



Cybersecurity risk and bank risk-taking

Zunaidah Sulong^{a,*}, Md. Habibur Rahman Fuszder^a, Mohammad Abdullah^{b,*},
Emmanuel Joel Aikins Abakah^{c,d}

^a Faculty of Business and Management, Universiti Sultan Zainal Abidin, Terengganu, Malaysia

^b TIFIES Research Group and Southampton Malaysia Business School, University of Southampton Malaysia, Iskandar Puteri, Johor, 79100, Malaysia

^c Department of Finance, University of Ghana Business School, Accra, Ghana

^d School of Construction Economics and Management, the University of the Witwatersrand, Johannesburg, South Africa

ARTICLE INFO

Keywords:

Cybersecurity risk
Bank risk-taking
Goodwill
Bank competition
Bank run

ABSTRACT

This paper investigates the influence of cybersecurity risk on banks' risk-taking behavior. Utilizing data from U.S. banks spanning 1998–2018, we find that heightened cybersecurity risk is associated with increased risk-taking by banks. These findings remain robust across various alternative proxies and persist even after addressing endogeneity issues. Further analysis indicates that this positive relationship is more pronounced among banks facing greater competitive pressure, higher IT investment, increased deposit withdrawals, and more negative disclosure sentiment. Conversely, the relationship is attenuated in banks with substantial goodwill and a more positive disclosure tone. Sub-sample analyses show that the effect is particularly strong for smaller banks and those with elevated financial vulnerability. These findings have important implications for the digital transformation of the banking sector.

1. Introduction

In recent years, the banking sector has witnessed an unprecedented surge in cybersecurity threats, coinciding with rapid digitalization and an increase in online financial transactions. Recent statistics by IMF¹ indicates a significant rise in cyber threats, particularly since the COVID-19 pandemic, with cyberattacks more than doubling. The financial sector is especially vulnerable due to its handling of sensitive data, with attacks on financial institutions representing nearly 20% of all incidents. The financial impact of severe cyber incidents has quadrupled since 2017 to \$2.5 billion, compounded by indirect costs like reputational damage and costly security upgrades. Additionally, smaller U.S. banks have seen modest but persistent deposit outflows following cyberattacks, raising concerns about the potential systemic effects on financial stability. This trend has raised significant concerns regarding the impact of cybersecurity risks on bank behavior, particularly in terms of risk-taking (Zhang et al., 2024).

Earlier studies highlighted significant concerns regarding the stability of the financial system due to the rising frequency and impact of cyberattacks. Eisenbach et al. (2022) underline that an attack on major

banks could disrupt around 31% of the U.S. wholesale payments network, severely affecting liquidity and economic output. Bounou (2023) emphasizes the negative effects on bank operations, leading to reduced deposits and credit supply. Crosignani et al. (2023) illustrate the spilling supply chain impacts from cyber incidents, exacerbating profit losses. Additionally, studies by Rodrigues et al. (2022) and Jin et al. (2023) explore the relationship between cybersecurity strategies, bank reputations, and financial reporting. Tian et al. (2023) note the implications of emerging cybersecurity risks for central bank digital currencies (CBDCs), while Carboni et al. (2024) find that traditional banks face less severe market reactions to cyber enforcement actions compared to fintech entities. Gatzert and Schubert (2022) highlight a growing awareness of cyber risks within banking, and Peihani (2022) suggests for a more resilient regulatory approach to cyber risk governance. Heo (2024) examined how cybersecurity risk is associated with bank fragility. However, research on the relationship between cybersecurity risk and bank risk taking remains unexplored.

Theoretically, cybersecurity risk influences bank risk-taking through multiple interconnected mechanisms. Cyber threats introduce a unique layer of uncertainty that affects banks' strategic behavior by increasing

* Corresponding authors.

E-mail addresses: zunaidah@unisza.edu.my (Z. Sulong), si4784@putra.unisza.edu.my (Md.H.R. Fuszder), M.Abdullah@soton.ac.uk (M. Abdullah), ejaabakah@ug.edu.gh (E.J.A. Abakah).

¹ Source: <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024>.

financial pressures, intensifying competition, and altering managerial decision-making. Faced with the threat of cyberattacks, banks often respond with significant investments in cybersecurity infrastructure, which, when excessive, may strain profitability and inadvertently push institutions toward riskier investments to recover losses or signal resilience (Uddin et al., 2020). Additionally, as cyber incidents threaten service continuity and customer trust, banks may engage in aggressive competitive strategies, thereby increasing their risk appetite to retain or expand market share (Bushman et al., 2016; Wang et al., 2024a). From a behavioral and governance standpoint, agency theory suggests that under rising cybersecurity pressure, managers may prioritize short-term gains or reputational signaling, especially when protected by advanced security systems, potentially leading to moral hazard and riskier operational decisions (Jensen and Meckling, 1979).

There is an extensive and diverse body of literature examining the determinants of bank risk-taking, with studies focusing on both external pressures and internal characteristics. External environmental factors, such as pollution, have been shown to influence risk behaviors; for instance, Pan et al. (2024) explore find that deteriorating air quality can increase bank risk-taking. In contrast, studies like Wang et al. (2024b) highlight the role of internal factors, such as interbank connectedness, in shaping banks' risk exposures. Other scholars emphasize governance and institutional dynamics, i.e., Heyert and Weill (2024) examine how public trust affects risk appetite, while Ibrahim and Rizvi (2018) explore how ownership structure moderates risk behavior. The competitive landscape and regulatory context are also key determinants, Wu et al. (2019) and Matabaro Borauzima and Muller (2023) find that market power and competition significantly influence banks' risk strategies. Furthermore, literature underscores the influence of governance and managerial incentives on risk-taking (Bushman et al., 2016; Dell'Araccia et al., 2017; Houston et al., 2010), who link board structure and regulatory frameworks to variations in risk levels. However, while these studies provide valuable insights into the broad determinants of bank risk-taking, only a few have explored the role of cybersecurity risk, which has become a rapidly emerging threat in the digital banking era.

In light of the increasing cybersecurity risks faced by banks and existing gaps in the literature, this study aims to investigate the relationship between cybersecurity risk and bank risk-taking. Our empirical analysis utilizes a comprehensive dataset comprising 9783 bank-year observations from the United States covering the period from 1998 to 2018. We employ a novel dataset of cybersecurity risk, as proposed by Lattanzio and Ma (2023), to proxy bank-level cybersecurity risk. Our baseline analysis reveals a significant and positive relationship between elevated cybersecurity risk and increased bank risk-taking behavior. To ensure that this finding is not driven by endogeneity, we apply a comprehensive set of robustness checks, including Two-Stage Least Squares (2SLS), two-step system GMM, staggered Differences-in-Differences (DiD), Impact Threshold of a Confounding Variable (ITCV), Propensity Score Matching (PSM), and Entropy Balancing (EB). The consistency of results across these methodologies confirms the validity of our main conclusion. Furthermore, the association remains robust when alternative measures of cybersecurity risk and bank risk-taking are employed, strengthening the credibility of our findings.

We also identify several important moderating factors that shape the strength of this relationship. Specifically, the effect of cybersecurity risk on bank risk-taking is more pronounced among banks operating in highly competitive environments. Sentiment in risk disclosures plays a crucial role, with positive sentiment tempering the impact and negative sentiment heightening it. Banks with higher IT investments exhibit a stronger link, potentially due to overconfidence in technological infrastructure. Conversely, banks with higher goodwill show a weaker association, suggesting that reputational capital may buffer against cybersecurity-induced risk-taking. This relationship is also more intense for banks experiencing high deposit withdrawals, reflecting greater vulnerability during periods of distress. Sub-sample analyses

further highlight that the effect is amplified in banks with higher cash flow volatility, more nonperforming loans, lower earnings per share, smaller size, and lower advertisement intensity, conditions indicative of financial fragility and limited market presence.

Our study makes several important contributions to the growing literature at the intersection of cybersecurity and financial risk. First, to the best of our knowledge, this is among the first empirical investigations to establish a direct link between cybersecurity risk and bank risk-taking behavior. While prior research has extensively explored the determinants of bank risk-taking (Ibrahim and Rizvi, 2018; Matabaro Borauzima and Muller, 2023; Pan et al., 2024; Wang et al., 2024b) and the broader implications of cybersecurity (Carboni et al., 2024; Crosignani et al., 2023; Eisenbach et al., 2022), our study uniquely integrates these domains. Second, we extend the arguments of earlier research that has explored the relationship between cybersecurity risk and bank fragility, firm innovation, and asset premiums (Florackis et al., 2023; Heo, 2024; Jiang et al., 2024; Lattanzio and Ma, 2023; Wang et al., 2024a).

In addition to enriching theoretical perspectives, our study provides valuable practical insights into how internal and external factors shape the cybersecurity and risk-taking nexus in banking. Through extensive analysis, we uncover several key moderating channels such as bank competition, disclosure sentiment, IT investment intensity, and goodwill that influence the strength and direction of the observed relationship. We also identify that the association is more pronounced in banks facing higher deposit withdrawals, pointing to increased vulnerability during periods of depositor uncertainty. Moreover, sub-sample analysis reveals that bank characteristics such as size, cash flow volatility, earnings performance, and advertising intensity play a critical role in conditioning the effect of cybersecurity risk. These findings offer actionable guidance for regulators and bank managers in designing tailored strategies that mitigate excessive risk-taking while enhancing cyber-resilience in an era where financial systems are increasingly exposed to digital threats.

The paper is organized as follows: The hypothesis is developed in Section 2. Our sample and variable measurements are described in Section 3. Results of the empirical study are presented in Section 4 and Section 5 concludes.

2. Literature review

There are several studies in the financial economics literature on the determinants of bank risk taking. The rise of FinTech, comprising developments like big data, artificial intelligence, blockchain, and cloud services, has significantly reshaped banking operations and risk profiles. Early-stage FinTech adoption often raises bank risk-taking, particularly among large, less efficient banks reliant on interest income. Over time, this relationship evolves into a U-shaped dynamic, where advanced FinTech maturity begins to mitigate risk (Wang et al., 2021). While Elekdag et al. (2025) found that FinTech expansion typically raises risk via its influence on financial intermediaries, their findings also acknowledge exceptions in jurisdictions with stronger institutional frameworks.

Other studies explore how specific banking characteristics affect this relationship. For instance, FinTech's risk-reducing effects are more pronounced in state-owned and smaller banks, or those with a larger share of non-interest income (He et al., 2023). Jia (2024) highlights how deepening FinTech adoption erodes the value of traditional bank charters, influencing long-term risk behavior. Another study by Uddin et al. (2020) found that excessive investment in technological infrastructure can increase bank risk taking. Specifically, once technological infrastructure spending surpasses a certain threshold, banks tend to assume disproportionately higher risks relative to the additional investment, ultimately undermining their overall stability.

A related stream of research investigates institutional and governance factors that shape risk attitudes. Ownership structure and internal

governance mechanisms play a significant role. Banks with greater shareholder power or influential independent directors often pursue more aggressive risk strategies (Amin et al., 2024; Laeven and Levine, 2009). Meanwhile, studies like those by Kutubi et al. (2018) emphasize how directors' workload can either constrain or amplify risk-taking, showing a U-shaped relation with bank performance. Macro- and micro-level policy environments also influence risk behavior. Financial liberalization and market openness affect risk differently depending on institutional development (Bui and Bui, 2019), while monetary policy and regulatory buffers like capital requirements can modulate bank behavior (Tran and Nguyen, 2025).

