7945 (0.1868)
Bank age	-0.0158 (0.0029)	-0.0026 (0.0039)	0.0067 (0.0052)	0.0069 (0.0062)
Constant	-0.0732 (0.5421)	-0.0683 (0.5602)	3.8253** (1.5823)	3.9173** (1.5901)
Year FE	Yes	Yes	Yes	Yes
Adjusted R^2	0.532	0.542	0.685	0.726
Prob > F	0.000	0.000	0.000	0.000
Observations	160	160	160	160

*Source: Outputs of data processing using EViews 13. Standard errors in parentheses; ** $p < 0.05$, * $p < 0.10$.*

In table 12. The Fixed Effects results for Net Profit Margin (NPM) show a similar pattern: Cybersecurity has a positive but statistically insignificant direct effect ($\beta = 0.0820$), while Financial Technology significantly improves net profit margin ($\beta = 0.5913$, $p < 0.05$).

The interaction coefficient ($\beta = 0.9435$, $p < 0.05$) is positive and statistically significant, offering further evidence that Financial Technology strengthens the relationship between Cybersecurity and profitability. The Adjusted R^2 rises from 0.685 to 0.726, indicating that the interaction model explains approximately 73% of the variation in banks' profit margins. These results support the hypothesis that cybersecurity investment generates greater financial returns when banks also possess substantial digital and financial-technology capability, consistent with Lee and Shin (2018) and Frame, Wall and White (2019), who document how FinTech infrastructure reshapes the competitive and operational landscape of financial institutions.

Across all three profitability measures, the Fixed Effects model shows greater explanatory power than the Random Effects model, even though the latter also returns positive and significant coefficients for CS × FinTech. The Hausman test in Table 13 formally confirms that the Fixed Effects specification is preferred.

Table 13. Hausman Test for Bank Profitability

	Test Statistic	Degrees of Freedom	p-value
Hausman Test	32.65	4	0.000

Source: Outputs of data processing using EViews 13.

The Hausman test rejects the null hypothesis ($\chi^2 = 32.65$, $p < 0.001$), confirming that the Fixed Effects estimator is more appropriate than the Random Effects estimator for this data.

The empirical findings provide mixed evidence with respect to the three hypotheses. For H1, the estimated cybersecurity (CS) coefficients are positive in all three Fixed Effects profitability models (ROA = 0.0654, ROE = 0.0743, NPM = 0.0820), but none is statistically significant ($p > 0.05$); the research therefore does not find empirical support for a direct positive impact of cybersecurity disclosure on bank profitability, and H1 is not supported.

For H2, financial technology shows a statistically significant positive effect in all three models, with estimated coefficients of 0.4247 for ROA, 0.5847 for ROE, and 0.5913 for NPM ($p < 0.05$), indicating that digital financial technology significantly enhances banks' financial performance; H2 is supported.

Finally, the interaction coefficient between cybersecurity and financial technology (CS × FinTech) is positive and statistically significant in every model (ROA = 0.8422, ROE = 0.8653, NPM = 0.9435), indicating that financial technology strengthens the relationship between cybersecurity and bank profitability, so that the positive effect of cybersecurity becomes more pronounced in banks that adopt FinTech more widely; H3 is supported.

5. Discussion

The overall pattern of results is consistent across all three profitability measures: cybersecurity disclosure alone has no statistically significant direct effect on bank profitability, financial technology has a significant positive direct effect, and the interaction between the two is positive and significant throughout. Read together, these results suggest that cybersecurity functions less as a direct driver of profitability than as a strategic input whose financial payoff depends on the technological infrastructure through which it is delivered and monitored.

This pattern helps reconcile some of the disagreement in the prior literature. Studies that find a direct, positive relationship between cybersecurity and bank performance, such as Al-Nimer et al. (2025) and Bruno, Pistolesi, and Teti (2025), typically examine banking sectors with mature digital infrastructure already in place, where the benefits of cybersecurity disclosure, in reduced losses, stronger customer trust, and lower regulatory friction, are more readily converted into measurable financial performance. By contrast, the absence of a significant direct effect in this study aligns with the strand of literature finding no significant relationship between cybersecurity disclosure and financial performance when it is examined in isolation from complementary technological capability. Taken together with the present findings, this suggests that the presence or strength of a direct cybersecurity-profitability link may itself

depend on a bank's underlying technological capability, precisely the moderating mechanism this study sets out to test.

