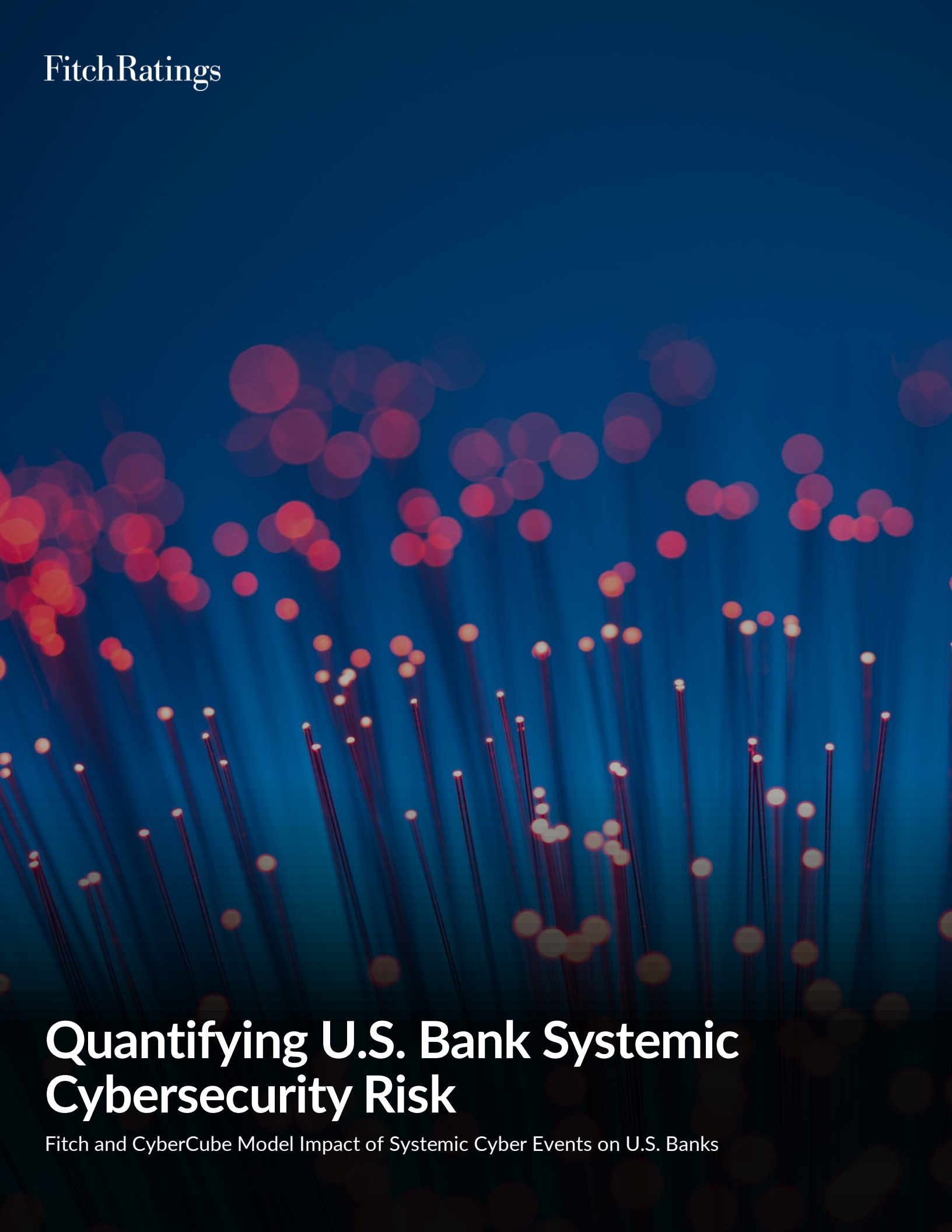
FitchRatings



Quantifying U.S. Bank Systemic Cybersecurity Risk

Fitch and CyberCube Model Impact of Systemic Cyber Events on U.S. Banks

Quantifying U.S. Bank Systemic Cybersecurity Risk

Fitch and CyberCube Model Impact of Systemic Cyber Events on U.S. Banks

"Cyber risk is evolving into broader aggregations and concentrations within the vendor management and supply chain as an incident at a single critical third- or fourth-party vendor could lead to significant business interruption losses."