Other determinants of risk-taking behavior include competitive pressure, bank efficiency, and structural factors such as homogeneity. For example, higher cost efficiency can buffer the impact of competitive risk (Fang et al., 2019), while homogeneity among banks tends to elevate risk exposure across the system (Ren et al., 2023). Ownership concentration, particularly during relaxed capital standards, is also negatively linked to credit and liquidity risks (Agusman et al., 2014). Environmental and financial inclusion dimensions have recently been incorporated into the literature. Song et al. (2025) revealed a nonlinear effect of green credit on risk-taking, where small-scale green credit increases risk, while large-scale adoption mitigates it. Similarly, financial inclusion via FinTech enhances both risk control and mobility in developing regions (Banna et al., 2021). Lastly, foreign equity participation and corporate governance reforms have shown potential to curb excessive risk, with outcomes depending on ownership structure and the extent of foreign involvement (Nguyen, 2024).

2.1. Hypothesis development

Cybersecurity risk, unlike traditional forms of operational or credit risk, introduces a dynamic and often unpredictable layer of vulnerability to banks, which can alter strategic behavior in several nuanced ways. Rather than being merely another manifestation of general riskiness, cybersecurity threats can directly shape decision-making within banks through distinct channels such as increased cost burdens, competitive pressures, and behavioral responses to perceived threats. One key mechanism through which cybersecurity risk may influence bank risk-taking is through its financial implications. Cyber incidents can lead to direct financial losses, reputational damage, and regulatory penalties. To prevent such outcomes, banks often invest heavily in cybersecurity infrastructure. However, excessive IT infrastructure spending, particularly when it exceeds optimal levels, can negatively impact bank stability, as shown by Uddin et al. (2020), who find that banks tend to take on disproportionately higher risks with every additional dollar spent beyond a threshold. Faced with rising costs and shrinking margins, banks may be incentivized to pursue higher-yield, and inherently riskier, investments in an attempt to recover lost profitability or signal market resilience. While not always rational from a risk-adjusted return perspective, such behavior can reflect the pressure to deliver consistent performance amid rising operational expenditures and cyber-related uncertainty.

Another important channel is the behavioral response to operational uncertainty. As cybersecurity threats increasingly disrupt digital banking operations and erode consumer trust, banks may adopt aggressive strategies to protect or regain market share. The perceived need to demonstrate resilience and innovation under threat conditions can lead to a higher tolerance for risk, especially in product offerings, lending practices, or investment portfolios. This aligns with findings from Bushman et al. (2016) and Wang et al. (2024a), who highlight that heightened competitive pressures, which often intensified during periods of technological transition or crisis and encourage risk-taking as banks strive to outperform rivals and retain customers. In a cyber-threatened environment, competition may not only be for profitability but also for perceived robustness in digital capability, which could further motivate risk-laden strategic decisions.

Moreover, from a governance perspective, agency theory offers additional insight into how cybersecurity risk interacts with managerial behavior. According to Jensen and Meckling (1979), agents (i.e., bank managers) may prioritize short-term performance or personal objectives over long-term shareholder value. When confronted with increasing cybersecurity threats, managers might opt for riskier decisions to signal effectiveness or achieve short-term recovery, particularly if compensation structures or market expectations reward such outcomes. This is further complicated by the concept of moral hazard, when banks invest heavily in protective measures, such as advanced cybersecurity systems, they may develop a false sense of security and engage in riskier behavior under the belief that they are shielded from the consequences of failure (Jensen and Meckling, 1979). This behavioral shift may mirror findings in other domains, such as Houston et al. (2010), where stronger external protections, such as creditor rights, were associated with higher internal risk-taking. Thus, considering above arguments we conjecture that the increasing cybersecurity risks faced by banks may lead them to engage in higher risk-taking activities as they navigate and adapt to this evolving threat landscape and our hypothesis is:

H1: Cybersecurity risk increases bank risk-taking.

3. Model and data

3.1. Dependent variable: bank risk-taking

Following extant literature of bank risk-taking (Abakah and Li, 2023; Ashraf, 2017; Dalwai et al., 2022; Heyert and Weill, 2024; Houston et al., 2010; Khan et al., 2017; Pozo, 2023), we employ five proxies to measure bank risk-taking. First, we use the ratio of Risk-Weighted Assets (RWA), which scales a bank's regulatory capital by its risk-weighted assets. This metric reflects the capital adequacy and the risk profile of the bank's asset base. Second, we consider the Nonperforming Loans (NPL) ratio, which is the proportion of nonperforming loans to gross loans, indicating the quality of the bank's loan portfolio and its exposure to credit risk. Third, we use the three-year standard deviation of Return on Assets (ROA_SD), capturing the volatility of the bank's profitability over a medium-term period, thus providing insight into earnings stability. Fourth, we compute the Z-score, which is a composite measure of bank stability. The Z-score is calculated by taking the sum of the capital-to-assets ratio (CAR) and the return on assets (ROA), dividing the result by the standard deviation of ROA, taking the natural logarithm and then multiplying it by -1 . It is expressed as:

$$ZSCORE_{i,t} = (-1) \times \ln\left(\frac{CAR_{i,t} + ROA_{i,t}}{ROA_{volatility_{i,t}}}\right) \quad (1)$$

Lastly, we use default probability (DEFAULT) to proxy bank risk taking measured by Bloomberg (Bondioli et al., 2021). The Bloomberg estimates default probability using a hybrid approach that combines logistic regression with structural modeling. Unlike traditional Z-score models, it directly outputs default probabilities by incorporating real-time market data such as stock volatility, market capitalization, and debt levels.

3.2. Independent variable: cybersecurity risk

We use 10-K base proxy of cybersecurity risk proposed by Lattanzio and Ma (2023) (denoted as CYBER_LM). Lattanzio and Ma (2023) constructed this measure by developing a comprehensive dictionary (Gordon et al., 2010). They selected only those phrases that could be clearly attributed to cybersecurity, distinguishing their approach from (Berkman et al., 2018) by excluding words from a Congressional Research Service report on cybersecurity laws described in study by Fisher (2016). To avoid duplicate matches, they included phrases like

"system security," which would also capture more specific terms such as "computer system security" from Gordon et al. (2010). The short-listed dictionary is weighted using an algorithm from Loughran and McDonald (2011)². This algorithm assigns a weight to each term based on its frequency and commonality, using the formula:

$$w_{ij} = \begin{cases} \frac{(1 + \log(tf_{ij}))}{(1 + \log(\alpha_j))} \log \frac{N}{df_i} & \text{if } tf_{ij} \geq 1 \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

where, w_{ij} denotes the measured weight in term i for j^{th} document and total number of documents is denoted by N and df_i the quantity of documents where the term i appears at least once. The raw word count in the j^{th} document is shown by tf_{ij} , whereas the average word count in the document is indicated by α_j . This approach balances high frequency terms and corrects for term commonality, with the natural logarithm of the weighted word count serving as the baseline cybersecurity score, mitigating the impact of outliers. See study by Lattanzio and Ma (2023) for detailed methodology of CYBER_LM.

We also use two other proxies for robustness test. Our first robustness cybersecurity risk variable is proposed by Florackis et al. (2023) denoted as CYBER_FLMW. Florackis et al. (2023) developed CYBER_FLMW using textual information from the "Item 1 A Risk Factors" section of 10-K reports. This measure assesses the similarity of a firm's cybersecurity risk disclosure to past disclosures from a training sample of firms. Our second robustness test variable is firm-level measure of cyber risk (CYBER_JKYZ hereafter) proposed by Jiang et al. (2024). They employed machine learning algorithms to develop real-time estimates of the likelihood that individual firms will experience cyberattacks in subsequent periods.

3.3. Control variables

We include several control variables in our analysis based on earlier literature (Abakah and Li, 2023; Ashraf, 2017; Dalwai et al., 2022; Delis and Kouretas, 2011; Heyert and Weill, 2024; Houston et al., 2010; Khan et al., 2017; Pozo, 2023; Ren et al., 2023; Zhao et al., 2023). Bank age (AGE) and size (SIZE), both expressed in natural logarithms, capture institutional maturity and market presence, respectively. Operating performance is controlled through cash flow scaled by total assets (CASH_FLOW) and operating efficiency (OE), while the dividend payout ratio (DPR) reflects management's risk preference and confidence in future earnings. Asset growth (AG) accounts for expansion dynamics, and non-interest income as a share of total income (NNID) helps differentiate between traditional and diversified income sources. An acquisition dummy (ACQ) is included to capture the effects of strategic growth via mergers or acquisitions. Capital adequacy ratio (CAR) controls for solvency strength, while total loans to total deposits (LDR) indicates lending aggressiveness. Net interest margin (NIM) reflects core profitability, and loan loss provisions relative to total loans (LLP) serve as a proxy for credit risk management practices.

3.4. Data and sample

To construct our dataset, we begin by collecting data from the US Compustat Bank Fundamentals database. We then gather data for CYBER_LM and other cyber risk measures. After merging these datasets and removing observations with missing data, our baseline dataset comprises 9783 bank-year observations. Specifically, the CYBER_FLMW and CYBER_JKYZ measures include 4674 and 3651 bank-year observations, respectively. The dataset spans the period from 1998–2018,

chosen based on the availability of CYBER_LM data. To treat outliers, we winsorize our variables at the 1 % and 99 % levels. Detailed descriptions of the variables and their sources are provided in Table A.1.

Descriptive statistics and yearly distribution of the sample are presented in Table 1. The mean NPL is 1.20 % with a standard deviation of 1.30 %, indicating relatively low but slightly dispersed credit risk across the sample. The RWA stand at 11.89, with a standard deviation of approximately 2.99, reflecting variation in the capital intensity and risk exposure of different banks. The ROA_SD has a mean of 0.003 and a low standard deviation of 0.004, suggesting moderate variation in earnings stability. The Z-score, has a mean value of -4.15 with a standard deviation of 1.10. The mean value of DEFAULT is 4.02, with a standard deviation of 2.30, suggesting notable heterogeneity in credit risk across banks. For cybersecurity risk variables, CYBER_LM has a relatively low mean of 0.060 with a standard deviation of 0.048, indicating modest but varied levels of reported cyber exposure. The alternative proxies, CYBER_FLMW and CYBER_JKYZ have higher means of 0.287 and 0.464 respectively, with CYBER_JKYZ showing relatively less dispersion (standard deviation of 0.085). Table A.2 presents the results of the correlation analysis and the VIF result indicates there is no multicollinearity issue.

Table 1
Summary statistics.

