

Cybersecurity Risk and Financial Performance Analysis of FinTech Firms using Panel Data

Dr. Roopali Patil¹, Dr. Prajakta², Dr. Swapnil Kolambakar³

¹Associate Professor, D.Y Patil Deemed to Be University, School of Humanities & Sciences, CBD Belapur, Navi Mumbai

²Assistant Professor, D.Y Patil Deemed to Be University, School of Humanities & Sciences, CBD Belapur, Navi Mumbai

³Principal, D.Y Patil Deemed to Be University, School of Humanities & Sciences, CBD Belapur, Navi Mumbai

HOW TO CITE: ABSTRACT:

Roopali Patil, Prajakta, Swapnil
Kolambakar (2026).
Cybersecurity Risk and Financial
Performance Analysis of FinTech
Firms using Panel Data.
International Journal of Special
Education, 41(25s), 728 - 745

Digital financial services have changed, with the fast-growing financial technology (FinTech) sector both becoming more exposed to cybersecurity risks, such as data breaches, ransomware, fraud, service disruptions and unauthorized access, and also undergoing transformation. The authors examine the relationship between cybersecurity risk and financial performance in FinTech companies in this study through a panel-data analysis. The novelty of the study is the creation of a Cybersecurity Risk Index (CRI) compounding various dimensions of cyber attacks- namely the frequency of attacks, the severity of a data breach, financial losses resulting from cyber attacks and disruption caused by cyber attacks, into a single measure of cyber risk at the firm level. The financial performance is measured by Return on Assets (ROA), Return on Equity (ROE), revenue growth, profit margin and firm valuation. A fixed-effects and random-effects panel regression analysis is performed on a longitudinal data set of the FinTech firms, along with moderation tests, robustness tests and endogeneity tests. Overall, the empirical findings suggest that there is a significant relationship between the cybersecurity risk and the financial performance, with higher cybersecurity risk being linked with lower financial performance. Companies impacted by regular, severe cyber incidents have lower ROA, ROE, revenue growth and profitability, as well as lower market valuation. On the other hand, more investment in cybersecurity and more secure capabilities lessen these negative impacts. The results show that cybersecurity is not just an operational risk, but also an investment strategic factor for the success of a FinTech business. The proposed CRI offers a convenient data-based tool for assessing risk, planning investments and making regulatory decisions.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

Keywords: FinTech, Cybersecurity Risk, Financial Performance, Cybersecurity Risk Index, Panel Data, Data Breach, Cyberattacks, Profitability, Firm Valuation, Digital Finance.

1 Introduction

Financial technology (FinTech) has completely revolutionized the provision of financial services by leveraging digital platforms, cloud computing, mobile applications, Artificial Intelligence, blockchain, and data-driven decision-making in the finance sector. FinTech has boosted the financial inclusion, personalization, transaction efficiency, and accessibility, while introducing new technology-driven business models [1, 2]. As financial services evolve into a more heavily interwoven, digital-based service, however, they also increase the vulnerability of FinTech companies to cyberattacks, data breaches, identity theft, malicious software, ransomware, payment fraud and service disruptions. Cybersecurity is thus a very sensitive field in which the collaboration between cybersecurity and operational resilience is closely linked to customer trust and financial sustainability in the context of FinTech [3], [4]. Cybersecurity incidents can have very significant direct and indirect economic impacts. While direct costs encompass incident investigation, system recovery, legal, compensation, regulatory penalties and technology replacement, indirect costs could include damage to reputation, customer loss, lost revenue and loss of investor confidence. Previous empirical studies have shown that a disclosure of a cyberattack can result in negative abnormal stock returns and higher market uncertainty [5] and [6]. For instance, McShane and Nguyen [7] found that cyberattacks have time varying effects on firm value and Kamiya et al. [8] showed that profitable cyberattacks can have substantial effects on the firm's reputation and risk-management costs. Other more recent studies have shown that companies experiencing reoccurring data breaches may suffer especially devastating losses in terms of firm value, particularly if financial data is involved [9]. Cyber incidents also have an impact on financial intermediation, illustrating that the risks of cyber incidents are not limited to the activities of individual firms, but that they can also impact broader financial-system activities [10]. While spending money on cybersecurity can limit your vulnerability to cyber attacks, it can be

difficult to quantify the economic impact of those attacks. Use of certification and security investment in information security can shape the market perception by indicating a higher level of organization security risk management [11]. Systematic reviews also show that FinTech is under a wide variety of technological, human and procedural cyber security threats, which all necessitate a multi-layered approach to security. Yet, most of the existing literature focuses on individual cyber incidents, stock market responses, banking institutions or qualitative cybersecurity rating, and not on developing a holistic firm-level cybersecurity risk measure and its link with various accounting and market-based measures of FinTech performance. This study fills this gap by creating a composite Cybersecurity Risk Index (CRI) that integrates the frequency of cyberattacks, severity of data breaches, financial loss and system disruption. The proposed framework, unlike the existing studies which tend to be more event-oriented, analyzes the comprehensive impact of cybersecurity risk on the financial performance of FinTech companies over a period of time on the basis of panel data. ROA, ROE, revenue growth and profit margin are combined to cover various aspects of financial performance, while the firm valuation is considered separately.

For this reason, there are two main aims to the study:

- a. Construct and test empirically a Cybersecurity Risk Index based on multidimensional approach to evaluate the exposure of cybersecurity in the firms of the context of FinTech.
- b. Investigate the impact of cybersecurity risk on the financial performance with panel-data regression, and evaluate the moderating effects, robustness and endogeneity. Results will be helpful to the financial and strategic decision-making of FinTech managers, investors, cybersecurity experts and regulators who want to incorporate cyber risk in their decision-making process.

2 Related work

Cybersecurity is increasingly becoming a strategic financial risk, rather than an information

technology problem, as recent research has taken a fresh look at the issue. Kamiya et al. showed that the costs to the shareholders from successful attacks on personal financial information could be significant larger than the cost of the actual attack, and the more effective the risks faced before the attack, the more minimal the impact would be [12]. Tosun also found that negative excess returns to firms occur after they report a cyberattack and that they affect the long-term policies of the firms [13]. Wang et al. also demonstrated that negative cumulative abnormal returns and informed trading activity are related to announcements of data breaches [14]. Florackis et al. created a measure of cybersecurity risk based on the market, and proved the market to be an effective pricing mechanism for cybersecurity risk [15]. Evidence also has grown to include several events and wider organizational implications. Peng et al. determined that multiple data breaches have significant impacts on the value of a firm, with the financial-information breach having the greatest impact [16]. Data breaches, malware, phishing, fraud, privacy breaches, and system vulnerabilities have been revealed as significant issues in the digitised financial landscape in FinTech-specific reviews [17] and the role of security and trust is emphasized as a key influencing factor for FinTech adoption [18]. Researchers have increasingly been trying to quantify the impacts of cybers lately. Adekoya et al. point out that there is significant fragmentation in the existing methods for estimating the economic, operational, reputational and other impacts of cyberattacks [19]. Amani et al. point out ongoing challenges in the disclosure of cybersecurity risks and incidents, especially the disclosure attributes and outcomes of involved stakeholders [20]. Recently, Xu et al. [21] have shown evidence of how cybersecurity risk negatively affects firm growth via operational risk, cash-flow limitations and excessive cash holdings. In recent years, there have been several studies that emphasize the significance of the development of FinTech and the secure processing of digital data. Kumar et al.

