Finance and Economics Discussion Series

Federal Reserve Board, Washington, D.C.
ISSN 1936-2854 (Print)
ISSN 2767-3898 (Online)

Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers

Jin-Wook Chang, Jacob Dice, Shengwu Du, Adam Flury, Sam Jerow, Seung Jung Lee, Stacey Schreft, and Craig Vandre

2025-103

Please cite this paper as:
Chang, Jin-Wook, Jacob Dice, Shengwu Du, Adam Flury, Sam Jerow, Seung Jung Lee, Stacey Schreft, and Craig Vandre (2025). "Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers," Finance and Economics Discussion Series 2025-103. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.103.

NOTE: Staff working papers in the Finance and Economics Discussion Series (FEDS) are preliminary materials circulated to stimulate discussion and critical comment. The analysis and conclusions set forth are those of the authors and do not indicate concurrence by other members of the research staff or the Board of Governors. References in publications to the Finance and Economics Discussion Series (other than acknowledgement) should be cleared with the author(s) to protect the tentative character of these papers.

Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers*

Jin-Wook Chang[a], Jacob Dice[b], Shengwu Du[a], Adam Flury[a], Sam Jerow[a], Seung Jung Lee[a], Stacey Schreft[c], and Craig Vandre[a]

[a] *Board of Governors of the Federal Reserve System*
[b] *Federal Reserve Bank of Kansas City*
[c] *Robert H. Smith School of Business, University of Maryland*

November 25, 2025

Abstract

This paper examines cyber vulnerabilities across the 100 largest US banks, non-bank financial institutions (NBFIs), and their third-party service providers. Our analysis, based on a proprietary cyber risk analytics model, shows NBFIs exhibit greater cyber vulnerabilities than banks, though banks face larger relative losses from routine incidents. We identify third-party service providers as a hidden cyber fault line in the financial system, often having greater vulnerabilities than the institutions they serve and creating systemic risks. Scenario analyses of catastrophic cyber events targeting these providers reveal potential losses up to about 60 times larger than routine incidents for both large banks and large NBFIs, with business interruptions driving most losses. Our findings highlight the need for a holistic cyber risk management approach addressing both individual vulnerabilities and systemic risks from interconnectedness in the financial system.

Keywords: Banks, Nonbank Financial Institutions (NBFIs), Third-Party Service Providers, Cyber Vulnerabilities, Cybersecurity, Scenario Analysis

JEL Codes: C15, G2

*The views expressed in this paper are solely those of the authors and do not reflect the opinions of the Board of Governors of the Federal Reserve System or the Federal Reserve Bank of Kansas City. Generative AI was used in the editing and proofreading of this paper. All errors are the authors'. Contact information: jin-wook.chang@frb.gov, seung.j.lee@frb.gov.

1. Introduction

Cyber risks have become an increasingly critical concern for the U.S. financial system, with both routine incidents and more systemic events involving third-party service providers posing significant threats to the financial system. For instance, in November 2023, a ransomware attack on ICBC's US operations led to disruptions in its ability to manage US Treasury trades and repo financing, briefly impacting the entire Treasury market. A more systemic event was the MOVEit Transfer Vulnerability Exploit, which led to data theft at more than two thousand entities including many financial institutions, which resulted in an estimated total cost of more than $10 billion. This incident, along with more recent ones such as the faulty software update from CrowdStrike in July 2024, underscores the hidden fault lines within the financial system's cyber infrastructure, where a single point of failure can cascade across multiple institutions.

This paper aims to quantify and compare cyber vulnerabilities in large U.S. banks and non-bank financial institutions (NBFIs), with a particular focus on the systemic risks posed by third-party service providers.[1] By analyzing data from CyberCube, a cyber risk analytics platform, and employing their advanced simulation techniques, we seek to illuminate the potential financial impacts of both routine cyber incidents and more systemic events. Our research objectives include assessing the relative cyber risk profiles of banks versus NBFIs, quantifying potential losses from various cyber scenarios, and identifying key vulnerabilities in the financial institution-service provider nexus. Through this analysis, we aim to contribute to a more comprehensive understanding of cyber risks in the U.S. financial system and inform policy considerations for enhancing cyber resilience.

Our analysis reveals several critical insights into cyber vulnerabilities across the U.S. financial system. Using CyberCube data that measures cyber vulnerabilities of firms, we find that large NBFIs generally exhibit greater cyber vulnerabilities than large banks, with 42%

[1] See Boyens et al. (2022) and Keskin et al. (2021), for example.

of NBFIs falling in the “high-risk region,” defined by CyberCube measures, compared to 27% of banks. Regression analysis confirms that the CyberCube measures strongly predict cyber incident probability. Paradoxically, while NBFIs show greater vulnerabilities, simulation results indicate banks face potentially larger 99th percentile losses relative to revenue from routine cyber incidents, with banks’ losses representing 41 basis points of annual revenue versus 20 basis points for NBFIs.

Our most significant finding is the identification of a hidden cyber fault line within the financial system: third-party service providers. These providers, particularly those identified as modeled single points of failure (SPoFs) by CyberCube, often have greater cyber vulnerabilities than the financial institutions they serve, with approximately 55% falling within the “high-risk region.” Many critical services that are provided by cloud service providers and cybersecurity firms, for example, are shared across nearly all major financial institutions, creating concentrated systemic risk. Scenario analyses of so-called catastrophic cyber events targeting these and other third-party providers reveal that the 99.9th percentile losses are up to about 60 times larger than those from routine incidents for large banks and large NBFIs. Business interruptions emerge as the primary driver of losses across most catastrophic scenarios, highlighting the need for robust business continuity planning that accounts for important third-party dependencies.

We first begin with a brief literature review in the following section, followed by a section on the data and methodology. We then go over the results of our analysis, after which we conclude.

2. Literature Review

The literature on cybersecurity in financial institutions has grown substantially in recent years, reflecting the sector’s increasing digitalization and the evolving threat landscape. Kopp et al. (2017) provide a comprehensive overview of cyber risks in finance, highlighting the unique vulnerabilities of financial institutions due to their critical role in the economy and their attractiveness as targets for cyber criminals. Kashyap and Wetherilt (2019) argue why cyber risk differs from other operational risks in the financial sector due to its intent, probability of success, possibility of a hidden phase, and evolving form of the risks. Duffie and Younger (2019) show that even though cyberattacks may not induce bank runs, as banks have access to substantial additional emergency liquidity from the Federal Reserve, cyberattacks can still damage the real economy because nonbanks may be reluctant to send funds through customary bank payment nodes. Bouveret (2019) emphasizes the need to improve the modeling of cyber risk from an operational risk perspective.

Relatedly, third-party risk management in financial institutions has gained increasing attention as the sector's reliance on external service providers has grown. Kotidis and Schreft (forthcoming) provide evidence of both direct and indirect contagion effects of a cyberattack on a core technology service provider on the banking sector. Crosignani et al. (2023) examines the supply chain effects of one of the most damaging cyberattacks in history, the NotPetya cyberattack of 2017. Although most of the downstream disruptions to operations were at nonfinancial firms, these firms in turn had to tap into their liquidity buffers and increase their reliance on external finance, drawing down their credit lines at banks. Ottonello and Rizzo (2024) show that software companies are a systemic source of cyber risk, because software vulnerabilities can spread to customer firms throughout the digital supply chain.

A recent strand of literature finds evidence of the effect of cybersecurity on firms' returns, costs, and defaults. Florackis et al. (2023) use textual analysis to develop a firm-level measure of cybersecurity risk based on SEC 10-K filings. They show that cybersecurity risk is priced in the cross-section of stock returns and that high-exposure firms perform poorly during times of high cybersecurity risk. Heo (2023) utilize the bank-level cybersecurity measure developed by Florackis et al. (2023) and show that an increase in cybersecurity risk raises the probability of bank default. Jamilov et al. (2021) use computational linguistics to develop a measure of firm-level cyber-risk exposure using corporate filings across 85 countries. Their measure also predicts cyberattacks and is reflected in stock returns. Jiang et al. (2024) use machine learning techniques to develop a firm-level measure of cyber risk and find that firms with higher cyber risk earn higher average stock returns. Kamiya et al. (2021) develop a model that explains how a successful attack leads to a significant loss in shareholder value and changes a firm's risk appetite and the stock price in the target's industry. They provide empirical evidence using publicly available cyber incidents data. These papers utilize publicly available price, accounting, and corporate filings data, and derive indirect evidence of cybersecurity risk. Unlike such papers in the literature, we utilize data from CyberCube to provide additional information that is more directly related to measures of cybersecurity to analyze the cybersecurity risk of financial institutions.

