Measuring Cyber Risk in the Financial Services Sector: Conference Summary (Detailed)

Sponsored by
The Board of Governors of the Federal Reserve System
The Federal Reserve Bank of Richmond
The Massachusetts Institute of Technology – Internet Policy Research Initiative

14 Nov 2022
# Table of Contents

**Opening session** .................................................................................................................. 4  
  Keynote: Daniela Rus ............................................................................................................ 4  
  Fireside chat: Tom Barkin / Andrew Lo / Daniel Weitzner ............................................... 4  
  Kemba Walden ..................................................................................................................... 5  
  Andrew Lo ............................................................................................................................ 5  

**Panel: Cybersecurity, operational resilience, and financial stability** ......................... 6  
  Catastrophic risk .................................................................................................................. 6  
  Risk agility and responding to failure ............................................................................... 6  
  The expanding attack surface ......................................................................................... 6  
  Interconnectedness of the banking system ....................................................................... 6  

**Panel: Evaluating cyber incidents** .................................................................................. 7  
  Leveraging historical examples ......................................................................................... 7  
  The insurability question around cyber .......................................................................... 7  
  Vulnerabilities, threats, and consequences .................................................................... 7  
  Rapid recovery as a defense .............................................................................................. 8  
  Loss frequencies and impacts to drive business decisions ............................................. 8  
  The need-to-know pieces of data ..................................................................................... 8  
  Examples of how data has changed security perceptions ............................................... 9  

**Panel: Risk metrics and predictive statistics** ................................................................. 9  
  Risk metrics still a developing field .................................................................................. 10  
  ORX as an industry model ................................................................................................ 10  
  Better risk metrics could free up risk capital .................................................................. 10  
  Re-insurers and cyber insurance sustainability ............................................................. 10  
  Risk metrics: Challenges and initiatives ......................................................................... 10  

**Panel: Threat analysis and scenario development** ......................................................... 12  
  No idiosyncratic risk in cyber ......................................................................................... 12  
  Passing the “use test”: Integrating risk results into firm decision making ..................... 12  
  Measuring reductions in cyber risk ................................................................................. 13  
  Building a physiology for cyber risk .............................................................................. 13
Recent progress in quantification .................................................................................................................. 13
How scenarios are run .................................................................................................................................. 14
Where are the data gaps .............................................................................................................................. 15
Keynote: Jim Routh ..................................................................................................................................... 16
Panel: Next steps ......................................................................................................................................... 17
  Culture and technology: Focus on questions to address first ................................................................. 17
  Threats are well established, but the attack surface is unique ............................................................... 17
  Learning from incidents ............................................................................................................................ 17
  Continuous improvement using incident and loss data ........................................................................... 17
  Stitching existing pieces together ............................................................................................................ 17
  Standardization and the need for a common language ........................................................................... 18
  Addressing biases in existing data sets .................................................................................................... 18
  Global data: Risks are global, but data sets are national ....................................................................... 18
  Beyond loss data linked to lessons learned ............................................................................................ 18
  Determining an organization’s risk tolerance threshold / risk appetite ................................................. 18
  Collaboration recommendations coming out of this meeting ............................................................... 19
MIT and the Federal Reserve System hosted a joint conference on Measuring Cyber Risk in the Financial Services Sector on September 7-8, 2022 on MIT’s campus in Cambridge, Massachusetts. Over 300 participants attended the conference either in person (80) or virtually (250+).

**Context for the event**
Financial service firms, researchers, and policymakers struggle to measure and evaluate cyber risk despite the large amounts of money organizations spend securing information networks. Data on cyber defenses, failures, and losses are often deemed too sensitive to share or disclose. This lack of data also limits our ability to measure, benchmark and evaluate cyber risks.

The Federal Reserve Board of Governors, the Federal Reserve Bank of Richmond and the Massachusetts Institute of Technology’s Internet Policy Research Initiative hosted experts from industry, government, and academia to discuss the status of efforts to measure and track cyber risk across the financial system.

---

**Opening session**

**Keynote: Daniela Rus**
MIT professor and CSAIL Director Daniela Rus opened the meeting. MIT has long been at the forefront of cybersecurity with early contributions from Shafi Goldwasser, Silvio Micali, and Ron Rivest on private key cryptography and now from researchers such as Vinod Vaikuntanathan who are pioneering approaches to homomorphic encryption – the ability to compute over encrypted data. She explained that the next set of advances in cybersecurity will require interdisciplinary collaboration to address current challenges as our lives become increasingly dependent on data-driven decisions.