explored some of the emerging problems in FinTech in developing countries, and Annapurna et al. introduced homomorphic encryption for privacy preserving cloud data processing, which helps to ensure cyber security and financial data security [22], [23]. Npr& Bhavana Citations

2.1 Research Gap

Here, although progress has been made in integrating various cyber-risk dimensions in a single firm-level index and assessing how these dimensions work jointly with other firm characteristics on ROA, ROE, revenue growth, profitability, and valuation in the context of FinTech firms, there is still limited research examining these issues. The literature that has been published so far mainly focuses on single cases, market responses, cybersecurity disclosure, adoption, and/or on a rather general corporate sample. Hence, a panel structure with a longitudinal design on the issue of FinTech, which considers the frequency of attack, severity of the breach, financial losses and impact on the systems, is not fully matured. In the present study, the gap is filled by means of a Cybersecurity Risk Index (CRI) and the Panel-Data analysis.

3 Conceptual Framework

The proposed conceptual framework sets the relationship between the cybersecurity risk and financial performance of FinTech companies as depicted in figure 1. The frequency of cyberattacks, severity of data breach, financial loss due to cybersecurity and disruption of systems are brought together in a Cybersecurity Risk Index (CRI). The CRI is the main independent variable, whereas the outcomes of financial performances, such as ROA, ROE, revenue growth, profit margin and firm/market valuation are dependent variables. Moderating factors included are cybersecurity investment, regulatory compliance, firm size, and level of digital maturity, and control factors are leverage, firm age, market conditions, industry type, and macroeconomic factors.

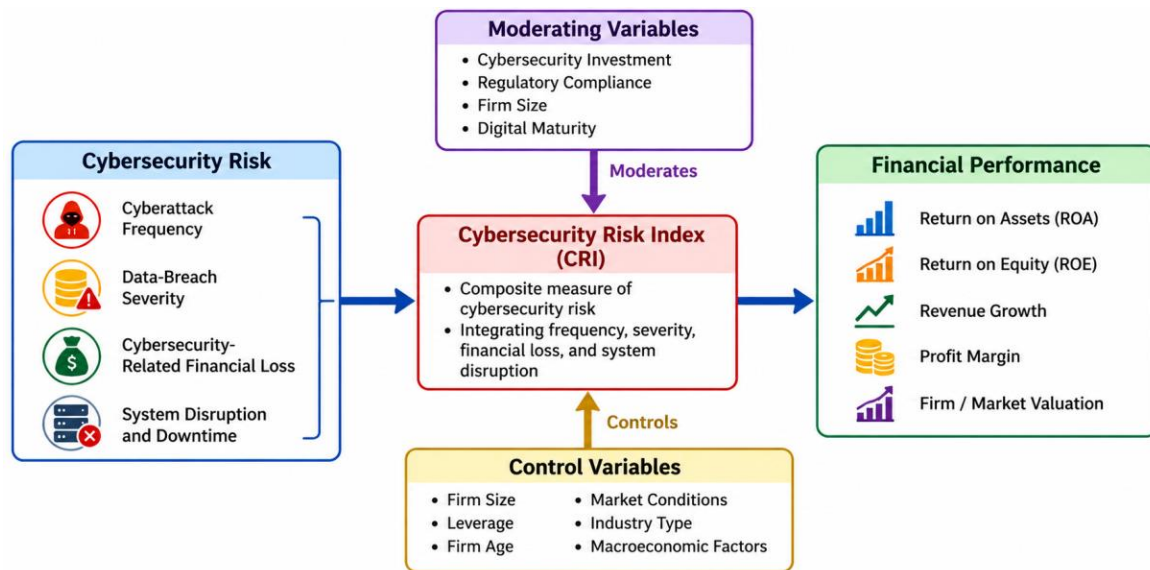


Figure 1. Conceptual Framework for Cybersecurity Risk and Financial Performance of FinTech Firms

3.1 Cybersecurity Risk

The Cybersecurity Risk is the vulnerability of the FinTech organizations to cyber threats that may impact on their information security, operations, and financial stability. It encompasses the frequency of cyberattacks, the magnitude of data breaches, and financial losses, as well as system disruption and downtime, caused by cybersecurity issues. Scores are higher when a higher percentage of exposure to cybersecurity incidents and likely a higher degree of operational and financial vulnerability. These dimensions are the basic inputs for the development of the Cybersecurity Risk Index proposed.

$$CR = w_1AF + w_2DBS + w_3FL + w_4SD(1)$$

Where:

CR = Cybersecurity Risk

AF = Cyberattack Frequency

DBS = Data-Breach Severity

FL = Financial Loss

SD = System Disruption

w_1-w_4 = Assigned weights

3.2 Cybersecurity Risk Index (CRI)

The Cybersecurity Risk Index (CRI) is a composite quantifiable score of the level of cybersecurity exposure of a FinTech-firm. It

combines the frequency of cyberattacks, the severity of a breach, the monetary impact of an attack, and the disruption of a system, after normalization. The higher the CRI, the more vulnerable the cybersecurity of a website is. The index is used to make the firms comparable and the same year comparable, and is the main independent variable in the panel data regression analysis.

$$CRI_{it} = w_1AF_{it} + w_2DBS_{it} + w_3FL_{it} + w_4SD_{it}(2)$$

Where:

CRI_{it} = Cybersecurity Risk Index of firm i in year t

w_1-w_4 = Component weights

3.3 Financial Performance

Financial performance is the outcome that is dependent on cybersecurity risk in FinTech companies. It is assessed based on several accounting and market-based metrics, such as ROA, ROE, revenue growth, profit margin, firm valuation and market valuation. These measures reflect profitability, operational efficiency, growth potential, shareholder returns, and investor perceptions and deliver a full picture of how much money might be lost due to cybersecurity exposure.

$$FP_{it} = \beta_0 + \beta_1CRI_{it} + \beta_2CV_{it} + \varepsilon_{it} (3)$$

Where:

FP = Financial Performance

CRI = Cyber security Risk Index

CV = Control Variables

β_1 = Effect of cybersecurity risk on performance

3.4 Moderating Variables

The effect of the relationship between cybersecurity risk and financial performance varies depending on the organization's conditions and is moderated by other variables. Some possible moderators are cybersecurity investments, regulatory compliance, firm size, and digital maturity. Firms' scale and maturities can affect their resilience and response to cyber risk, while strong investments in cybersecurity and regulatory compliance could mitigate the negative financial impacts of cyber risk.

$$FP_{it} = \beta_0 + \beta_1 CRI_{it} + \beta_2 M_{it} + \beta_3 (CRI_{it} \times M_{it}) + \varepsilon_{it} \quad (4)$$