Cyber risks can be more relevant to larger institutions, which may have larger systemic implications due to their spillover effects on other institutions in the sector or the entire economy (Aldasoro et al., 2022). Chang et al. (2024) show that larger establishments (in terms of revenue and number of employees) and publicly traded companies are more likely to be targets of cyberattacks, based on analysis of a large granular dataset representing the population of all establishments in the US. Ramírez (2025) develops a simple equilibrium model in which larger institutions could be more likely targets of cyberattacks, but attackers become less selective as cybersecurity improves. Cong et al. (2025) find that the growth of crypto and digital assets has opened up new payment channels for cybercrimes, leading dominant organized criminal gangs to operate like firms that adopt modern revenue models and carefully manage their reputations. Such a trend can exacerbate attackers' tendency to target larger and more systemically important institutions. That said, Amir et al. (2018) find that small and medium firms underreport cyberattacks due to their private nature and lack of analyst coverage. We complement the findings in the literature by using cybersecurity data that does not depend on self-reporting.

Research on systemic cyber risks in the financial sector continues to evolve. Eisenbach et al. (2022) develop a model to assess how cyberattacks on banks can lead to liquidity disruptions and potential systemic crises, focusing on the wholesale payments network. Kosse and Lu (2022) also utilize the same framework and find how cyber risk can be amplified through the Canadian wholesale payment system. Brando et al. (2022) delves deeper into the systemic nature of cyber risks. They argue that the interconnectedness of the financial system amplifies the potential impact of cyber incidents. Their work emphasizes the need for a holistic approach that considers both individual institutional resilience and system-wide vulnerabilities. Anand et al. (2022) develop a model in which cyberattacks can induce bank runs and banks can prevent them by investing in cybersecurity. In their model, banks can free-ride on the security measures of others, resulting in underinvestment in cybersecurity in equilibrium. Ahnert et al. (2024) also develop a model, which shows that firms under-invest in cybersecurity in equilibrium even if firms can signal their investment to attract clients. They argue that imposing a minimum level of security investment can induce an efficient level of investment in cybersecurity. Eisenbach et al. (2025) show that systemic consequences of a successful cyberattack are higher when financial markets are strained.

There is a recent strand of literature that utilizes commercial ratings data, such as BitSight and CyberCube, as we do, and many studies have found these data to be useful. Baker and Ratnadiwakara (2025) show that commercial ratings, capturing externally observable, technical cyber hygiene and configuration indicators, meaningfully predict future bank cyber incidents above and beyond the balance sheet fundamentals. Murphy et al. (2025) also use CyberCube data, which is the main data of this paper, to model average annual loss (AAL) rates from "attritional" cyberattacks combined with standard bank performance measures to estimate cyber-related loss rates.

Notably, there is a lack of comprehensive studies that quantitatively compare cyber vulnerabilities across different types of financial institutions (e.g., banks vs. NBFIs) and assess the potential for contagion through shared third-party service providers. Additionally, while scenario analyses exist, they often fail to fully capture the complex interdependencies within the financial system and the potential for cascading effects from cyber incidents through supply chains.

3. Data and Methodology

We use data from CyberCube on various cyber security and exposure metrics for measuring cyber vulnerabilities at firms. The *security score* serves as a proxy for cybersecurity practices mostly based on externally observable data. A higher overall score, which considers more than 40 risk factors such as the existence of end-of-life products and unpatched software, indicates better cyber hygiene. The *exposure score* summarizes a firm's exposure to cyber incidents and incorporates both the firm's size and the external threat landscape. A higher exposure score indicates potentially more frequent cyberattacks. Firms with both a low security score and a high exposure score can be considered to be "high risk" for cyber incidents. The data are as of September 2025.

For our base analysis, we compare cyber security scores and exposure scores of the 100 largest banks and 100 largest NBFIs in terms of total assets as of end of 2024. The 100th firm in both samples are approximately the same in terms of total assets at around $6 to $8 billion, though their revenue profiles differ significantly. As seen in Figure 1, banks have more diverse asset sizes, from many small to a few giant ones. NBFIs cluster in the middle, with two common size groups, lacking the extremes seen in banks. In regard to revenue, banks cluster around lower revenues, peaking around $1 billion. NBFIs spread more widely, peak higher at around $10 billion, and have more high-revenue entities, suggesting they often outperform banks in revenue generation. We later run simulations to see the distribution of losses one can expect over the next year from routine cyber incidents.

We also look at the service providers connected to our sample of banks and NBFIs that constitute "modeled single points of failures" or modeled SPoFs—CyberCube identifies these as service providers whose vulnerabilities, if exploited, could lead to significant financial losses for many firms simultaneously due to their widespread use and interconnectedness. We can

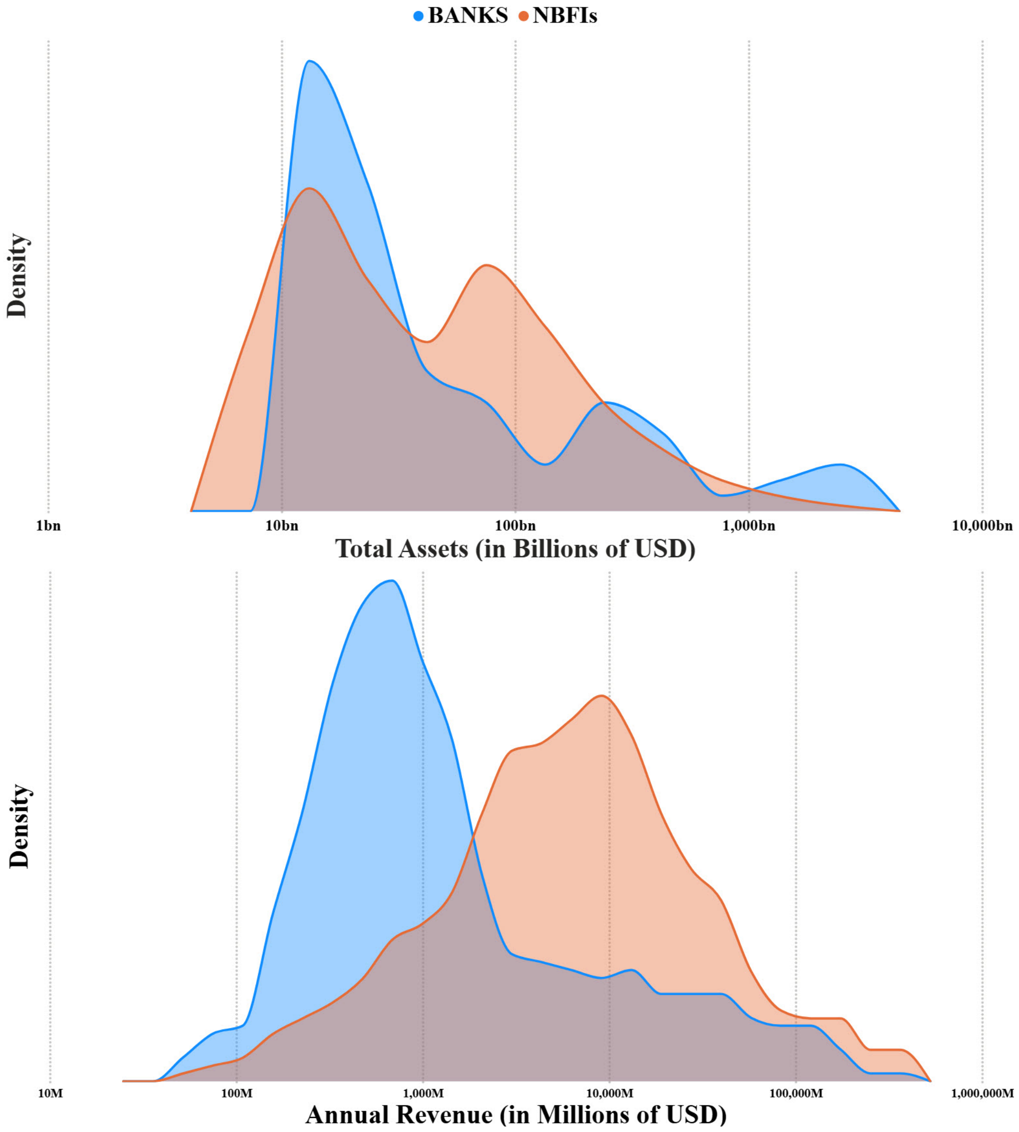

Figure 1: Distribution of Assets and Revenues for Top 100 Banks and NBFIs

Note: The top chart shows the distribution of assets, and the bottom chart shows the distribution of revenues. The blue area represents the distribution of banks, and the orange area represents the distribution of NBFIs. The horizontal axis in both charts indicates the $ amount, and the vertical axis indicates the empirically smoothed density. The top chart shows that banks have more diverse asset sizes, from many small to a few giant ones. NBFIs cluster in the middle, with two common size groups, lacking the extremes seen in banks. The bottom chart shows that banks cluster around lower revenues, peaking around $1 billion. NBFIs spread more widely, peak higher at around $10 billion, and have more high-revenue entities, suggesting they often outperform banks in revenue generation.