**Fireside chat: Tom Barkin / Andrew Lo / Daniel Weitzner**
The fireside chat with Tom Barkin, Andrew Lo, and Daniel Weitzner explored the biggest risks in the financial services industry, looked at cyber risk in financial markets, and discussed how the future state of cybersecurity in the sector should look.

**Biggest risks**
Tom Barkin, the President of the Federal Reserve Bank of Richmond, explained that the biggest risk to the system is if people wake up and think their money isn’t available to them, which would trigger bank runs. The Federal Reserve is assessing how it can improve its cyber defense metrics based on this understanding.

**Measurement needs**
Andrew Lo, a professor at the MIT Sloan School of Management, focused on measurement of risk and said, “you can’t manage what you can’t measure.” He explained how financial markets are great at managing any risks that they can quantify, but without measurements, that process
breaks down. Barkin explained that for other lines such as credit risk, the industry and regulators have good metrics upon which they can base decisions. For example, there is good data on the performance of a loan portfolio, loan loss reserves, and we have models that can provide a good understanding of risk within an institution. But we do not have those lined up on the cyber side. What cyber metrics could be similar to the default rate or an overdue loan rate? There is a gap between where we sit today and where we want to get to. Lo talked about the need to start with metrics. We need to develop them, open them up to criticism, and then improve them so eventually we can trade securities and deploy risk mitigation strategies such as insurance coverage based on these measures.

Barkin and Lo laid out the core sets of data we need:
- 1. How big of a target is the organization?
- 2. What is the quality of their defenses?
- 3. What are the overall risks?
- 4. What is the frequency of failure?
- 5. What is the severity of attacks / size of the losses

Kemba Walden
Principal Deputy National Cyber Director at The White House’s Office of the National Cyber Director Kemba Eneas Walden provided a keynote and discussed the importance of quantifying cyber risk. In her keynote remarks, she acknowledged that there are significant challenges with obtaining cyber risk metrics but highlighted the need for these metrics internally within the financial service sector but also more broadly to understand systemic risk. Walden also praised efforts to bring government, industry, and academia together to share developments in cybersecurity, highlighting ongoing federal initiatives to better understand cross-sector risk and strengthen underwriting in the burgeoning cyber insurance industry through work led by the Departments of Homeland Security and Treasury. She also pointed to the Cyber Information Sharing Act of 2015 that makes it easier to share cyber information that is not subject to freedom of information requests or sunshine laws. Finally, she explained that her office maintains its commitment to using empirical metrics at the highest levels of government.

Andrew Lo
MIT Professor Andrew Lo spoke of how security needs to evolve, but we lack the data to guide those decisions. This is evident in the the inherent compromise between privacy and transparency. But new technological developments can address the existing tradeoffs that were previously thought to be solid. He presented MIT’s work on Secure Cyber Risk Aggregation and Measurement (SCRAM) and explained how techniques such as secure multi-party computation can aggregate data without requiring anyone to disclose their own sensitive data. Regulation needs to be updated to account for new technologies like this. He concluded with a call for all of us to partner together to build the financial system 2.0.
Panel: Cybersecurity, operational resilience, and financial stability

The first panel of the event focused on cybersecurity, operational resilience, and financial stability. Cyber resilience is a key component of firms’ overall operational resilience. A lack of cyber resilience at individual or groups of firms makes the financial system, as a whole, more vulnerable to cyber events and bouts of financial instability. This panel discussed how firms protect their most critical operations and core business lines with their own cyber resilience in mind, as well as the financial system’s cyber resilience, considering their firms’ critical role in the financial system. It also explored how measures of cyber risk and resilience fit within larger measures of overall operational resilience.

Catastrophic risk

Art Lindo moderated the session and is a Deputy Director in Supervision & Regulation in the Board of Governors at the Federal Reserve. Lindo kicked off the discussion talking about the catastrophic risk category and its effect on financial stability. There are certain risks that only the government can pick up.

