STAFF
REPORTS

NO. 1186
FEBRUARY 2026

Systemic Cyber Risk

Steven D. Baker | Michael Junho Lee

FEDERAL RESERVE BANK *of* NEW YORK

Systemic Cyber Risk

Steven D. Baker and Michael Junho Lee

Federal Reserve Bank of New York Staff Reports, no. 1186
February 2026
https://doi.org/10.59576/sr.1186

Abstract

We propose a quantitative framework to track systemic risk arising from cyber vulnerabilities of the U.S. financial system. Synthesizing financial, economic, cyber, and network data that covers thousands of financial institutions and technological firms, we develop an index that tracks financial-system-level cyber vulnerability (SCV) for the financial system. Geopolitical risk, ransomware and malware incidents, and seasonal factors significantly drive the estimated adversarial component. Estimated technological and financial components exhibit fat tails in the distribution. In the cross-section, SCV is attributable to a small set of the largest firms. Large technology firms, including Microsoft, Google, Cisco, and Apple, emerge as key contributors to SCV. These providers also represent the largest cumulative count of vulnerabilities, pointing to financial stability considerations arising from the common exposure to client firms. SCV for service providers co-varies with that of financial institutions, which could amplify financial stability risks. The framework puts forth an approach to include a broad set of entities into an aggregate assessment of cyber vulnerability.

JEL classification: G21, G23, G28, G29, O33
Key words: financial system architecture, index, cyber risk, systemic risk, financial stability

Lee: Federal Reserve Bank of New York (email: michaeljunholee@gmail.com). Baker: Federal Reserve Bank of Richmond (email: steven.baker@rich.frb.org). This paper has greatly benefited from discussions and feedback from Seung Lee, Beth Klee, Stacey Schreft, Jin-wook Chang, and members of the Guardians and CRDCs. The authors give special thanks to Sarah Wang and Sakshee Singh for exceptional research assistance.

This paper presents preliminary findings and is being distributed to economists and other interested readers solely to stimulate discussion and elicit comments. The views expressed in this paper are those of the author(s) and do not necessarily reflect the position of the Federal Reserve Bank of New York, the Federal Reserve Bank of Richmond, or the Federal Reserve System. Any errors or omissions are the responsibility of the author(s).

To view the authors' disclosure statements, visit
https://www.newyorkfed.org/research/staff_reports/sr1186.html.

1 Introduction

Among cybersecurity experts, the question is not *if* a cyber attack will trigger a systemic event, but *when*. Cyber risk has grown to be broadly recognized as a source of financial stability vulnerability (Healey et al., 2018; Kashyap and Wetherilt, 2019; Brando et al., 2022). Just in the past five years, virtually every layer of the financial system architecture has experienced a material cyber attack, including the Treasury market (e.g. ICBC-FS), Derivatives markets, global payments and settlement (e.g. Finastra), and technical infrastructure (e.g. Move, Solar Winds).

Significant work is dedicated to understanding the financial stability risks posed by cyber risk. Quantitatively tracking systemic cyber vulnerability requires accounting for a complex set of factors, including the strategic behavior of threat actors, evolving technological vulnerabilities and exploits, cybersecurity strengths and resilience of financial and non-financial firms (Erol and Lee, 2025; Hastings and Sethumadhavan, 2025), and amplifications through operational and financial linkages (Duffie and Younger, 2019; Eisenbach et al., 2022; Welburn and Strong, 2022; Eisenbach et al., 2024).

This paper addresses this void. We propose a quantitative framework of cyber vulnerability for the U.S. financial system to monitor financial stability implications arising from cyber risk that is comprehensive, dynamic, and interpretable. We build a measure of financial system-level cyber vulnerability (SCV) that tracks aggregate financial stability risks over time, using granular data from financial disclosures, cyber ratings, cyber incidents, operational and technological linkages, and various other sources covering roughly 5,000 financial institutions, technological service providers, and financial service providers.

The contribution of this paper is threefold. First, this paper serves as a blueprint for financial institutions, regulators, and cybersecurity experts to develop a rigorous economic framework for evaluating and tracking aggregate cyber exposure. Though this paper is decidedly focused on the U.S. financial system, the approach readily applies to other jurisdictions, sectors, and systems where systemic risk is a salient concern. In particular, it provides a tractable path to synthesizing a breadth of financial, cyber, and economic data into an index that is interpretable and actionable. Second, the index sheds light on latent factors that drive each component of systemic cyber risk in the US financial system. Notably, the adversarial contribution to systemic cyber risk rises with geopolitical tension and seasonalities. A dominant pattern is the rise of systemic risk associated with vulnerabilities associated with ransomware and zero-days, and concurrently firm-level weakeness in their defenses against malware exposure. Third, the index offers comprehensive evidence of significant systemic risks arising from technology providers, through shared dependencies of financial institutions.

We first present a theoretical model of system cyber vulnerability, in which vulnerability is jointly determined by cyber adversaries and firms. Cyber adversaries allocate resources across various attack vectors to infiltrate firms, with (limited) information on the cyber defenses of individual firms. Firms make investments to shore up their cyber defenses, based on (limited) information on adversarial activity. Importantly, firms do not fully internalize the system-level impact of cyber vulnerabilities, which could arise due to operational concentration or financial amplifications. These create potential for systemic vulnerabilities to arise that are not sufficiently factored into firms' in their financial and technological choices, whether they be banks, non-banks, or non-financial firms.

The model provides a decomposition of factors that each contribute to system cyber vulnerability. Each factor of vulnerability can be mapped to modular components, consisting of ″adversarial,″ ″technological,″ and ″financial.″ Intuitively, each component can be described as follows:

- **Adversarial.** captures vulnerabilities associated with the set of exploits and vulnerabilities, as well as the strategic behavior of adversaries and its related impact on the threat landscape;

- **Technological.** captures firm-level cyber vulnerabilities arising from its cyber defenses;

- **Financial.** captures systemic relevance of vulnerabilities based on the underlying operational and financial linkages between an individual firm and the financial system.

Guided by the model, we build an index for tracking systemic cyber risk, or System Cyber Vulnerability Monitoring Index ("SCyMoN"). Each component is estimated using a tailored procedure drawing from a broad set of financial stability, vendor, and/or publicly-sourced data. The *adversarial* component leverages economy-wide cyber incident and various indicators of cyber stress to track developments in attack-level vulnerabilities. The *technological* component incorporates firm-level cybersecurity signals and the history of cyber incidents to assess individual firms' cyber vulnerability. The *financial* component evaluates the systemic importance of individual firms using scenario-based measures, one that is liquidity-based and another that is asset-based, using payment and asset holdings data. These components are then synthesized into a top-level quarterly index.

In addition to being grounded by the model, there are practical advantages to the modular structure. First, each component can be estimated using a procedure tailored to the source of vulnerability. Given the heterogeneity of data and their associated characteristics for each component, this flexibility to approaching each component is valuable. Second, modularity supports interpretability. Fluctuations in system cyber vulnerability can be attributed to different components, which is useful to distill intuition based on changing contribution of each vulnerability. Third, it is easier to manage incremental improvements to the index over time, especially as more new data or insights emerge. This aspect fits the fast-paced developments in cybersecurity space.

Estimates of each component exhibit intuitive features. The adversarial component is strongly driven by measures of geopolitical risk and the global frequency of ransomware and malware attacks. These relationships establish links between structural factors, such as geopolitical tensions and the industrialization of cyber criminal enterprises, and adversarial activity targeting US companies. The technological component is driven by factors related to weak controls and practices, such as encryption protocol issues and risky internal behavior, and exposure to malware and ransomware. The financial component attributes systemicness to large financial institutions and demonstrates that a broad set of financial markets could be materially affected through common asset holdings across various types of financial institutions.

The index tracks financial system cyber vulnerability over time, and can be used to identify the underlying factors that contribute to system cyber vulnerability. Changes in the index can also be attributed to each component. Throughout 2022, the liquidity-based index trends downward, largely due to drops in the financial component associated with declining payment-related liquidity needs (Eisenbach et al., 2024). In mid-2023, The index spikes in tandem with the technological component, which indicates an increase in firm-level cyber vulnerability. Varying the approach to the financial component of the index sheds light on other financial stability risks originating from cyber vulnerability. An asset-based approach allows a breakdown of system cyber vulnerability by asset class. In our sample, loans represent the most exposed asset class, due in part to their illiquid nature.

The quantitative framework is extended to assess financial stability vulnerability arising from service providers. The model-implied cyber vulnerability of service providers co-moves with that of financial institutions, which is largely attributed to co-movement in realized cyber incidents for both set of firms. Service providers' systemicness is derived from the collective financial systemicness of dependent financial institutions. We identify service providers with the largest contribution to system cyber vulnerability.