Source: S&P Global, Capital IQ Pro Platform, Compustat, CyberCube Analytics, Inc. and authors' calculations.

also look at the portion of these service providers that are high risk as defined above in terms of cyber risks, as well as their security and exposure scores. In addition, the term "modeled" refers to CyberCube's framework for analyzing different scenarios that could impact these modeled SPoFs and potentially cause financial losses to their many interconnected firms all at once.[2] This framework (called the CyberCube Portfolio Manager) employs a probabilistic Monte Carlo simulation method. It allows us to run 50,000 simulations of financial losses that can then inform the user of the scenarios we should be concerned about given a portfolio of firms we are interested in.[3] In our case, the portfolio of firms consists of the 100 largest banks and 100 largest NBFIs in terms of total assets.

The largest limitations of this study are two-fold. First, we do not observe the actual cyber risk management practices and operational resilience at these financial institutions. One could have the best cyber hygiene, but if risk controls and resilience are lacking, even small cyber events could lead to prolonged disruptions in operations or large financial losses. Second, the scenario analyses do not account for possible and, in some cases, likely spillover effects, which can cause losses to propagate throughout the financial system, for example through amplification of losses through counterparty losses, further disruptions to important nodes of the financial system, or accompanying large swings in market sentiment.

In addition to these limitations, another important consideration stems from CyberCube's use of a fuzzy entity resolution process, which attempts to match input company data with its internal data sources. This process is not infallible and can occasionally result in false positive matches. Consequently, there's a risk that incorrect Exposure, Security, or Single Point of Failure (SPoF) metrics may be assigned to a portfolio entity, potentially affecting the accuracy of the analysis.

[2] We find that the modeled SPoFs have a larger portion of exposure to security scores above the two mark than their unmodeled counterparts, implying that the modeled SPoFs have a higher likelihood of suffering a cyber incident. As modeled SPoFs are defined as service providers whose vulnerabilities, if exploited, could lead to significant financial losses for many firms at once due to their widespread use and interconnectedness, this illustrates that they are also more likely to suffer a cyberattack as well.

[3] CyberCube's Portfolio Manager was utilized in the creation of both the first ever private and publicly-placed cyber catastrophe bonds. They were issued in January and November of 2023, respectively. Similar to their natural disaster-related catastrophe bond counterparts, cyber catastrophe bonds are designed to provide insurance against catastrophic and systemic cyber events that have a fairly low probability of realization.

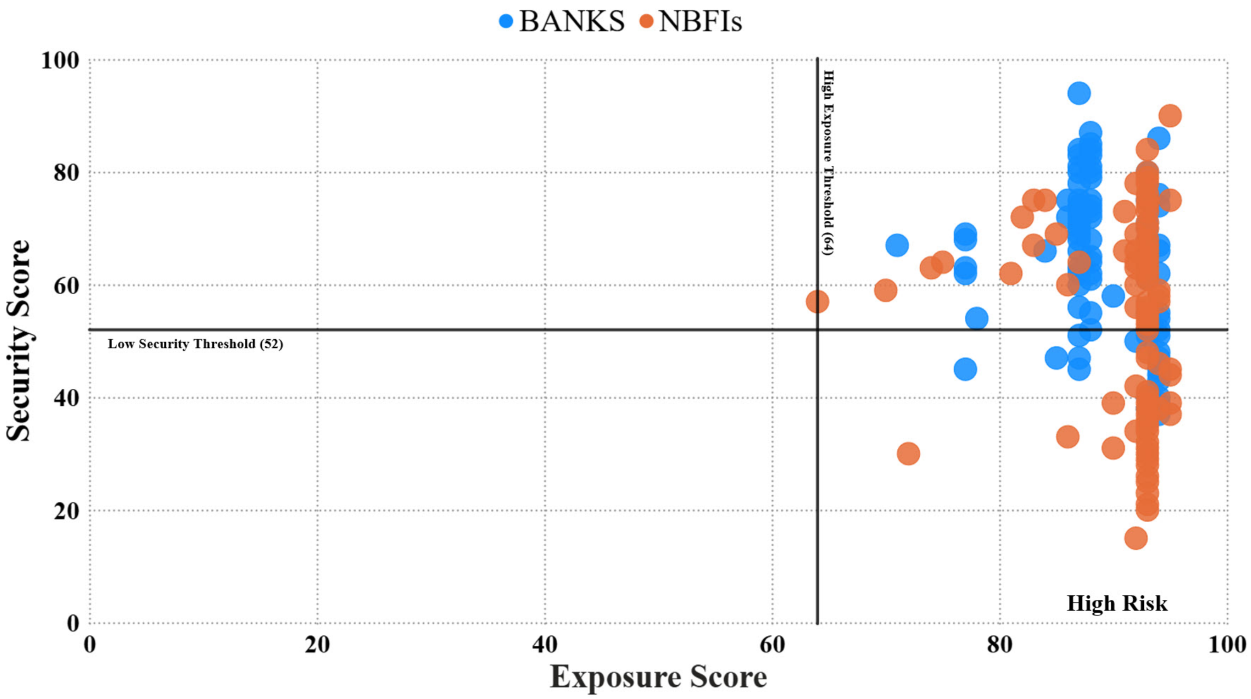

Figure 2: Security Scores and Exposure Scores for Top 100 Banks and NBFIs

Note: The horizontal axis indicates exposure score (measure of a firm's exposure to cyber incidents), and the vertical axis indicates security score (measure of a firm's cybersecurity practices), both ranging from 0 to 100. The vertical and horizontal black lines represent the threshold values of high exposure score (64) and low security score (52), respectively. The lower right quadrant indicates the entities with high risk of cyber vulnerabilities. 42 NBFIs are located in the "High Risk" quadrant compared to 27 banks, out of the top 100 each.

Source: CyberCube Analytics, Inc. and authors' calculations.

4. Results and Analysis

4.1. Comparison of cyber vulnerabilities – Banks vs. NBFIs

A simple scatter plot of cybersecurity scores against exposure scores for the top 100 banks and top 100 NBFIs reveals that more NBFIs are in the "High Risk" quadrant on the bottom right, which is defined by CyberCube as having security scores below 52 and exposure scores above 64 (Figure 2), than banks are. Indeed 42 NBFIs are located in that quadrant compared to 27 banks out of the top 100 each.

In order to see how the security and exposure scores help predict cyber incidents, we use a logit regression to estimate the relationship between the two variables and the probability of cyber incidents. The model is specified as below:

$$\ln\left(\frac{p_{i,t+1}}{1-p_{i,t+1}}\right) = \alpha_t + \beta X_{i,t} + \varepsilon_{i,t}, \tag{1}$$

where $p_{i,t+1}$ is the likelihood of a cyber incident for firm i provided by CyberCube, at time $t+1$, α_t is a time fixed effect, $X_{i,t}$ is a vector of explanatory variables with coefficient β, and $\varepsilon_{i,t}$ is a error term. We run four different regressions: first, we run the regression using the exposure score as the explanatory variable; second, we use the security score as the explanatory variable; third, our regression uses both; and the last regression uses the ratio of those two variables.

Table 1 provides the regression results. The results show that the security score has a consistently significant negative effect on cyber incident probability (coefficient -0.001 in Models 1 and 2, with $p < 0.001$ for both), indicating that better security measures reduce the likelihood of incidents. The exposure score shows a significant positive effect across models as well, indicating that greater exposures increase the likelihood of incidents. Notably, Model 4 introduces the Exposure/Security Ratio, which demonstrates a significant positive relationship with cyber incident probability (coefficient 0.083, with $p < 0.001$). This suggests that as the ratio of exposure to security increases, so does the likelihood of a cyber incident. The adjusted R^2 and F-statistic indicate that Model 4 has the strongest support. The models are based on a large sample size of 6,082 observations with 151 firms and approximately 4.5 years of monthly historical data.[4]

Figure 3 illustrates the relationship between the Exposure/Security Score Ratio and the predicted probability of a cyber incident, based on the logistic regression model (similar to model 4 but without considering the fix-effects). The figure shows a clear positive relationship between the Exposure/Security Score Ratio and the probability of a cyber incident occurring. As the ratio increases from 1.0 to 2.5, the predicted probability of an incident

[4] Some of the 200 firms are dropped due to unavailability in the time-series data source. There are 170 cyber incidents that are matched with the firms in our sample.