Risk agility and responding to failure

Mahi Dontamsetti (Global Head of Non-Financial Risk & Chief Technology Risk Officer, State Street) used the Covid pandemic as an example of a resilience crisis. Frameworks, planning, metrics, and measures can only go so far and may not survive the heat of battle. What organizations need is “risk agility”. He highlighted three core needs for resiliency: First, risk management is a new frontier that organizations need to embrace. Second, resilience is a public good, so industry and regulators should work together. He emphasized that “We need to collectively work together, or we will individually fail”. Third, he stated that the focus needs to “shift left” in the lifecycle and also “shift right” to start with clients and markets. This requires a significant paradigm shift. In the past, we put the focus on ensuring that security will not fail. The new paradigm requires that we assume there will be failures, but we need to focus on what we do WHEN we fail. When this is the approach, failures are less important if we can recover quickly.

The expanding attack surface

Ajoy Kumar, the Chief Information Security Officer at the DTCC, also highlighted how the Covid pandemic led the introduction of new products and services that have been integrated into workflows and can increase the threat surface. VPNs are prime targets with home/hybrid work environments and software as a service (SAAS) is increasingly popular and comes with its own set of controls that need to be understood and monitored. Kumar also emphasized that free and open source software (FOSS) is a particularly important threat with many systems not maintained over the previous two years. He called for better lifecycle management for FOSS.

Interconnectedness of the banking system

Nicole M. Clement, Senior VP of Global Information Security at Bank of America, focused on the interconnectedness of the banking system. She explained that “if one of us has a bad security
day, then all of us have a bad security day” in relation to how a breach in one bank starts a chain-reaction of alerts and responses in across firms looking to measure and react to their own exposure. Clement also focused on the need for security teams to become more “threat led”. This includes understanding the bank’s current exposure to a specific threat, understanding what increases that threat exposure, and what could be done about it with controls. The key is ensuring control owners become experts in the threats. This also allows the company to examine and measure any new threats in a holistic way across the various control owners. She also called for increased industry collaboration, and to examine events that happen throughout the industry. But Clement also highlighted that shared data is very valuable to threat actors and needs to be secured itself.

Panel: Evaluating cyber incidents

The second panel explored how firms classify and evaluate individual cyber incidents within their organizations and how these data are used to quantify and communicate risk.

Leveraging historical examples

Josephine Wolff, Associate Professor of Cybersecurity Policy at The Fletcher School at Tufts University, moderated the session. She explained that her recent research includes case studies about cyber incidents. She suggested that looking at historical examples of what has gone wrong is useful for cyber risk management, even if they are sometimes dismissed as less useful.

The insurability question around cyber

Martin Eling, a professor and director of the Institute of Insurance Economics at the University of St. Gallen, provided data focused on answering the question of whether cyber risk is actually insurable. He explained that while the estimated annual cost of global cyber crime was USD 900 billion in losses, the estimated global premium volume for cyber insurance was USD 9 billion – a 100-to-1 ratio. This shows that the risk is heavily uninsured. When compared to natural catastrophe insurance that had USD 280 billion in losses with USD 120 billion insured – a 2.3-to-1 ratio. The global protection gap for cyber is USD 891 billion while natural catastrophe is USD 160 billion. He explained that the fundamental reason for this gap is a lack of data. There are some data sources becoming available, but the industry still lacks the data it needs to insure cyber risk. The other challenge is that even with data, cyber risk is difficult to model. It is characterized by heavy tail distributions similar to earthquake risk and can lead to a non-diversification trap. In the end, insurance providers wonder if they should even set up a portfolio given the heavy tails, non-linear dependences, modeling and parameter uncertainty, and asymmetric information costs.

Vulnerabilities, threats, and consequences

Matt McCabe is the General Counsel and Risk Officer at Kivu Consulting, a firm that runs ransomware negotiations for firms. He explained that cyber is essentially risk management that depends on three factors: vulnerabilities, threats, and consequences. In terms of threats, technology companies are very good at identifying vulnerabilities. Governments also have lots
of information on threats, but the information is typically classified. The financial service sector has done well at collecting and sharing information about threats. But there is still a big gap between pre-incident and post-incident information sharing. McCabe explained that post-incident information sharing is difficult for the legal departments in firms to agree to. The best cyber loss data are those that are put out in dollar terms.

Rapid recovery as a defense

David Stone from the Office of the Cloud CISO at Google explained that security professionals need to ensure they are measuring the right things. Often the industry focuses on measuring the symptoms rather than prevention. Is there enough automation in the environment with clean images that can be updated and deployed on a regular basis (e.g. 7 days)? And if so, what would that do to the threat surface? He also talked about the difficulty of quantifying and explaining the role of capabilities of threat actors. Security controls may work against less-sophisticated opportunistic attackers, but nation-state attackers would still be successful. That is difficult to explain in quantitative terms. We also need to leverage the data we have within our systems, for example in the cloud, to better defend the perimeters. Stone also talked about Google’s “Shared Fate” model where Google takes some of the responsibility for the secure design of systems running in its cloud. As a benefit, its customers can have lower premiums from partnering insurance companies.