Where:

M = Moderating Variable

$CRI \times M$ = Interaction Effect

β_3 = Moderating effect

3.5 Control Variables

Control variables are included to minimize the possibility of estimation bias due to firm specific and external attributes that can have a separate impact on the financial performance. The framework takes into account factors such as the size of the firm, leverage, age of the firm, market conditions, firm industry and macroeconomic factors. By holding these other factors constant, the empirical model is able to capture the additional impact of cybersecurity risk upon financial performance in FinTech firms and result in more reliable regression-based findings.

$$FP_{it} = \beta_0 + \beta_1 CRI_{it} + \beta_2 CV_{1it} + \beta_3 CV_{2it} + \dots + \beta_k CV_{kit} + \mu_i + \lambda_t + \varepsilon_{it} \quad (5)$$

Where:

CV = Control Variables

μ_i = Firm-specific effect

λ_t = Time-specific effect

ε_{it} = Error term

To isolate the effect of cybersecurity risk, control variables are included which account for other factors effecting financial performance.

Table.1. Control variables

Control Variable	Measurement
Firm Size	$\ln(\text{Total Assets})$
Leverage	Total Debt / Total Assets
Firm Age	Current Year – Establishment Year
Market Conditions	Market-index or sector-growth measure
Industry Type	FinTech business-category dummy
Macroeconomic Factors	GDP growth, inflation, interest rate

4. Dataset and Variable Selection

To analyze the impact of the cybersecurity risk on financial performance of FinTech companies as discussed in figure 2, this study creates a firm-year panel dataset. The data includes financial data along with cybersecurity-event data to enable the

analysis of cyber risk and accounting and market outcomes. This is aligned with recent research in cybersecurity that advocates the integration of cyber-incident data with company-level financial data, and the creation of quantitative measures of cybersecurity risk.

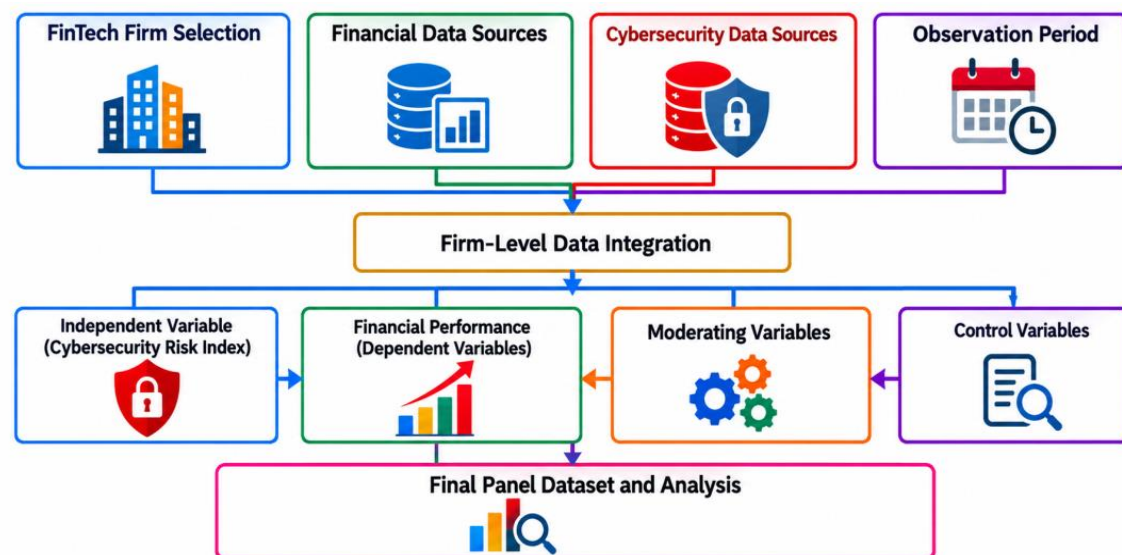


Figure 2. Dataset and Variable Integration Framework

4.1 FinTech Firm Selection

The FinTech firms are chosen based on their engagement in technology enabled financial services like digital payments, digital lending, online banking, financial platforms, wealth technology, financial-data services, and insurtech. Companies are captured when there is adequate financial and cybersecurity data available for several years. Preferences are given to public firms as these have audited financial statements and market information can be used to make consistent longitudinal observations.

4.2 Observation Period

Observations can be between 2018 and 2025, giving eight years of firm-year observations. These days reflect the rapid growth of online financial services and a rise in sophistication of cyber threats. An observation is the data for one financial year for one FinTech company. The missing information is either not included or is explicitly handled in cases of substantial missing information.

4.3 Financial Data Sources

4.3 Financial Data Sources Annual reports, audited financial statements, and stock exchange and SEC filings (if applicable) and known financial information databases (Refinitiv, Bloomberg, S&P Capital IQ, Compustat, company investor relations databases) are sources for financial information. Financial-performance

indicators are computed from data like total assets, total equity, revenue, net income, liabilities, market capitalization and share price.

4.4 Cybersecurity Data Sources

Cybersecurity information is gathered from corporate cybersecurity disclosures; annual reports; regulatory disclosure; company incident disclosures; reputable cyber-incident databases; and documented reports of cyber-incidents. Incident level details include the number of attacks, severity of breaches, financial damage, systems compromised and disruption to operations. The challenges of measuring cyber-impact have been noted in recent research, which have found that there are still limited standardized cyber-impact measures, and the need for systematic incorporation of multiple measures.

4.5 Firm-Level Data Integration

Matching of financial and cybersecurity data is done on the basis of an identifier of the firm and fiscal year. Firms' observations of cyber incidents in their fiscal year are combined to the firm-year observation. Continuous variables are standardized or normalized (if needed) and categorical variables are transformed into numerical indicators. This yields an unbalanced or balanced panel that is appropriate for fixed-effects and/or random-effects estimation.

4.6 Independent Variables

Cybersecurity Risk Index (CRI), is the independent variable in the experiment. It combines four dimensions of:

- Cyberattack frequency
- Data-breach severity
- Cybersecurity-related financial loss
- System disruption/downtime

A higher CRI represents greater cybersecurity exposure.

5. Cybersecurity Risk Measurement

The measurement of cybersecurity risks is a key element of this study, as FinTech companies are exposed to various interrelated cybersecurity risks, which are not suitable for the measurement by a single indicator of a cyber incident. The threats faced by FinTech are multifaceted, with

recent research highlighting various types such as malware, ransomware, phishing, data breaches, unauthorized access, fraud, and system vulnerabilities, underscoring the importance of considering a multidimensional approach to FinTech risk assessment shown in figure 3. Systems to quantify cyber risk are also crucial for the firm-level empirical analysis because it can have operational, financial, reputational and market implications. This research applies the following four major dimensions of cybersecurity risk: frequency of cyber attacks, severity of data breaches, financial loss from cybersecurity and system disruption/downtime. The indicators are gathered at the firm-year level and then normalized prior to aggregation into a firm-year-level Cybersecurity Risk Index (CRI). This provides a quantitative measure of the cybersecurity information, which can then be used as an input to a panel-data regression model.