Panel A: Descriptive statistics					
Variable	Obs	Mean	Std. dev.	Min	Max
NPL	10,382	0.012	0.013	0.001	0.048
RWA	10,401	11.886	2.991	7.110	18.460
ROA_SD	10,403	0.003	0.004	0.000	0.014
ZSCORE	10,285	-4.154	1.104	-5.981	-1.812
DEFAULT	3709	4.016	2.304	-0.327	29.511
CYBER_LM	9913	0.060	0.048	0.000	0.177
CYBER_FLMW	4744	0.287	0.227	0.000	0.684
CYBER_JKYZ	3720	0.464	0.085	0.215	0.964
AGE	10,407	2.529	0.545	1.386	3.466
SIZE	10,407	7.435	1.310	5.649	10.399
CASH_FLOW	10,407	0.009	0.008	-0.001	0.024
DPR	10,407	0.307	0.252	0.000	0.876
AG	10,407	0.087	0.106	-0.070	0.352
NNID	10,407	0.163	0.134	0.000	0.429
ACQ	10,407	0.380	0.485	0.000	1.000
CAR	10,407	14.627	3.480	10.500	23.960
OE	10,407	0.824	0.132	0.633	1.176
LDR	10,407	0.894	0.164	0.589	1.229
NIM	10,407	3.729	0.694	2.490	5.170
LLP	10,407	0.498	0.621	0.007	2.406
Panel B: Yearly sample distribution					
Year	Freq.	Percent	Year	CYBER_LM	
1998	448	4.300	11.471	0.037	
1999	501	4.810	11.188	0.030	
2000	547	5.260	11.067	0.028	
2001	516	4.960	10.967	0.030	
2002	520	5.000	11.118	0.029	
2003	491	4.720	11.540	0.032	
2004	460	4.420	11.682	0.031	
2005	517	4.970	11.330	0.049	
2006	549	5.280	11.287	0.051	
2007	571	5.490	10.954	0.052	
2008	577	5.540	11.059	0.057	
2009	555	5.330	11.516	0.062	
2010	537	5.160	12.414	0.064	
2011	532	5.110	12.956	0.071	
2012	514	4.940	13.214	0.078	
2013	493	4.740	13.318	0.085	
2014	483	4.640	13.177	0.098	
2015	457	4.390	12.686	0.107	
2016	435	4.180	12.493	0.111	
2017	414	3.980	12.529	0.118	
2018	290	2.790	12.544	0.114	

Note: Table A.1 provides descriptions for all variables. The imbalanced panel dataset causes variations in the number of observations across variables.

² List of keywords and dictionary is presented in study by Lattanzio and Ma (2023).

3.5. Regression model

To examine the effect of cybersecurity risk on bank risk-taking, the following regression model is employed:

$$Y_{i,t} = \alpha + \beta_1 \times \text{CYBER}_{i,t} + \beta \text{Bank-level Controls}_{i,t} + \text{YearFE} + \text{BankFE} + \varepsilon_{i,t} \quad (3)$$

here, t stand for year and i for bank. The dependent variables NPL, RWA, ROA_SD, ZSCORE, and DEFAULT are denoted with $Y_{i,t}$. $\text{CYBER}_{i,t}$ denotes bank level cyber risk proxied by CYBER_LM, CYBER_FLMW, and CYBER_JKYZ. $\beta \text{Bank-level Controls}_{i,t}$ denotes bank level control variables. The impacts of unobserved temporal and bank factors are captured by YearFE and BankFE. The error term denoted as $\varepsilon_{i,t}$ captures the unexplained variations in the model.

4. Results and discussions

4.1. Baseline analysis results

Table 2 presents result for baseline analysis. Models 1 and 3 represent bivariate models, where RWA and NPL serve as dependent variables, with CYBER_LM as the independent variable. In contrast, Models 2 and 4 are multivariate models that incorporate bank-level control variables. Across all models, the results consistently indicate a positive and statistically significant association between CYBER_LM and the

Table 2
Baseline model results.

	(1)	(2)	(3)	(4)
VARIABLES	RWA	RWA	NPL	NPL
CYBER_LM	6.395*** (0.572)	1.954*** (0.361)	0.032*** (0.003)	0.006*** (0.001)
AGE		0.250*** (0.059)		0.006*** (0.000)
SIZE		−0.061 (0.045)		0.000 (0.000)
CASH_FLOW		4.268** (1.998)		0.049*** (0.013)
DPR		0.157** (0.063)		−0.004*** (0.000)
AG		−0.330** (0.129)		−0.012*** (0.001)
NNID		0.067 (0.168)		0.001 (0.001)
ACQ		−0.196*** (0.037)		−0.001*** (0.000)
CAR		0.751*** (0.005)		0.000*** (0.000)
OE		−0.617*** (0.179)		0.026*** (0.001)
LDR		−0.308** (0.122)		−0.009*** (0.001)
NIM		0.277*** (0.032)		0.000 (0.000)
LLP		−0.142*** (0.032)		0.008*** (0.000)
Constant	11.492*** (0.040)	0.460 (0.419)	0.010*** (0.000)	−0.026*** (0.003)
Observations	9783	9783	9764	9764
R-squared	0.597	0.891	0.388	0.754
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES

Note: Results analyzing the relationship between cybersecurity risk and bank risk-taking are displayed in this table. RWA is the dependent variable in Models 1 and 2, while NPL is used in Models 3 and 4. CYBER_LM is the independent variable in all of the models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. Level of significance is denoted by *** at 1 %, ** at 5 %, and * at 10 %.

measures of bank risk-taking. This result shows, for instance, in Model 2, a one standard deviation increase in CYBER_LM is associated with a 0.789 % increase in RWA.³ Moreover, a 1 % increase in CYBER_LM leads to a 16.44 % (=1.954/11.886) increase in RWA relative to the mean, indicating its economic significance. These findings support our hypothesis, suggesting that increased cybersecurity risk leads to heightened bank risk-taking behaviors.

This result can be attributed to several interconnected factors, including heightened exposure to cyber threats, the rising costs associated with maintaining cybersecurity measures to meet regulatory scrutiny, and intensified competition within the banking sector. As banks operate an environment fraught with cyber vulnerabilities, they may feel compelled to adopt riskier strategies to maintain profitability and market share, thereby exacerbating their exposure to potential financial instability. This finding is consistent with earlier studies that have documented the detrimental impact of cybersecurity risk on banking behavior, linking it to various dimensions of bank fragility, competition, and overall risk management (Liu et al., 2024; Pan et al., 2024; Wang et al., 2024a).

4.2. Endogeneity concerns

To address potential endogeneity concerns in our analysis, we employ a range of robust econometric techniques. Specifically, we use Two-Stage Least Squares (2SLS) with an instrumental variable to mitigate reverse causality and omitted variable bias. Additionally, we implement the two-step system Generalized Method of Moments (GMM), which controls for dynamic endogeneity and unobserved heterogeneity in panel data. To capture causal effects in the presence of staggered treatment timing, we apply a Staggered Differences-in-Differences (DiD) approach. Furthermore, we assess the sensitivity of our results to potential omitted confounders using the Impact Threshold of a Confounding Variable (ITCV). To ensure comparability between treated and control groups, we also employ Propensity Score Matching (PSM) and Entropy Balancing (EB), which reweight the sample to balance observed covariates. Collectively, these methods strengthen the credibility of our findings by addressing various sources of endogeneity.

4.2.1. Instrumental variable regression

To begin with, we implement the Two-Stage Least Squares (2SLS) method, which helps mitigate endogeneity arising from potential reverse causality, omitted variable bias, or measurement error. In the context of our study, endogeneity may occur if unobserved factors simultaneously influence both cybersecurity risk and bank risk-taking, biasing the estimated relationship. 2SLS addresses this by using an instrumental variable (IV) that is correlated with the potentially endogenous regressor (relevance condition) but uncorrelated with the error term in the main regression equation (exclusion restriction). We use the global share of science, technology, engineering, and mathematics (STEM) bachelor graduates as an instrumental variable to address endogeneity. Prior studies suggest that advancements in cybersecurity frameworks and the occurrence of cyber incidents are closely linked to the availability of STEM-educated professionals, indicating a strong relevance between STEM education and cybersecurity capacity (Dutta and Mathur, 2012; LeClair et al., 2014). However, there is no empirical evidence to suggest that the global share of STEM graduates directly influences individual bank-level risk-taking behavior, thereby satisfying the exclusion restriction.

Furthermore, following Hoang (2025), we consider the annual average cybersecurity risk scores by state for non-financial firms

³ Calculated as 0.789 % = (1.954 × 0.048)/11.886.

(CYBER_STATE) as our second instrumental variable.⁴ This variable meets the relevance condition, as cybersecurity risk within a state's broader corporate environment can influence the cybersecurity landscape in which banks operate, thereby affecting banks' exposure to cybersecurity threats. Regions with higher cyber risk among non-financial firms are likely to reflect a weaker cybersecurity infrastructure or greater digital vulnerability, which could influence banks' own cybersecurity risk. At the same time, this instrument satisfies the exclusion restriction, as there is no clear theoretical or empirical reason to believe that cybersecurity risk scores of non-financial firms in a given state directly affect an individual bank's risk-taking behavior, independent of the bank's own cybersecurity exposure. Thus, it serves as a valid instrument to help isolate the causal effect of cybersecurity risk on bank risk-taking.

Table 3 presents the results of our instrumental variable regression analysis. In the first-stage regression, the instrumental variables, global STEM graduates and CYBER_STATE, show a positive and statistically significant association with CYBER_LM, confirming the relevance of the instruments. In the second-stage regression, the fitted values of CYBER_LM exhibit a statistically significant positive association with both RWA and NPL across all models, indicating that higher cybersecurity risk is associated with greater bank risk-taking. Furthermore, the diagnostic tests support the validity of the instruments. The Kleibergen-Paap rk LM statistic confirms that the models are not under identified, while the Kleibergen-Paap rk Wald F statistic exceeds the Stock-Yogo critical values, suggesting the instruments are not weak. Additionally, the Hansen J statistic indicates that the exclusion restriction is not violated. These findings collectively reinforce our baseline hypothesis that increasing cybersecurity risk contributes to elevated risk-taking behavior in banks.

4.2.2. Two-step system GMM results

In this section, we employ the two-step system GMM estimator to further address potential endogeneity concerns, particularly those arising from unobserved heterogeneity, simultaneity, and dynamic relationships. System GMM is well-suited for panel data settings with a short time dimension and large cross-sections, such as ours. It combines equations in levels and first differences, using internal instruments derived from the lagged values of the explanatory variables (Arellano and Bond, 1991; Blundell and Bond, 1998). By doing so, system GMM effectively controls for time-invariant unobserved effects and mitigates reverse causality by instrumenting endogenous variables with their past values.

Table 4 reports the findings from the Two-Step System GMM estimation. Across all models, the lagged dependent variables related to bank risk-taking are positive and statistically significant, suggesting a strong persistence in risk-taking behavior over time. The diagnostic checks, including the Arellano-Bond tests for first- and second-order serial correlation (AR(1) and AR(2)) and the Hansen test of instrument validity, indicate no concerns regarding instrument relevance or model misspecification. Notably, the coefficient for CYBER_LM remains negative and significant, lending further support to the hypothesis that elevated cybersecurity risk is linked to increased risk-taking by banks. These results confirm the consistency and reliability of our earlier conclusions.

4.2.3. Dynamic staggered DiD results

Following earlier study by Wang et al. (2024a), we employ dynamic staggered Difference-in-Differences (DiD) model. In our dynamic DiD approach, we leverage the staggered implementation of data breach notification laws across U.S. states, which required organizations to

inform individuals when their data had been compromised. These laws were adopted at different times across states (see Appendix Table A3), creating a quasi-natural experiment setting (Ashraf and Sunder, 2023; Boasiako and Keefe, 2021; Wang et al., 2024a). The introduction of such regulations is expected to prompt firms to strengthen their cybersecurity measures to avoid reputational harm and legal consequences, thereby reducing cybersecurity risk. In line with existing studies, we utilize this exogenous variation to evaluate the impact of reduced cybersecurity risk on bank risk-taking. We replace our main cybersecurity risk variable with a binary indicator, set to one if the state has enacted the law and zero otherwise, to measure this shift. To verify the parallel trends assumption, we conduct a dynamic DiD analysis by incorporating leads and lags of the law's implementation. As shown in Table 5, the insignificant coefficients in the pre-treatment periods suggest no systematic differences prior to the adoption, validating the identification strategy. Post-enactment, the results show a decline in cybersecurity risk and consistent effects across bank risk-taking variables, reinforcing our core finding that lower cybersecurity risk, prompted by regulatory changes, correlates with a reduction in bank risk-taking.