Loss frequencies and impacts to drive business decisions

Sean Downey, the Head of Cybersecurity Operations and Analytics at Fidelity Investments, explained that decisionmakers need as much data as possible to understand what is happening. Firms have better visibility for their cloud deployments but much less from legacy systems on premises. Cyber teams need a standard set of processes and procedures, and preferably an approach used across the industry, that they can use to communicate with the CEO and board when there is an incident. He explained that the key metrics security teams need to communicate with governance boards are loss frequency and the overall impact to business. Without those, the metrics often fail to resonate. Outside data from incidents and about threat actors is also critical for his team.

The need-to-know pieces of data

The group highlighted the metrics they considered need-to-know pieces of data.

- **How did they get in? How far did they move? Can we recover alone?**
  McCabe highlighted the key fundamental pieces he sees: 1) How did they get in? 2) How far did they move? 3) What is the chance of recovering without needing to interact with the threat actor?

- **Real loss event data**
  Eling explained that we need real loss information linked to events. Some of the current data is of questionable quality, but reporting requirements are bringing more trust to the data we have.
• **Better frequency data**
  Eling also said the industry needs better frequency data on attacks and incidents. There is crude information on the frequency of incidents in the academic literature, but this is an area that needs improvement. Stone also highlighted the need for data on frequency. The more data you have, the better you can piece together what you need to do.

• **Systemic information**
  Eling also explained that we need better information on systemic relationships and effects.

• **Classes of issues**
  In cyber, the next incremental dollar for security spending can go toward either prevention or remediation. We need better information about the classes of issues that firms face to target security spending at items with the best returns.

• **Indicators of compromise**
  Downey explained that we need better indicators of compromise. After an incident, it is important to know what series of controls failed that led to the incident.

Examples of how data has changed security perceptions
Wolff asked the panel about times when access to new security data let to new insights or operational changes. The panel put forward several examples.

• **PCI protection**
  Once the insurance industry understood the attack vectors for payment card information, they quickly told companies to encrypt their data lines and tokenize their data if they wanted to keep their insurance. This led to a massive and rapid improvement in security. McCabe explained that insurance was the driver.

• **The persistence of heavy tails for loss severity**
  Eling explained that early data showed that loss severity is heavy tailed, but he expected things to change as more data became available and attacks evolved. His research partners were surprised that the tail index remains stable over time as they evaluate more data.

• **Appropriate vs. inappropriate access permissions**
  Loss data sets such as the DBIR continue to highlight inappropriate data permissions are less of a problem than insiders changing their normal behavior with respect to data that they legitimately have access to. That indicates a different set of controls are needed.

• **Old things becoming new**
  Stone said that attackers are smart and quick to adapt. They have seen that attackers are revisiting old methods and using them in new ways to get past defenses.

---

Panel: Risk metrics and predictive statistics

The quantification and analysis of cyber risk is a developing field and has not yet matured to the point where it can be consistently measured and managed against corporate risk appetites. This
panel discussed the current state-of-the-art methodologies used in evaluating cyber risk, as well as existing gaps and future directions

Risk metrics still a developing field
Tammy Hornsby-Fink, the Chief Information Security Officer at the Federal Reserve System, chaired the panel and introduced the topics. She explained that risk metrics are still a developing field and more work is needed.

ORX as an industry model
Steve Bishop, the Research & information Director at ORX, provided background on their organization and the new line of cyber data they are building. Their organization has 130 members and 30 of them are subscribers to the new cyber line that is based on a give-data-get-data model. They have been focused on developing industry standards and references such as a risk taxonomy, a controls library, and an indicators library.

Better risk metrics could free up risk capital
Ni Kenney, a Senior Business Director at Capital One, framed part of her work around oversight for the operational risk management team at Capital One. Their teams leverage internal loss data, actual loss data from industry, run scenario analyses and provide guidance for capital allocations to cover risk. She highlighted that more accurate risk metrics could potentially free up capital that is set aside for incidents to be used by other parts of the organization.