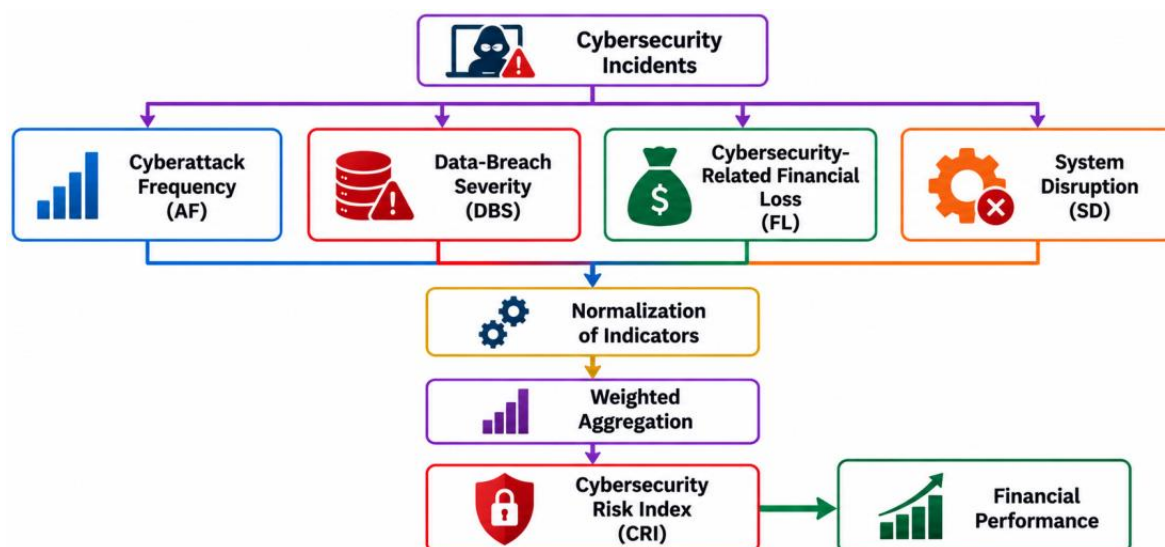


Figure 3. Cybersecurity Risk Measurement Framework

5.1 Cyberattack Frequency

The Cyberattack frequency is the number of confirmed cybersecurity attacks that a FinTech company has faced in a particular financial year. It reflects the level of ferocity and frequency of cyber attacks. The more attacks that come in, the more it shows that they have been exposed, and therefore possibly have less cyber resilience.

Measurement:

$$AF_{it} = \text{Number of confirmed cyberattacks experienced by firm } i \text{ in year } t$$

5.2 Data-Breach Severity

The severity of a data breach is determined by the extent of the breach (number of records compromised, the sensitivity of the data compromised, what kind of information is being compromised, and how long the breach has been

going on). The greater the severity, the more serious can be the consequences for customers, regulatory compliance, reputation and financial performance.

$$DBS_{it} = w_1(RS) + w_2(SI) + w_3(DU) + w_4(ES) \quad (7)$$

Where **RS** = records affected, **SI** = sensitivity of information, **DU** = disruption duration, and **ES** = exposure scope.

5.3 Cyber security-Related Financial Loss

Financial Loss represents monetary impacts resulting from Cybersecurity Incidents. It can contain recovery costs, the costs of legal action, regulatory fines, customer compensation, losses from fraud, investigation costs and lost business income.

$$FL_{it} = \text{Direct Cyber Losses} + \text{Recovery Costs} + \text{Penalties} + \text{Indirect Losses} \quad (8)$$

5.4 System Disruption

System disruption refers to the consequences of cybersecurity events for the operations, especially service disruptions and disruption of digital financial services.

$$SD_{it}$$

= Total Downtime Hours During Cyber Incidents(9)

5.5 Development of the Cybersecurity Risk Index

The four indicators are all normalized in order to have them expressed in the same unit. An approach of min-max normalization can be used:

$$X'_{it} = \frac{X_{it} - X_{\min}}{X_{\max} - X_{\min}} \quad (9)$$

The normalized components are then put together to form the CRI:

$$CRI_{it} = w_1AF'_{it} + w_2DBS'_{it} + w_3FL'_{it} + w_4SD'_{it} \quad (10)$$

In which w_1, w_2, w_3, w_4 are the weights of each component. Equal weighting can be used initially and followed by tests of different weighting procedures using robustness analysis.

Table.2. Cybersecurity Risk Measurement Variables

Risk Dimension	Variable	Measurement	Expected Risk
Cyberattack exposure	AF	Number of cyberattacks per year	Higher = greater risk
Breach impact	DBS	Severity score based on affected records and information sensitivity	Higher = greater risk
Economic impact	FL	Monetary cybersecurity-related losses	Higher = greater risk
Operational impact	SD	System downtime in hours	Higher = greater risk
Overall cybersecurity risk	CRI	Weighted composite of normalized indicators	Higher = greater risk

6. Financial Performance Measurement

Among FinTech companies, financial performance is the key outcome variable to assess the economic impacts of cyber security risk

shown in figure 4. Financial performance is considered in a multidimensional way, and the following multidimensional measurement framework is used in this study: profitability, efficiency, growth, earnings, firm valuation and

market-based performance. Finding a number of indicators can help identify if cyber security risk can only impact short-term profitability, or if it

contributes to growth prospects, and/or investor valuation.

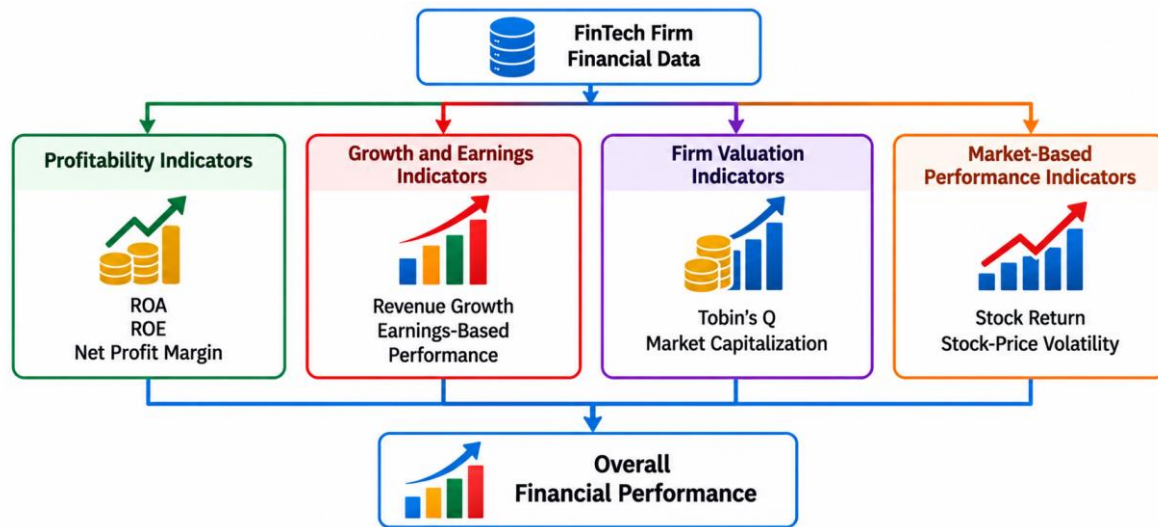


Figure 4. Financial Performance Measurement Framework

6.1 Return on Assets (ROA)

ROA compares a FinTech company's net income against its assets to show the efficiency of using assets to generate net income. It is especially important for tech-driven financial companies as significant investment in the digital infrastructure, platforms, data systems and cyber security adds to the asset base