This list includes Microsoft, Google, Cisco, and Apple and roughly corresponds to technology providers with the largest cumulative count of vulnerabilities over the past half decade. This points to financial stability considerations arising not only from the commonality in service providers for multiple large financial institutions, but also from the common exposure to vulnerabilities originating from service providers, which has been associated with higher likelihood of a cyber incident for dependent firms (Ottonello and Rizzo, 2024).

Literature Review. Our paper relates to the cyber risks to financial stability. A growing literature recognizes the financial stability implications of disrupting the flow of liquidity within the financial system. Scenario-based analyses demonstrate how cyber attacks result in aggregate liquidity dislocations, which can then be amplified through strategic timing by adversaries, liquidity hoarding behavior, and by adverse financial conditions (Duffie and Younger, 2019; Eisenbach et al., 2022, 2024). Kotidis and Schreft (2023) provides a real-life account of these mechanisms in play. Erol and Lee (2025) shows general shortcoming of cyber resiliency of financial and technological infrastructure. Ottonello and Rizzo (2024) provides evidence that shows cyber risk spillovers from software providers to downstream firms.

Our work relates to the literature on quantifying systemic risk. A segment of the literature focuses on financial vulnerabilities arising from shared asset holdings, which can act as a nexus of contagion through fire-sales (Greenwood et al., 2015; Cetorelli et al., 2016; Duarte and Eisenbach, 2021; Falato et al., 2021; Cetorelli et al., 2023). This paper puts forth a framework to track and analyze the technological sources of systemic risk, a dimension that is yet underexplored. Importantly, we build on existing approaches to evaluating financial systemicness of firms, including those pioneered by Duarte and Eisenbach (2021) and Eisenbach et al. (2022) to contexualize the financial implications of cyber vulnerability.

Our paper contributes to the literature on cyber risk forecasting models. A sizable literature focuses on forecasting cyber incidences, using machine learning techniques (Sun et al., 2018; Fang et al., 2019; Almahmoud et al., 2023). The adversarial component of the index builds on this literature by using a bayesian encoder-decoder long short-term memory network to forecast adversarial trends. At the institution level, Baker and Ratnadiwakara (2025) develop and analyze cyber exposure of financial institutions. We introduce a generalized approach to estimate the firm-level technological component for a broader set of firms and institutions, including financial and technology service providers.

Section 2 overviews the quantitative framework for system cyber vulnerability, including theoretical foundations and estimation procedures. Section 4 examines the index for financial institutions, and applies the quantitative framework to service providers. Concluding remarks are provided in Section 6.

2 A Model of the System Cyber Vulnerability

To quantify and monitor system cyber vulnerability over time, we build a model that links primitive technological vulnerabilities at the firm-level to system-level disruption and losses.

2.1 Environment

There is a network of financial and non-financial firms i, and cyber adversaries. Financial and non-financial firms form a network that is assumed to be determined by exogenous factors, and can change over time.

Security. There is a set of attack types $\alpha \in \mathcal{A}$. Each period, each firm chooses a defense intensity d_{it} at unit cost c_{it}. Cyber adversaries are able to endogenously affect the magnitude of a cyber vulnerability arising from a weakness in a firm's network or systems through investments. Specifically, adversaries choose an allocation of attack resources across firms a_{it}^{α} per firm i at unit cost c_t^{α}. Firm i's vulnerability to attack type α is given by:

$$\chi_{it}^{\alpha} = \sqrt{a_{it}^{\alpha}\phi_{it}^{\alpha}(d_{it})}, \tag{1}$$

where $\phi_{it}^{\alpha}(d_{it}) = \phi(d_{it}) + \epsilon_{it}^{\alpha}$ is the firm-level vulnerability level associated with defense intensity d_{it}. Adversaries choose attack intensity a_{it}^{α} to maximize:

$$v_t^{\alpha}\omega_{it}\chi_{it}^{\alpha} - \frac{1}{2}c_t^{\alpha}a_{it}^{\alpha}, \tag{2}$$

where v_t^{α} represents an attack-level vulnerability of the network at time t, and ω_{it} represents the attacker's targeting weight of firm i.

Firms are assumed to have limited information regarding adversarial activity. To capture this, individual firm i incorporates broad trends into its defense strategy, but does not perfectly tailor defenses to attack-level vulnerabilities. The firm's defense intensity

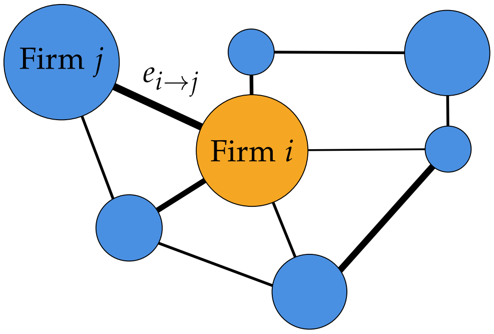


Figure 1: Illustration of service provider links to dependent firms.

is chosen to minimize:

$$-\psi_{it}\sum_{\alpha} x_t^{\alpha}\chi_{it}^{\alpha} - d_{it}c_{it} \tag{3}$$

where x_t^{α} represents firms' collective defense posture at the attack-level and ψ_{it} represents firm i's cyber posture.

Externalities. Although firms take into account firm-specific exposure resulting from adversarial targeting ω_{it}, they do not fully internalize the cost borne by the system. Let the systemic importance of an individual firm be given by F_{it}.

Firm-level vulnerabilities of technology and financial service providers can result in disruptions at downstream financial firms. Thus, technological and operational linkages result in multiple institutions becoming impaired as a result of a shock at a single technology firm. For a given technology firm i connected to a set of financial firms $i \to j$ with exposure $e_{i\to j}$, technological and operational systemicness is given by:

$$F_i = \sum e_{i\to j}F_{i\to j} \tag{4}$$

Discussion on Assumptions. There are three core assumptions made in the framework.

- Attackers are less informed about the systemic impact of individual firms. Attackers target firms based on the expected cyber vulnerabilities of individual firms, and their relative importance ω_i, but not the systemic value F_{it}.
- Firms are less informed about attack-level vulnerabilities. Firms choose their defense intensity based on expected adversarial attack intensity, but do not tailor their resources to attack-specific defenses. This captures the notion that firms have

limited intelligence on the adversarial strategy and exploitations being targeted by adversaries.

- Firms do not fully internalize the system-level costs associated with individual cyber vulnerability. The existence of externalities is self-evident. Firms may fail to internalize costs due to a variety of reasons, including incomplete information, incentive misalignment, or constrained resources.

2.2 Equilibrium Vulnerability

Given primitives, in each period, adversaries make an attack allocation choice. Adversaries' (unconstrained) allocation for attack vector α targeting firm i is given by:

$$a_{it}^{\alpha} = \left(\frac{v_t^{\alpha}}{c_t^{\alpha}} \cdot \omega_{it}\right)^2 \cdot \phi_{it}^{\alpha}(d_{it}) \tag{5}$$

$$= (\tilde{v}_t^{\alpha} \cdot \omega_{it})^2 \cdot \phi_{it}^{\alpha}(d_{it}) \tag{6}$$

where $\tilde{v}_t^{\alpha} = \frac{v_t^{\alpha}}{c_t^{\alpha}}$ represents the cost-adjusted vulnerability of attack α. Individual firms choose their defense strategies, taking as given adversaries' strategies. The objective is given by:

$$-\psi_{it} \sum_{\alpha} x_t^{\alpha} \tilde{v}_t^{\alpha} \omega_{it} (\phi(d_{it}) + \epsilon_{it}^{\alpha}) - d_{it} c_{it} \tag{7}$$

Let $\sum_{\alpha} x_t^{\alpha} \tilde{v}_t^{\alpha} = \tilde{v}_t$, which represents aggregate technical vulnerability. Firm-level technological vulnerability of firm i given its defense strategy is:

$$\phi(d_{it}) = \frac{c_{it}}{\psi_{it} \omega_{it} \tilde{v}_t}. \tag{8}$$

Given the strategies of adversaries and firms, we can characterize vulnerabilities arising from attack types. Equilibrium vulnerability of firm i to attack vector is:

$$\chi_{it}^{\alpha} = \frac{\tilde{v}_t^{\alpha}}{\tilde{v}_t} \cdot \frac{c_{it}}{\psi_{it}}. \tag{9}$$

Aggregating across all attack vectors, we obtain the total firm-level vulnerability:

$$\chi_{it} = \frac{c_{it}}{\psi_{it}} \sum_{\alpha} \frac{\tilde{v}_t^{\alpha}}{\tilde{v}_t}. \tag{10}$$

We can further aggregate across firms to obtain the system-level vulnerability:

$$\chi_t = \sum_i \frac{c_{it}}{\psi_{it}} \sum_\alpha \frac{\tilde{v}_t^\alpha}{\tilde{v}_t}. \tag{11}$$

Note that although firms internalize the costs associated with adversarial targeting ω_{it}, they do not fully internalize the cost borne by the system. Individual firms' financial systemicness is given by F_i.