Re-insurers and cyber insurance sustainability
Martin Kreuzer, a Senior Risk Manager at Munich Re, explained that Munich RE is the market leaders with 13-14% of the re-insurance market share in the cyber insurance space. His role is to make sure that Munich RE’s cyber insurance offering is sustainable.

Risk metrics: Challenges and initiatives
Hornsby-Fink focused first on the challenges of developing risk metrics and asked for examples of initiatives to address them. The group identified various data needs and challenges.

- **Data needs**
  - **Benchmarking against peers**
    Firms need the ability to benchmark against their peers. Bishop explained that sophisticated firms can build their own internal metrics, but they cannot respond to questions from the governance board about their situation relative to peers.
  - **Loss data**
    Several panelists mentioned the need for actual loss data. Kenny explained that firms do not have enough actual loss data to do modeling effectively but said that the existing data can still be used for measurement. The goal, however, is to get enough data to do modeling well. Kreuzer also touched on the need for loss data and wants it linked to what caused the losses and more intricate statistics such as correlations across the kill chain. Kreuzer explained that there are two large drivers
of losses from cyber events: business interruption and liability from data breaches. What kind of KPIs can address these two elements?

- **Risk exposure**
  Firms need good risk exposure metrics so they can look at ways to offload some of the risk via insurance, said Kenney.

- **Linking severity with likelihood**
  To preform risk measurement, firms need to link the likelihood of an incident with its expected severity, according to Kenney.

- **Interconnectedness**
  When there is a data breach, there is no way to determine if follow-up fraud using the stolen data was from a particular breach or if it was already out and available from earlier incidents. Kenny explained that this presents a challenge for modeling.

### Challenges

- **Need for a common language and quantification methods**
  The industry needs a common language to talk about cyber risk. Kenney said that engineers use technical language and measure risk in red/yellow/green heatmaps, while business decision marker talk about cyber risk in financial terms (e.g. US dollars). Organizations need to bridge this gap.

- **Data quality**
  There are cyber risk data available on the market, but the participants highlighted the need for better data quality. Kenny said that the industry needs to figure out how to ensure that the data quality is good. Kreuzer went farther and laid out the four important data quality characteristics. The data needs to be unchangeable, comparable, consistent, and meaningful. Kreuzer also mentioned that, as of now, there are no key performance indicators that support automated underwriting. Bishop talked about the need for consistency across companies for data collections, and that will require a broad dialogue.

- **Agreeing on a data-gathering process**
  In addition to call for a common language, the industry would benefit from agreeing on a data-gathering process. Tammy Hornsby-Fink and Steve Bishop both mentioned the need for a standardized data gathering process to support benchmarking.

- **Getting groups to share the data**
  Firms are reluctant to share sensitive data about their security, so getting firms to share data is important and a challenge according to Bishop and Hornsby-Fife.

- **Rapidly changing environment**
  Firms struggle to constantly adapt to the ever-changing cybersecurity environment. This change is coming from all directions – regulatory changes, evolving technology that requires new controls, and new defensive approaches according to Kenney.

- **Talent pool**
  The panelists also highlighted challenges with building the cybersecurity talent pool. “Bilingual” specialists who understand technical risk and quantification are in high demand according to Kenney.

- **Firm culture**
  Some of the challenges are inward facing and involve whether the firm’s culture is
ready to adapt to quantitative measures for cybersecurity, according to Kenny. Bishop categorized what they see from firms into three camps.

- 1) Firms evolving what they did in the qualitative space
- 2) Quantification being done by the wider operational risk teams in a firm
- 3) Firms doing exposure-based modelling with risk drivers and metrics

**Approaches**

- **Scenario analysis**
  Kenney explained that the highest levels of the business care about top level risk exposure so they can set aside necessary capital. They find that scenario analysis has been an important tool to develop these high-level numbers.

- **Continuing this type of dialogue**
  Hornsby-Fink closed off the session saying that the industry needs more partnerships and events like this to get people on the same page.

---

**Panel: Threat analysis and scenario development**

This panel focused on discussing existing approaches to understanding the major factors and players behind cyber risk threats, as well as the techniques used, and the process of analyzing these threat and materialized events.

**No idiosyncratic risk in cyber**

**Patricia Mosser**, a director and senior research scholar at Columbia University’s School of International and Public Affairs, moderated the session. She doesn’t believe that there is true idiosyncratic cyber risk in financial services because once there is a cyber incident at one bank, it affects all the others. She put a particular emphasis on rare, long tail events where we still lack good data. Scenario analysis is one of the tools that firms use effectively to understand the impacts of these rare events in individual firms and in the broader market.