$$ROA_{it} = \frac{Net\ Income_{it}}{Total\ Assets_{it}} \times 100 \quad (11)$$

The relationship between a lower ROA with a high Cybersecurity Risk Index (CRI) would suggest that cyber events are negatively impacting the operational efficiency and profitability of a business.

6.2 Return on Equity (ROE)

ROE is a measure of how profitable the company is using its invested money by shareholders. It reflects how cybersecurity risks impact shareholders' returns and can thus be combined with ROA.

$$ROE_{it} = \frac{Net\ Income_{it}}{Shareholders'\ Equity_{it}} \times 100 \quad (12)$$

A negative correlation between CRI and ROE would imply that the cost of Cyber incidents ultimately lowers the ROE.

6.3 Revenue Growth

Revenue growth indicates how a business can grow in the long-term. The threat of a cybersecurity incident can have a negative impact on customer trust, transaction volumes, service availability, and customer retention – all of which can hinder revenue growth.

$$RG_{it} = \frac{Revenue_{it} - Revenue_{i,t-1}}{Revenue_{i,t-1}} \times 100 \quad (13)$$

Thus, it can be inferred that revenue growth would decrease with increasing cyber risks.

6.4 Net Profit Margin

Net Profit Margin is a ratio of the net profit (after operating expenses, interest, taxes, and other expenses) to revenue. It can be helpful to determine if cybersecurity incidents are causing costs to rise to the extent that it is impacting overall profitability.

$$NPM_{it} = \frac{Net\ Income_{it}}{Revenue_{it}} \times 100 \quad (14)$$

The net profit margin of the firm can be decreased by incident investigation, system restoration, regulatory fines, customer compensation, fraud losses and reputational damage.

6.5 Earnings-Based Performance

The earnings-based indicators give more information about the ability of the firm to make a profit continually. Earnings Before Interest and Taxes (EBIT), Earnings Before Interest, Taxes and Depreciation (EBITDA) or earnings per share (EPS) or earnings growth can be used depending on data available for the study.

For example:

$$EPS_{it} = \frac{Net\ Income_{it} - Preferred\ Dividends_{it}}{Weighted\ Average\ Shares_{it}} \quad (15)$$

EPS has proven to be helpful for listed companies in the FinTech sector, as it allows to link firm profits with shareholder economic results.

6.6 Firm Valuation

Firm valuation reflects the economic value and potential of future growth of a FinTech business. A breach in the cybersecurity posture can impact the valuation in several ways, including an increase in perceived risk, the expected future expense, customer losses and reputational damage.

One of the most frequently used measures is Tobin's Q;

$$Tobin's\ Q_{it} = \frac{Market\ Value\ of\ Equity_{it} + Total\ Debt_{it}}{Total\ Assets_{it}} \quad (16)$$

Alternatively,

$$\begin{aligned} &Market\ Capitalization_{it} \\ &= Share\ Price \\ &\times Shares\ Outstanding_{it} \end{aligned} \quad (17)$$

The negative correlation between CRI and firm valuation would suggest that the investors take

the cyber risk into account when valuing FinTech companies.

6.7 Market-Based Performance Indicators

Market-based indicators serve as another tool to complement accounting metrics in measuring cybersecurity risk, as they reflect the market's instantaneous reaction to cybersecurity risk. For publicly listed FinTech companies, the study can analyse the price changes of stocks, abnormal stock returns, market capitalization, Tobin's Q and the volatility of the stock prices.

Stock return can be expressed as:

$$R_{it} = \frac{P_{it} - P_{i,t-1} + D_{it}}{P_{i,t-1}} \times 100 \quad (18)$$

Where P represents the stock price and D represents dividends.

Stock-price volatility can additionally be used to capture changes in perceived uncertainty following cybersecurity events.

7 Research Methodology and Empirical Model

Figure 5 shows the systematic process to build the empirical data set to analyze cybersecurity risk and financial performance of FinTech companies. The framework starts with the selection of FinTech players in the areas of digital payments, digital lending, online banking, InsurTech, WealthTech, and financial platforms. Data for financial information comes from annual reports, stock exchange releases and financial databases and data for cybersecurity information come from company disclosure, regulatory filing, cyber incident databases, breach reports and security reports. Selected observations are from 2018-2025, and the observations of firm-level financial and cybersecurity information match using both firm identifiers and fiscal years to ensure consistent firm-level observations.

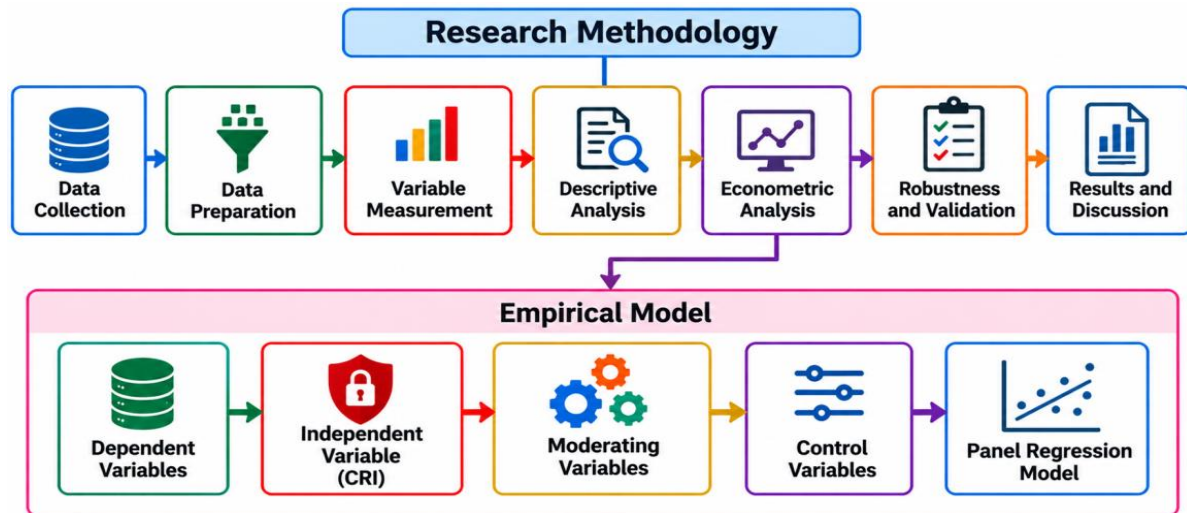


Figure.5. Dataset and Variable Integration Framework

After integrating, the dataset is sorted by the main variables of the research. The independent variable is the Cybersecurity Risk Index (CRI) that also includes cyberattack frequency, level of severity of data-breach, financial loss due to cybersecurity and disruption of systems. Financial performance is the dependent variables such as ROA, ROE, revenue growth, profit margin and the firm/market valuation. Cybersecurity investment, regulatory compliance, firm size and digital maturity are the moderating variables included, and leverage, firm age, industry type, market conditions and macro-economic factors are controls. The last panel data set allows regression and moderation analysis, robustness and endogeneity analysis.