Theorem 1 (Systemic Cyber Risk). *The system-level cyber vulnerability SCV is:*

$$SCV_t = \sum_i \underbrace{\sum_\alpha \frac{\tilde{v}_t^\alpha}{\tilde{v}_t}}_{A_t,\ \textit{adversarial}} \overbrace{\frac{c_{it}}{\psi_{it}}}^{T_i,\ \textit{technological}} \underbrace{F_{it}}_{\textit{financial}} \tag{12}$$

The system-level cyber vulnerability can be decomposed into three components: A_t, an adversarial component, which takes into account the contribution to cyber vulnerability arising by adversaries; T_i, a technological component, which takes into account the firm-level technological vulnerabilities; and F_i, which takes into account the systemic relevance of an individual institution i from a financial stability standpoint. We will build on the modular representation of cyber vulnerability.

Before moving to the estimation of SCV, we make some basic observations.

- Adversaries may target firms based on beliefs regarding the economic impact of a successful attack (larger ω_{it}). However, firms take into account adversaries' targeting, and increase defense intensity, matching higher attack intensity with greater defense intensity.

- Firms that anticipate larger adverse impact conditional on a successful attack (large ψ_{it}) also increase defense intensity, which lowers vulnerability. When firms fully internalize their financial systemicness (i.e. $\psi_{it} = F_{it}$), firm-level cyber vulnerability equates to adversarial vulnerability A_t scaled by firm-level defense cost c_{it}. This also implies that when ψ_{it} diverges from a firm's financial systemicness F_i, defenses are suboptimal from a system standpoint.

- Adversarial vulnerability depends on aggregate posture regarding specific attack-level vulnerabilities. If aggregate-level vulnerabilities are fully accounted for, i.e. $x_t^\alpha = 1$ for all $a \in \mathcal{A}$, then although there is variation in attack-level vulnerability, aggregate vulnerability stays constant. On the other hand, if aggregate posture regarding specific attack-level vulnerabilities lag (i.e. $x_t^{\alpha} < 1$), vulnerabilities are magnified and amplified by increasing aggression from adversaries through its impact on attack intensity.

The model yields several implications for system cyber vulnerability. First, accounting for adversarial activity is necessary for assessing system cyber vulnerability if there is an information gap between adversaries and firms in terms of attack vectors. The fact that the number of known exploited vulnerabilities (KEV) grows in tandem with common vulnerabilities and exposures (CVE) and adversaries have become increasingly effective in operationalizing emerging vulnerabilities indicate that cyber gaps exist in practice. Second, accounting for the systemic relevance of individual firms is necessary whenever firms do not fully internalize the system-level impact of a cyber attack. That is, although firms that anticipate greater adverse impact from an attack choose greater investment into defense, this is generally suboptimal from a system standpoint.

Altogether, the framework provides a foundation for a system cyber vulnerability index comprised of the three components, "adversarial," "technological," and "financial," which contribute to system-level cyber vulnerability:

$$SCV_t = \underbrace{A_t}_{\text{Adversarial}} \sum_i \overbrace{T_{it}}^{\text{Technological}} \cdot \underbrace{F_{it}}_{\text{Financial}}, \tag{13}$$

where A_t represents adversarial contribution to aggregate cyber vulnerability, T_{it} represents the cyber vulnerability of firm i, and F_i represents the financial systemicness of firm i.

We take a modular approach to the index by estimating each component using domain-specific methodology. This approach allows us to apply techniques to estimate the contribution of vulnerability that best fits the data and environment pertaining to each source. There are practical advantages to the modular structure. First, each component can be estimated using a procedure tailored to the source of vulnerability. Given the heterogeneity of data and their associated characteristics for each component, this flexibility to approaching each component is valuable. Second, modularity supports interpretability. Fluctuations in system cyber vulnerability can be attributed to different components, which is useful to distill intuition based on changing contribution of each vulnerabilities. Third, it is easier to manage incremental improvements to the index over time, especially as more new data or insights emerge. This aspect fits the fast-paced developments in the cybersecurity space.

3 System-level Cyber Vulnerability Index

The framework described in Section 2 provides a foundation for building a system cyber vulnerability index comprised of the three components pertaining to adversarial, technological, and financial contributions to system-level cyber vulnerability.

System Cyber Monitoring Index:

$$SCV_t = \sum_i \underbrace{\sum_\alpha \frac{\tilde{v}_t^\alpha}{\tilde{v}_t}}_{A_t,\text{ adversarial}} \overbrace{\frac{c_{it}}{\psi_{it}}}^{T_i,\text{ technological}} \underbrace{F_{it}}_{\text{financial}} . \tag{14}$$

The index is estimated using a modular approach. Specifically, we use a separate methodology for each component. This approach allows us to apply different techniques to estimating the contribution of vulnerability that best fit the data and environment pertaining to each source. This analysis follows Federal Reserve statistical disclosure practices: results are presented at aggregate levels across multiple institutions, no institution-specific vulnerability metrics are disclosed, and scenario-based outputs are reported for groups of five or more entities.

3.1 Adversarial Component

3.1.1 Context

Cyber attacks are driven by adversaries, who strategically choose the timing, target, and intensity (Eisenbach et al., 2022; Erol and Lee, 2025). Cyber risk exhibits larger uncertainty and greater tail risk (Eling et al., 2023). The adversarial component captures attack-level vulnerabilities, which are determined by the evolving set of cyber vulnerabilities and exploits, and, in particular, adversaries' strategic allocation of resources to exploit these. Although allocations cannot be directly observed, adversarial activity is driven by cost-adjusted, impact-adjusted attack-level vulnerabilities that are common across firms.

3.1.2 Data

To estimate the contribution of cyber vulnerability arising from adversarial activity, we build a longitudinal panel dataset on cyber incidents by attack type from multiple sources. The key data source is cyber incident data from Zywave, formerly Advisen, which provides detailed accounts of the nature, losses, and other relevant information

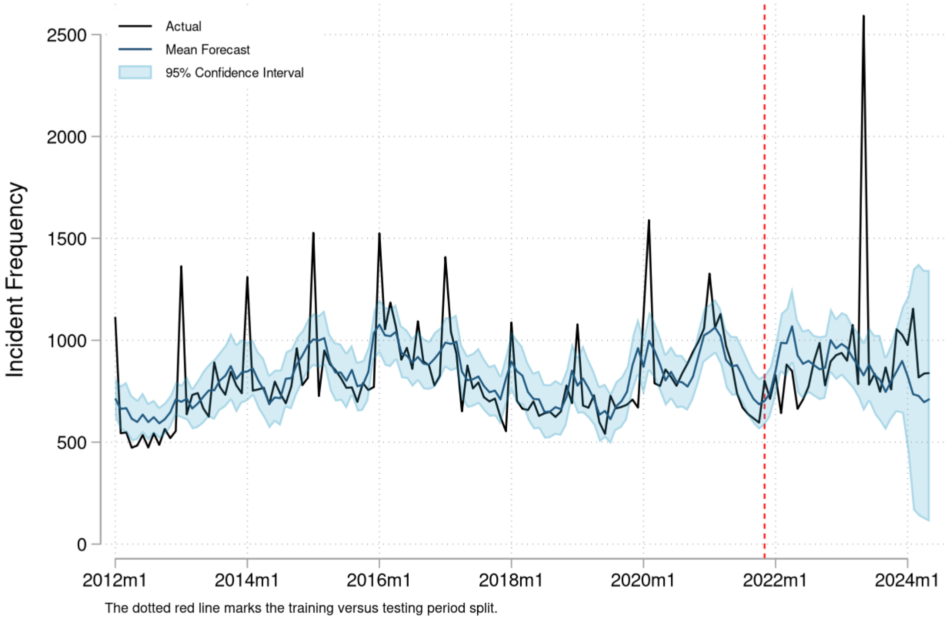


Figure 2: Adversarial component over the training and testing Period.

regarding cyber incidents in the US. In total, our dataset has a little over 300,000 incidents between 2012 to 2024. We augment the dataset using data from Hackmageddon, a volunteered public timeline of cyber attacks across multiple countries.[1] Both sources provide adversarial activity that extends beyond the core firms of interest, which allows for a broader evaluation of adversarial activity. We incorporate a variety of other data sources to be used as features. We build a dataset of vulnerabilities based on common vulnerabilities and exposures (CVE), severity scores based on the Common Vulnerability Scoring System (CVSS), known exploited vulnerabilities (KEV), and classifications from Common Attack Pattern Enumerations and Classifications (CAPEC). For indicators of geopolitical risk, we include the monthly series of the Geopolitical Risk Index developed by Caldara and Iacoviello (2022), and the PyPI library tracking the frequency of US holidays as a seasonal factor shown to be relevant for cyber incidents.