Chris Wolfe, Managing Director

Modeled Average and Extreme Cyber Risk Losses

Bank Segment	AAL ($ Mil.)	AAL (bp of Revenue)	AAL (bp of Equity)	Extreme Loss[a] ($ Mil.)	Extreme Loss[a] (bp of Revenue)	Extreme Loss[a] (bp of Equity)
Large	176	1.9	0.8	3,314	36	15
Medium	15	2.3	0.8	312	48	17
Small	18	2.0	0.7	378	42	15
Micro	4	3.3	1.0	60	53	15
Total	**213**	**2.0**	**0.8**	**3,643**	**33**	**13**

[a]The aggregate loss amount that may be exceeded with a given probability (beyond the 1 in 200 return period).
Source: Fitch Ratings, CyberCube.

Related Research

Exploring Bank Cybersecurity Risk (April 2021)

Fitch Ratings Cyber Risk Topic Page

Analysts — Fitch Ratings

Christopher D. Wolfe
+1 212 908 0771
christopher.wolfe@fitchratings.com

Konstantin Yakimovich
+44 20 3530 1789
konstantin.yakimovich@fitchratings.com

Gerald Glombicki
+1 312 606 2354
gerry.glombicki@fitchratings.com

George Tsiantos
+44 20 3530 1796
george.tsiantos@fitchratings.com

CyberCube

Rebecca Bole
+44 7931453336
rebeccab@cybcube.com

Souki Chahid
+44 7415 358 244
soukic@cybcube.com

Modeled Industry Cyber Risk Loss Modest

Fitch Ratings worked with CyberCube to model the impact of systemic cyber events on the U.S. banking sector under various cyber risk scenarios. CyberCube's model focuses on a "single point of failure" (SPoF) for cyber incidents that could affect parts of the U.S. banking system. SPoFs refer to technologies (e.g. operating systems, cloud service providers, etc.) for which connectivity and dependencies are identified by company.

A cyber-attack on a particular SPoF may have a cascading impact on the identified connected banks. Using CyberCube's model, losses are calculated on an industrywide basis. Bank-specific impact varies by the scenario run and each bank's reliance on the particular attack vector.

The modeling indicates the average annual loss (AAL), i.e. industry loss per year averaged over many years for U.S. banks, is $213 million. This loss is manageable for the industry as a whole and represents 2 basis points (bps) of the aggregate industry revenue and less than 1bp of the industry capital.

Individual Bank Loss and Tail Risks Could be Material

While AAL for the industry is modest, the most impactful scenarios can generate much higher losses, i.e. "tail risks," which could be many multiples of the AAL. Furthermore, the impact of tail events could be concentrated among banks, leading to possibly material and rating-relevant implications for affected entities. Our analysis indicates that smaller institutions would likely be more adversely affected by a cyber event on aggregate, while medium-sized banks are more severely affected relative to their weight in the industry given their strong dependencies on certain SPoFs.

Connecting Vulnerability with Impact

This analysis follows and complements our initial report "Exploring Bank Cybersecurity Risk" that evaluated individual bank vulnerability to a cybersecurity risk through the lens of cyber risk scores. In this report, our analysis assesses the potential aggregate impact on the industry in the event of a systemic cyber incident.

While the focus of the financial impact of a cyber event is often on the reported remediation or, in the case of ransomware, the requested ransom payment, the financial cost from a cyber event is likely to extend well beyond just headline figures. Additional costs can include data restoration, investigation and response, regulatory legal fines, and brand damage. Some of these costs may be mitigated by the use of cyber risk insurance.