4.2.4. Impact threshold of a confounding variable (ITCV) results

To further address endogeneity concerns, we apply the Impact Threshold of a Confounding Variable (ITCV) method. ITCV helps assess the robustness of our estimated relationship by quantifying the strength a potential unobserved confounder would need to have with both the independent and dependent variables to invalidate our results (Busenbark et al., 2022; Lee et al., 2025). This approach provides a diagnostic tool to evaluate whether omitted variable bias is likely to be a serious threat. Table 6 presents the results from the ITCV analysis, which estimates the minimum required product of partial correlations between CYBER_LM and a potential unobserved confounder that could invalidate our findings. Specifically, for the observed relationship to be spurious, the correlation between CYBER_LM and any omitted variable would need to exceed thresholds of 0.189 in Model 1 and 0.079 in Model 2. However, the partial effects of all observed control variables fall below these critical values. This indicates that no single unmeasured factor is likely to exert a strong enough influence to undermine our results, thereby affirming the robustness of our main conclusions.

4.2.5. Propensity Score Matching and Entropy Balancing sample results

To further alleviate endogeneity concerns arising from sample selection bias, we apply Propensity Score Matching (PSM) and Entropy Balancing (EB) techniques. These methods aim to construct comparable treatment and control groups by balancing observed covariates. In our analysis, treatment status is defined based on the median split of the CYBER_LM variable, where observations with CYBER_LM above the median form the treatment group, and those below the median comprise the control group (Hainmueller, 2012; Rosenbaum and Rubin, 1983). PSM estimates the probability of receiving treatment given observed characteristics and matches similar units across groups, while EB directly reweights the control group to match the treatment group on key covariates, achieving balance without discarding observations. Table 7 presents the results from these matched samples. Consistent with our main findings, the positive link between cybersecurity risk and bank risk-taking holds even after adjusting for sample selection bias, underscoring the robustness of our conclusions.

4.3. Robustness test results

This section presents robustness checks using alternative measures for both cybersecurity risk and bank risk-taking to validate the stability of our findings. Table 8 summarizes these results. In Panel A, we replace our main bank risk-taking indicators with alternative proxies: ROA_SD, Z-SCORE, and DEFAULT. The results remain consistent with our primary analysis, demonstrating that higher cybersecurity risk is associated with elevated risk-taking behavior by banks. This consistency across different

⁴ We use the CYBER_LM measure proposed by Lattanzio and Ma (2023) to calculate CYBER_STATE, defined as the annual average cybersecurity risk score by state for non-financial firms.

Table 3
Instrumental variable approach results.

VARIABLES	(1) First Stage DV=CYBER_LM	(2) Second Stage DV=RWA	(3) Second Stage DV=NPL	(4) First Stage DV=CYBER_LM	(5) Second Stage DV=RWA	(6) Second Stage DV=NPL
STEM	0.018*** (0.002)					
CYBER_STATE				0.802*** (0.028)		
$\widehat{CYBER\_LM}$		1.015*** (0.124)	0.064*** (0.007)		2.615*** (0.376)	0.029*** (0.007)
Observations	1718	1718	1714	9774	9774	9755
Bank FE	YES	YES	YES	YES	YES	YES
Year FE	NO	NO	NO	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES
Kleibergen-Paap rk LM statistic		83.781	83.781		689.310	682.695
Kleibergen-Paap rk Wald F statistic		72.401	72.401		821.347	813.865
Stock-Yogo weak ID test critical values: 10 % maximal IV size		16.380	16.380		16.380	16.380
Hansen J statistic		0.000	0.000		0.000	0.001

Note: The results of the 2SLS regression are presented in this table. The 2SLS regression is conducted using STEM and CYBER_STATE as the instrumental variables. Model 1 reports the first-stage regression, where CYBER_LM is regressed on STEM and control variables. Models 2 and 3 present the second-stage regression results using the fitted values of CYBER_LM as the independent variable. Table A.1 provides the descriptions of all variables used. Bank-level control variables are included in all models. Robust standard errors, clustered at the bank level, are reported in brackets. Statistical significance is denoted by *** at the 1 % level, ** at the 5 % level, and * at the 10 % level.

Table 4
Two-step system GMM results.

VARIABLES	(1) RWA	(2) NPL
L.RWA	0.314*** (0.015)	
L.NPL		0.630*** (0.009)
CYBER_LM	1.937*** (0.734)	0.085*** (0.028)
Constant	0.421 (0.351)	−0.007*** (0.001)
Observations	8659	8636
Number of Banks	1054	1055
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES
AR(1)	0.000	0.000
AR(2)	0.569	0.701
Hansen	0.257	0.364
Number of Instruments	215	215

Note: This table displays the findings for two-step system GMM model. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. All models used CYBER_LM as an independent variable. First-order autocorrelation is indicated by AR(1), while second-order autocorrelation is shown by AR(2). Hansen p-value statistics to assess overidentification of the model. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. Level of significance is denoted by *** at 1 %, ** at 5 %, and * at 10 %.

risk-taking indicators reinforces the reliability of our initial conclusions.

Table 8, Panel B further tests the robustness of our results by introducing alternative proxies for cybersecurity risk, specifically CYBER_FLMW and CYBER_JKYZ. These measures capture different dimensions of cyber risk and exposure. The regression results using these proxies continue to show a significant and positive association between cybersecurity risk and bank risk-taking. The persistence of this relationship across multiple specifications highlights the robustness of our findings and suggests that the link between cybersecurity threats and bank behavior is not driven by a specific choice of variable but reflects a broader underlying dynamic.

Table 5
Dynamic DiD results.

VARIABLES	(1) CYBER_LM	(2) RWA	(3) NPL
STATE_DBDL t−2	0.013*** (0.001)	0.056 (0.046)	0.018 (0.013)
STATE_DBDL t−1	0.000 (0.002)	−0.014 (0.053)	0.047 (0.165)
STATE_DBDL t = 0	0.012*** (0.002)	0.045 (0.034)	0.000 (0.000)
STATE_DBDL t > +1	−0.004*** (0.001)	0.177*** (0.055)	0.089** (0.043)
Constant	−0.057*** (0.013)	0.789* (0.417)	−0.014*** (0.003)
Observations	9768	10,254	10,235
R-squared	0.643	0.887	0.755
Bank FE	YES	YES	YES
Year FE	YES	YES	YES

Note: The results of dynamic DiD are displayed in this table. STATE_DBDL used to proxy state data breach discloses law dummy variable for DiD regression. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. Level of significance is denoted by *** at 1 %, ** at 5 %, and * at 10 %.

4.4. Channel analysis results

4.4.1. Role of high bank competition

In this section, we explore the potential channels through which bank competition may amplify the effect of cybersecurity risk on bank risk-taking. Prior research suggests that intensified competition in the banking sector can lead institutions to take on greater risks in an effort to maintain market share and profitability (Bushman et al., 2016; Mata-baro Borauzima and Muller, 2023). In highly competitive environments, banks may lower lending standards, increase exposure to volatile markets, or adopt riskier strategies. Building on this literature, we hypothesize that the effect of cybersecurity risk on bank risk-taking is more pronounced among banks operating in markets characterized by high competition.

To empirically test this, we use the Herfindahl-Hirschman Index (HHI) based on bank deposits to measure market competition. A lower HHI indicates greater competition. We create a dummy variable that equals one if a bank operates in a market with below-median HHI (i.e.,

Table 6
Impact threshold of a confounding variable results.

	(1)	(2)	(3)	(4)
	Raw impact	Partial impact	Raw impact	Partial impact
	RWA	RWA	NPL	NPL
ACQ	0.055	0.050	0.103	0.028
CAR	0.050	0.027	0.059	0.015
CASH_FLOW	0.050	0.007	0.030	0.013
OE	0.013	0.005	0.015	0.007
LDR	0.010	0.003	0.015	0.005
AG	0.004	0.001	0.014	0.001
LLP	0.000	0.000	0.002	−0.001
NNID	−0.001	0.000	0.000	−0.002
DPR	−0.003	−0.001	−0.002	−0.008
AGE	−0.014	−0.001	−0.005	−0.008
NIM	−0.022	−0.008	−0.022	−0.010
SIZE	−0.036	−0.020	−0.042	−0.015
Impact Threshold	0.189		0.079	

Note: This table presents result for impact threshold of a confounding variable. Table A.1 contains the variable descriptions.

Table 7
PSM and EB matched sample analysis results.

	(1)	(2)	(3)	(4)
	PSM Sample		EB Sample	
	RWA	NPL	RWA	NPL
CYBER_LM	2.036*** (0.345)	0.006*** (0.002)	2.229*** (0.354)	0.006*** (0.002)
Constant	0.334 (0.398)	−0.030*** (0.003)	0.507 (0.414)	−0.026*** (0.003)
Observations	9676	9644	9783	9764
R-squared	0.901	0.778	0.890	0.761
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES

Note: The results of regression using PSM and EB sample are displayed in this table. Models 1 and 3 is developed with RWA as dependent variable while Models 2 and 4 use NPL. All models used CYBER_LM as an independent variable. The treatment and control groups for are identified based on the median value of CYBER_LM. The treatment group includes observations where the CYBER_LM variable is above the median, while the control group includes those below the median. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. Level of significance is denoted by *** at 1 %, ** at 5 %, and * at 10 %.

higher competition), and zero otherwise. Table 9 presents the interaction results between cybersecurity risk (CYBER_LM) and the high bank competition dummy. The interaction term CYBER_LM × High Bank Competition is positive and statistically significant, indicating that banks in more competitive environments exhibit stronger risk-taking behavior in response to increased cybersecurity risk. This finding supports the view that competitive pressure may exacerbate risk-taking incentives when banks are exposed to cyber threats, possibly as they attempt to signal resilience or outperform rivals.

4.4.2. Role of risk disclosure sentiment

Given that our measure of cybersecurity risk is derived from textual disclosures in firms' 10-K filings, we further investigate the moderating role of disclosure sentiment. Prior studies in financial linguistics and risk communication suggest that the tone of disclosure plays a crucial role in shaping market perceptions and managerial signaling (Qin et al., 2024; Yu et al., 2023; Zreik and Louhichi, 2017). Specifically, positive sentiment in risk disclosures is generally associated with lower perceived risk and greater managerial confidence, while negative sentiment often signals heightened risk exposure and uncertainty. Building on this literature, we hypothesize that negative sentiment in risk disclosures

Table 8
Results of robustness tests.