3.1.3 Model and Validation

We use a Bayesian Long Short-term Memory (B-LSTM) model to forecast monthly US incident frequency. LSTM networks belong to a class of non-linear recurrent neural networks (RNNs) to capture complex, path-dependent, and non-linear patterns, which traditional linear econometric models may sometimes struggle to capture. We adopt a

[1] Statistics and timeline for incidences are provided on the Hackmageddon website.

Bayesian approach, which treats model parameters, including weights and biases, as random variables and quantifies forecast uncertainty. This helps mitigate concerns of overfitting whilst incorporating a large set of predictive variables. The model's weight distributions are estimated using variational inference and involve an optimization-based method that balances data fit against a regularization term, i.e. Kullback-Leibler divergence.

Model fit and performance is shown in Figure 2. Model-implied adversarial activity is driven by several key features. First, a rise in geopolitical risk, proxied by the geopolitical risk index (Caldara and Iacoviello, 2022), is associated with great adversarial activity in the US. The geopolitical risk index measures adverse geopolitical events and associated risks and indicates that heightened geopolitical tensions can motivate and embolden cyber adversaries to increase aggression. Second, increases in global malware and ransomware incidents are associated with greater adversarial activity. This supports the view that the industrialization of ransomware-based cyber-criminal enterprises has contributed to greater adversarial activity. Third, adversarial activity exhibits strong seasonalities. We find that periods with more holidays in the US are associated with greater intensity of adversarial activity, consistent with the view that firms are strategically targeted during periods in which cyber response and resiliency are expected to be lower due to under-staffing.

3.2 Technological Component

3.2.1 Context

Individual firms may vary significantly in their cybersecurity stance and resiliency and may face different exposures based on their attractiveness as targets (Florackis et al., 2023; Jamilov et al., 2021). In the case of the financial sector, cyber risks posed to the financial sector have been shown to vary significantly over time (Aldasoro et al., 2022). The technological component captures the vulnerability of individual firms, based on various signals on relative strengths and exposures.

3.2.2 Data

Several types of data are used for the estimation of the technological component. The first is firm-level granular cybersecurity ratings from Bitsight and CyberCube. These ratings serve as cyber signals indicative of the cybersecurity practice, hygiene, and weaknesses of firms. Second, we collate incidence data from BitSight and Cybercube. The sample period is January 2021 through December 2024. While the ultimate set of firms in the index requires representation across all components, the set of firms in the technological component includes about 4,200 unique firms, spanning banks (87%), non-banks (6%), and financial and technology service providers (6%).

3.2.3 Model and Validation

Our approach involves two steps. First, we perform a two-stage Principal Component Analysis (PCA) for dimensionality reduction on the 51 cyber signals provided by the two vendors. The first-stage PCA targets subcategory ratings for each vendor, and the second-stage PCA is used to further compress the vendor-level PCs to produce composite PCs. Intuitively, this process condenses the informational content of the cyber signals that best explains the variation across firms.

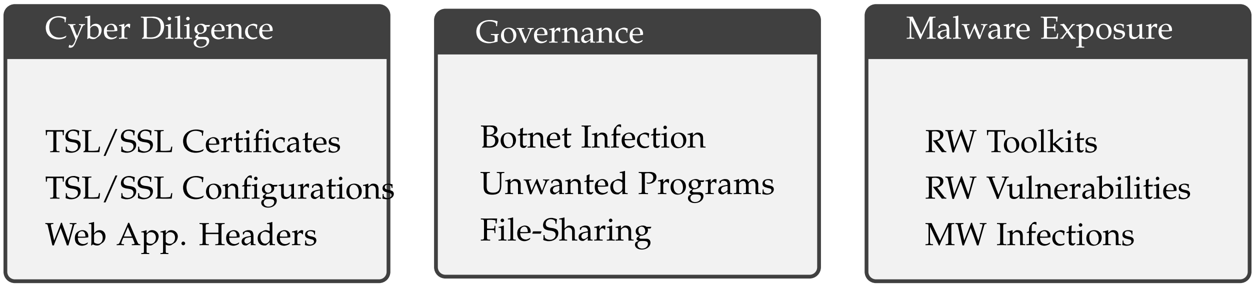
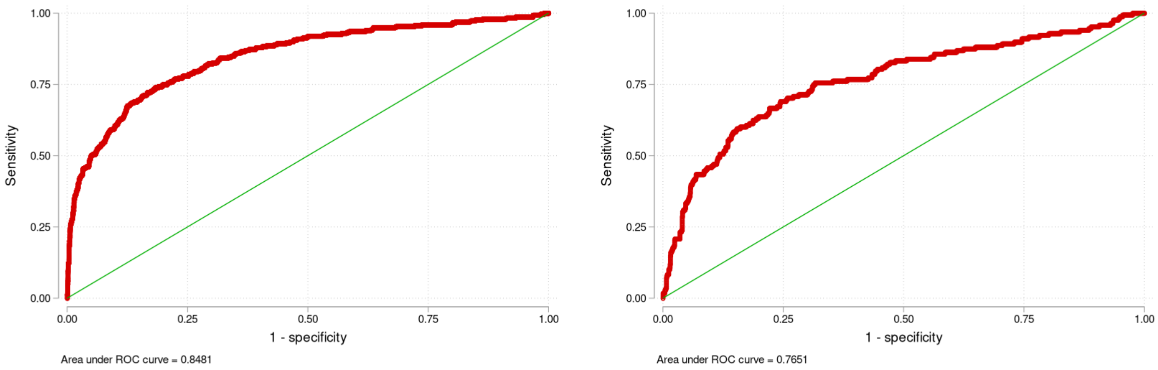


Figure 3: Cybersecurity signal clusters.

The cyber signals underpinning these composite PCs reveal several thematic factors, summarized in Figure 3. The first relates to cyber diligence and other standard hygiene measures, including the management of TSL/SSL certificates and configurations, as well as security practices relating to web application headers. The second relates to weak governance that could compromise systems with botnet infections and unwanted programs, and enable employees to engage in risky behavior, such as file-sharing. The third relates to exposure to malware, including exposure to CVEs relating to ransomware attacks, and signals of malware or ransomware infections.

In the second step, we develop a model to estimate individual firm's cyber vulnerability. Firm-level variables, including firm characteristics, past incidents, and composite PCs, are used to fit a negative binomial regression model for next-quarter incidents at the firm level. Hence, the forecasted frequency of cyber incidents are used as a quantitative measure for a firm's cyber vulnerability. Specifically, our model is given by:

$$\text{Incidents}_{i,t+1} = \text{Past Incidents}_{i,t} + \text{S}_{i,t} \times \text{R}_i + \text{S}_{i,t} + \text{R}_i + \ln(\text{Revenue})_i + \epsilon_{i,t} \qquad (15)$$



(a) ROC Curve for full sample.

(b) ROC Curve for full sample.

Figure 4: Out-of-sample performance.

where Incidents$_{i,t-n}$ is a decaying cumulative count of incidents, S$_{i,t}$ is a vector of principal components extracted from our security ratings for a firm i, R$_i$ $\in \{[P_0, P_{10}), [P_{10}, P_{90}), [P_{90}, P_{100}]\}$ is a firm's bin within the sample's distributional revenue, and $\ln(\text{Revenue})_i$ is a firm i's natural log of revenue. The data is split into training and testing periods, with the testing period from 2021Q1 through 2023Q2, and the testing period from 2023Q4 through 2024Q3.

Out-of-sample performance, based on classifications, for the entire sample and top 10% by revenue is shown in Figure 4. The model's classification performance is generally good for both the entire sample and large firms, with AUC of 0.85 and 0.77, respectively. These levels match in-sample fit, alleviating concerns regarding over-fitting.

Median, 25th, and 75th percentiles of the model-implied T_{it} are shown in Figure 5. The log count of a cyber incident at the median firm is low, with 0.257 per quarter in our sample from 2021Q4 to 2024Q2. However, the distribution of T_i exhibits a long right tail. This is particularly relevant from a financial stability standpoint, given that the right end of the distribution primarily consists of the top 10 percent of firms by size.

3.3 Financial Component

3.3.1 Context

How might a cyber incident at a firm, system, or service provider impact the financial system? The potential for financial amplification of a technological shock has been well recognized. Vulnerabilities at a firm may result in an adverse impact on itself, its counterparties, and markets where it is active. We take two established scenario-based approaches to quantitatively evaluating the financial systemicness of institutions.