Key Findings from Review

- Smaller banks, in aggregate, are more impacted by cyber events than medium-sized banks due to the higher number of entities and share in sector revenue. Medium-sized banks are more severely affected relative to their weight in the industry, largely due to strong dependencies on certain SPoFs.
- The AAL for U.S. banks is manageable for the industry; however, less frequent but high severity tail events could be multiples of the AAL.
- Modeled loss costs vary by scenario, but the highest modeled costs for the five largest scenarios are business interruption and financial fraud.
- Higher-rated banks generally tend be larger and have better cybersecurity risk hygiene. At the same time, they are not immune to failures at their vendors and service providers. Banks rated in the 'AA' category had the largest contribution to the sample AAL.
- The use of cyber risk insurance varies by bank size. Larger banks are more likely to protect against low frequency but high severity tail events and reduce costs with a higher deductible and risk mitigation strategies. Conversely, smaller banks have lower deductibles and purchase cyber insurance for more frequent but less severe cyber events.

Methodology

For the purpose of this research, Fitch and CyberCube analyzed the entire U.S. banking sector comprising approximately 4,900 banks with over $1.1 trillion in total revenues. This portfolio went through CyberCube's proprietary model to quantify the potential impact of cybersecurity incidents on the U.S. banking industry over a one-year period. All data are based on YE 2020 data.

Banks were classified into four broad categories based on total revenue. CyberCube's model ran 50,000 simulations to generate an exceedance probability (EP) loss curve to assess how likely a cyber scenario level of loss will be exceeded. For more details on CyberCube's approach, refer to Appendix 1.

Analyzed Portfolio

	Revenue Band	No. of Banks	Share in Sector Revenue (%)	Share in Sector Total Equity (%)
Large	>$1 Bil.	94	85	83
Medium	$250 Mil.–$1 Bil.	132	6	7
Small	$10 Mil.–$250 Mil.	2,247	8	9
Micro	<$10 Mil.	2,400	1	1

Source: Fitch Ratings.

Key Findings

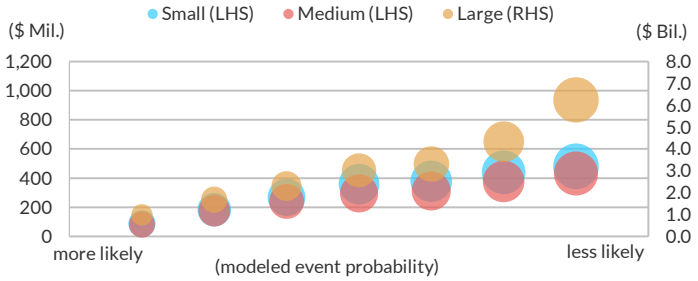
Banking System Structure Leads to Higher Losses for Smaller Banks Relative to Medium Banks

Fitch's analysis of CyberCube's data shows that small banks, in aggregate, have higher gross economic cybersecurity losses than medium-sized banks. This was true regardless of the probability of loss and becomes more pronounced for extreme events that are less frequent (extreme cyber catastrophic events).

The chart below shows small, medium, and large banks' aggregate losses for various return periods — or in other words, the levels of losses that might be exceeded at a given probability/level of confidence. Micro banks, contributing circa 1% of industry revenues, had losses that were too low and are not plotted.

Unsurprisingly, large banks, which account for 85% of industry revenue, contribute most to the modeled loss distribution. Large bank losses are multiples higher compared to small and medium-sized banks, often 10 times or more. However, the size of economic cybersecurity loss is not perfectly correlated with bank size. Small U.S. banks (8% of sector revenue) on aggregate appear more exposed to a cybersecurity event than medium-sized U.S. banks (6% of sector revenue).