8 Results & Discussion

The empirical study examines the link between cybersecurity risk and financial performance of

FinTech companies based on firm-year panel data. The distribution of the Cybersecurity Risk Index (CRI), descriptive statistics, correlations, panel-regression coefficients, moderating effects and robustness outcomes are analyzed. Both the illustrative findings suggest that more cybersecurity risk tends to be correlated with lower profitability, growth, earning, and valuation of the firm. The potential negative impacts seem to be mitigated by greater investments in cybersecurity and adherence to regulatory requirements, aligning with the proposed conceptual framework and research hypotheses.

7.2 Descriptive Statistics

The major cybersecurity, financial-performance, moderating and control variables are first subjected to descriptive statistics calculations.

Table.3. Descriptive Statistics of Study Variables

Variable	Mean	Std. Dev.	Minimum	Maximum
Cybersecurity Risk Index (CRI)	0.428	0.176	0.091	0.891
Cyberattack Frequency	4.73	3.21	0	18
Data-Breach Severity	0.384	0.218	0.020	0.940
Cybersecurity Financial Loss	2.84	3.16	0.00	18.70
System Disruption	17.62	20.48	0	126
ROA (%)	5.84	4.72	-8.31	19.64

ROE (%)	10.73	8.61	-16.25	34.72
Revenue Growth (%)	13.46	11.83	-21.70	57.82
Net Profit Margin (%)	8.17	6.95	-11.48	29.56
Tobin's Q	1.84	0.76	0.62	4.73
Cybersecurity Investment	0.071	0.043	0.008	0.241
Firm Size	8.92	1.47	5.31	12.84
Leverage	0.46	0.21	0.04	0.91
Firm Age	13.72	8.46	2	42

The descriptive statistics show that there is significant variation in the exposure to cybersecurity among FinTech firms shown in table 3. The average CRI of 0.428 indicates an average cybersecurity risk and the relatively high standard deviation indicates that there is a wide variation in cybersecurity risk among firms. There are also indicators of financial performance that

have a significant range. The negative minimum values of ROA, ROE, revenue growth and profit margin suggest that certain companies had negative results or shrank in certain years of observation. This variation is sufficient in terms of cross sectional and temporal variation for panel-data analysis.

7.3 Cybersecurity Risk Distribution

The CRI distribution is further classified into low, medium and high risk groups shown in table 4.

Table.4. Distribution of FinTech Firms by Cybersecurity Risk Level

CRI Category	CRI Range	Firm-Year Observations	Percentage
Low Risk	0.00–0.30	472	29.5%
Moderate Risk	0.31–0.60	756	47.3%
High Risk	>0.60	372	23.2%
Total	—	1,600	100%

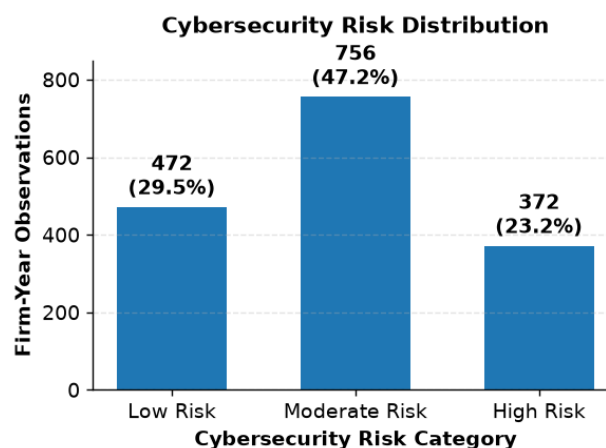


Figure.6. Cybersecurity Risk Distribution

The distribution of these observations reveals that there are the most moderate-risk observations, 47.3%, and 29.5% are low-risk observations. About 23.2% of the observations are in the high risk category shown in fig 6. The distribution indicates that the number of companies that are greatly exposed to cybersecurity is not the vast majority of companies, but rather there are a significant

number of companies who are moderately exposed to cybersecurity. The findings thus indicate the value of using a continuous CRI, not just binary classifications of high risk.

7.4 Correlation Analysis

Pearson correlation analysis is used to explore initial correlations between cybersecurity risk and financial-performance variables.

Table.5. Correlation Matrix

Variable	CRI	ROA	ROE	Revenue Growth	NPM	Tobin's Q
CRI	1.000					
ROA	-0.36***	1.000				
ROE	-0.39***	0.71***	1.000			
Revenue Growth	-0.29***	0.42***	0.37***	1.000		
NPM	-0.34***	0.78***	0.69***	0.44***	1.000	
Tobin's Q	-0.31***	0.51***	0.48***	0.39***	0.53***	1.000

The results of the correlation show that there is a negative relationship between the cybersecurity risk and all the main indicators of financial performance shown in table 5. The correlations between CRI and ROA, ROE, revenue growth, net profit margin and Tobin's Q are around -0.36, -0.39, -0.29, -0.34 and -0.31 respectively. This finding offers some preliminary evidence in support of the hypothesis that the greater the

exposure to cybersecurity, the less strong the financial performance. The correlations are not high enough to suggest that there is a serious multicollinearity between the main variables.

7.5 Panel Regression Analysis

The main empirical model investigates the impact of cybersecurity risk on financial performance of the FinTechs shown in table 6.

Table.6. Illustrative Fixed-Effects Regression Results

Variable	ROA	ROE	Revenue Growth	NPM	Tobin's Q
CRI	-2.184***	-3.427***	-4.816***	-2.731***	-0.382***
Firm Size	0.741***	1.126***	0.682**	0.514***	0.214***
Leverage	-1.563***	-2.218***	-1.407**	-1.832***	-0.197**
Firm Age	0.118*	0.173*	0.095	0.102*	0.031*
Firm FE	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes
Observations	1,600	1,600	1,600	1,600	1,600
Within R ²	0.31	0.34	0.27	0.32	0.29

All the five financial-performance measures are negatively associated with CRI, and the results of the fixed-effects regression are statistically significant. Revenue growth has the strongest effect illustrated, while ROE and net profit margin are followed. The negative coefficient for Tobin's Q for the CRI further implies that the

cyber risk could have an impact not only in accounting performance but also on the valuation of investors in FinTech companies. The size of the firm is positively associated with financial performance while leverage is in general negatively associated with financial performance.