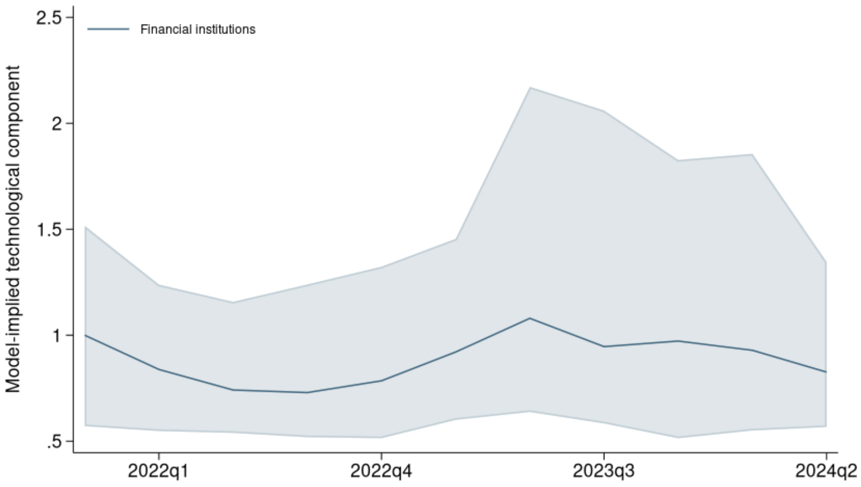


Figure 5: Model-implied technological component (median, p25, p75).

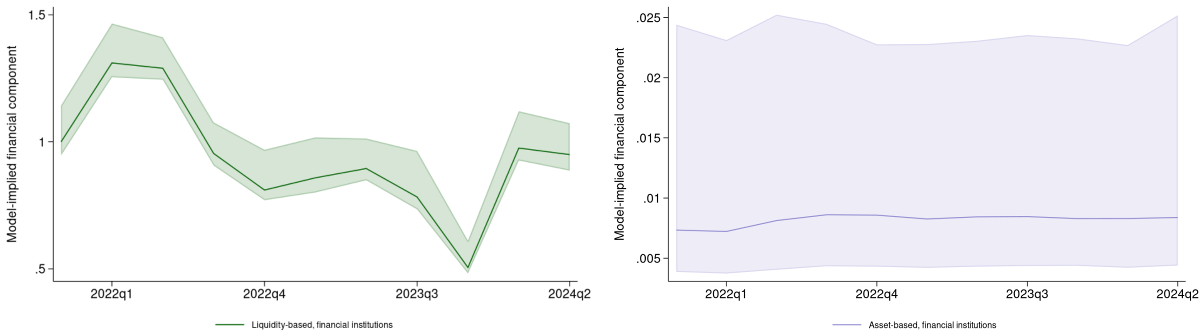
1. *Liquidity-based*. Systemicness by how cyber shock at an individual institution could lead to system-wide illiquidity event.

2. *Asset-based*. Systemicness by how a cyber shock at an individual institution could have financial and information spillovers through commonality in asset holdings between financial institutions.

3.3.2 Data

The liquidity-based measure uses wholesale payment data from Fedwire. The two main datasets we use are the intraday payment data between banks in the Fedwire Funds Service payment system and the individual banks' end-of-day reserve balance, with approximately 5,500 banks represented.

For the financial vulnerability analysis, we use balance sheet and liquidity data from Y-9C for bank holding companies, N-PORT forms for mutual funds and ETFs, and N-MFP forms for money market mutual funds. We use the flow-of-funds data for portfolio holdings for other non-bank institution types, including insurance companies and finance companies. The entity-level data include 335 banks, 360 money market funds, and about 12,000 mutual funds, and total assets of the financial system represented in scenario are on average 116 trillion dollars over the sample period.



(a) Liquidity-based

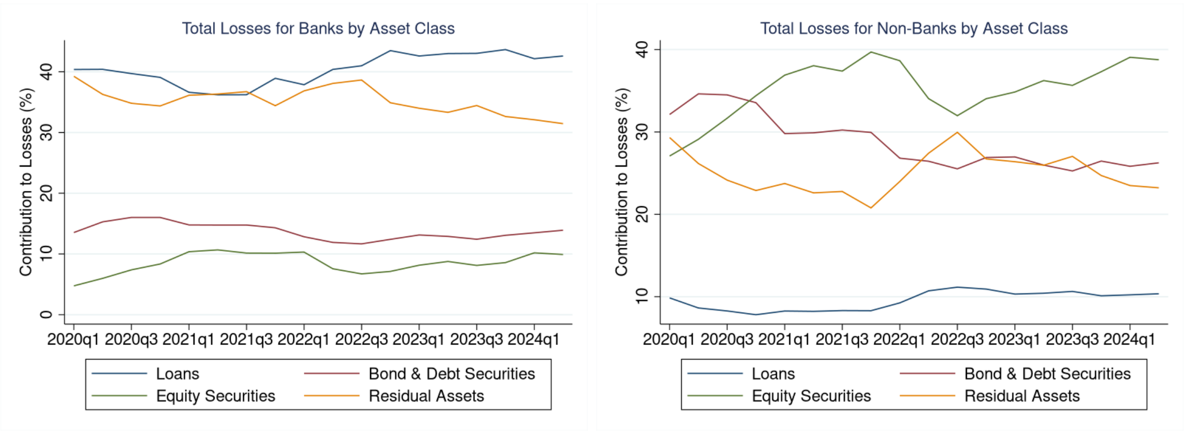
(b) Asset-based

Figure 6: Model-implied financial component (median, p25, p75).

3.3.3 Model and Validation

For the liquidity-based financial component, we follow the cyber scenario in Eisenbach et al. (2022). In the scenario, an attacked institution is assumed to receive payments, but is unable to send payments. By accumulating payments from its counterparties, the attacked institution soaks up system liquidity, resulting in liquidity dislocation within the system. Systemicness under this scenario is given by the size-weighted share of financial institutions that experience liquidity impairment, defined by material drops in a bank's counterfactual reserve balance. The liquidity-based financial component is estimated for the top 200 banks by payments value.

The asset-based financial component can be used for a broader set of financial institutions, including non-bank financial institutions. Our methodology follows the scenario-based analysis developed by Duarte and Eisenbach (2021) and Cetorelli et al. (2023), which consider the impact of an unexpected asset sell-off by a shocked institution on other institutions. The scenario is detailed in Appendix A.2. Asset linkages are used to evaluate the potential for market-level spillovers that may arise if one or a group of financial institutions are impacted by a cyber incident. A cyber incident upon an institution can spillover to other institutions with common asset holdings through various channels. Disruptions in market activity of a key player or system, either due to system impairment or irregular behavior, could materially impact market conditions, resulting in an illiquidity spiral. An attack could also result in a sudden loss of trust in the institution, resulting in large outflows and fire-sales. Alternatively, an attack could be amplified through information channels. Self-fulfilling beliefs could result in sudden drops in asset values, forcing leveraged institutions to further sell assets to lower leverage, or trigger outflows at a fund to similar effect. Linkages through asset holdings serve



(a) Banks

(b) Funds

Figure 7: Share of losses across asset classes.

as a way to infer interconnectedness between a broad set of financial institutions.

Median, 25th, and 75th percentiles of the model-implied F_{it} are shown in Figure 5. The distribution of liquidity-based and asset-based financial components exhibit fat tails, evidenced by the asymmetry in the 25th and 75th percentile ranges. On average, the liquidity-based financial component trends downward from 2022 to the end of 2023, owing to lower payment-related liquidity needs (Eisenbach et al., 2024).

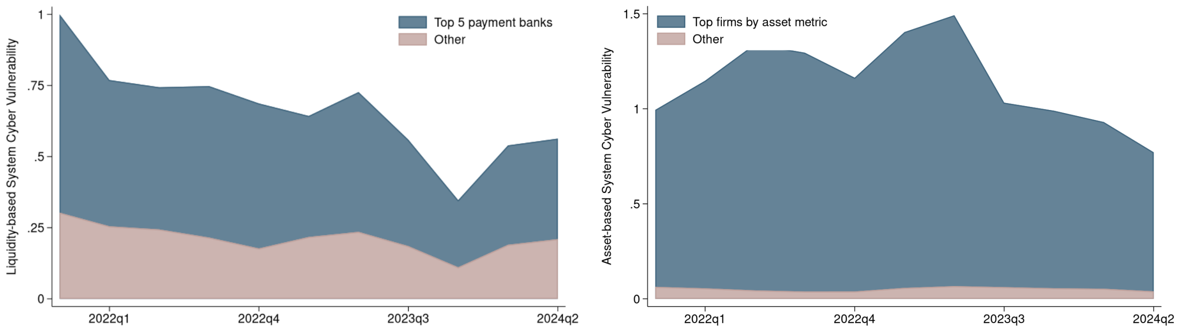
The asset-based financial component is stable and trends upward over our sample. The upward trend is driven by different asset classes, depending on the underlying shocked institutions. For banks, loans constitute the largest share in terms of hypothetical losses. In contrast, for mutual funds, changes in the financial component are driven by losses associated with equity securities. The share of losses across asset class by the shocked institution type are shown in Figure 7.[2]

4 System Cyber Vulnerability Monitoring Index

4.1 Financial Firms

In this section, we combine the three components to an aggregate index. While the index is built to quantify system cyber vulnerability, it is useful to consider the statistical interpretation based on the estimation process. The adversarial component A_t tracks cyber incident frequency in the US and thus measures a common exposure faced by US firms resulting from adversarial activity. The technological component T_t

[2] Residual assets include Derivatives, Commodities, Real estate, and any other unspecified assets reported by institutions.