**Passing the “use test”: Integrating risk results into firm decision making**

**Nedim Baruh**, the head of operational risk measurement and analytics at JP Morgan Chase, highlighted that the discussions about cyber in this conference sound very familiar to discussions from 20 years ago on operational risk. He referenced Andrew Lo’s statement on the previous day that “you cannot manage what you cannot measure” and Tom Barkin’s call for new metrics and collaboration. Over the past 20 years, the industry has indeed found ways to measure operational risk to produce capital requirement numbers for the firm, but he argues few would say that we do it well. Early efforts on operational risk produced industry groups such as ORX and many data and academic partnerships. But then he raised the question of why we still struggle with operational risk measurement after two decades. He argues that the industry failed at the “use test” for several reasons. The “use test” refers to line one using the
measures produced often by line 2 on risk as part of their decision making. He questioned if operational risk data are used by management to manage risk better, or if they are simply used to capture the capital amount. He also mentioned there is a shift in the industry away from the complex models to determine capital amounts to be set aside to simpler formulas. He concluded by stating that the lessons we have learned over the past 20 years on operational risk should be applied now in the cyber risk setting.

Measuring reductions in cyber risk

Karmen Yu, Assistant Vice President of the National Incident Response Team at the Federal Reserve, explained how cyber of the past 15 years has shifted from listing risks on note cards in the past to quantifying risks based on data now. She highlighted there is keen interest in understanding how to quantify any reductions in cyber risk from the implementation of controls but doing so will required a holistic approach and will depend on industry collaboration.

Building a physiology for cyber risk

Jack Jones, Chairman of the FAIR institute, explained how early in his career as a CISO he was asked by an executive at a meeting how much risk the firms has. He answered “lots”. Then the executive followed up asking if they spent the millions he was requesting to fix the problem how much less risk would they have, and he sheepishly answered, “less”. That turning point highlighted the need for cyber risk quantification and metrics that could be communicated in the language of decision makers, and it was the beginning of Factor Analyses of Information Risk (FAIR) in 2001. He said that cybersecurity is a real challenge because it is complex and dynamic, but that also means that it is never boring. Next, Jones compared progress on cyber risk to medicine 1800s when doctors finally realized that bloodletting doesn’t work. He explained that in the 1800s, the doctors knew the anatomy well but did not understand the physiology - how the anatomic elements worked together. His current work on a FAIR Controls Analytics Model is attempting to create similar types of linkages between how controls (anatomy) affect risk (physiology).

Recent progress in quantification

The first question to the panel focused on recent progress in quantification.

- **Recognition that risk can be quantified**
  It seems fundamental, but few believed that cyber risk could be quantified 20 years ago according to Jones. Now we are in the phase of “how to do it” and how to do it at scale. Jones did state that “believers” in risk quantification are still in the minority because you don’t need to go far to find another heatmap.

- **Supplementing quantitative data with expert opinions**
  We need to understand the loss-generating mechanism. Baruh explained that typically means a particular focus on severity. There has been real progress with using quantitative measures that are then supplemented by expert opinions where there are
gaps until new data is available. Baruh explained that the industry is approaching the problem in a healthy way.

- **People responsible for managing the risk should measure the risk**
  Historically there has been a gap between the groups managing the risk (e.g. line 1) and those measuring the risk (e.g. line 2). Banks are getting better at giving responsibility for measuring risk to the teams that ultimately need to manage the risk according to Baruh. Yu said she has seen similar progress away from old approaches that prepared top-ten lists of the largest risks that get put away for the year and not used by line 1. Now she sees a more collaborative process between lines 1 and 2.

**How scenarios are run**
The next discussion item focused on approaches and best practices surrounding scenario modeling. The panel identified five important elements to consider.

- **Layered approach**
  Jones explained that he uses a layered approach where he begins with fundamental items that need protection and adds on layers from there. He recommends identifying what processes and data are valuable and need protecting in the business for the first layer. Second, explore the technical assets that can support (or expose) these valuables. For the third layer, he recommends looking at how these technical assets can be affected by threat agents. Importantly, once these layers are in place, firms can then filter or triage the risks. Baruh also talked about approaching this in levels. Organizations don’t need to start with the most complex factor model. They can start at a high level and then start decomposing the elements into more levels, as needed, depending on their context. Yu reiterated that breaking down the various pieces and focusing on each layer provides the necessary granularity to calculate the risks for scenarios.