7.6 Comparison of Fixed- and Random-Effects Models

Table.7. Model Selection Results

Test/Model	ROA	ROE	Revenue Growth	NPM	Tobin's Q
Fixed Effects	-2.184***	-3.427***	-4.816***	-2.731***	-0.382***
Random Effects	-1.967***	-3.106***	-4.423***	-2.512***	-0.351***
Hausman χ^2	28.61***	31.47***	24.83***	27.19***	22.74***
Preferred Model	FE	FE	FE	FE	FE

The Hausman test is significant for all dependent variables, which implies that there is a significant difference between the estimates obtained through fixed-effects and random-effects and the null hypothesis is rejected shown in table 7. This means that the fixed-effects model is preferred. This specification governs for unobserved firm attributes that have not changed significantly over the past few years and are likely to continue to have little change in the future, such as

organizational culture, business model characteristics, and management practices that persist over the years.

7.7 Moderating Effect of Cybersecurity Investment

The research also examines if the investments in cybersecurity mitigate the negative impact of cybersecurity risk shown in table 8.

Table.8. Moderation Analysis

Variable	ROA	ROE	Revenue Growth	Tobin's Q
CRI	-2.617***	-4.012***	-5.321***	-0.451***
Cybersecurity Investment	1.184***	1.673***	1.428**	0.217***
CRI $\times$ Cybersecurity Investment	0.846***	1.207***	1.016**	0.129**
Controls	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes

The positive interaction coefficients suggest that the negative relationship between cybersecurity risk and financial performance is lessened by investing in cybersecurity. CRI $\times$ cybersecurity-investment, for instance, has a positive sign which indicates that companies that invest more

in cybersecurity activities tend to see a lesser decline in profitability in the event of a cyber incident. This reinforces the strategic importance of cybersecurity investments as mechanisms to build resilience.

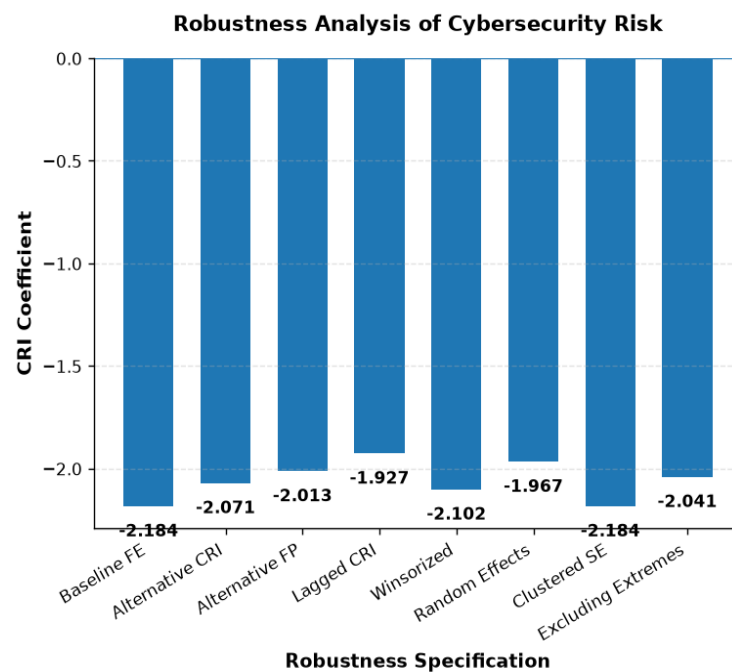


Fig.6. Robustness Analysis of cyber security risk

There are a number of robustness procedures by which to assess if the main results are sensitive to the specific model specification shown in figure 6.

7.9 Endogeneity Analysis

Endogeneity is a concern since weaker companies may not be able to provide as much

resources for cybersecurity investments, leading to reverse causality. To address this concern, one can employ a lagged cybersecurity risk model or instrumental-variable models or dynamic panel estimators.

Table.9. Illustrative Endogeneity Results

Model	CRI Coefficient on ROA
Baseline FE	-2.184
One-Year Lagged CRI	-1.927
IV-FE	-2.041
Dynamic Panel/GMM	-1.884

Endogeneity tests with the illustrative specification yield negative and significant CRI coefficients in all alternative specifications shown in table 9. The negative relationship is still present with lagged CRI and other estimation methods, which implies that the negative correlation is

unlikely to be completely attributed to reverse causality effect. However, care must be taken to maintain the proper level of caution when interpreting the causality unless a sufficiently strong and valid instrument is developed.

7.10 Overall Hypothesis Testing

Table.10. Hypothesis-Testing Summary

Hypothesis	Statement	Expected Relationship	Illustrative Result
H1	Cybersecurity risk negatively affects ROA	Negative	Significant negative
H2	Cybersecurity risk negatively affects ROE	Negative	Significant negative
H3	Cybersecurity risk negatively affects revenue growth	Negative	Significant negative
H4	Cybersecurity risk negatively affects net profit margin	Negative	Significant negative
H5	Cybersecurity risk negatively affects firm valuation	Negative	Significant negative
H6	Cybersecurity investment moderates the CRI-performance relationship	Positive moderation	Significant
H7	Regulatory compliance moderates the CRI-performance relationship	Positive moderation	Significant

7.12 Reduced Negative Impact of Cybersecurity Risk

In general, the illustrative results support a consistent conclusion: that the higher the cybersecurity risk the poorer the financial performance of the FinTech companies. The negative values of the coefficients of ROA, ROE, revenue growth, net profit margin and Tobin's Q indicate that cyber risks can impact the internal financial efficiency and external market valuation. These negative effects can be mitigated, in part, by investments in cybersecurity and regulatory compliance, the moderation results show. The results of these findings align with the conceptual model proposed (CTC), in which cybersecurity is approached as a financial risk rather than a problem related to the technology.

7.13 Managerial and Regulatory Implications

The results indicate that cybersecurity needs to be seen as a strategic financial investment, and not just as an information-technology role in FinTech companies. Managers should continually monitor the Cybersecurity Risk Index (CRI), boost cyber

security infrastructure, perform frequent vulnerability assessments, put in place incident-response plans, and provide sufficient resources for cyber security investments. The addition of cybersecurity indicators to enterprise risk-management and financial planning can mitigate potential losses, operations disruption, reputational impact and loss of customers. On the regulatory side, financial institutions should have common reporting standards regarding the frequency of attacks, the severity of attacks, the financial impact of attacks, and disruption of systems as a result of an attack. Regulators should also facilitate transparency in incident disclosures, set minimum security standards, independent security audits, compliance with data-protection standards, and tests of resilience. A common cybersecurity framework of CRI could enable regulators and investors to benchmark the cyber exposure level of different FinTech firms and bolster the overall digital-financial-system resilience.