(a) Liquidity-based Index

(b) Asset-based Index

Figure 8: SCyMoN, normalized by 2021Q4 levels.

forecasts the likelihood of incident at firm i, and the financial component F_t estimates the impact conditional on an incident. Hence, the index can be roughly interpreted as a time-varying measure of the aggregated expected losses from cyber risk on the financial system.

Figure 8 provides the liquidity-based and asset-based indices, normalized by the 2021Q4 levels. The liquidity-based and asset-based index share certain features. First, given commonality in the A_t and T_{it} components, both indices show a spike in mid-2023, driven by a sharp increase in the technological component. Second, both indices demonstrate a significant concentration of system cyber vulnerability arising from large institutions. In the case of the liquidity-based index, the majority of system cyber vulnerability is attributed to the top 5 payment banks, consistent with studies that have shown a significant concentration in wholesale payment activity (Eisenbach et al., 2022). Similarly, in the case of the asset-based index, the vast majority of system cyber vulnerability is attributed to the top 25 firms by asset-based systemicness.

Using a symmetric decomposition, we can parse out the relative contribution of each component to changes in the index. A decomposition for the liquidity-based index is shown in Figure 9. The decomposition reveals a nuanced picture with regards to the interaction between different components. For instance, in 2022Q1, a large spike in adversarial component coincides with a drop in technological component, resulting in a muted change in the index itself. In contrast, a positive shock to the financial component in 2024Q1 is expressed in the index as the other components remain at similar levels as the previous period.

The asset-based index can be decomposed by asset classes, by using the hypothetical total losses per asset class associated with firms' F_{it}. Figure 10 shows the breakdown of SCV by asset class. For the sample of firms, the largest asset class is loans, due to

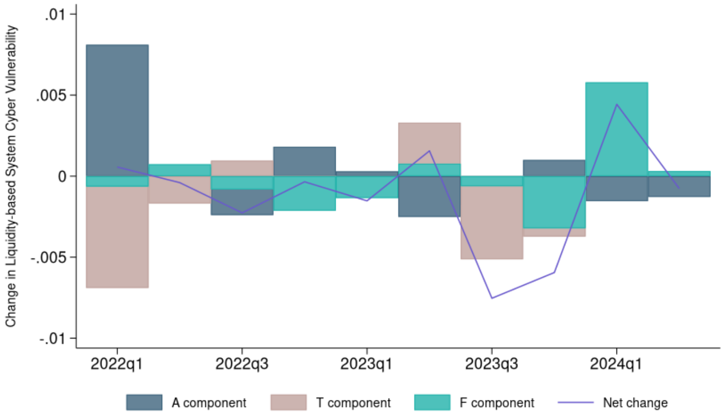


Figure 9: Decomposition of index changes.

the large representation of banks in our sample and their illiquid nature, which results in larger losses under the asset-based scenario. Other illiquid assets are also associated with SCV, including corporate bond and debt securities, equity securities, and residual assets, which includes other assets such as derivatives, commodities, real estate. An asset-based breakdown in SCV allows us to see how cyber vulnerability may realize in various financial markets.

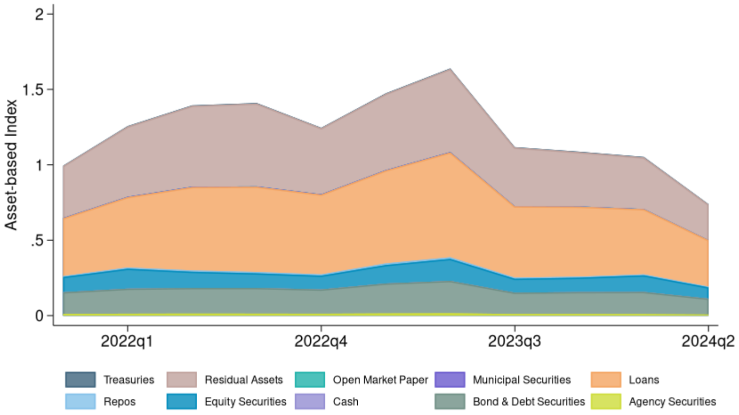
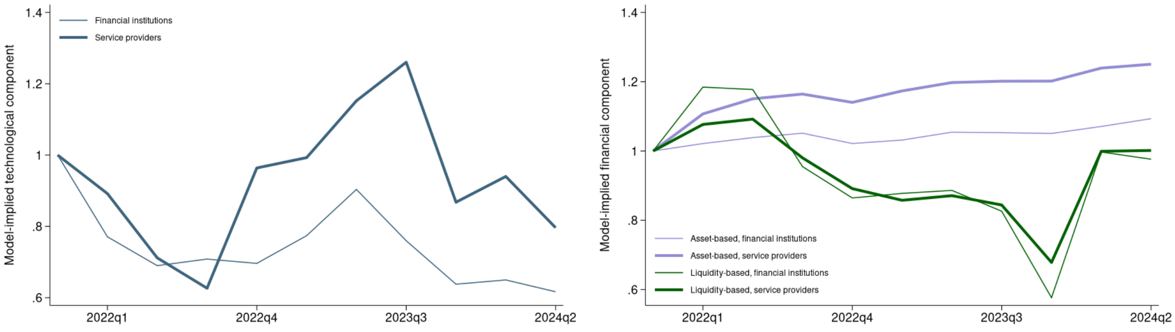


Figure 10: Index by asset class, normalized by 2021Q4 level.

5 Service Providers

In this section, we extend our analysis to service providers. Financial and technology service providers may provide critical functions in the operations of financial institutions. Shared operational dependencies to a single service provider could have systemic consequences on the financial system. The risks associated with the concentration of services could be further exacerbated if firms do not have adequate contingencies, either due to the lack of redundancy or the lack of information to adequately mitigate risks.

We explore the financial stability implications arising from the cyber vulnerability of financial and technology service providers. We can apply the technological component model specified in Section 3.2. The set of service provider consists of 331 service providers spanning service segments including Cloud Infrastructure, Cloud Software, Data Aggregators, Engineering and Security Technology, Enterprise Technology, Money System, Network Services, Operating Systems & Programming Languages, and Operational Technology.



(a) Technological Component

(b) Financial Component

Figure 11: Average components for service providers, normalized by 2021Q4 levels.

The average technological component for service providers is shown in Figure 11. The model-implied cyber vulnerability of service providers co-moves significantly with that of financial institutions, with a correlation of 0.488 in our quarterly sample from 2021Q4 to 2024Q2. Notably, in mid-2023, both financial institutions and service providers experienced a surge in cyber incidents, which resulted in a spike in the average technological component.

A key consideration is the potential for service providers to provide critical services for multiple institutions, as in Figure 1. A service provider's financial systemicness is assumed to be proportional to the financial systemicness of its dependent firms, weighted by dependence. With this approach, the financial components for service providers can be derived from the measures specified in Section 3.3. A key limitation to evaluating service providers is the lack of information regarding technological and operational linkages (Eisenbach et al., 2022). We mend this gap by aggregating data on linkages between service providers and financial institutions from Bitsight and Cybercube. In total, this represents roughly 12,000 links between 121 service providers and approximately

800 financial institutions.