Panel A: Test of robustness using different indicators of bank risk-taking

	(1)	(2)	(3)
VARIABLES	ROA_SD	ZSCORE	DEFAULT
CYBER_LM	0.003*** (0.001)	1.140*** (0.267)	3.679*** (1.372)
Constant	−0.011*** (0.001)	−7.230*** (0.312)	3.683** (1.692)
Observations	9909	9669	3459
R-squared	0.445	0.576	0.144
Bank FE	YES	YES	YES
Year FE	YES	YES	YES
Controls	YES	YES	YES

Panel B: Test for robustness using a different indicators of cybersecurity risk

	(1)	(2)	(3)	(4)
VARIABLES	RWA	RWA	NPL	NPL
CYBER_FLMW	0.649*** (0.121)		0.829*** (0.196)	
CYBER_JKYZ		0.749*** (0.009)		1.131*** (0.265)
Constant	0.550 (0.775)	4.212*** (1.151)	−0.015*** (0.006)	−0.008 (0.007)
Observations	4674	3651	4667	3647
R-squared	0.890	0.885	0.825	0.845
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES

Note: The results of the robustness test with alternate proxies are shown in this table. Panel A displays the robustness test results using a different bank risk-taking proxy. The results of the robustness test employing a different cybersecurity risk proxy are shown in Panel B. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. Level of significance is denoted by *** at 1 %, ** at 5 %, and * at 10 %.

Table 9
Role of bank competition results.

	(1)	(2)
VARIABLES	RWA	NPL
CYBER_LM	1.350** (0.537)	0.147** (0.063)
High bank competition	0.171*** (0.049)	0.003*** (0.000)
CYBER_LM × High bank competition	2.683*** (0.450)	0.727*** (0.183)
Constant	0.613 (0.421)	−0.023*** (0.003)
Observations	9783	9764
R-squared	0.891	0.760
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES

Note: This table displays the result for role of high bank competition. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. High bank competition is a dummy variable where 1 indicates a bank competition denoted by Herfindahl-Hirschman Index of bank deposit higher than the median, and 0 indicates otherwise. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

strengthens the positive relationship between cybersecurity risk and bank risk-taking, whereas positive sentiment may temper this effect.

To empirically test this, we first collect the 10-K reports of all sample banks and extract the “Item 1 A. Risk Factors” section using a Python-

Table 10
Role of disclosure sentiment results.

VARIABLES	(1)	(2)	(3)	(4)
	RWA	NPL	RWA	NPL
CYBER_LM	0.771*** (0.012)	0.007*** (0.002)	0.769*** (0.012)	0.029** (0.011)
POS_SENT	−3.179 (4.079)	−0.035 (0.025)		
CYBER_LM × POS_SENT	−1.324*** (0.282)	−0.008*** (0.002)		
NEG_SENT			10.380 (8.929)	0.158*** (0.055)
CYBER_LM × NEG_SENT			1.686*** (0.553)	0.281*** (0.104)
Constant	3.060*** (0.950)	−0.014** (0.006)	3.063*** (0.960)	−0.018*** (0.006)
Observations	2326	2316	2326	2316
R-squared	0.910	0.780	0.910	0.780
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES

Note: This table displays the result for role of risk disclosure sentiment. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

based text extraction algorithm.⁵ The extracted text is then cleaned by removing stop words, numbers, punctuation, and irrelevant symbols to ensure consistency. We use the Loughran and McDonald (2011) sentiment dictionary, which is tailored specifically for financial texts, to classify each disclosure into positive and negative sentiment categories. Table 10 presents the results of this analysis. The coefficient on the interaction term CYBER_LM × POS_SENT is negative and statistically significant, suggesting that a more optimistic tone in cybersecurity-related risk disclosures reduces the influence of cybersecurity risk on bank risk-taking. Conversely, the interaction term CYBER_LM × NEG_SENT is positive and significant, indicating that banks with more negatively toned disclosures tend to exhibit stronger risk-taking responses to cybersecurity risk.

4.4.3. Role of IT investment

We further explore the role of IT investment as a potential channel through which cybersecurity risk affects bank risk-taking behavior. In response to rising cyber threats, banks often allocate substantial resources toward strengthening their information technology (IT) infrastructure, including cybersecurity systems, data management platforms, and network protections. However, as noted by Uddin et al. (2020), excessive IT investment, particularly beyond an optimal threshold, may paradoxically lead to increased risk-taking. This occurs because banks might pursue riskier strategies to justify or recoup high expenditures, or because a false sense of security may embolden managers to relax traditional risk controls. Building on this insight, we hypothesize that the relationship between cybersecurity risk and bank risk-taking is amplified among banks with higher IT investment levels.

To empirically test this hypothesis, we employ IT budget data from the CI Technology Historical Dataset (Spiceworks Ziff, 2024). This is a survey-based measure capturing firm-level IT expenditure across multiple categories such as hardware, servers, storage, communication services, and software (Kwan et al., 2024). We construct a binary variable, High IT Investment, which equals 1 if a bank's IT spending exceeds the sample median and 0 otherwise. Table 11 reports the results of our

analysis. The coefficient on the interaction term CYBER_LM × High IT Investment is positive and statistically significant, indicating that banks exposed to higher cybersecurity risk and simultaneously maintaining elevated IT budgets are more likely to increase their risk-taking. This supports the view that aggressive IT spending, while aimed at enhancing security, may inadvertently encourage behaviors that elevate financial risk, particularly when the spending surpasses efficiency-optimal levels.

4.4.4. Role of goodwill

In this section, we explore the moderating role of goodwill in the relationship between cybersecurity risk and bank risk-taking. Goodwill, often understood as the value of a firm's brand reputation, customer relationships, and other intangible assets, has been shown to buffer the negative effects of external shocks, including those related to cybersecurity. Prior research suggests that firms with higher goodwill may be perceived as more trustworthy and resilient (Kamiya et al., 2021; Rodrigues et al., 2022), allowing them to better weather reputational damage caused by data breaches or cyberattacks. In this context, we hypothesize that banks with higher levels of goodwill are less sensitive to cybersecurity risk in terms of altering their risk-taking behaviors.

To empirically test this hypothesis, we create a binary indicator variable High Goodwill, which equals 1 if a bank's goodwill exceeds the sample median and 0 otherwise. Table 12 presents the regression results assessing this interaction. The coefficient on CYBER_LM × High Goodwill is negative and statistically significant, indicating that banks with greater goodwill experience a weaker association between cybersecurity risk and risk-taking behavior. This finding suggests that goodwill serves as a reputational cushion, dampening the pressure to take on additional risk in response to cyber threats.

4.4.5. Role of bank run

In this section, we investigate the role of bank. Existing literature suggests that cyberattacks can erode depositor confidence, triggering rapid and large-scale withdrawals, similar to modern-day bank runs (Dinger and te Kaat, 2020). When depositors perceive increased vulnerability due to data breaches or operational failures, they may respond by pulling out their funds, especially in a highly digital and connected banking environment. This sudden liquidity pressure can incentivize banks to adopt riskier financial strategies as they attempt to recover profitability or stabilize operations, thereby intensifying the link between cybersecurity risk and risk-taking.

Table 11
Role of IT investment results.

VARIABLES	(1)	(2)
	RWA	NPL
CYBER_LM	0.572*** (0.131)	0.033*** (0.006)
High IT investment	0.288*** (0.085)	0.050** (0.025)
CYBER_LM × High IT investment	1.119*** (0.387)	0.725*** (0.13)
Constant	2.047* (1.139)	0.045*** (0.007)
Observations	2567	2561
R-squared	0.898	0.824
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES

Note: This table displays the result for role of IT investment. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. High IT investment is a dummy variable where 1 indicates IT investment higher than the median, and 0 indicates otherwise. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

⁵ 10k files are collected from <https://sraf.nd.edu/sec-edgar-data/cleaned-10x-files/>.

Table 12
Role of goodwill results.

	(1)	(2)
VARIABLES	RWA	NPL
CYBER_LM	0.191*** (0.050)	0.007** (0.003)
High goodwill	−0.121** (0.058)	−0.001 (0.000)
CYBER_LM × High goodwill	−1.136* (0.635)	−0.440*** (0.138)
Constant	3.148*** (0.496)	−0.014*** (0.003)
Observations	8941	8925
R-squared	0.896	0.798
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES

Note: This table displays the result for role of high goodwill. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. High goodwill is a dummy variable where 1 indicates a goodwill higher than the median, and 0 indicates otherwise. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

To empirically test this channel, we use high deposit withdrawal as a proxy for bank runs, calculated by the annual change in bank deposits. A dummy variable is constructed, set to 1 for banks with deposit withdrawals above the sample median and 0 otherwise. Table 13 presents the regression results. The interaction term CYBER_LM × High Deposit Withdrawal is found to be positive and statistically significant, indicating that banks facing larger withdrawals show a stronger relationship between cybersecurity risk and risk-taking. This suggests that under potential bank-run conditions, cyber risks translate into more aggressive behavior in risk exposure, supporting our hypothesis that liquidity shocks exacerbate the effects of cybersecurity threats on bank behavior.

4.5. Further analysis results

To further assess the robustness of our findings, we conduct an additional analysis by excluding the years surrounding the Global

Table 13
Role of bank run.

	(1)	(2)
VARIABLES	RWA	NPL
CYBER_LM	1.789*** (0.647)	0.004*** (0.000)
High deposit withdrawal	0.043 (0.053)	0.001*** (0.000)
CYBER_LM × High deposit withdrawal	4.418** (2.001)	0.045*** (0.013)
Constant	0.398 (0.424)	−0.024*** (0.003)
Observations	9783	9764
R-squared	0.891	0.756
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES

Note: This table displays the result for channel analysis of bank run. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. High deposit withdrawal is a dummy variable where 1 indicates a bank run denoted by changes in bank deposit higher than the median, and 0 indicates otherwise. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

Financial Crisis (GFC). Our original sample spans from 1998 to 2018, a period that includes the 2007–2009 financial crisis, which was marked by extreme market volatility, heightened risk aversion, and significant regulatory shifts. Such a systemic shock could potentially distort the relationship between cybersecurity risk and bank risk-taking, leading to concerns about the generalizability of our results. To address this, we re-estimate our model using a restricted sample covering the post-crisis period from 2010 to 2018. As shown in Table 14, the coefficient for CYBER_LM remains positive and statistically significant across key specifications. These consistent findings suggest that our main results are not driven by crisis-related anomalies and hold true even in more stable economic environments.

To further explore the heterogeneity in the relationship between cybersecurity risk and bank risk-taking, we perform a sub-sample analysis based on several bank characteristics. The results of this analysis are presented in Table 15. Panel A of Table 15 examines the role of cash flow volatility. Sub-samples are divided based on the three-year standard deviation of the operating cash flow ratio. We find that the positive association between cybersecurity risk and bank risk-taking is more pronounced among banks with high cash flow volatility, suggesting that financial instability may amplify risk-taking behavior in the presence of cybersecurity threats. Panel B analyzes the effect of nonperforming loans (NPL), using the median NPL ratio as a cutoff. Results show that the relationship is stronger for banks with higher levels of NPLs, implying that already risk-exposed banks may react more aggressively when facing cyber threats.

Panel C evaluates how earnings performance influences this relationship by segmenting banks based on median earnings per share (EPS). The findings indicate that banks with lower EPS show a stronger link between cybersecurity risk and risk-taking, perhaps due to the pressure to compensate for weak performance through riskier strategies. In Panel D, we consider the role of bank size, categorizing banks into small and large based on median total assets. The results reveal that smaller banks exhibit a more significant positive association, possibly reflecting limited resources for cybersecurity infrastructure and risk mitigation. Finally, Panel E explores the impact of advertisement expenditure. Banks with lower advertising intensity show a stronger link between cybersecurity risk and risk-taking, which may suggest that less reputationally exposed banks are more inclined to take on risk when cyber threats are present. Overall, these sub-sample analyses underscore that the relationship between cybersecurity risk and bank behavior is shaped by bank-specific characteristics and operational conditions.