Annual Exceedance Probability by Bank Size Cohort



Note: Bubble size represents tail VaR. Large banks' tail VaR is on a different scale.
Source: Fitch Ratings, CyberCube.

This partially reflects the U.S. banking system, with a large number of smaller entities. However, medium-sized banks are more severely affected in relation to their weight in the U.S. banking sector by revenue or number of entities. This is largely due to greater dependencies on certain SPoFs in CyberCube's model.

Aggregation resulting in reliance on fewer third-party vendors reduces complexity and costs but exposes banks to a greater cyber

risk concentration from disruption of a SPoF. This lack of diversification is more apparent in extreme (tail) events.

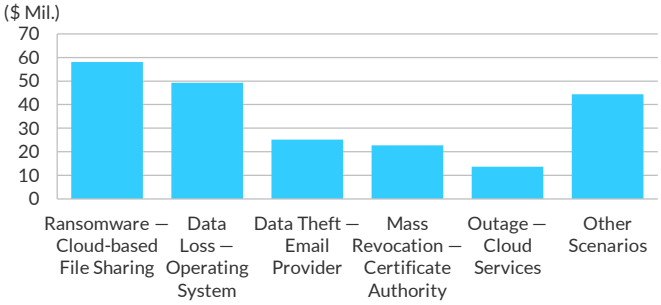
SPoFs include hardware, software, mechanical infrastructure, assets, and key entities in the supply chain. The 2020 SolarWinds attack and 2021 Microsoft Exchange Server data breach are recent examples of SPoFs that provide service to many businesses.

More recently, ransomware gangs are targeting cloud computing infrastructure such as hypervisor systems, a critical security element in virtual machines. CyberCube estimates that more than 80% of the world's applications are estimated to run on virtual machines today. The infection of a SPoF is a force multiplier for threat actors creating significantly larger footprints of compromise than in traditional attacks that infect one system at a time.

Average Annual Losses Manageable for the Industry

CyberCube's catastrophe modeling produces an AAL of $213 million for the U.S. banking sector or approximately 1bp of industry capital. The AAL is the expected industry loss per year averaged over many years. The low number in the industry context reflects the relatively low probability of multiple cyber incidents occurring within the same year, even though losses in case of an event can be significant, as discussed in more detail below. Of 19 scenarios involving attacks on various types of SPoFs deemed relevant for the banking sector and considered in the analysis, five generate AAL in excess of $10 million. These top-five scenarios together account for close to 80% of the industry AAL.

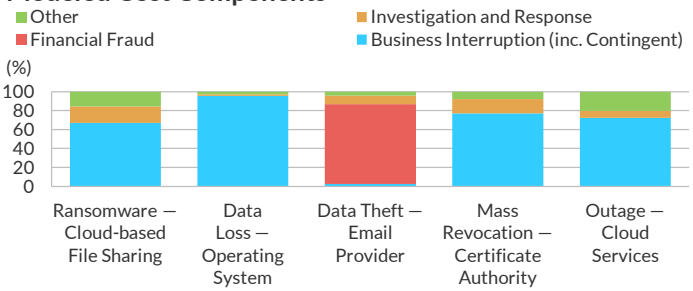
Scenario Contribution to Total AAL



Source: CyberCube.

The most impactful scenarios for banks are those resulting in long-lasting outage of critical systems and create material business interruptions or data theft leading to a significant amount of fraud; business interruption accounts for most of overall incident costs. Direct modeled costs associated with these scenarios, such as investigation and response, costs of data restoration or potential fines are a relatively low proportion of the total (below 20%).

Modeled Cost Components



Note: Other includes fines, legal liabilities and data restoration costs.
Source: CyberCube.

Notably, in the largest loss scenario by AAL (ransomware at a cloud-based file sharing provider), the bank is not exposed to ransomware. It is the cloud-based file sharing provider that suffers from the attack, of which the bank is a customer. That is why business interruption costs make up the bulk of modeled loss costs. Each ransomware attack is unique; therefore, ransomware payments can range from small to large amounts of total cost but these are excluded from this analysis. Other costs such as forensics, legal, fines, and new hardware and software can be just as expensive, if not more than, the ransom payment.