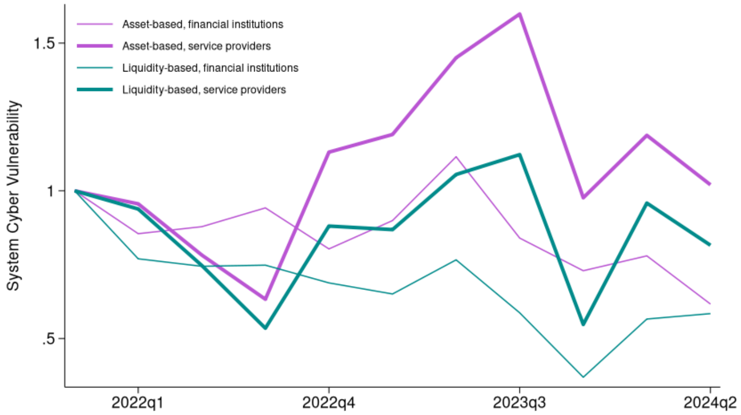


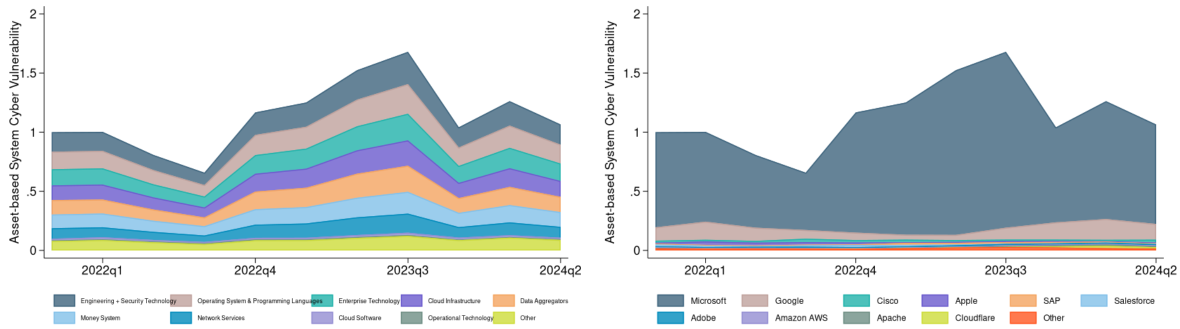
Figure 12: Index for service providers, normalized by 2021Q4 levels.

The liquidity-based and asset-based indices for service providers and financial firms, are shown in Figure 12. The co-movement in the underlying components translates into co-movement in the indices between service providers and financial firms. Co-movements are driven by correlation in the technological component, and correlation in the financial component as key service providers are linked to multiple large financial firms. Overall, this suggests another amplification channel through the co-movement in system cyber vulnerability arising from financial firms and their service providers.

System cyber vulnerability from service providers can be further decomposed by the service category and service provider (Figure 13). Large technology companies are represented as key contributors to the index, with Microsoft representing over half of the index, followed by Google, Cisco, Apple, SAP, and Salesforce. The ranking of top service providers by contribution roughly corresponds to the cumulative vulnerability count in the past 5 years, with CVEs associated with Microsoft products and services consistently toping the list, followed by Google, Apple, and Cisco. These point to yet another amplification channel through as technology firms serve not only as a common source of exposure, but those more systemically relevant also experience a greater rate of vulnerabilities in their products and services.

6 Final remarks

This paper presents a quantitative framework for system cyber vulnerability. Tracking system cyber vulnerability requires a quantitative approach to adversarial, technological, and financial dimensions. Using a modular approach to estimating each compo-



(a) Asset-based index by service category. (b) Asset-based index by service provider.

Figure 13: Index Decomposition.

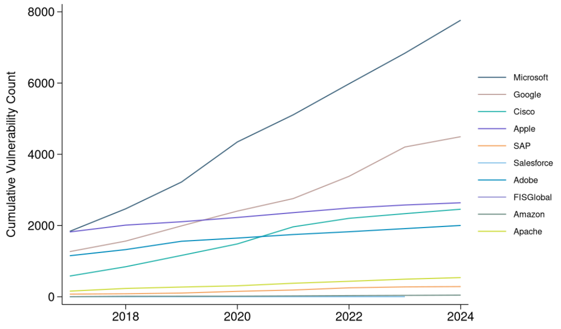


Figure 14: Cumulative count of CVEs.

nent, a broad set of data is incorporated. Early results show the potential for systematically and comprehensively evaluating system cyber vulnerability for financial stability monitoring.

There are a number of directions for future work. One of the key determinants of the index's power is data quality. Expanding on and improving the underlying data can have significant impact in strengthening the quantitative evaluation of cyber vulnerability. The coverage of data also dictates the capacity for the index to include a broader set of institutions and firms. The current analysis demonstrates how firms outside of the regulatory perimeter can still be incorporated into an aggregate assessment of cyber vulnerability. The index could be used as a tool to expand the monitoring capabilities for cyber threats to financial stability.

References

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach, "The drivers of cyber risk," *Journal of Financial Stability*, 2022, *60*, 100989.

Almahmoud, Zaid, Paul D Yoo, Omar Alhussein, Ilyas Farhat, and Ernesto Damiani, "A holistic and proactive approach to forecasting cyber threats," *Scientific Reports*, 2023, *13* (1), 8049.

Baker, Steven D and Dimuthu Ratnadiwakara, "Cyber Risk in Banking: Measuring and Predicting Vulnerability," *Available at SSRN 5498259*, 2025.

Brando, Danny, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey L Schreft, "Implications of cyber risk for financial stability," 2022.

Caldara, Dario and Matteo Iacoviello, "Measuring geopolitical risk," *American economic review*, 2022, *112* (4), 1194–1225.

Cetorelli, Nicola, Fernando M Duarte, and Thomas M Eisenbach, "Are asset managers vulnerable to fire sales?," Technical Report, Federal Reserve Bank of New York 2016.

_ , Mattia Landoni, and Lina Lu, "Non-Bank Financial Institutions and Banks' Fire-Sale Vulnerabilities," *FRB Boston Risk and Policy Analysis Unit Paper No. SRA*, 2023, pp. 23–01.

Duarte, Fernando and Thomas M Eisenbach, "Fire-sale spillovers and systemic risk," *The Journal of Finance*, 2021, *76* (3), 1251–1294.

Duffie, Darrell and Joshua Younger, *Cyber runs*, Brookings, 2019.

Eisenbach, Thomas M, Anna Kovner, and Michael Junho Lee, "Cyber risk and the US financial system: A pre-mortem analysis," *Journal of Financial Economics*, 2022, *145* (3), 802–826.

_ , _ , and _ , "When It Rains, It Pours: Cyber Vulnerability and Financial Conditions," *Economic Policy Review*, 2024.

Eling, Martin, Anastasia V Kartasheva, and Dingchen Ning, "The supply of cyber risk insurance," *Swiss Finance Institute Research Paper*, 2023, (23-118).

Erol, Selman and Michael Junho Lee, "Financial System Architecture and Technological Vulnerability," 2025.

Falato, Antonio, Ali Hortacsu, Dan Li, and Chaehee Shin, "Fire-sale spillovers in debt markets," *The Journal of Finance*, 2021, *76* (6), 3055–3102.

Fang, Xing, Maochao Xu, Shouhuai Xu, and Peng Zhao, "A deep learning framework for predicting cyber attacks rates," *EURASIP Journal on Information security*, 2019, *2019*, 1–11.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber, "Cybersecurity risk," *The Review of Financial Studies*, 2023, *36* (1), 351–407.

Greenwood, Robin, Augustin Landier, and David Thesmar, "Vulnerable banks," *Journal of Financial Economics*, 2015, *115* (3), 471–485.

Hastings, Adam and Simha Sethumadhavan, "Voluntary Investment, Mandatory Minimums, or Cyber Insurance: What Minimizes Losses?," in "34th USENIX Security Symposium (USENIX Security 25)" 2025, pp. 101–117.

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, "The future of financial stability and cyber risk," *The Brookings Institution Cybersecurity Project*, 2018, pp. 1–18.

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun, "The anatomy of cyber risk," 2021.

Kashyap, Anil K and Anne Wetherilt, "Some principles for regulating cyber risk," in "AEA Papers and Proceedings," Vol. 109 American Economic Association 2014 Broadway, Suite 305, Nashville, TN 37203 2019, pp. 482–487.

Kotidis, Antonis and Stacey Schreft, "The propagation of cyberattacks through the financial system: Evidence from an actual event," Technical Report, Technical report, Federal Reserve System Working Paper 2022-25 2023.

Ottonello, Giorgio and Antonino Emanuele Rizzo, "Do Software Companies Spread Cyber Risk?," *Available at SSRN*, 2024.

Sun, Nan, Jun Zhang, Paul Rimba, Shang Gao, Leo Yu Zhang, and Yang Xiang, "Data-driven cybersecurity incident prediction: A survey," *IEEE communications surveys & tutorials*, 2018, *21* (2), 1744–1772.

Welburn, Jonathan W and Aaron M Strong, "Systemic cyber risk and aggregate impacts," *Risk Analysis*, 2022, *42* (8), 1606–1622.

A Description of Scenarios

A.1 Liquidity-based Scenario

Our framework estimates the single-day network impact of cyber attack on individual institutions

1. **Initial shock:** An attack on a institution impairs systems. Targeted institution receives payments, but is unable to release payments.