Table 1: Incident Probability Logit Regression

	Cyber Incident Probability			
	(1)	(2)	(3)	(4)
Exposure Score	0.002^{***}		0.001^{***}	
	(0.0003)		(0.0003)	
Security Score	-0.001^{***}	-0.001^{***}		
	(0.0002)	(0.0002)		
Exposure/Security Ratio				0.083^{***}
				(0.009)
Observations	6,082	6,082	6,082	6,082
R^2	0.012	0.008	0.003	0.013
Adjusted R^2	0.005	0.0005	-0.004	0.006
F Statistic	36.698^{***} (df = 2; 6036)	46.912^{***} (df = 1; 6037)	20.883^{***} (df = 1; 6037)	78.859^{***} (df = 1; 6037)

rises from approximately 2 percent to 10 percent. The relationship follows a typical logistic curve, with a steeper increase in probability as the ratio gets higher. The gray shaded area around the black line represents the confidence interval, which widens as the ratio increases, indicating greater uncertainty in the predictions at higher ratios. This visualization effectively demonstrates that firms with a higher exposure relative to their security measures (i.e., a higher Exposure/Security Score Ratio) face a substantially increased risk of experiencing a cyber incident. This underscores the importance of maintaining a balance between a company's cyber exposure and its security measures to mitigate the risk of cyber incidents.

Based on this analysis, we can summarize the comparison of cyber vulnerabilities at banks vs. NBFIs in one dimension by drawing a kernel density distribution of the exposure to security score ratio as in Figure 4. We see that many more NBFIs have more extreme exposure to security score ratios, consistent with the two-dimensional view in Figure 2. Therefore, NBFIs appear to be more susceptible to cyber incidents.

4.2. Routine cyber incident impacts

Next, we consider simulation results of routine cyber incidents referred to as "attritional losses." Attritional losses encompass two types: small losses, which are frequent cyber events affecting single companies with low severity, and large losses, which are less frequent but more

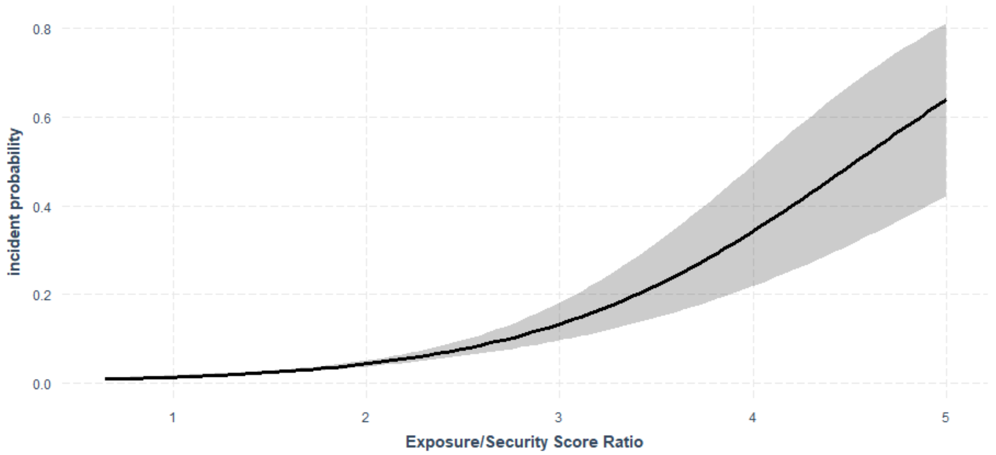

Figure 3: Exposure/Security Score Ratio and Cyber Incident Probability

Note: The horizontal axis indicates the ratio between exposure score and security score, and the vertical axis indicates incident probability. The black line represents the point estimates of the incident probability for each Exposure/Security Score Ratio, and as the ratio increases from 1.0 to 2.5, the predicted probability of an incident rises from approximately 2 percent to 10 percent. The gray shaded area around the black line represents the confidence interval, which widens as the ratio increases, indicating greater uncertainty in the predictions at higher ratios. This figure demonstrates that firms with a higher exposure relative to their security measures (i.e., a higher Exposure/Security Score Ratio) face a substantially increased risk of experiencing a cyber incident.

Source: CyberCube Analytics, Inc. and authors' calculations.

severe events also typically impacting individual companies. Table 2 illustrates that largest simulated losses come from malware attacks, followed by data breaches, and then network outages. But even all together, the 99.9th percentile of the simulated aggregate losses is about $7.8 billion for a given year (approximately $3.5 billion for banks and $4.3 billion for NBFIs), amount to 41 basis points (0.41%) and 20 basis points (0.20%) of aggregate annual revenue for the top 100 banks and the top 100 NBFIs, respectively.[5] This implies that while the 99.9th percentile losses are slightly higher for NBFIs, the losses relative to revenue from severe incidents are significantly larger at banks. The average annual losses show a similar pattern, with banks experiencing lower absolute losses ($104 million vs. $205 million) but higher losses relative to revenue compared to NBFIs.

[5] We run Monte Carlo simulations up to 50,000 times per possible scenario, so the 99.9th percentile is up to the 50th highest result per scenario.

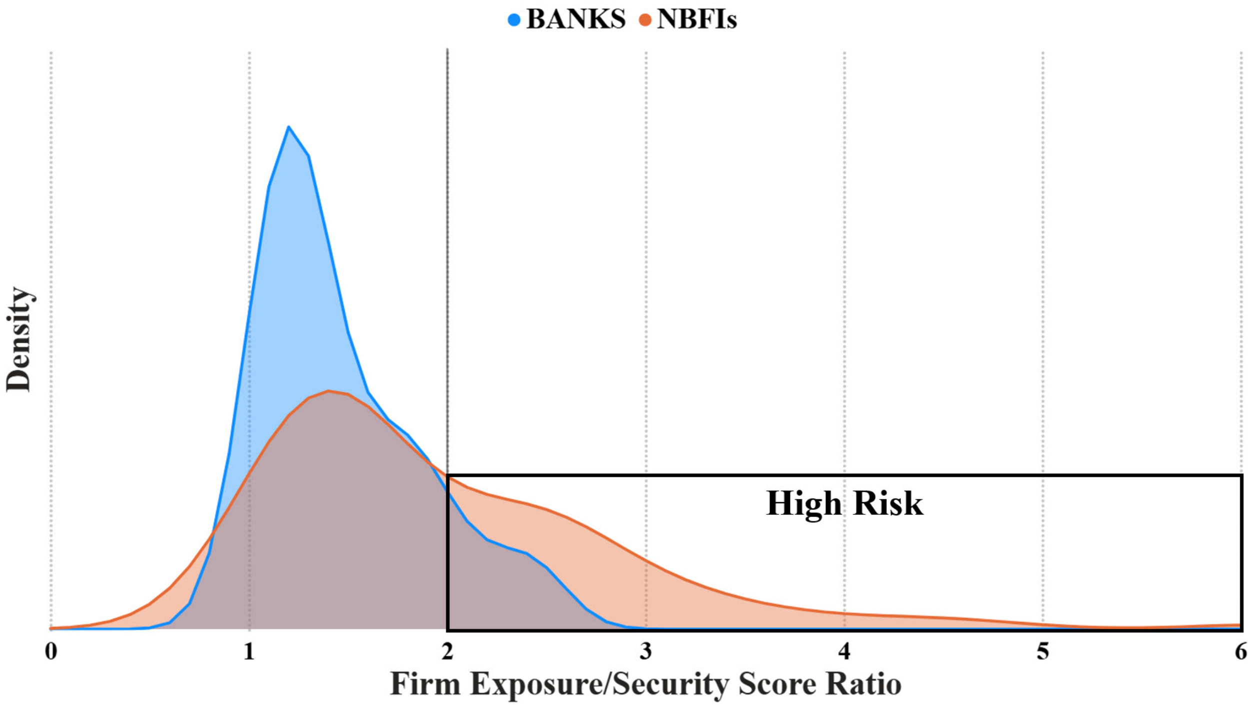

Figure 4: Distribution of Exposure/Security Score at the Largest Banks and NBFIs

Note: The horizontal axis indicates the ratio between exposure score and security score, and the vertical axis indicates the empirically smoothed density. The blue area represents the distribution of banks, and the orange area represents the distribution of NBFIs. The black box indicates the "High Risk" region, which is Exposure/Security Score Ratio being greater than 2. The figure shows that many more NBFIs have more extreme exposure to security score ratios, consistent with the two-dimensional view in Figure 2. Therefore, NBFIs appear to be more susceptible to cyber incidents.

Source: CyberCube Analytics, Inc. and authors' calculations.

4.3. Third-party service provider analysis

Next, we identify all the 200 or so modeled SPoF third-party service providers that service the banks and NBFIs in our sample. A comparison of provider families (Table 3) reveals similar technology adoption solutions between banks and non-banks across most provider categories, with Cloud Services, Security Tools, Communications Technology, and Network Computing being widely implemented by at least 97% of firms in both sectors. As can be seen in Figure 5, many of the same modeled SPoFs service both the top banks and NBFIs. For example, services such as Microsoft Exchange Online, AWS, DigiCert, CloudFlare, and Microsoft Azure are all connected to 95 or more of the top 100 banks and 95 or more of the top 100 NBFIs, respectively, according to the data (as of December 2024).