Business interruption costs represent loss of income from direct physical loss or damage to the business. Contingent business interruption costs are similar but are extended to include the premises of a customer or supplier as well. Some of these costs could be recovered through business and contingent business interruption insurance depending on policy wording.

Top Five Loss Scenarios for U.S. Banks in CyberCube's Model by AAL

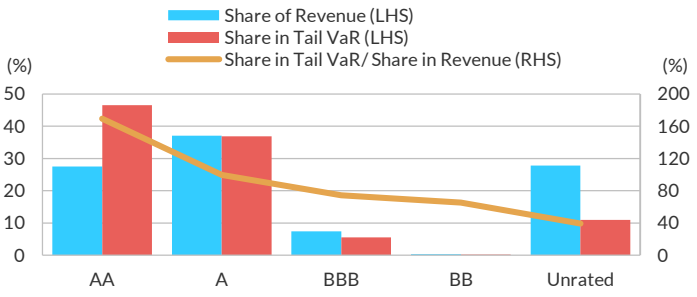
- Long lasting outage at a cloud services provider— several instances of a major cloud services provider down for several hours, impacting global cloud services users.
- Large scale ransomware at a leading cloud-based enterprise file sharing provider—a major online data storage firm and all data stored on behalf of customers are encrypted by ransomware, causing organizations around the globe to lose access to their data for several days.
- Large scale data loss at a leading operating system provider—mega malware attack spreads globally to computers running a specific operating system, erasing hard drive data and severely damaging devices.
- Large scale data theft at a leading e-mail services provider— cyber criminals conduct a massive phishing campaign targeting a leading e-mail services provider, resulting in a large scale data breach impacting millions of enterprises.
- Mass revocation of a leading certificate authority—attackers gain access to the systems of a major certificate authority and implement a mass revocation, causing major failures and outages for enterprises.

Nearly Half of Tail Losses from Highest-Rated Banks

Within the analyzed portfolio, Fitch rates about 70 banks which accounted for about 70% of the sample aggregate revenue and generated 74% of the sample AAL and almost 90% of its tail VaR (calculated for a 1 in 250 years return period). Banks rated in the 'AA' category had the largest contribution to the sample AAL and tail VaR, although the latter was still low at about 1% of their aggregate revenue. Higher-rated banks generally tend be larger and have better cybersecurity risk hygiene, as we explored in our previous report. At the same time, they are not immune to failures at their vendors and service providers, Highest Fitch-rated U.S. banks also have the strongest retail franchises, which may inflate the costs of business interruption or fraud in case of a breach.

However, the numbers above do not consider the potential protection offered by cyber insurance, the use of which we expect to be more widespread among higher-rated banks, but dollar loss cyber risk insurance will likely be more costly over time.

Contribution to Expected Cyber Losses by Rating Category



Source: Fitch Ratings, CyberCube.

Tail Losses Drive High Costs

AAL is a helpful metric to ascertain expected losses over the next year; however, AAL does not account for tail events. Tail events have a low likelihood of occurring, but economic losses can be extreme when they occur, often many multiples of the AAL. The chart below shows the top five loss scenarios and the distribution of potential loses that can occur. Each of the top-five scenarios contributing to the AAL are capable of generating gross losses in excess of $1 billion according to CyberCube's simulation model.

Interestingly, the costliest modeled scenario at the tail is a large-scale data loss from a leading operating system provider, which is only the second largest contributor to the industry AAL. This scenario demonstrates how cybersecurity losses are not linear and tail events are likely to be more severe than shown by historical losses and AAL

In this scenario, aggregate losses for the U.S. banking sector could exceed $3.5 billion, although such an event is highly unlikely--corresponding to a return period beyond 1 in 300 years. Such losses may become rating-relevant if they are concentrated in a limited number of smaller banks. The same scenario can generate a very wide range of losses reflecting different possible SPOFs affecting which entities will likely be impacted.