The significant positive effect of FinTech on all three profitability measures is consistent with Berisha and Rayfield (2025) and Chand et al. (2025), reinforcing the view that FinTech adoption is now a central determinant of bank performance rather than a peripheral operational choice, and is broadly consistent with the wider literature on digital transformation in banking (Lee & Shin, 2018; Ozili, 2018; Frame, Wall & White, 2019).

The significant, positive CS × FinTech interaction is the study's central finding. It indicates that cybersecurity disclosure and FinTech are complementary rather than independent drivers of profitability: cybersecurity investment appears to generate a stronger financial return precisely where a bank has already built the technological infrastructure to operationalise it, whether through automated monitoring, digital channels, or data-driven risk management. This complementarity is consistent with the Resource-Based View and Dynamic Capabilities Theory, discussed further in Section 6, both of which suggest that a strategic resource such as cybersecurity yields its full value only when combined with the organisational and technological capabilities needed to deploy it effectively. The finding also helps explain why the direct-effects literature on cybersecurity and profitability is so mixed: studies that omit FinTech, or that examine banking sectors with markedly different levels of digital maturity, may be capturing different points along the same underlying moderated relationship rather than genuinely conflicting effects.

6. Theoretical Implications

These findings carry several implications for theory. First, they extend the Resource-Based View (RBV) to the domain of bank cybersecurity. The RBV, originally proposed by Barney (1991), holds that resources which are valuable, rare, inimitable, and non-substitutable are a source of sustained competitive advantage. Cybersecurity disclosure, on its own, meets the criteria of value and rarity but does not translate into a significant direct profitability effect in this study, suggesting that cybersecurity alone is not sufficient to generate a competitive advantage. It becomes a genuinely strategic resource, in the RBV sense, only once it is combined with FinTech capability, which supplies the complementary infrastructure needed to exploit it.

Second, the results are consistent with Dynamic Capabilities Theory (Teece, Pisano & Shuen, 1997), which emphasises an organisation's capacity to integrate, build, and reconfigure internal

and external competences in response to a changing environment. The significant, positive interaction between cybersecurity and FinTech suggests that banks with stronger dynamic capabilities, reflected here in more advanced FinTech infrastructure, are better able to reconfigure cybersecurity investment into a source of financial performance, rather than treating it purely as a defensive or compliance-driven cost.

Third, by modelling FinTech as a moderator rather than solely as an independent predictor, this study responds to calls in the literature for research that examines how digital capabilities condition the performance effects of other strategic investments, rather than treating cybersecurity, FinTech, and profitability as three separately estimated, bilateral relationships (Amer & Al-Omar, 2023; Elsayed, Ismail & Ahmed, 2024). The consistent significance of the interaction term across all three profitability measures (β = 0.8422 for ROA, 0.8653 for ROE, and 0.9435 for NPM) offers converging empirical support for treating cybersecurity and FinTech as jointly determined, rather than independent, drivers of bank performance.

7. Practical Implications

For bank managers, the central practical implication is that cybersecurity and FinTech investment should be planned jointly rather than as separate budget lines. Because the direct effect of cybersecurity disclosure on profitability is not statistically significant on its own, banks that treat cybersecurity purely as a compliance or risk-management cost may see limited financial return from that investment in isolation. The significant, positive CS × FinTech interaction (β = 0.8422 for ROA, 0.8653 for ROE, and 0.9435 for NPM) indicates that the financial payoff from cybersecurity is substantially larger for banks that have also invested in FinTech infrastructure, such as digital channels, automated monitoring systems, and data analytics capability.

This suggests several concrete actions for bank management. Cybersecurity budgets should be evaluated alongside, rather than separately from, digital-transformation and FinTech investment plans, since the two appear to reinforce one another's financial return. Banks with less-developed FinTech infrastructure may see limited profitability gains from cybersecurity disclosure alone and should consider sequencing investment, building foundational digital capability before, or alongside, expanding cybersecurity disclosure. Finally, because FinTech shows a significant positive direct effect on all three profitability measures, banks should continue to prioritise digital-channel expansion, automation, and data-driven service delivery

as core profitability drivers in their own right, independent of the interaction effect documented here.