Table 2: Simulation Results for Attritional Losses

Top 100 Banks			
Type of Attack	Average Annual Loss ($ million)	99.9th Percentile Loss Systemwide ($ million)	99.9th Percentile Loss Systemwide (bps of revenue)
Integrity (Malware)	63	1,649	19
Confidentiality (Data Breach)	34	1,215	14
Availability (Network Outage)	7	593	7
Total Attritional Losses	104	3,457	41

Top 100 NBFIs			
Type of Attack	Average Annual Loss ($ million)	99.9th Percentile Loss Systemwide ($ million)	99.9th Percentile Loss Systemwide (bps of revenue)
Integrity (Malware)	112	2,176	10
Confidentiality (Data Breach)	80	1,492	7
Availability (Network Outage)	13	644	3
Total Attritional Losses	205	4,312	20

Source: CyberCube Analytics, Inc. and authors' calculations.

More importantly, one can see that a large portion of these modeled SPoFs are in the high-risk quadrant. Specifically, the majority or approximately 55 percent of all modeled SPoFs fall within the high-risk quadrant, which is a greater percentage than the banks and NBFIs that appear in the same region as shown in Figure 2. Only 14 modeled SPoFs (approximately 6% of the total) are not shared between banks and NBFIs in the high risk quadrant (Figure 6). Specifically, 4 SPoFs are used exclusively by banks, impacting 4 banking institutions, while the remaining 10 SPoFs are used exclusively by NBFIs, affecting 16 non-bank entities. Therefore, the third-party service providers can be considered a hidden cyber fault line; just below the financial system lie many service providers that support large financial firms. However, these service providers appear to have a higher probability of suffering a cyberattack than the financial firms they are servicing.

Figure 7 illustrates that the cyber vulnerabilities of the third-party service providers

Table 3: Bank and NBFI Modeled Technology Provider Families

Banks

Technology Provider Family	# of firms
Cloud Services	98
Security Tools	98
Communications Technology	97
Network Computing	97
Miscellaneous	96
Productivity Solutions	96
Financial	95
Operating Systems Computing Languages and Software	93
Data Storage Solutions	17

NBFIs

Technology Provider Family	# of firms
Cloud Services	100
Network Computing	99
Security Tools	98
Communications Technology	98
Financial	96
Miscellaneous	96
Productivity Solutions	96
Operating Systems Computing Languages and Software	95
Data Storage Solutions	18
Hardware	1

Source: CyberCube Analytics, Inc.

(modeled SPoFs) are worse than those of the top 100 banks and the top 100 NBFIs. The figure shows that a larger portion of modeled SPoFs fall within the high-risk region than the banks or NBFIs they serve, implying that the service providers have a higher likelihood of suffering a cyber incident. Interestingly, the distribution of NBFIs has a thicker tail than that of both groups of service providers. Also, there is no discernible difference in distribution of Exposure/Security Score Ratios between the bank service providers and NBFI service providers.

Lastly, our analysis of modeled SPoFs reveals distinct cloud provider dependency patterns across global data center locations (Figure 8). Note that our sample of firms consists of the top 100 banks and NBFIs in the USA, so their primary business operations are likely within the US. Amazon's cloud infrastructure shows predominant usage across geographic regions for both banks and NBFIs. Microsoft Azure shows a stronger representation in

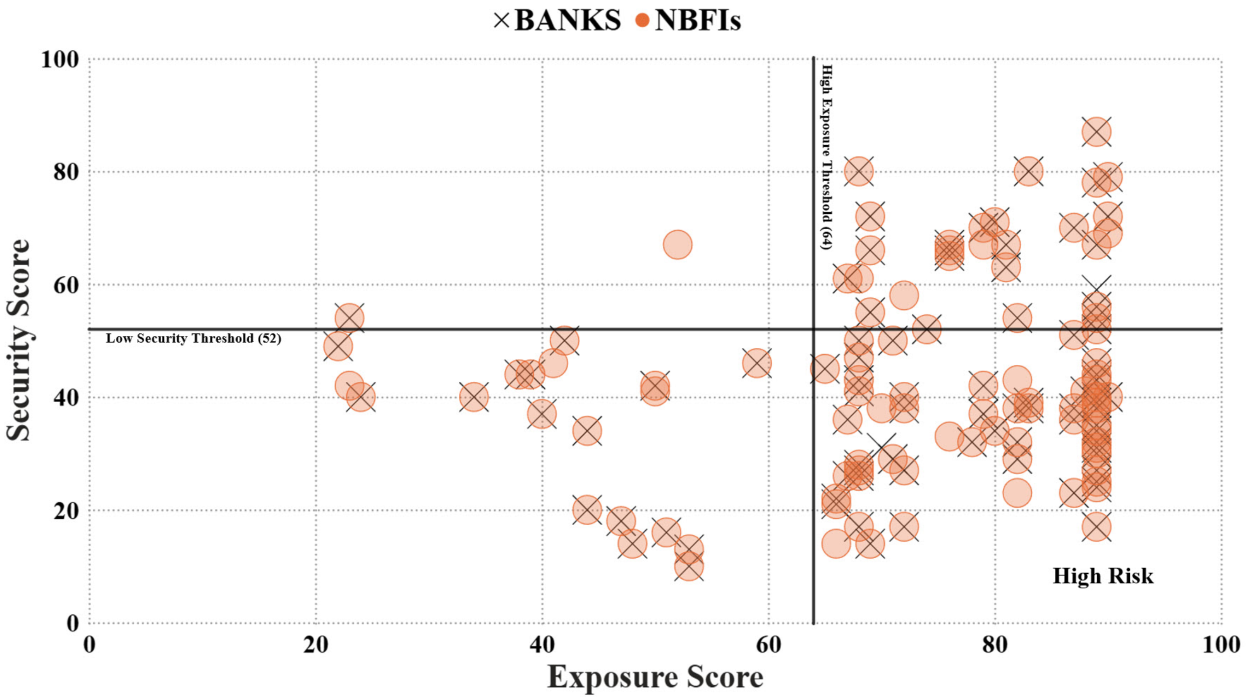

Figure 5: Bank and NBFI Modeled SPoF Security and Exposure Scores

Note: The horizontal axis indicates exposure score (measure of a firm's exposure to cyber incidents), and the vertical axis indicates security score (measure of a firm's cybersecurity practices), both ranging from 0 to 100. The vertical and horizontal black lines represent the threshold values of high exposure score (64) and low security score (52), respectively. The lower right quadrant indicates the entities with high risk of cyber vulnerabilities. Each point represents the exposure score and security score of a modeled Single Point of Failure (SPoF)—a significant service provider identified by CyberCube. The cross-marked points are modeled SPoFs that provide services to top 100 banks, the orange-circled points are modeled SPoFs that provide services to top 100 NBFIs, and the points with both cross mark and orange circle are modeled SPoFs that provide services to both top 100 banks and NBFIs. The figure shows that many of the same modeled SPoFs service both the top banks and NBFIs. The figure also shows that a large portion (approximately 55 percent) of these modeled SPoFs are in the high-risk quadrant. These service providers appear to have a higher probability of suffering a cyberattack than the financial firms they are servicing.

Source: CyberCube Analytics, Inc. and authors' calculations.

the USA. Google Cloud Platform shows lower adoption rates compared to AWS and Azure across all regions, possibly indicating a third-place position in the financial services cloud market serving banks and NBFIs. NBFIs appear to have more geographically diversified cloud infrastructure compared to banks, which show higher concentration in fewer locations, though both sectors maintain their highest presence in the USA and Germany.