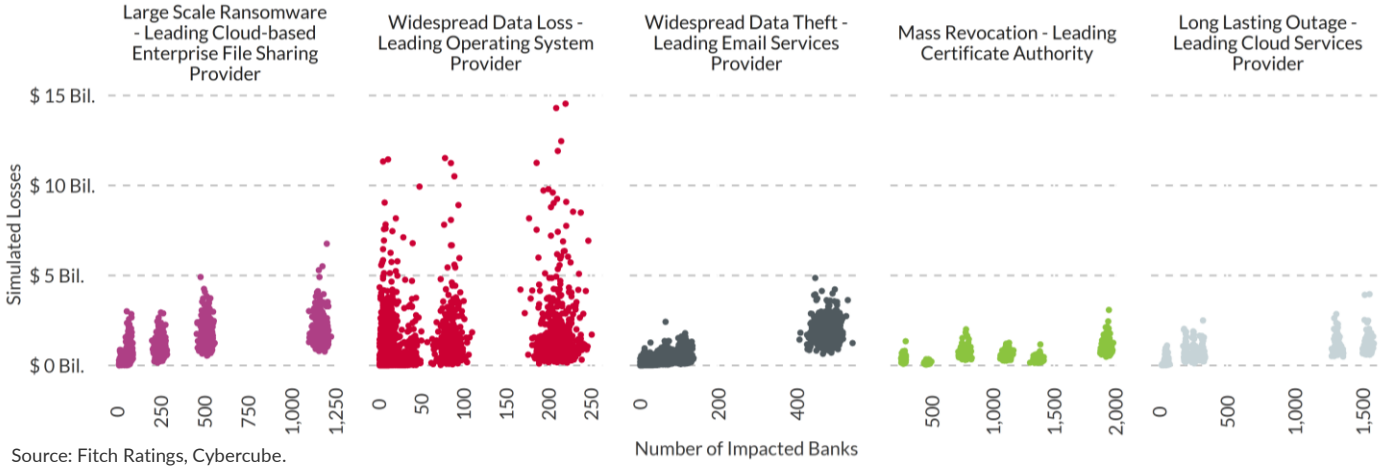
Five Most Impactful Scenarios for U.S. Banking System

	Impacted Banks (No.)			Simulated Losses ($)	
	Min.	Avg.	Max.	Potential Max per-Bank Average Impact	Potential Max Systemwide Impact
Widespread Data Loss — Leading Operating System Provider	1	58	251	4.3 Bil.	14.5 Bil.
Large Scale Ransomware — Leading Cloud Enterprise File Sharing Provider	10	322	1,225	54.7 Mil.	6.8 Bil.
Widespread Data Theft — Leading Email Services Provider	1	76	542	376.9 Mil.	4.9 Bil.
Long Lasting Outage — Leading Cloud Services Provider	18	512	1,582	20.7 Mil.	4.0 Bil.
Mass Revocation — Leading Certificate Authority	247	1,003	1,983	4.7 Mil.	3.1 Bil.

Source: Fitch Ratings, CyberCube.

Certain extreme realizations of these scenarios could lead to losses exceeding $10 billion across the U.S. banking system. The number of impacted banks varies (see table above), but some scenario realizations generate billions of dollars in losses in a small number of banks. For example, the most extreme per-bank average loss of $4 billion would be considerable for even the largest banks, while average losses of $5 million should be manageable for small regional banks.

Five Most Impactful Scenarios for U.S. Banking System



Source: Fitch Ratings, Cybercube.