8. Policy Recommendations

For the Central Bank of Egypt and other banking regulators, the findings suggest that cybersecurity and FinTech policy should be developed in a coordinated rather than parallel fashion. Because the profitability benefit of cybersecurity disclosure depends on a bank's FinTech capability, regulatory frameworks that mandate cybersecurity disclosure without corresponding support for digital-infrastructure development may fall short of their intended effect on sector-wide financial resilience and performance.

Specific recommendations include: first, integrating cybersecurity-disclosure requirements with the Central Bank of Egypt's existing financial-inclusion and digital-transformation initiatives, so that smaller or less digitally mature banks receive support in building the FinTech infrastructure needed to convert disclosure into genuine resilience; second, considering differentiated cybersecurity-disclosure requirements or timelines based on a bank's existing level of digital maturity, to avoid imposing compliance costs on banks that are not yet positioned to benefit from them; and third, encouraging industry-wide standards for both cybersecurity disclosure and FinTech reporting, so that future supervisory data can more precisely track how the two interact across the sector over time.

9. Limitations

This study has several limitations that suggest directions for future research. First, the sample is limited to 16 Egyptian commercial banks over 2016-2025; while this provides a reasonably long panel, the sample size and single-country focus limit the generalisability of the findings to other banking sectors or regulatory environments, particularly outside the MENA region.

Second, cybersecurity disclosure is measured using a binary checklist-based indicator drawn from annual reports. While this approach is consistent with prior disclosure-based studies (Elsayed, Ismail & Ahmed, 2024), it captures the presence of disclosure rather than the quality, depth, or actual effectiveness of a bank's underlying cybersecurity practices, and it may not fully reflect cybersecurity investment or incident history that banks do not publicly disclose.

Third, the FinTech measure combines several sub-indicators (cost, ATM count, card-based credit, and branch network) into a single moderating variable; this composite approach, while

practical given data availability, may obscure which specific dimensions of FinTech adoption drive the moderating effect observed here.

Finally, the study relies on secondary, annual-report-based data and an interaction-term regression design, which can establish statistical association but not causal mechanism. Future research could usefully extend this work by testing the framework across a larger, multi-country MENA sample; by using more granular or continuous measures of cybersecurity disclosure quality; by disaggregating the FinTech index to identify which components drive the moderating effect most strongly; and by employing mediation analysis or qualitative case studies to better understand the mechanisms through which FinTech converts cybersecurity investment into financial performance.

References

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.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60, Article 100989. https://doi.org/10.1016/j.jfs.2022.100989

Al-Nimer, M., Badwan, N., Al Zobi, M., Al-Khazaleh, S., Abdallah-Ou-Moussa, S., & Hamdan, M. (2026). Impact of corporate governance on bank performance in the MENA region: The moderating role of cybersecurity policy. *Information and Computer Security*. Advance online publication. https://doi.org/10.1108/ICS-11-2025-0477

Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, 14(8). https://doi.org/10.14569/IJACSA.2023.0140841

Baltagi, B. H. (2021). *Econometric analysis of panel data* (6th ed.). Springer.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Berisha, V., & Rayfield, B. (2025). Impact of internal fintech on bank profitability. *Investment Management and Financial Innovations*, 22(1), 384–404. https://doi.org/10.21511/imfi.22(1).2025.29

Breitung, J. (2000). The local power of some unit root tests for panel data. In B. H. Baltagi (Ed.), *Advances in econometrics, Vol. 15: Nonstationary panels, panel cointegration, and dynamic panels* (pp. 161–177). Emerald.

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. *International Review of Economics & Finance*, 99, Article 104053. https://doi.org/10.1016/j.iref.2025.104053

Chand, S. A., Singh, B., Narayan, K., & Chand, A. (2025). The impact of financial technology (FinTech) on bank risk-taking and profitability in small developing island states: A study of Fiji. *Journal of Risk and Financial Management*, 18(7), Article 366. https://doi.org/10.3390/jrfm18070366

Chanda, R. C., Vafaei-Zadeh, A., Hanifah, H., & Nikbin, D. (2024). Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA. *Computers & Security*, 149, Article 104208. https://doi.org/10.1016/j.cose.2024.104208

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal*, 10(1), Article 115. https://doi.org/10.1186/s43093-024-00402-9

Frame, W. S., Wall, L. D., & White, L. J. (2019). Technological change and financial innovation in banking: Some implications for fintech (Working Paper 2018-11). Federal Reserve Bank of Atlanta. https://doi.org/10.29338/wp2018-11

Gujarati, D. N., & Porter, D. C. (2009). *Basic econometrics* (5th ed.). McGraw-Hill.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2018). *Multivariate data analysis* (8th ed.). Cengage Learning EMEA.