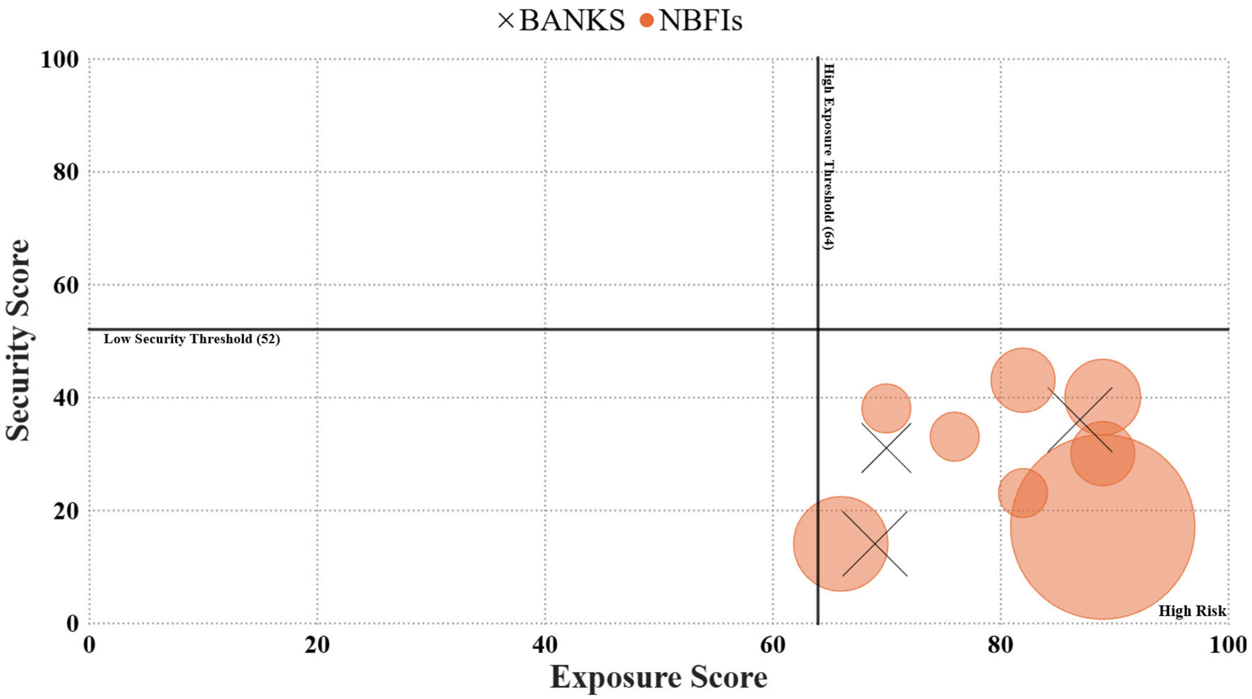

Figure 6: Bank and NBFI Modeled SPoFs not shared in High Risk quadrant

Note: The horizontal axis indicates exposure score (measure of a firm's exposure to cyber incidents), and the vertical axis indicates security score (measure of a firm's cybersecurity practices), both ranging from 0 to 100. The vertical and horizontal black lines represent the threshold values of high exposure score (64) and low security score (52), respectively. The lower right quadrant indicates the entities with high risk of cyber vulnerabilities. Each point represents the exposure score and security score of a modeled Single Point of Failure (SPoF)—a significant service provider identified by CyberCube. The cross-marked points are modeled SPoFs that provide services to top 100 banks, and the orange-circled points are modeled SPoFs that provide services to top 100 NBFIs. The figure depicts only the 14 modeled SPoFs (approximately 6% of the total) that are not shared by both the top banks and NBFIs. The size of a point is commensurate with the number of financial firms that the SPoF provides service to. The figure shows that only 4 SPoFs are used exclusively by banks, impacting 4 banks, while the remaining 10 SPoFs are used exclusively by NBFIs, affecting 16 NBFIs.

Source: CyberCube Analytics, Inc. and authors' calculations.

4.4. Systemic cyber event scenario analysis

Next, we investigate which types of cyberattack scenarios impacting third-party service providers potentially lead to the most financial losses for banks and NBFIs that they serve, respectively. We use CyberCube's Portfolio Manager to run 50,000 simulations to determine which type of "catastrophic" scenarios may lead to the most significant losses to these firms. Out of the 24 scenarios analyzed, Table 4 lists the six most catastrophic events by firm type,

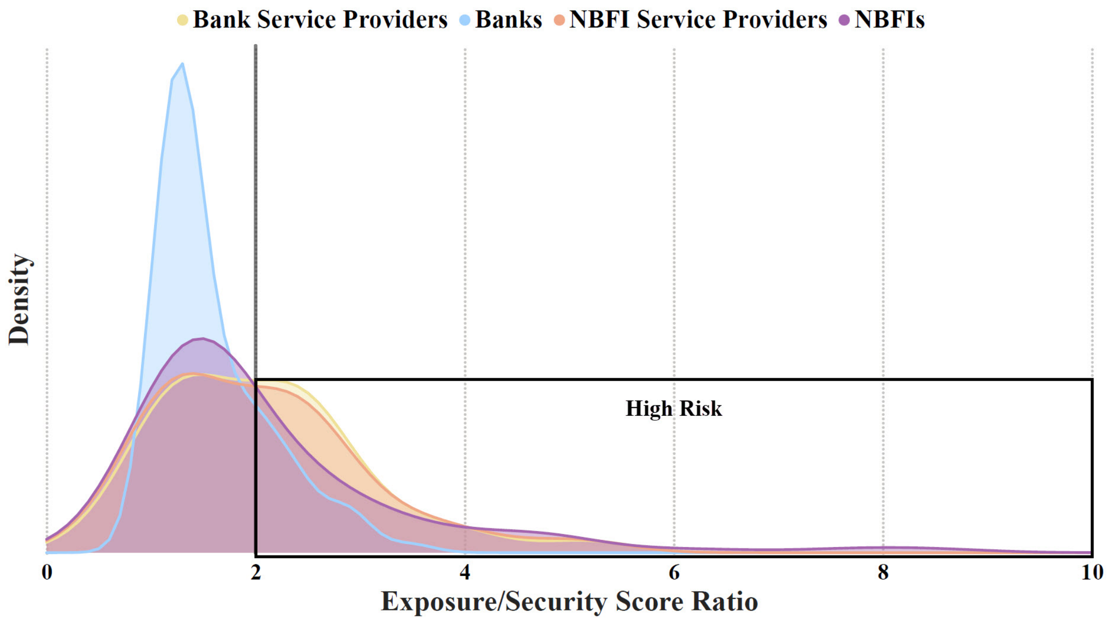

Figure 7: Exposure to Security Score Distribution of Banks/NBFIs vs. Their SPoFs

Note: The horizontal axis indicate the ratio between exposure score and security score, and the vertical axis indicate the empirically smoothed density of firms. The light-blue area represents the distribution of banks, the purple area represents the distribution of NBFIs, the yellow area represents the distribution of the modeled SPoFs servicing banks, and the orange area represents the distribution of the modeled SPoFs servicing NBFIs. The black box indicates the "High Risk" region, which is Exposure/Security Score Ratio being greater than 2. The figure shows that a larger portion of modeled SPoFs fall within the high-risk region than the banks or NBFIs they serve, implying that the service providers have a higher likelihood of suffering a cyber incident.

Source: CyberCube Analytics, Inc. and authors' calculations.

determined by the 99.9th percentile amount of aggregate simulated losses.[6] The greatest 99.9th percentile losses suffered by banks are driven by a large data breach scenario involving an E-commerce platform. At NBFIs, the largest 99.9th percentile losses are driven by a destructive malware attack on a significant cloud service provider. A destructive malware attack on server operating systems ranks as the second most catastrophic scenario according to the 99.9th percentile losses for NBFIs, while for banks it represents the fourth highest potential loss. Interestingly, if we look at the 90th percentiles of the scenarios, the destructive malware attack on a significant cloud service provider is more impactful than any data theft scenario for NBFIs. The 90th percentile losses are an order of magnitude smaller than the 99.9th percentile losses. The 50th percentile losses are a lot smaller still. In general, a

[6] The 99.9th percentile is the 50th highest result per scenario.

destructive malware attack on a cloud service provider affects many more firms, whether banks or NBFIs, than a large data theft scenario involving a service provider.

Compared to the losses associated with non-catastrophic cyber events in Table 2, the losses stemming from the top six catastrophic events in aggregate are far more severe—with the 99.9th percentile losses summing to be more than 66 times larger in the case of banks and more than 59 times larger in the case of NBFIs. Likewise, the events are also more impactful as a share of revenue than in the case for non-catastrophic routine events, for both banks and NBFIs. It's also interesting that for both banks and NBFIs' top catastrophic scenarios, cybercriminal groups are the most likely actor class to commit such attacks, accounting for approximately three-quarters of these attacks, followed by nation states.