Use of Cyber Insurance Varies by Bank Size

Together with CyberCube, Fitch analyzed several banks across the size spectrum to ascertain any findings on the purchase of cyber insurance. Based on this sampling, large banks tend to purchase significantly higher cyber insurance limits than smaller banks to protect against extreme events. Large banks also tend to retain higher portions of lower risks given the size of capital, extensive cyber mitigations, and to lower cost of insurance. Essentially, large banks are less willing to take tail risk exposure from a cyber event.

Conversely, small banks, in particular micro banks, are more willing to expose capital to low frequency but high severity tail events and instead use cyber insurance to transfer the more probable but less severe risks to insurance companies. This involves lower deductibles and higher cost of insurance, as a percentage of revenue, to account for higher probability of transferring loss.

Several factors influence the cost of cyber insurance, including the amount of insurance purchased, the size of the deductible, historical/current performance/expectations of the bank and industry, insurance financial strength and reputation of the insurance carriers, and vulnerability assessment of the bank as performed by the insurance company.

From our assessment, small banks tend to protect the income statement from volatility at the expense of the balance sheet for extreme events, whereas large banks protect the balance sheet at the expense of income statement volatility,

Take up rates are a measure of cyber insurance purchased and varies by industry. According to Marsh McLennan, YE 20 cyber insurance take up rates ranged from a high of 76% in education to a low of 33% in financial institutions. While this shows financial institutions generally purchase less cyber insurance than other sectors, it does not account for the purchased limits.

What Fitch Will Do with These Findings

The results of the analysis of cyber risk within the U.S. banking sector show that, in aggregate, the banking sector's revenue and capital are robust enough to absorb modeled average annual cyber loss events; however, tail event losses can be extreme and a potential rating concern, particularly if concentrated in one or a handful of banks.

The results from this analysis can help inform Fitch around the potential financial impact if and when a cyber event occurs.

First, the modeling helps identify SPoFs and the scenarios likely to generate the largest financial impact and, therefore, potentially rating relevant. For example, the expected financial impact of a ransomware attack on a cloud-based file sharing platform is significantly higher than for data theft of an email provider and, therefore, potentially more rating relevant.

Second, the results of this analysis could help serve as benchmarks as to when a cyber event is outside of the expected impact to revenue and/or capital, which could be important rating or rating sensitivity considerations.

Finally, this analysis highlights the role of risk mitigation strategies, such as the use of cyber insurance, which transfers some of this risk to insurance carriers.

Fitch's analysis also recognizes the limitations in models, in particular cyber models, as they still are maturing and will become more refined with accruing of better data sets and loss events. Modeled losses also do not account for factors like brand damage.

Appendix 1: Who is CyberCube?

CyberCube is a software-as-a-service (Saas) technology company focused exclusively on delivering analytics to quantify cybersecurity risk.

CyberCube represents the largest dedicated investment in cyber risk quantification in the insurance sector. It began as a research unit within cybersecurity leader, Symantec, in 2015 and launched as a standalone, venture capital-backed company in 2018. More recently, CyberCube added insurance specialist investors to its board of directors. Insurance industry clients use Portfolio Manager to:

- Get broad insight for risk mitigation from 29 scenario classes offering insights on hundreds of possible cyber catastrophe events.
- Pricing and capital decisions.
- Identifying risk accumulations across portfolios with granularity to reflect company specific views of risk and stress testing.

To enable reliable risk decision-making, CyberCube's cyber risk modeling solutions combine:

- External, internal, and proprietary data.
- One of the largest dedicated team of multidisciplinary cyber risk quantification experts.
- Cloud-native SaaS technology delivery.

CyberCube's data ecosystem underlies its risk quantification and analytics tools. It includes internal security data, external network data, digital supply chain data, historical losses and enterprise data.

CyberCube's internal security data is unique in the market and powered by Symantec endpoint solutions.