Table 14
Results excluding global financial crisis sample.

	(1)	(2)
VARIABLES	RWA	NPL
CYBER_LM	0.435*** (0.073)	0.013*** (0.001)
Constant	2.620** (1.131)	−0.001 (0.007)
Observations	3701	3695
R-squared	0.894	0.843
Bank FE	YES	YES
Year FE	YES	YES
Controls	YES	YES

Note: This table displays the result for results excluding global financial crisis sample. Model 1 is developed with RWA as dependent variable while Model 2 use NPL. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models. Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

Table 15
Sub-sample analysis results.

Panel A: Results for high vs. low cash flow volatility				
	(1)	(2)	(3)	(4)
	High cash flow volatility		Low cash flow volatility	
VARIABLES	RWA	NPL	RWA	NPL
CYBER_LM	0.752*** (0.011)	0.380*** (0.114)	0.291*** (0.084)	0.163** (0.067)
Constant	2.133*** (0.803)	−0.021*** (0.005)	4.668*** (0.884)	−0.021*** (0.006)
Observations	3642	3638	3669	3658
R-squared	0.908	0.772	0.917	0.838
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES
Panel B: Results for high vs. low nonperforming loans				
	(1)	(2)	(3)	(4)
	High nonperforming loans		Low nonperforming loans	
VARIABLES	RWA	NPL	RWA	NPL
CYBER_LM	1.031* (0.606)	0.264** (0.119)	0.217*** (0.074)	0.006*** (0.000)
Constant	5.216*** (0.867)	−0.003 (0.003)	1.645** (0.735)	−0.008* (0.004)
Observations	4822	4828	4788	4788
R-squared	0.909	0.720	0.902	0.856
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES
Panel C: Results for high vs. low earnings per share (EPS)				
	(1)	(2)	(3)	(4)
	High EPS		Low EPS	
VARIABLES	RWA	NPL	RWA	NPL
CYBER_LM	0.138** (0.062)	0.005*** (0.000)	0.284*** (0.069)	0.008*** (0.000)
Constant	0.316 (0.834)	−0.018*** (0.005)	4.156*** (0.683)	−0.025*** (0.004)
Observations	4753	4752	4746	4728
R-squared	0.890	0.825	0.922	0.686
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES
Panel D: Results for small vs big banks				
	(1)	(2)	(3)	(4)
	Small Banks		Big Banks	
VARIABLES	RWA	NPL	RWA	NPL
CYBER_LM	0.966* (0.574)	0.785*** (0.279)	0.263*** (0.072)	0.008*** (0.000)
Constant	2.694*** (0.896)	−0.025*** (0.006)	1.826*** (0.683)	−0.023*** (0.004)
Observations	4900	4895	4816	4803
R-squared	0.913	0.806	0.891	0.819
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES
Panel E: Results for high vs. low advertisement expense				
	(1)	(2)	(3)	(4)
	High advertisement expense		Low advertisement expense	
VARIABLES	RWA	NPL	RWA	NPL
CYBER_LM	0.012*** (0.001)	0.008** (0.003)	1.464** (0.572)	0.735*** (0.009)
Constant	2.106** (0.929)	−0.029*** (0.006)	3.136*** (0.688)	−0.022*** (0.004)
Observations	4248	4243	4188	4181
R-squared	0.910	0.811	0.898	0.812
Bank FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Controls	YES	YES	YES	YES

Note: This table shows the result for additional analyses. Panel A displays the result for sub-sample analysis for high vs. low cash flow volatility. Panel B the result for sub-sample analysis for high vs. low nonperforming loans. Panel C displays the result sub-sample analysis for high vs. low earnings per share. Panel D shows the result for sub-sample analysis for small vs big banks. Panel E displays the result for sub-sample analysis for high vs. low advertisement expense. Models 1 and 3 is developed with RWA as dependent variable while Models 2 and 3 use NPL. All models used CYBER_LM as an independent variable. Bank-level control variables, bank and year fixed effects are included in all models.

Table A.1 contains the variable descriptions. In brackets are robust standard errors that are clustered at the bank level. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

5. Conclusions

This study explores the association between cybersecurity risk and bank risk-taking. Our baseline analysis indicates a significant relationship between higher levels of cybersecurity risk and increased risk-taking behaviors among banks. To address potential endogeneity concerns, we employed a range of robust techniques including Two-Stage Least Squares, two-step system GMM, staggered Differences-in-Differences, Impact Threshold of a Confounding Variable, Propensity Score Matching, and Entropy Balancing. Across all methods, the results consistently support our main findings, indicating that the observed relationship between cybersecurity risk and bank risk-taking is not driven by endogeneity bias. This association persists robustly, even after employing alternative proxies for cybersecurity risk.

Moreover, we find that this association is significantly stronger for banks facing higher levels of market competition, indicating that competitive pressures may drive riskier behavior when cybersecurity threats are present. Disclosure sentiment also plays a critical role; positive sentiment in cybersecurity-related risk disclosures dampens the risk-taking response, whereas negative sentiment amplifies it. Additionally, banks with high IT investment show a stronger link between cybersecurity risk and risk-taking, suggesting that extensive IT spending may, paradoxically, embolden riskier strategies. In contrast, banks with higher goodwill appear more resilient, as goodwill mitigates the influence of cybersecurity risk on risk-taking. Lastly, the relationship is intensified in banks experiencing high deposit withdrawals, pointing to heightened vulnerability during periods of potential bank runs. These findings collectively reinforce the robustness of our core argument while uncovering key moderating factors. Our sub-sample analysis reveals that the positive relationship between cybersecurity risk and bank risk-taking is more pronounced for banks with high cash flow volatility, high nonperforming loans, and low earnings per share. Additionally, the effect is stronger among smaller banks and those with lower advertisement intensity. These findings suggest that financial vulnerability, limited scale, and lower market engagement may intensify the risk-taking response to cybersecurity threats.

The findings of our study offer several important implications for regulators, financial institutions, and policymakers. Given the robust link between cybersecurity risk and increased bank risk-taking, regulatory bodies should prioritize strengthening cybersecurity governance frameworks across the financial sector. Enhanced oversight mechanisms, standardized reporting of cyber incidents, and stricter compliance requirements can help reduce the risk spillovers from cyber vulnerabilities. Moreover, the contrasting effects of disclosure tone and IT investment suggest that positive disclosure sentiment, which likely reflects proactive cybersecurity efforts, can help reduce bank risk-taking. In contrast, excessive IT investment appears to increase risk-taking, possibly due to a false sense of security that encourages moral hazard. These results indicate that while investments to enhance cybersecurity are valuable, regulators should consider establishing guidelines for responsible IT spending and promoting transparent, balanced communication in risk disclosures. These steps can prevent overconfidence in technological infrastructure while encouraging banks to adopt a more proactive stance on cyber risk management.

Furthermore, our results suggest that market structure and bank-specific characteristics play a critical role in shaping how banks respond to cybersecurity threats. Policymakers should recognize that banks operating in highly competitive environments or facing financial vulnerabilities, such as high cash flow volatility, NPLs, or low earnings, may be more inclined to engage in riskier behavior when exposed to cyber risks. To mitigate these dynamics, policies aimed at fostering sectoral stability, such as measures to reduce excessive competition or to

support financially weaker institutions in enhancing their cybersecurity resilience, may be warranted. Additionally, intangible assets like goodwill and brand reputation serve as valuable buffers against the adverse effects of cyber threats. Therefore, encouraging banks to invest in long-term trust-building initiatives and reputational capital can further help temper the risk-taking tendencies triggered by cybersecurity concerns.

Future studies may explore the relationship between cybersecurity risk and the cost of capital in the banking sector to further expand upon our argument. Additionally, since our sample period does not include recent developments, future research could extend our findings by incorporating updated data that covers significant recent events such as the COVID-19 pandemic and ongoing geopolitical crises. Furthermore, we acknowledge a key limitation in our use of multiple proxies for bank risk-taking, as these indicators largely reflect the overall risk level in banks and do not fully differentiate between risks that result from deliberate managerial decisions and those that arise passively due to external factors. This limitation suggests that some of the observed risk may not stem from banks' active pursuit of risk but rather from their exposure to uncontrollable events. Future studies could work toward addressing this issue by adopting measures that more clearly capture strategic risk-taking behavior, thereby offering a more precise understanding of the relationship between cybersecurity risk and bank conduct.

Appendix A

Table A1
Description of the variables

Variables	Description	Data source
Panel A: Dependent variables		
RWA	Bank regulatory capital scaled risk-weighted assets	Compustat Bank Fundamentals (CBF)
NPL	Bank nonperforming loans scaled gross loans ratio	CBF
ROA_SD	3 years standard deviation of ROA	CBF
ZSCORE	Z-score is computed as the product of the capital-to-assets ratio (CAR) and return on assets (ROA), divided by the standard deviation of ROA. The natural logarithm of z-score is multiplied by -1 . $ZSCORE_{i,t} = (-1) \times \ln\left(\frac{CAR_{i,t} + ROA_{i,t}}{ROA_{volatility_{i,t}}}\right)$	CBF
DEFAULT	Probability of default	Bloomberg
Panel B: Independent variables		
CYBER_LM	CYBER LM, developed by Lattanzio and Ma (2023) , which employs a comprehensive dictionary of cybersecurity-related terms to analyze risk disclosures in 10-K reports.	Lattanzio and Ma (2023)
CYBER_FLMW	CYBER FLMW, proposed by Florackis et al. (2023) , measures cybersecurity risk by assessing the similarity of a firm's risk disclosures in the "Item 1 A Risk Factors" section of 10-K reports to past disclosures from a training sample.	Florackis et al. (2023)
CYBER_JKYZ	CYBER JKYZ, introduced by Jiang et al. (2024) , which leverages machine learning algorithms to estimate the likelihood of cyberattacks on individual firms.	Jiang et al. (2024)
Panel C: Bank-level control variables		
AGE	Natural logarithm of bank age	CBF
SIZE	Natural logarithm of total assets	CBF
CASH_FLOW	Operating cashflow scaled by total assets	CBF
DPR	Dividend payout ratio	CBF
AG	Asset growth calculated by the changes in bank size (natural logarithm of total assets)	CBF
NNID	Non-interest income scaled by the sum of interest-and non-interest incomes	CBF
ACQ	A dummy variable that represents acquisition spending that is not zero	CBF
CAR	Capital Adequacy Ratio	CBF
OE	Operating income divided by total costs is measured for operating efficiency.	CBF
LDR	Total loan scaled by total deposit	CBF
NIM	Net interest margin	CBF
LLP	Total loan loss provision scaled by total loans	CBF
Panel D: Instrumental Variable		
STEM	Yearly global average shares of science, technology, engineering, and mathematics graduates	OECD
CYBER_STATE	State-wise yearly average cybersecurity risk scores of non-financial firms	Authors calculation from Lattanzio and Ma (2023)

(continued on next page)

CRediT authorship contribution statement

Md. Habibur Rahman Fuszder: Writing – review & editing, Writing – original draft, Resources, Data curation, Conceptualization. **Zunaidah Sulong:** Writing – review & editing, Writing – original draft, Validation, Investigation, Funding acquisition, Conceptualization. **Emmanuel Joel Aikins Abakah:** Writing – review & editing, Writing – original draft, Supervision, Conceptualization. **Mohammad Abdullah:** Writing – review & editing, Writing – original draft, Software, Methodology, Formal analysis, Conceptualization.