Halunga, A. G., Orme, C. D., & Yamagata, T. (2017). A heteroskedasticity robust Breusch–Pagan test for contemporaneous correlation in dynamic panel data models. *Journal of Econometrics*, 198(2), 209–230. https://doi.org/10.1016/j.jeconom.2016.12.005

Heikal, M., Khaddafi, M., & Ummah, A. (2014). Influence analysis of return on assets (ROA), return on equity (ROE), net profit margin (NPM), debt to equity ratio (DER), and current ratio (CR) against corporate profit growth in automotive in Indonesia Stock Exchange. *International Journal of Academic Research in Business and Social Sciences*, 4(12), 101–114.

Herrmann, D., & Pridöhl, H. (2020). Basic concepts and models of cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (The International Library of Ethics, Law and Technology, Vol. 21, pp. 11–44). Springer. https://doi.org/10.1007/978-3-030-29053-5_2

Hijazin, A., & Badwan, N. (2026). The impact of financial technology development (FinTech) on the profitability of conventional and Islamic banks listed on the Palestine Stock Exchange. *Journal of the Knowledge Economy*, 17(1), 138–168. https://doi.org/10.1007/s13132-025-02622-y

Hsiao, C. (2003). *Analysis of panel data* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511754203

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 17(2), 13–22.

Lamothe-López, P., Lamothe-Fernández, P., Escribano-Sotos, F., & Segovia-Vargas, M.-J. (2024). A global analysis of bank profitability factors. *Humanities and Social Sciences Communications*, 11, Article 124. https://doi.org/10.1057/s41599-024-02604-4

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003

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

Mirović, V., Kalaš, B., Milenković, N., Andrašić, J., & Đaković, M. (2024). Modelling profitability determinants in the banking sector: The case of the Eurozone. *Mathematics*, 12(6), Article 897. https://doi.org/10.3390/math12060897

Nguyen, T. T. T. (2025). The impact of fintech on bank profitability and bank stability in emerging country. *Journal of Organizational Behavior Research*, 10(2), 12–19. https://doi.org/10.51847/eDpAhqzcox

Opuni-Frimpong, J., Adefunso Dzorka, M., & Boadi, I. (2025). Governance's role in bank performance: Cybersecurity committee assessment. *Journal of Financial Reporting and Accounting*, 23(2), 788–810. https://doi.org/10.1108/JFRA-12-2023-0774

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329–340. https://doi.org/10.1016/j.bir.2017.12.003

Ozili, P. K., & Ndah, H. (2024). Impact of financial development on bank profitability. *Journal of Economic and Administrative Sciences*, 40(2), 238–262. https://doi.org/10.1108/JEAS-12-2021-0230

Saha, S., Siddiki, M. S., Mondal, R. S., Bhuiyan, M. N. A., & Kamruzzaman, M. (2025). Risk assessment of cyber security in the banking sector. *Journal of Business and Management Studies*, 7(4), 208–218. https://doi.org/10.32996/jbms.2025.7.4.12

Shehadeh, M., Arabiat, O., Alshurafat, H., Hussainey, K., & Musleh Al-Sartawi, A. M. A. (2026). Gender dynamics and banks' performance: Does cybersecurity disclosure matter? Evidence from Jordan. *International Journal of Financial Studies*, 14(4), Article 84. https://doi.org/10.3390/ijfs14040084

Tarawneh, A., Abdul-Rahman, A., Mohd Amin, S. I., & Ghazali, M. F. (2024). A systematic review of fintech and banking profitability. *International Journal of Financial Studies*, 12(1), Article 3. https://doi.org/10.3390/ijfs12010003

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z

Yuan, X., Puah, C.-H., & Marikan, D. A. b. A. (2025). An empirical study on the impact of financial technology on the profitability of China's listed commercial banks. *Journal of*

Risk and Financial Management, 18(8), Article 440. https://doi.org/10.3390/jrfm18080440

Zulfikar, & Stp. (2018). Estimation model and selection method of panel data regression: An overview of common effect, fixed effect, and random effect model. *INA-Rxiv*. https://doi.org/10.31227/osf.io/9qe2b