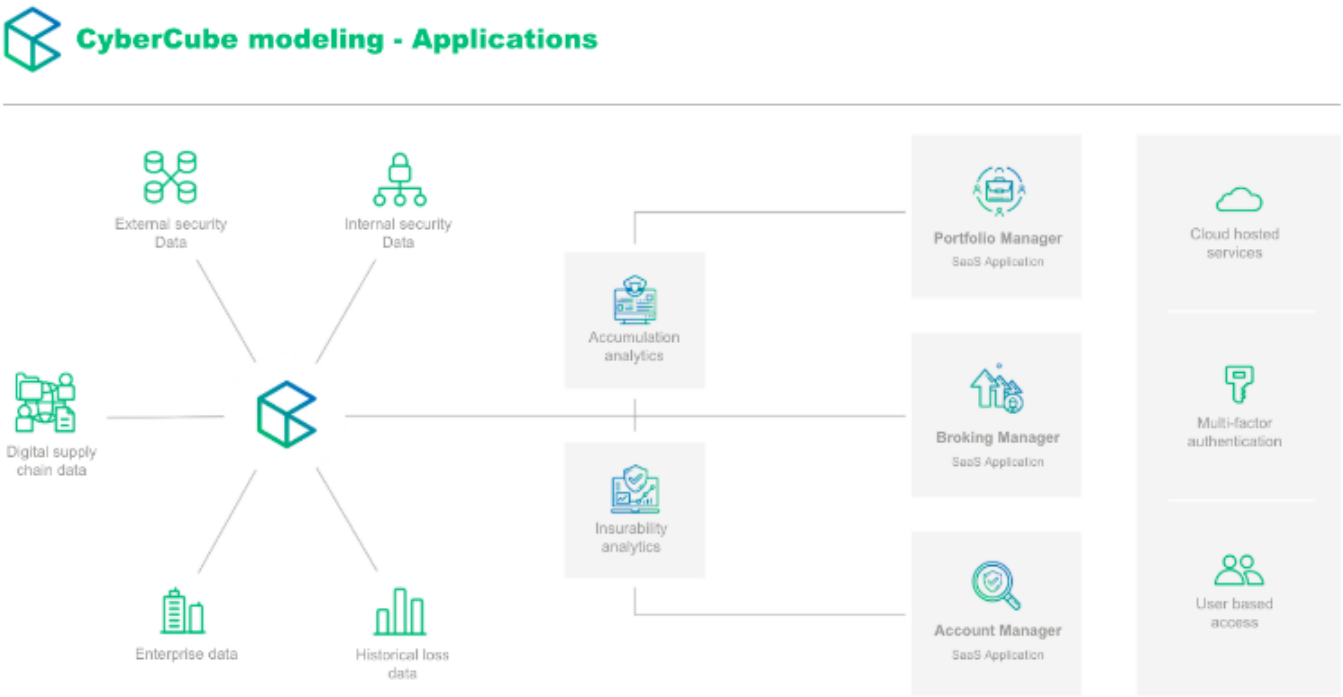
This wide range of data types allows CyberCube to assess the cyber risk of a various industries and company sizes around the globe.

Portfolio Manager Catastrophic Loss Model

For this study, CyberCube applied its Portfolio Manager v3.0 catastrophic loss cyber aggregation model to analyze the U.S. banking sector.

Portfolio Manager is a scenario-based data-driven model with:

- 29 modeled systemic, catastrophic scenario classes, ranging from attacks on critical infrastructure to third-party technology aggregation scenarios to attacks that affect the cloud environment;
- a comprehensive list of over 20,000 technology dependencies ("single points of failure," or SPoF), which could lead to cascading failures through the digital supply chain or proliferate an attack, aligned with the aforementioned modeled scenario classes as well as 45 unmodeled risk aggregation scenario classes;
- frequency models that incorporate kill-chain analysis, expert surveys and historical events;
- footprint modeling, to map the companies impacted in a cyber attack; and
- a severity model, detailing six major cost components of a cyber attack on a company.



Source: CyberCube.