Declaration of Competing Interest

disclosure on behalf of all authors, the corresponding author states no conflict of interest.

Acknowledgements

We thank the three anonymous reviewers for their valuable comments. The authors gratefully acknowledge the Ministry of Higher Education (MOHE), Malaysia, for funding this study through the Fundamental Research Grant Scheme (FRGS/1/2023/SS01/UNISZA/02/10). Also, we thank the conference participants at the 2nd Emerging Countries International Conference (ECIC), University of Ghana Business School, Ghana, December 2024 for helpful comments. Moreover, this paper is a part of PhD thesis of the second author.

Table A1 (continued)

Variables	Description	Data source
Panel E: Other variables		
High bank competition	Dummy variable indicating high bank competition, where bank operates in a market with below-median HHI (i.e., higher competition), and zero otherwise. Bank competition is measured by Herfindahl-Hirschman Index of bank deposit	Authors calculation from CBF
POS_SENT	Positive sentiment score of “Item 1 A Risk Factors” of 10-K reports measured using Loughran and McDonald (2011) dictionary.	Authors calculation from 10-K files
NEG_SENT	Negative sentiment score of “Item 1 A Risk Factors” of 10-K reports measured using Loughran and McDonald (2011) dictionary.	
High IT investment	A dummy variable for high IT investment, coded as 1 if IT investment exceeds the median and 0 otherwise. IT investment is measured by CI Technology Historical Data.	Spiceworks Ziff (2024)
High goodwill	A dummy variable for high goodwill, coded as 1 if goodwill exceeds the median and 0 otherwise.	Authors calculation from CBF
High deposit withdrawal	A dummy variable for high deposit withdrawal, set to 1 if withdrawals exceed the median and 0 otherwise. Deposit withdrawal is measured by changes in yearly deposit.	Authors calculation from CBF
STATE_DBDL	US state level data breach disclosure law.	Perkins Coie Website

Table A2

Correlation matrix

Variables	RWA	CYBER_LM	AGE	SIZE	CASH_FLOW	DPR	AG	NNID	ACQ	CAR	OE	LDR	NIM	LLP
RWA	1.00													
CYBER_LM	0.12***	1.00												
AGE	-0.04***	0.29***	1.00											
SIZE	-0.14***	0.25***	0.60***	1.00										
CASH_FLOW	0.16***	0.30***	0.33***	0.18***	1.00									
DPR	0.06***	-0.06***	0.14***	0.10***	0.01	1.00								
AG	-0.09***	-0.04***	-0.21***	0.05***	-0.20***	-0.04***	1.00							
NNID	-0.01	0.07***	0.35***	0.41***	0.06***	0.13***	-0.05***	1.00						
ACQ	-0.17***	-0.32***	-0.22***	0.04***	-0.56***	0.09***	0.21***	0.11***	1.00					
CAR	0.73***	0.06***	-0.10***	-0.16***	0.05***	0.06***	-0.15***	-0.14***	-0.12***	1.00				
OE	-0.18***	-0.07***	-0.12***	-0.22***	-0.11***	-0.26***	-0.22***	-0.08***	-0.12***	-0.07***	1.00			
LDR	-0.27***	-0.03***	-0.08***	0.02**	0.00	0.01	0.06***	-0.17***	-0.01	-0.16***	0.03***	1.00		
NIM	0.16***	-0.14***	-0.13***	-0.11***	0.00	0.02**	0.18***	-0.01	0.19***	-0.11***	-0.30***	-0.07***	1.00	
LLP	-0.10***	0.00	0.08***	0.08***	0.08***	-0.19***	-0.21***	0.05***	-0.12***	-0.11***	0.65***	-0.01	0.00	1.00
VIF	-	1.26	1.99	2.19	1.72	1.14	1.26	1.34	1.81	1.16	2.73	1.1	1.42	2.29

Note: VIF= Variance inflation factor. At the 1 % level, significance is indicated by ***, at the 5 % level by **, and at the 10 % level by *.

Table A3

US State Data breach disclosure law

State	State Code	Law Year	State	State Code	Law Year
Alabama	AL	2018	Montana	MT	2006
Alaska	AK	2008	Nebraska	NE	2006
Arizona	AZ	2006	Nevada	NV	2005
Arkansas	AR	2005	New Hampshire	NH	2007
California	CA	2003	New Jersey	NJ	2006
Colorado	CO	2006	New Mexico	NM	2017
Connecticut	CT	2006	New York	NY	2005
Delaware	DE	2005	North Carolina	NC	2005
Washington, D.C.	DC	2007	North Dakota	ND	2005
Florida	FL	2014	Ohio	OH	2006
Georgia	GA	2005	Oklahoma	OK	2008
Hawaii	HI	2007	Oregon	OR	2007
Idaho	ID	2006	Pennsylvania	PA	2006
Illinois	IL	2006	Puerto Rico	PR	2006
Indiana	IN	2006	South Carolina	SC	2009
Iowa	IA	2008	South Dakota	SD	2018
Kansas	KS	2007	Tennessee	TN	2005
Kentucky	KY	2014	Texas	TX	2009
Louisiana	LA	2006	Utah	UT	2007
Maine	ME	2006	Vermont	VT	2012
Maryland	MD	2008	Virginia	VA	2008
Massachusetts	MA	2007	Washington	WA	2005
Michigan	MI	2007	West Virginia	WV	2008
Minnesota	MN	2006	Wisconsin	WI	2006
Mississippi	MS	2011	Wyoming	WY	2007
Missouri	MO	2009			

Note: Data is compiled from Perkins Coie LLP website at: <https://perkinscoie.com/insights/publication/security-breach-notification-chart>.