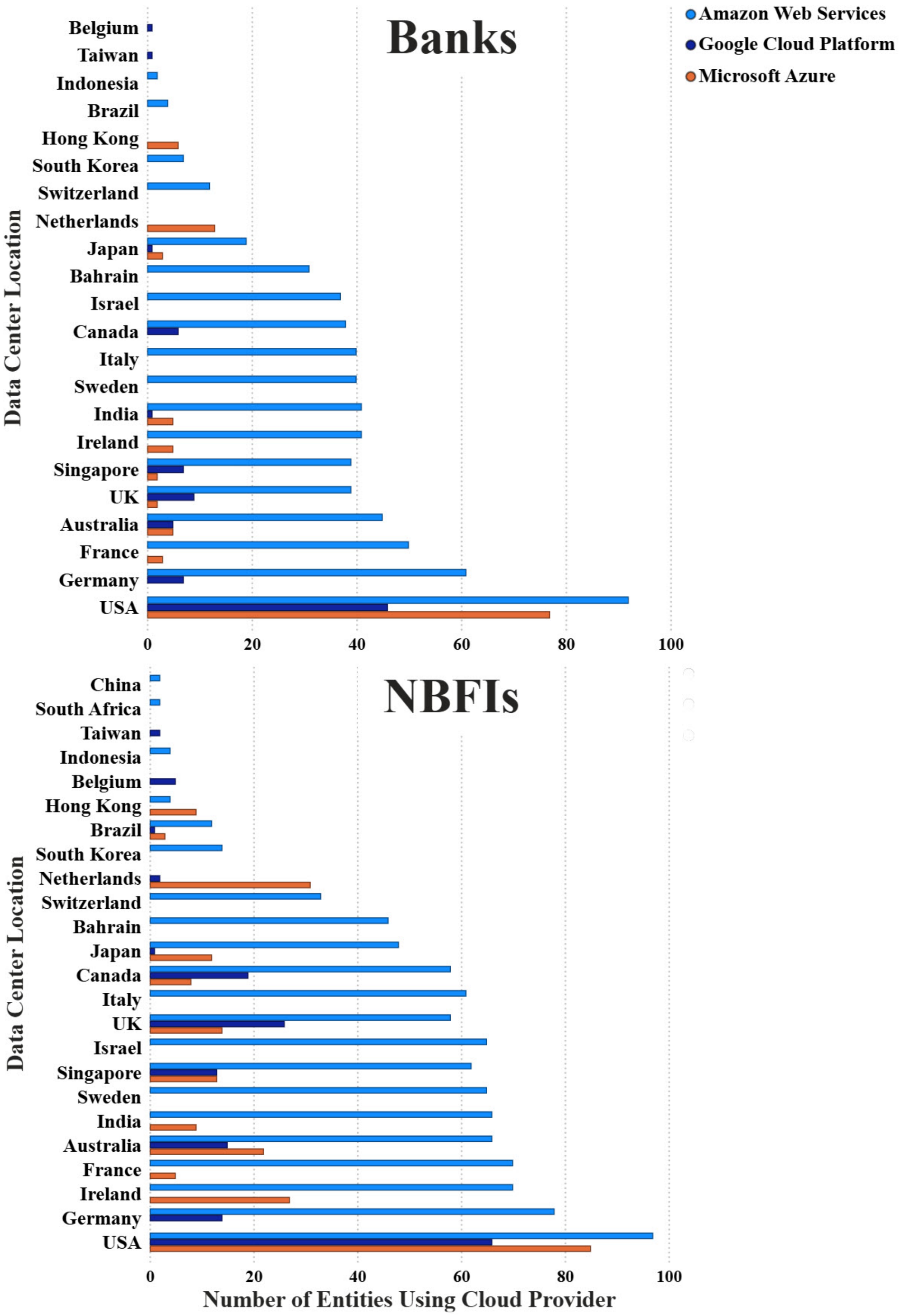

Figure 8: Cloud Providers by Data Center Location

Note: This figure shows cloud provider usage across global data centers for banks (top) and for NBFIs (bottom). NBFIs demonstrate greater geographic diversification in their cloud infrastructure, while banks concentrate in fewer locations. Both sectors maintain their strongest presence in USA and Germany.

Source: CyberCube Analytics, Inc. and authors' calculations.

Table 4: The Six Most Catastrophic Scenarios for the Largest Banks and NBFIs

	Number of Affected Entities		Simulated Losses			
	Min.	Max	99.9th Percentile Loss Systemwide ($billion)	99.9th % (bps of revenue)	90th % ($billion)	50th % ($billion)
Top 100 Banks						
Large Scale Data Theft - Leading E-Commerce Platform	1	4	83.9	988	5.5	0.1
Destructive Malware - Cloud Services Provider	1	90	43.5	513	5.5	0.2
Ransomware - Server Operating System	1	80	28.1	331	2.0	0.1
Destructive Malware - Server Operating System	1	77	32.1	378	4.3	0.0
Ransomware - Endpoint Operating System	1	92	27.6	325	2.5	0.2
Large Scale Ransomware - Leading Cloud-based Enterprise File Sharing Provider	1	63	16.0	189	0.7	0.2
Total			231	2,724		
Top 100 NBFIs						
Destructive Malware - Cloud Services Provider	1	92	80.6	377	11.4	1.0
Destructive Malware - Server Operating System	1	75	47.6	223	4.7	0.3
Large Scale Data Theft - Leading Asset Manager Fund Administrator	1	31	44.5	208	2.3	0.2
Destructive Malware - Endpoint Operating System	1	76	41.8	196	6.6	0.8
Ransomware - Endpoint Operating System	1	82	23.5	110	4.1	0.4
Ransomware - Cloud Services Provider	1	93	19.6	92	3.7	0.2
Total			258	1,206		

Source: CyberCube Analytics, Inc. and authors' calculations.

CyberCube also enables the user to break down where the losses are attributed to based on the different scenarios. The simulated losses incurred under a given scenario are determined by several firm characteristics, such as revenue, industry, and cybersecurity, as well as scenario characteristics, including severity and the targeted third-party service provider. In Figure 9, the events, each represented by a bar, are in descending order left to right based on the 99.9th percentile losses across the top 6 catastrophic scenarios. Generally, losses at banks are primarily driven by business interruptions. It is worth noting, however, that business interruptions can sometimes be helpful in preventing an issue from persisting undetected, which in turn raises investigation and response costs as seen in the scenario involving ransomware affecting a leading cloud based enterprise file sharing provider. Additionally, regulatory costs become more significant when there are events involving consumer data as in the case involving a leading E-commerce platform. The results for NBFIs are similar to banks in that business interruptions are a key driver of losses across several events. In addition, a data theft event involving a fund administrator is the third top catastrophic event for NBFIs, and this mostly consists of losses associated with fund transfer fraud. This loss component does not show up under any of the top 6 catastrophic events for banks, reflecting the unique role that some asset manager fund administrators play in servicing NBFIs.

5. Discussion and Conclusion

This study attempts to provide a comprehensive analysis of cyber vulnerabilities in the U.S. financial system, with a particular focus on the largest banks and NBFIs, as well as their third-party service providers. Our findings reveal several critical insights that have significant implications for cybersecurity risk management and financial stability.

First, our analysis demonstrates that NBFIs generally exhibit greater cyber vulnerabilities compared to banks. This is evidenced by the higher proportion of NBFIs falling into the "High Risk" quadrant based on their security and exposure scores. The logistic regression

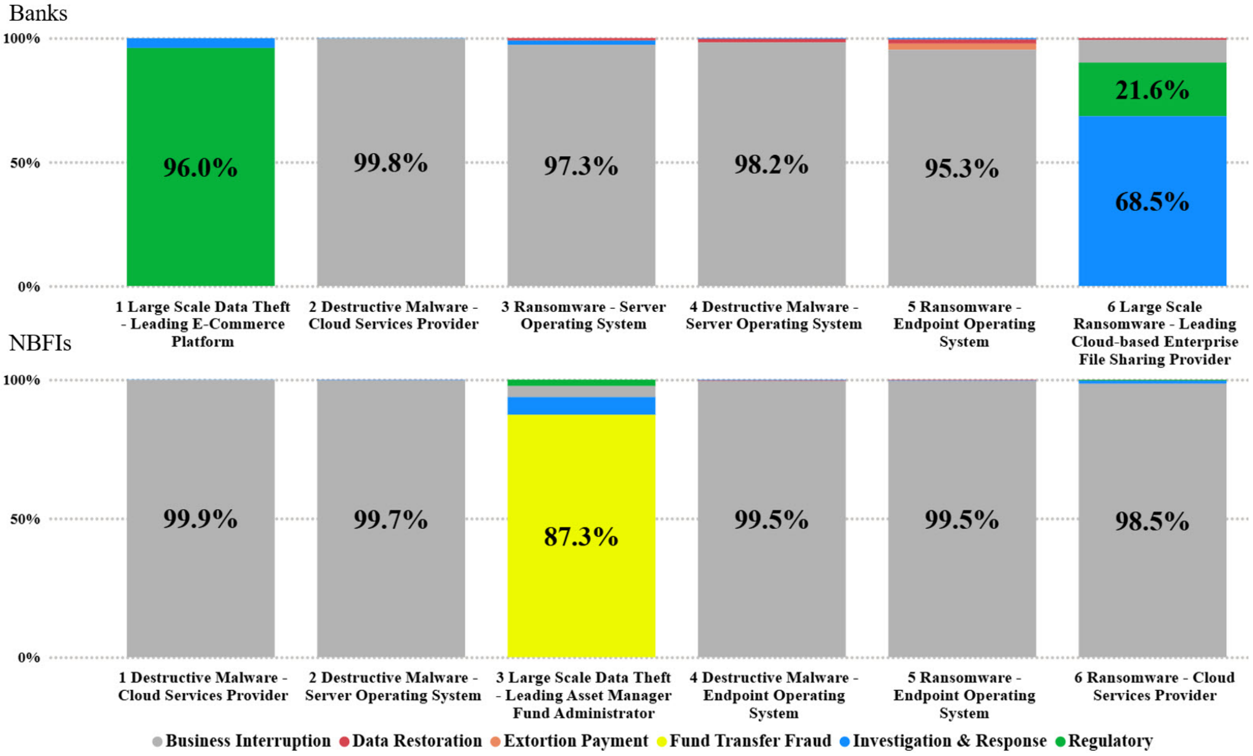

Figure 9: Loss Components of the Six Scenarios with Largest 99.9th Percentile Losses at Banks and NBFIs

Note: This figure shows the composition of sources of losses for the top 6 catastrophic scenarios, each represented by a bar, for banks (top chart) and for NBFIs (bottom chart). The top chart shows that losses are primarily driven by business interruptions for banks. Regulatory costs become more significant when there are events involving consumer data as in the case involving a large-scale data theft of a leading E-commerce platform. The bottom chart shows that for NBFIs, business interruptions are also a key driver of losses across several events as for banks. In addition, a data theft event involving a fund administrator is the third-highest catastrophic event for NBFIs, and this mostly consists of losses associated with fund transfer fraud. This loss component does not show up under any of the top 6 catastrophic events for banks, reflecting the unique role that some asset manager fund administrators play in servicing NBFIs.

