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

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

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

Introduction: The Growing Cyber Threat

Cyber risks threaten U.S. financial stability through both routine incidents and systemic events involving third-party providers.

Recent Major Incidents:

- **November 2023:** ICBC ransomware attack disrupted Treasury market operations
- **MOVEit Vulnerability:** Data theft at 2,000+ entities, >$10 billion cost
- **July 2024:** CrowdStrike outage exposed systemic infrastructure vulnerabilities

Research Questions:

- How do cyber vulnerabilities differ between banks and NBFIs?
- What are potential losses from routine vs. catastrophic events?
- What systemic risks do third-party providers pose?

Data & Methodology

Sample: Top 100 US banks and 100 NBFIs by total assets (end of 2024), plus ~200 modeled single points of failure (SPoFs) among third-party providers.

CyberCube Metrics:

- **Security Score:** Cybersecurity practices based on 40+ risk factors (higher = better)
- **Exposure Score:** Firm's exposure to cyber incidents (higher = more exposure)
- **High Risk:** Security score <52 + Exposure score >64

Analysis:

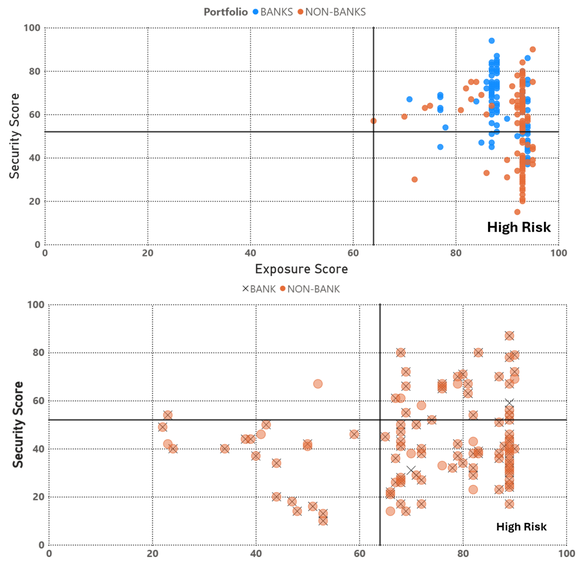
- Logistic regression (6,082 observations, 151 firms, 4.5 years data)
- Catastrophic event scenario analysis (CyberCube model)

Select References

- Baker, S. D. and D. Ratnadiwakara (2025): "*Cyber Risk in Banking: Measuring and Predicting Vulnerability.*" Working paper.
- Brando, D., A. Kotidis, A. Kovner, M. J. Lee, and S. L. Schreft (2022): "*Implications of Cyber Risk for Financial Stability.*" FEDS Note.
- Eisenbach, T. M., A. Kovner, and M. J. Lee (2022): "*Cyber risk and the US financial system: A pre-mortem analysis.*" Economic Policy Review.
- Kotidis, A. and S. Schreft (2025): "*The Propagation of Cyberattacks through the Financial System: Evidence from an Actual Event.*" Journal of Finance.
- Kopp, E., L. Kaffenberger, and C. Wilson (2017): "*Cyber Risk, Market Failures, and Financial Stability.*" IMF Working Paper 17/185.

Result #1: Service Providers Most Vulnerable

~55% of modeled service providers fall in the "high-risk region" vs. **42% of NBFIs** vs. **27% of banks.** This indicates that service providers are a potential source of systemic risks for the financial system.



Result #2: Cyber Scores Predict Cyber Incidents

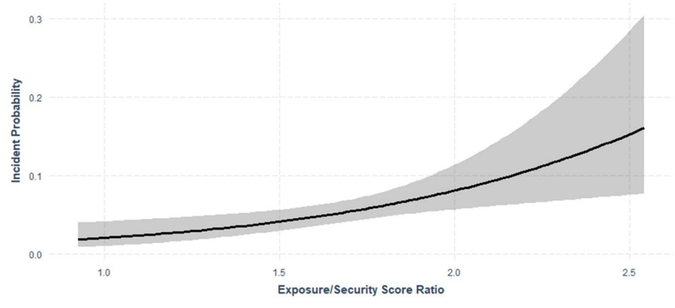
Logistic Regression Results:

- **Exposure/Security Ratio:** Strongest predictor (coef. 0.083, p < 0.001) of cyber incidents
- As ratio increases 1.0 → 2.5, incident probability rises 2% → 10%
- Exposure (+) and security (-) scores also significantly predict incidents

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

Where:

- $p_{i,t+1}$ is the likelihood of a cyber incident for firm *i* at time *t+1*
- $X_{i,t}$ is the ratio of the Exposure score to the Security score for firm *i* in time *t*



Result #3: Routine Losses are Higher for Banks

Despite higher NBFI vulnerabilities, **banks face larger losses relative to revenue** from routine incidents. These routine losses are driven by things such as malware attacks, data breaches, and network outages.

	Avg. Annual Loss ($millions)	99.9th Percentile Loss Systemwide ($millions)	99.9th Percentile Loss Systemwide (bps of revenue)
Banks	104	3,457	41
NBFIs	205	4,312	20

Result #4: Catastrophic Scenarios Drive Large Losses

99.9th percentile losses from catastrophic events are approximately 60x larger than routine incidents for both banks and NBFIs. Cybercriminal groups are the most likely actor class to commit such attacks, accounting for approximately three-quarters of these attacks, followed by nation states.

Simulated Losses

	99.9th Percentile Loss Systemwide ($billion)	99.9th % (bps of revenue)	90th % ($billion)	50th % ($billion)
Banks				
Data Theft - E-Commerce Platform	83.9	988	5.5	0.1
Destructive Malware - Cloud Provider	43.5	513	5.5	0.2
Ransomware - Server OS	28.1	331	2.0	0.1
NBFIs				
Destructive Malware - Cloud Provider	80.6	377	11.4	1.0
Destructive Malware - Server OS	47.6	223	4.7	0.3
Data Theft - Fund Administrator	44.5	208	2.3	0.2

Losses are driven primarily by business disruptions – approximately 68.5-99.8% of catastrophic losses for both banks and NBFIs. Other loss components include data restoration, extortion payment, investigation & response, regulatory costs.

Conclusions

Major Findings:

- **NBFIs exhibit greater cyber vulnerabilities than banks** (42% vs. 27% high-risk), but **service providers are most vulnerable** (~55% high-risk)
- **Cyber scores can robustly predict likelihood of a cyber incident**
- **Banks face larger relative losses** from routine incidents (41 vs. 20 bps)
- **Catastrophic events 60x larger** than routine incidents
- **Business interruptions dominate** (68.5-99.8% of catastrophic losses)

As cyber threats evolve, ongoing research and adaptive policy responses are crucial for safeguarding US financial system resilience.