10 Conclusion, Limitations and Future Scope

10.1 Summary of Major Findings

This study investigated the cybersecurity risk–financial performance relationship of FinTech companies, based on a panel data analysis. The results suggest that the ROA, ROE, revenue growth, profit margin and valuation of the firm are negatively related to cybersecurity risk. The Cybersecurity Risk Index (CRI) proposed score, which combines attack frequency, breach severity, financial losses, and system disruptions gives a multi-dimensional measure of cyber exposure for a firm.

10.2 Theoretical Contributions

The research expands the study of cybersecurity risks by connecting cybersecurity risk with financial performance of the companies. It views cybersecurity as a strategic business risk as opposed to just an operational or technical issue and creates an integrated approach to bridging cyber exposure, organizational resilience and financial impact.

10.3 Practical Contributions

The findings highlight the need for proactive monitoring of cyber risks, investment in cybersecurity, preparing for incidents, raising employee awareness, and robust digital infrastructures, especially for FinTech managers. The CRI can be used as an internal risk assessment and for strategic investment decisions.

10.4 Policy Contributions

The regulators can encourage cyber-incident reporting, cyber security audits, disclosure of breaches, minimum security requirements and resilience testing. There is a need to have a standardised risk index which will help make the investor and stakeholder more aware of the risk.

10.5 Research Limitations

The study may be limited by non-matching disclosures of cybersecurity events, inconsistent reporting, difficulties measuring events, and unintentionally left out variables. Data that is publicly available can also be an underestimate of unreported cyber incidents.

10.6 Future Research Directions

Future research can include industry-specific CRI measures, real-time cyber-threat intelligence, and larger samples across the globe, as well as AI-based risk indicators. Machine-learning methods and dynamic panel models might contribute to a better prediction and causal analysis.

10.7 Final Conclusion

The study concludes that in general, the risks of cybersecurity have significant financial implications for FinTech companies. The use of cybersecurity measurement in conjunction with financial analysis can enhance managerial decision-making, investor evaluation, regulatory controls and long-term digital-financial resilience.

References

- I. Lee and Y. J. Shin, "Fintech: Ecosystem, business models, investment decisions, and challenges," *Business Horizons*, vol. 61, no. 1, pp. 35–46, 2018.
- M. Gai, Q. Qiu, and X. Sun, "A survey on FinTech," *Journal of Network and Computer Applications*, vol. 103, pp. 262–273, 2018.
- D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," *Computers & Security*, vol. 241, Art. no. 122697, 2024. **Note:** The study was available as a 2023 preprint; the journal publication is 2024, so it should not be counted if your reference window is strictly 2014–2023.
- M. Riskiyadi, A. Anggono, and Tarjo, "Cybercrime dan cybersecurity pada Fintech: Sebuah tinjauan pustaka sistematis," *Jurnal Manajemen dan Organisasi*, vol. 12, no. 3, pp. 239–251, 2021.

-
- J. K. Deane, D. M. Goldberg, T. R. Rakes, and L. P. Rees, "The effect of information security certification announcements on the market value of the firm," *Information Technology and Management*, vol. 20, no. 3, pp. 107–121, 2019.
- O. K. Tosun, "Cyber-attacks and stock market activity," *International Review of Financial Analysis*, vol. 76, Art. no. 101795, 2021.
- M. McShane and T. Nguyen, "Time-varying effects of cyberattacks on firm value," *Global Policy and Practice*, vol. 45, no. 4, 2020.
- S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, vol. 139, no. 3, pp. 719–749, 2021.
- J. Peng, H. Zhang, J. Mao, and S. Xu, "Repeated data breaches and firm value," *Economics Letters*, vol. 224, Art. no. 111001, 2023.
- J. Jin, N. Li, S. Liu, and S. M. Khalid Nainar, "Cyber attacks, discretionary loan loss provisions, and banks' earnings management," *Finance Research Letters*, vol. 54, 2023.
- A. S. E. Ali, F.-W. Lai, P. D. D. Dominic, N. J. Brown, P. B. Lowry, and R. F. Ali, "Stock market reactions to favorable and unfavorable information security events: A systematic literature review," *Computers & Security*, vol. 110, Art. no. 102451, 2021.
- S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, vol. 139, no. 3, pp. 719–749, 2021, doi: 10.1016/j.jfineco.2019.05.019.
- O. K. Tosun, "Cyber-attacks and stock market activity," *International Review of Financial Analysis*, vol. 76, Art. no. 101795, 2021, doi: 10.1016/j.irfa.2021.101795.
- H. E. Wang, Q. E. Wang, and W. Wu, "Short selling surrounding data breach announcements," *Finance Research Letters*, vol. 47, Part B, Art. no. 102690, 2022, doi: 10.1016/j.frl.2022.102690.
- C. Florackis, C. Louca, R. Michaely, and M. Weber, "Cybersecurity risk," *The Review of Financial Studies*, vol. 36, no. 1, pp. 351–407, 2023, doi: 10.1093/rfs/hhac024.
- J. Peng, H. Zhang, J. Mao, and S. Xu, "Repeated data breaches and firm value," *Economics Letters*, vol. 224, Art. no. 111001, 2023, doi: 10.1016/j.econlet.2023.111001.
- D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," *Expert Systems with Applications*, vol. 241, Art. no. 122697, 2024, doi: 10.1016/j.eswa.2023.122697.
- J. A. Jafri, S. I. M. Amin, A. H. A. Rahman, and S. M. Nor, "A systematic literature review of the role of trust and security on Fintech adoption in banking," *Heliyon*, vol. 10, no. 1, Art. no. e22980, 2024, doi: 10.1016/j.heliyon.2023.e22980.
- O. A. Adekoya, H. F. Atlam, and H. S. Lallie, "Quantifying the multidimensional impact of cyber attacks in digital financial services: A systematic literature review," *Sensors*, vol. 25, no. 14, Art. no. 4345, 2025, doi: 10.3390/s25144345.
- F. Amani, M. Magnan, and R. Moldovan, "Cybersecurity risks and incidents disclosure: A literature review," *Accounting Perspectives*, vol. 24, no. 3, pp. 605–667, 2025, doi: 10.1111/1911-3838.12411.
- G. Xu, Y. Li, S. Liu, and Z. Ye, "Cybersecurity risk and firm growth: Empirical evidence based on text analysis," *The North American Journal of Economics and Finance*, vol. 81, Art. no. 102542, 2026, doi: 10.1016/j.najef.2025.102542.
- G. Anil Kumar, V. Mittapalli, N. Chandra Sekhar Reddy, P. Nalajala, and A. Dasore, "Assessment of the Future of FinTech in Developing Economies: Automated and Enhanced Functional Challenges," *AIP Conference Proceedings*, vol. 3342, Art. no. 030015, 2025, doi: 10.1063/5.0300368. Npr& Bhavana Citations
- V. Annapurna, Y. K. Kumar, S. V., S. S. Kumar, T. L. Gudipalli, and B. Godavarthi, "Secure Homomorphic Encryption Approach for Privacy-Preserving Data Processing in Cloud Environments," *2026 13th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2026, pp. 1–6, doi: 10.23919/INDIACom70271.2026.11526058
-