Source: CyberCube Analytics, Inc. and authors' calculations.

results further support this finding, showing that the ratio of exposure to security scores is a strong predictor of cyber incident probability. This suggests that NBFIs may need to be continuously improving their cybersecurity measures to reduce their vulnerability to attacks.

However, our simulations of routine cyber incidents reveal that banks face potentially larger losses relative to their revenue compared to NBFIs. This paradoxical finding implies that while NBFIs may be more susceptible to cyberattacks, the impact of such attacks on banks could be more severe relative to revenue. This underscores the need for robust cyber risk management strategies across all types of financial institutions, with banks potentially needing to focus more on mitigating the potential impact of cyber incidents or operational resilience.

Perhaps the most interesting finding of our study is the identification of a hidden cyber fault line within the financial system, represented by third-party service providers. Our analysis shows that these service providers, particularly those identified as modeled SPoFs, have even greater cyber vulnerabilities than the financial institutions they serve. This creates a systemic risk that extends beyond individual institutions and potentially threatens the stability of larger parts of the financial system.

The scenario analysis of catastrophic cyber events further emphasizes this point. The simulated potential losses from these events, which primarily target third-party service providers, are substantially larger than those from routine cyber incidents—up to 66 times larger for banks and 59 times larger for NBFIs based on just the top 6 scenarios for each type of firm. This highlights the critical importance of third-party risk management in the financial sector's overall cybersecurity strategy.

Moreover, our analysis of loss components reveals that business interruptions are a primary driver of losses across most catastrophic scenarios for both banks and NBFIs. This underscores the need for robust business continuity and disaster recovery plans. The unique vulnerability of NBFIs to fund transfer fraud in scenarios involving fund administrators also highlights the need for sector-specific cybersecurity measures.

These findings have several important implications for policy and practice. First, given the varying cybersecurity profiles and potential impacts on banks and NBFIs, regulators may need to consider tailored approaches to cybersecurity surveillance and response for different types of financial institutions. Second, there may be a need to consider more ways of ensuring better cyber hygiene at third-party service providers, particularly those identified as potential significant SPoFs. Critical third parties and the services provided will vary from firm to firm; however, even small, seemingly insignificant third parties with access to the institutions network can lead to a significant cyber event. Third, the financial sector and regulators could think about developing more comprehensive strategies to address the systemic risks posed by the concentration of critical services among a small number of third-party providers. Fourth, reaffirm the importance of financial institutions development and regular testing of robust business continuity and disaster recovery plans, with a particular focus on scenarios involving the failure of critical third-party services. Finally, enhanced information sharing mechanisms between financial institutions, service providers, and regulators could improve the sector's overall cyber resilience and ability to respond to threats.

While our study provides valuable insights, it's important to note its limitations. We do not directly observe the internal cybersecurity practices and operational resilience of the institutions studied, and our scenario analyses do not account for potential contagion effects, for example from broader financial market dynamics. Furthermore, the use of CyberCube's fuzzy entity resolution process in matching company data introduces a potential for false positive matches, which could lead to inaccuracies in assigned metrics and affect the overall analysis. Future research should aim to address these limitations and further explore the complex interdependencies within the financial system's cyber infrastructure.

In conclusion, this study underscores the critical importance of cybersecurity in maintaining stability in the financial system. It highlights the need for a holistic approach to cyber risk management that considers not only individual institutional vulnerabilities but also the systemic risks posed by the interconnected nature of the financial system and its reliance on third-party service providers. As cyber threats continue to evolve, ongoing research and adaptive policy responses will be crucial in safeguarding the resilience of the US financial system.

References

Ahnert, T., M. Brolley, D. A. Cimon, and R. Riordan (2024): “Cyber risk and security investment,” *Working paper.*

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach (2022): “The drivers of cyber risk,” *Journal of Financial Stability*, 60, 100989.

Amir, E., S. Levi, and T. Livne (2018): “Do firms underreport information on cyber-attacks? Evidence from capital markets,” *Review of Accounting Studies*, 23, 1177–1206.

Anand, K., C. Duley, and P. Gai (2022): “Cybersecurity and financial stability,” *Deutsche Bundesbank Discussion Paper.*

Baker, S. D. and D. Ratnadiwakara (2025): “Cyber Risk in Banking: Measuring and Predicting Vulnerability,” *Working Paper.*

Bouveret, A. (2019): “Estimation of losses due to cyber risk for financial institutions,” *Journal of Operational Risk*, 14, 1–20.

Boyens, J., A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon (2022): “Cybersecurity supply chain risk management practices for systems and organizations,” Tech. Rep. 800-161, National Institute of Standards and Technology.

Brando, D., A. Kotidis, A. Kovner, M. J. Lee, and S. L. Schreft (2022): “Implications of Cyber Risk for Financial Stability,” *FEDS Notes.*

Chang, J.-W., K. Jayachandran, C. A. Ramírez, and A. Tintera (2024): “On the anatomy of cyberattacks,” *Economics Letters*, 238, 111676.

Cong, L. W., C. R. Harvey, D. Rabetti, and Z. Y. Wu (2025): “An anatomy of crypto-enabled cybercrimes,” *Management Science*, 71, 3622–3633.

Crosignani, M., M. Macchiavelli, and A. F. Silva (2023): "Pirates without borders: The propagation of cyberattacks through firms' supply chains," *Journal of Financial Economics*, 147, 432–448.

Duffie, D. and J. Younger (2019): "Cyber Runs," *Hutchins Center Working Paper.*

Eisenbach, T. M., A. Kovner, and M. Lee (2025): "When It Rains, It Pours: Cyber Vulnerability and Financial Conditions," *Economic Policy Review*, 31, 1–24.

Eisenbach, T. M., A. Kovner, and M. J. Lee (2022): "Cyber risk and the US financial system: A pre-mortem analysis," *Journal of Financial Economics*, 145, 802–826.

Florackis, C., C. Louca, R. Michaely, and M. Weber (2023): "Cybersecurity risk," *The Review of Financial Studies*, 36, 351–407.

Heo, Y. (2023): "Cybersecurity and Bank Distance-to-Default," *Swiss Finance Institute Research Paper.*

Jamilov, R., H. Rey, and A. Tahoun (2021): "The anatomy of cyber risk," Working Paper w28906, National Bureau of Economic Research.

Jiang, H., N. Khanna, Q. Yang, and J. Zhou (2024): "The cyber risk premium," *Management Science*, 70, 8791–8817.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz (2021): "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, 139, 719–749.

Kashyap, A. K. and A. Wetherilt (2019): "Some principles for regulating cyber risk," in *AEA Papers and Proceedings*, American Economic Association 2014 Broadway, Suite 305, Nashville, TN 37203, vol. 109, 482–487.

Keskin, O. F., K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar (2021): "Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," *Electronics*, 10.

Kopp, E., L. Kaffenberger, and C. Wilson (2017): "Cyber Risk, Market Failures, and Financial Stability," IMF Working Paper 17/185, International Monetary Fund.

Kosse, A. and Z. Lu (2022): "Transmission of cyber risk through the Canadian wholesale payment system," *Journal of Financial Market Infrastructures*, 10, 1–28.

Kotidis, A. and S. Schreft (forthcoming): "The Propagation of Cyberattacks through the Financial System: Evidence from an Actual Event," *Journal of Finance*, forthcoming.

Murphy, A., M. L. Tindall, K. Klemme, J. I. Suek, and S. Dunbar (2025): "What Drives Cyber Losses at US Banks? Potential Statistical Markers," *FRB of Dallas Working Paper*.

Ottonello, G. and A. E. Rizzo (2024): "Do Software Companies Spread Cyber Risk?" *Working Paper*.

Ramírez, C. A. (2025): "On equilibrium cyber risk," *Economics Letters*, 251, 112307.