References

- Abakah, A.A., Li, J., 2023. Local religious beliefs and bank risk-taking. *J. Behav. Exp. Financ.* 40, 100856. <https://doi.org/10.1016/j.jbef.2023.100856>.
- Agusman, A., Cullen, G.S., Gasbarro, D., Monroe, G.S., Zumwalt, J.K., 2014. Government intervention, bank ownership and risk-taking during the Indonesian financial crisis. *Pac. Basin Financ. J.* 30, 114–131. <https://doi.org/10.1016/j.pacfin.2014.07.003>.
- Amin, A., Mollah, S., Kamal, S., Zhao, Y., Simsek, R., 2024. Independent directors' connectedness and bank risk-taking. *J. Financ. Stab.* 75, 101324. <https://doi.org/10.1016/j.jfs.2024.101324>.
- Arellano, M., Bond, S., 1991. Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Rev. Econ. Stud.* 58 (2), 277–297. <https://doi.org/10.2307/2297968>.
- Ashraf, B.N., 2017. Political institutions and bank risk-taking behavior. *J. Financ. Stab.* 29, 13–35. <https://doi.org/10.1016/j.jfs.2017.01.004>.
- Ashraf, B., Sunder, J., 2023. Can shareholders benefit from consumer protection disclosure mandates? evidence from data breach disclosure laws. *Account. Rev.* 98 (4), 1–32. <https://doi.org/10.2308/TAR-2020-0787>.
- Banna, H., Kabir Hassan, M., Rashid, M., 2021. Fintech-based financial inclusion and bank risk-taking: evidence from OIC countries. *J. Int. Financ. Mark. Inst. Money* 75, 101447. <https://doi.org/10.1016/j.intfin.2021.101447>.
- Berkman, H., Jona, J., Lee, G., Soderstrom, N., 2018. Cybersecurity awareness and market valuations. *J. Account. Public Policy* 37 (6), 508–526. <https://doi.org/10.1016/j.jaccpubpol.2018.10.003>.
- Blundell, R., Bond, S., 1998. Initial conditions and moment restrictions in dynamic panel data models. *J. Econ.* 87 (1), 115–143. [https://doi.org/10.1016/S0304-4076\(98\)00009-8](https://doi.org/10.1016/S0304-4076(98)00009-8).
- Boasiako, K.A., Keefe, M.O.C., 2021. Data breaches and corporate liquidity management. *Eur. Financ. Manag.* 27 (3), 528–551. <https://doi.org/10.1111/eufm.12289>.
- Bondiolì, M., Goldberg, M., Hu, N., Li, C., Maalaoui, O., & Stein, H.J. (2021). The bloomberg corporate default risk model (drsk) for private firms. Available at SSRN 3911330.
- Bougou, W., 2023. Cyber-attacks and banking intermediation. *Econ. Lett.* 233, 111354. <https://doi.org/10.1016/j.econlet.2023.111354>.
- Bui, D.T., Bui, T.M.H., 2019. How does institutional development shape bank risk-taking incentives in the context of financial openness? *Pac. Basin Financ. J.* 58, 101209. <https://doi.org/10.1016/j.pacfin.2019.101209>.
- Busenbark, J.R., Yoon, H., Gamache, D.L., Withers, M.C., 2022. Omitted variable bias: examining management research with the impact threshold of a confounding variable (ITCV). *J. Manag.* 48 (1), 17–48. <https://doi.org/10.1177/01492063211006458>.
- Bushman, R.M., Hendricks, B.E., Williams, C.D., 2016. Bank competition: measurement, decision-making, and risk-taking. *J. Account. Res.* 54 (3), 777–826. <https://doi.org/10.1111/1475-679X.12117>.
- Carboni, M., Dell'Atti, S., Gianfrancesco, I., Onorato, G., 2024. The impact of cyber enforcement actions on stock returns. *Res. Int. Bus. Financ.* 71, 102460. <https://doi.org/10.1016/j.ribaf.2024.102460>.
- Crosignani, M., Macchiavelli, M., Silva, A.F., 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *J. Financ. Econ.* 147 (2), 432–448. <https://doi.org/10.1016/j.jfineco.2022.12.002>.
- Dalwai, T., Singh, D., S. A., 2022. Intellectual capital, bank stability and risk-taking: evidence from Asian emerging markets. *Compét. Rev. Int. Bus. J.* 32 (6), 995–1024. <https://doi.org/10.1108/CR-03-2021-0031>.
- Delis, M.D., Kouretas, G.P., 2011. Interest rates and bank risk-taking. *J. Bank. Financ.* 35 (4), 840–855. <https://doi.org/10.1016/j.jbankfin.2010.09.032>.
- Dell'Ariccia, G., Laeven, L.U.C., Suarez, G.A., 2017. Bank leverage and monetary policy's risk-taking channel: evidence from the United States. *J. Financ.* 72 (2), 613–654. <https://doi.org/10.1111/jofi.12467>.
- Dinger, V., te Kaat, D.M., 2020. Cross-border capital flows and bank risk-taking. *J. Bank. Financ.* 117, 105842. <https://doi.org/10.1016/j.jbankfin.2020.105842>.
- Dutta, S., Mathur, R., 2012. Cybersecurity — An integral part of STEM, 9–9 March 2012 Pap. Presente IEEE 2nd Integr. STEM Educ. Conf.
- Eisenbath, T.M., Kovner, A., Lee, M.J., 2022. Cyber risk and the U.S. financial system: a pre-mortem analysis. *J. Financ. Econ.* 145 (3), 802–826. <https://doi.org/10.1016/j.jfineco.2021.10.007>.
- Elekdag, S., Emrullah, D., Ben Naceur, S., 2025. Does fintech increase bank risk-taking? *J. Financ. Stab.* 76, 101360. <https://doi.org/10.1016/j.jfs.2024.101360>.
- Fang, J., Lau, C.-K.M., Lu, Z., Tan, Y., Zhang, H., 2019. Bank performance in China: a perspective from bank efficiency, risk-taking and market competition. *Pac. Basin Financ. J.* 56, 290–309. <https://doi.org/10.1016/j.pacfin.2019.06.011>.
- Fisher, M.G., 2016. Ambassador for patient safety and the promotion, protection and support of cardiac theatre staff. *J. Perioper. Pract.* 26 (6), Suppl7. Retrieved from. (<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060668052&partnerID=40&md5=98bca2c2265f9c525812755c8dcaba45>).
- Florackis, C., Louca, C., Michaely, R., Weber, M., 2023. Cybersecurity risk. *Rev. Financ. Stud.* 36 (1), 351–407. <https://doi.org/10.1093/rfs/hhac024>.
- Gatzert, N., Schubert, M., 2022. Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value. *J. Risk Insur.* 89 (3), 725–763. <https://doi.org/10.1111/jori.12381>.
- Gordon, L.A., Loeb, M.P., Sohail, T., 2010. Market value of voluntary disclosures concerning information security. *MIS Q.* 34 (3), 567–594. <https://doi.org/10.2307/25750692>.
- Hainmueller, J., 2012. Entropy balancing for causal effects: a multivariate reweighting method to produce balanced samples in observational studies. *Political Anal.* 20 (1), 25–46. <https://doi.org/10.1093/pan/mpr025>.
- He, M., Song, G., Chen, Q., 2023. Fintech adoption, internal control quality and bank risk taking: evidence from Chinese listed banks. *Financ. Res. Lett.* 57, 104235. <https://doi.org/10.1016/j.frl.2023.104235>.
- Heo, Y. (2024). Cybersecurity and Bank Distance-to-Default. SSRN. doi:(<https://doi.org/10.2139/ssrn.4660090>).
- Heyert, A., Weill, L., 2024. Does distrust in banks reduce bank risk-taking? *Financ. Res. Lett.* 68, 105974. <https://doi.org/10.1016/j.frl.2024.105974>.
- Hoang, H.V., 2025. Who pays for cybersecurity? Corporate dividends in response to cybersecurity risk in US firms. *J. Knowl. Econ.* <https://doi.org/10.1007/s13132-025-02601-3>.
- Houston, J.F., Lin, C., Lin, P., Ma, Y., 2010. Creditor rights, information sharing, and bank risk taking. *J. Financ. Econ.* 96 (3), 485–512. <https://doi.org/10.1016/j.jfineco.2010.02.008>.
- Ibrahim, M.H., Rizvi, S.A.R., 2018. Bank lending, deposits and risk-taking in times of crisis: a panel analysis of Islamic and conventional banks. *Emerg. Mark. Rev.* 35, 31–47. <https://doi.org/10.1016/j.ememar.2017.12.003>.
- Jensen, M.C., Meckling, W.H., 1979. Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure. In: Brunner, K. (Ed.), *Economics Social Institutions: Insights from the Conferences on Analysis & Ideology*. Springer Netherlands, Dordrecht, pp. 163–231.
- Jia, X., 2024. FinTech penetration, charter value, and bank risk-taking. *J. Bank. Financ.* 161, 107111. <https://doi.org/10.1016/j.jbankfin.2024.107111>.
- Jiang, H., Khanna, N., Yang, Q., Zhou, J., 2024. The cyber risk premium. *Manag. Sci.* <https://doi.org/10.1287/mnsc.2022.02056>.
- Jin, J., Li, N., Liu, S., Khalid Nainar, S.M., 2023. Cyber attacks, discretionary loan loss provisions, and banks' earnings management. *Financ. Res. Lett.* 54, 103705. <https://doi.org/10.1016/j.frl.2023.103705>.
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *J. Financ. Econ.* 139 (3), 719–749. <https://doi.org/10.1016/j.jfineco.2019.05.019>.
- Khan, M.S., Scheule, H., Wu, E., 2017. Funding liquidity and bank risk taking. *J. Bank. Financ.* 82, 203–216. <https://doi.org/10.1016/j.jbankfin.2016.09.005>.
- Kutubi, S.S., Ahmed, K., Khan, H., 2018. Bank performance and risk-taking — Does directors' busyness matter? *Pac. Basin Financ. J.* 50, 184–199. <https://doi.org/10.1016/j.pacfin.2017.02.002>.
- Kwan, A., Lin, C., Pursiainen, V., Tai, M., 2024. Stress Testing Banks' Digital Capabilities: Evidence from the COVID-19 Pandemic. *J. Financ. Quant. Anal.* 59 (6), 2618–2646. <https://doi.org/10.1017/S0022109023000662>.
- Laeven, L., Levine, R., 2009. Bank governance, regulation and risk taking. *J. Financ. Econ.* 93 (2), 259–275. <https://doi.org/10.1016/j.jfineco.2008.09.003>.
- Lattanzio, G., Ma, Y., 2023. Cybersecurity risk and corporate innovation. *J. Corp. Financ.* 82, 102445. <https://doi.org/10.1016/j.jcorpfin.2023.102445>.
- LeClair, J., Hollis, K.M., & Pheils, D.M. (2014, 8–8 March 2014). Cybersecurity education and training and its Reliance on STEAM. Paper presented at the 2014 IEEE Integrated STEM Education Conference.
- Lee, C.-C., Wang, C.-W., Lin, W., Chen, E.-J., 2025. Cyber risk and corporate share repurchases. *Int. Rev. Financ. Anal.* 103, 104232. <https://doi.org/10.1016/j.irfa.2025.104232>.
- Liu, Z., Li, J., Sun, H., 2024. Climate transition risk and bank risk-taking: The role of digital transformation. *Financ. Res. Lett.* 61, 105028. <https://doi.org/10.1016/j.frl.2024.105028>.
- Loughran, T.I.M., McDonald, B., 2011. When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. *J. Financ.* 66 (1), 35–65. <https://doi.org/10.1111/j.1540-6261.2010.01625.x>.
- Matabaro Borauzima, L., Muller, A., 2023. Bank risk-taking and competition in developing banking markets: does efficiency level matter? Evidence from Africa. *Emerg. Mark. Rev.* 55, 100963. <https://doi.org/10.1016/j.ememar.2022.100963>.
- Nguyen, D., 2024. Corporate governance and bank risk-taking: transitional economic evidence. *J. Appl. Econ.* 27 (1), 2369429. <https://doi.org/10.1080/15140326.2024.2369429>.
- Pan, Z., Li, S., Li, J., Gong, C., 2024. Air pollution and bank risk taking: evidence from China. *Financ. Res. Lett.* 65, 105594. <https://doi.org/10.1016/j.frl.2024.105594>.
- Peihani, M., 2022. Regulation of cyber risk in the banking system: a canadian case study. *J. Financ. Regul.* 8 (2), 139–161. <https://doi.org/10.1093/jfr/fjac006>.
- Pozo, J., 2023. Bank risk-taking in emerging economies: empirical evidence and theory. *J. Financ. Stab.* 67, 101136. <https://doi.org/10.1016/j.jfs.2023.101136>.
- Qin, Z., Cui, M., Yan, J., Niu, J., 2024. Managerial sentiment and corporate risk-taking: evidence from Chinese listed companies' annual reports. *Manag. Res. Rev.* 47 (4), 485–511. <https://doi.org/10.1108/MRR-02-2023-0110>.
- Ren, M., Zhao, J., Ke, K., Li, Y., 2023. Bank homogeneity and risk-taking: evidence from China. *Q. Rev. Econ. Financ.* 92, 142–154. <https://doi.org/10.1016/j.qref.2023.09.002>.
- Rodrigues, A.R.D., Ferreira, F.A., Teixeira, F.J., Zopounidis, C., 2022. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Res. Int. Bus. Finance* 60, 101616.
- Rosenbaum, P.R., Rubin, D.B., 1983. The central role of the propensity score in observational studies for causal effects. *Biometrika* 70 (1), 41–55. <https://doi.org/10.1093/biomet/70.1.41>.
- Song, J., Cao, W., Shan, Y.G., 2025. Green credit and bank's risk-taking: evidence from China. *Int. J. Manag. Financ.* 21 (1), 157–184. <https://doi.org/10.1108/IJMF-03-2024-0144>.
- Spiceworks Ziff, D. Spiceworks Ziff, D. (2024). CI Technology Historical Data (1996–2022). Retrieved from: <https://doi.org/10.7910/DVN/MSNFCT>.
- Tian, S., Zhao, B., Olivares, R.O., 2023. Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Financ. Res. Lett.* 53, 103609. <https://doi.org/10.1016/j.frl.2022.103609>.

- Tran, D., Nguyen, T., 2025. Capital buffer and bank risk-taking in Vietnam: the moderating role of capital regulation and shadow banking. *J. Financ. Regul. Compliance* 33 (1), 48–66. <https://doi.org/10.1108/JFRC-06-2024-0106>.
- Uddin, M.H., Mollah, S., Ali, M.H., 2020. Does cyber tech spending matter for bank stability? *Int. Rev. Financ. Anal.* 72, 101587. <https://doi.org/10.1016/j.irfa.2020.101587>.
- Wang, P., Chen, M., Wu, J., Yan, Y., 2024b. Bank connectedness and excessive risk-taking: some cross-country evidence. *Financ. Res. Lett.* 60, 104921. <https://doi.org/10.1016/j.frl.2023.104921>.
- Wang, J., Ho, C.Y., Shan, Y.G., 2024a. Does cybersecurity risk stifle corporate innovation activities? *Int. Rev. Financ. Anal.* 91, 103028. <https://doi.org/10.1016/j.irfa.2023.103028>.
- Wang, R., Jiangtao, L., Luo, H., 2021. Fintech development and bank risk taking in China. *Eur. J. Financ.* 27 (4-5), 397–418. <https://doi.org/10.1080/1351847X.2020.1805782>.
- Wu, J., Guo, M., Chen, M., Jeon, B.N., 2019. Market power and risk-taking of banks: some semiparametric evidence from emerging economies. *Emerg. Mark. Rev.* 41, 100630. <https://doi.org/10.1016/j.ememar.2019.100630>.
- Yu, H., Liang, C., Liu, Z., Wang, H., 2023. News-based ESG sentiment and stock price crash risk. *Int. Rev. Financ. Anal.* 88, 102646. <https://doi.org/10.1016/j.irfa.2023.102646>.
- Zhang, Z., Wang, W., Song, C., 2024. Quantitative easing and bank risk-taking: evidence from the federal reserve's large-scale asset purchases. *Financ. Res. Lett.* 67, 105752. <https://doi.org/10.1016/j.frl.2024.105752>.
- Zhao, Y., Goodell, J.W., Wang, Y., Abedin, M.Z., 2023. Fintech, macroprudential policies and bank risk: evidence from China. *Int. Rev. Financ. Anal.* 87, 102648. <https://doi.org/10.1016/j.irfa.2023.102648>.
- Zreik, O., Louhichi, W., 2017. Risk sentiment and firms' liquidity in the French market. *Res. Int. Bus. Financ.* 39, 809–823. <https://doi.org/10.1016/j.ribaf.2014.11.003>.