2. **Externality to other banks:** Failure to receive payments affects other institutions' liquidity position.

3. **Liquidity impact:** Banks identified as impaired if counterfactual end-of-day reserve balance falls sufficiently below target balance.

A.2 Asset-based Scenario

Our framework quantifies each step in the following sequence of events in a fire sale:

1. **Initial shock:** An initial exogenous shock hits an institution, causing it to sell a share of its portfolio. This can be a shock to one or several asset classes. In our scenario:

   (a) all asset classes except cash are shocked.

   (b) all individual banks and funds are shocked, one at a time

   The asset sales have a price impact that depends on each asset's liquidity and the amount sold.

2. **First-round spillover losses:** All other institutions in the system holding the fire-sold assets suffer spillover losses due to the drop in price. In response to the first-round market-value losses suffered, institutions sell additional assets governed by their respective loss response functions.

3. **Second-round price impact:** The second round of asset sales in reaction to the first-round spillover losses cause an additional drop in price. All institutions holding the fire-sold assets suffer a second-round of spillover losses due to the additional price decline. Total losses are given by the sum of first-round and second-round losses suffered by the system.

B Liquidity-based Analysis

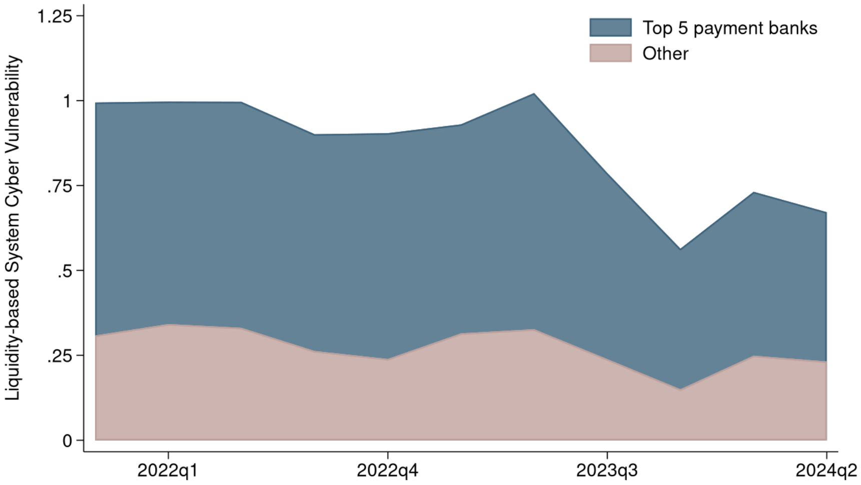


Figure 15: **Liquidity-based index.** The blue shaded area shows index contribution of the top 5 banks by payment share.

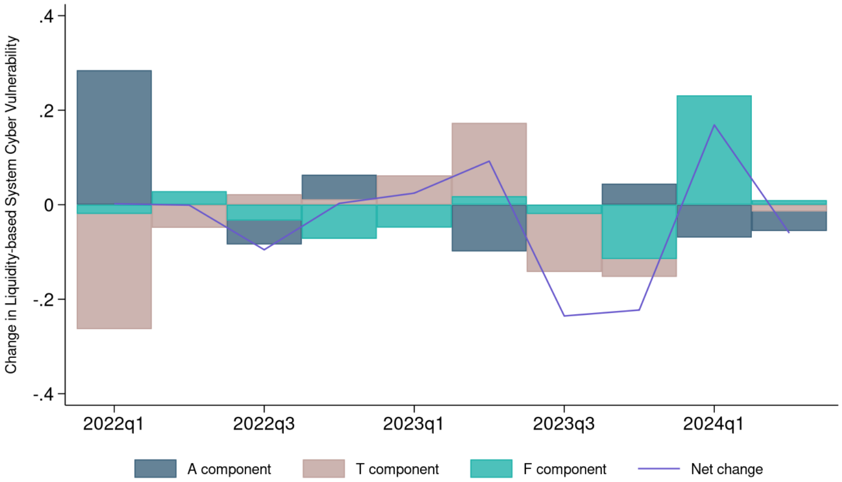


Figure 16: **Decomposition of changes in the liquidity-based index.**

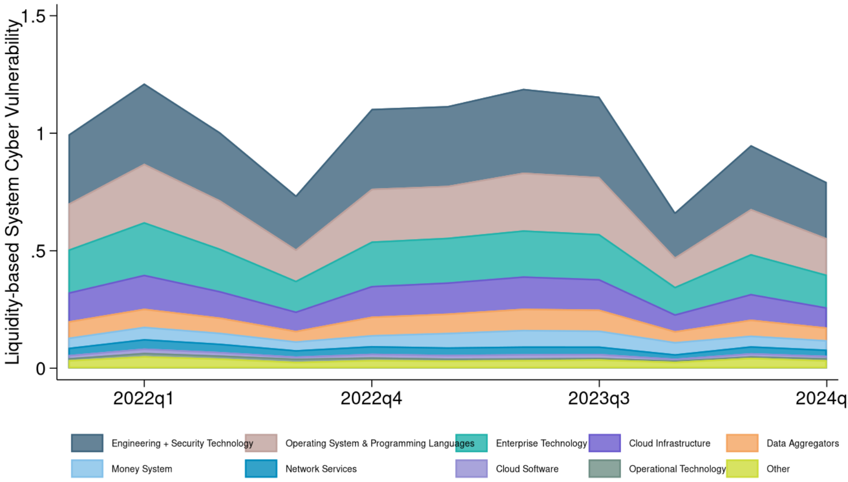


Figure 17: **Decomposition of the liquidity-based index by service type.**

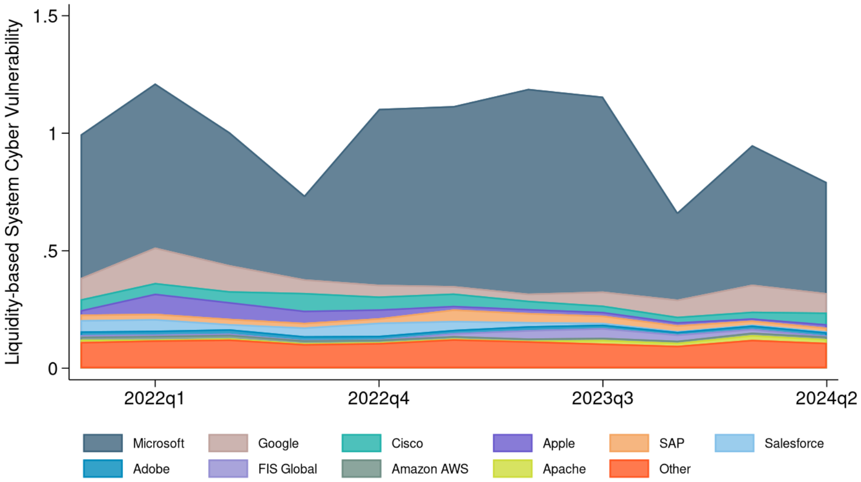


Figure 18: **Decomposition of the liquidity-based index by service provider.**

C Service Providers and Service Categories: Examples

Service Category	Sample Providers	Sample Service Type/Product
Cloud Infrastructure	• `aws.amazon.com` • `wordpress.com` • `microsoft.com`	• Cloud Service (Amazon Web Services) • Content Delivery Network (WordPress) • Content Mgmt System (Microsoft Azure)
Data Aggregators	• `microsoft.com` • `apache.org` • `atlassian.com`	• Database (Microsoft SQL Server) • Database (Apache Spark) • Database (Atlassian Bamboo)
Engineering and Security Technology	• `google.com` • `cloudflare.com` • `microsoft.com`	• App. Dev. & Mgmt (Google Maps) • Identity & Access Mgmt (Cloudflare SSL) • Automated Process/Workflow Systems (Microsoft PowerShell)
Enterprise Technology	• `google.com` • `microsoft.com` • `adobe.com`	• Web Analytics (Google Analytics) • Collaboration (Microsoft 365 Apps & Services) • Productivity Solutions (Adobe Creative Cloud)
Money System	• `bloomberg.com` • `paypal.com` • `stripe.com`	• Financial Applications (Bloomberg Professional Services) • Financial Transaction Provider (PayPal) • Financial Transaction Provider (Stripe)
Network Services	• `digicert.com` • `microsoft.com` • `godaddy.com`	• Certificate Authority (DigiCert) • Email Services Provider (Microsoft Exchange Online) • Certificate Authority (GoDaddy)
Operating Systems & Programming Languages	• `hp.com` • `apache.org` • `nginx.com`	• Programming Lang. & Frameworks (PHP) • Server (Apache) • Server (NGINX)

Table 1: Service categories and sample providers.