- **Describing the loss generating mechanism**
  Baruh broke down a simplified version of the approach they use at his firm:
  - Step 1: Describe the loss generating mechanism
  - Step 2: Categorize the factors in three components
    - Exposure: What is exposed?
    - Occurrence: How does the loss event occur?
    - Impact: What are the factors that affect the impact?

- **Business leaders should guide scenarios**
  Security people should be last to say what is important from a security perspective according to Jones. The firm’s leaders see the complete picture of what is happening in the business and are best placed to make those decisions. He also said that firms need to take the time to really define their loss scenario landscape well and not skimp.

- **Control relevancy is highly context dependent**
  Jones explained that the importance of controls (e.g. authentication) depends on the context. For example, authentication may seem like a more critical control than logging, but not if the attacker is an insider with sufficient permissions.

- **Understanding intent is critical to defending financial stability**:
  Mosser explained that in the context of financial stability, understanding the intent of
the threat actors is critical. Differing incentives (stealing funds vs. causing widespread disruption) will require different defensive mechanisms.

Where are the data gaps
Mosser asked the panel to identify the types of data they need but currently do not have access to.

- **Data quality issues**
  Yu explained that data quality issues are a challenge that should be addressed. How can the data we have be improved and how can new data be evaluated for data quality levels?

- **Having an accurate and comprehensive data inventory**
  Yu mentioned that you cannot protect what you do not know you have. She referenced a statement from yesterday saying, “it’s more important to understand what is NOT in your denominator”. Firms need an accurate and comprehensive data inventory.

- **Data around effectiveness of controls**
  Baruh said they need a better understanding of the factors that affect the severity of a loss, and this requires better data around the effectiveness of controls and how they ultimately affect risk.

- **Human element**
  We do not have good measurements on the human element around cyber attacks. In an audit that Jones ran several years ago, 75% of security failures were because a human did not do what they were supposed to do. Of those deficiencies, 75% were linked back to making deadlines or setting priorities that came before security concerns. Jones explained that metrics about the human elements are vitally important, but we don’t have them. That leads us to a “Groundhog Day” scenario where we see the same cyber risk concerns day after day. He also explained there is a difference between malicious internal actors and non-malicious. When modeling, that intent can cause huge risk swings.

- **Correlating security and risk data**
  Yu explained how we need better ways of linking pieces of security and risk data together to understand compounding risk. For example, clickthrough rates for phishing attacks may not say much on their own, but when paired with the types of data access the user has, it becomes much more valuable in understanding how the risk compounds. Jones followed on explained how logging data, by itself, isn’t useful. It needs to be paired with monitoring and normal/abnormal use differentiation. Those three parts need to be together for successful detection. He put it in statistical terms saying we need the Boolean “ANDs and ORs” to put an impact parameter on controls such as logging metrics.

- **Near real-time data**
  Jim Routh raised a question about the need for real-time data. Yu said the cyber threat landscape changes very quickly and gave an example of Russia and Ukraine. In the cyber context, she looks for real-time or near-real-time to make decisions. Baruh provided a counter example for operational risk where exposure is relatively static. Jones took the
middle ground saying sometimes data is available in real time, while other metrics will never be available so quickly (e.g. quarterly audits). It is a mixture. There is also a cost to invest in real-time data, so firms need to make sure it’s worth the investment.

- **Risk identification:**
  Baruh brought up the importance of risk identification. He said that regulators came in and said that risk identification should owned by the first line in financial service firms. This led to a big and successful shift in firms toward giving that responsibility to the first line. Early on the focus was on risk categories, but that didn’t speak to the people actually managing the risk. Now the risk inventory can be used as a basis for quantification. Mosser said that this is similar to general financial risk. It’s important to have communication between business and technical teams so that the technical teams have ownership, responsibility, and a use case for those risk measures.

---

**Keynote: Jim Routh**

Jim Routh, the former CISO of MassMutual and Aetna, gave a keynote presentation providing a CISO practitioner’s perspective on cyber security metrics. He said that organizations make the common mistake of measuring what they can measure rather than what they should measure. Choosing the wrong indicators has a cascading effect throughout the organization as analysts devote considerable time to collecting and analyzing the wrong statistics.

Routh also explained the difference between key performance indicators (KPIs) and key risk indicators (KRIs) using an example of the weather. KRIs are like weather forecasts to tell you the weather conditions people should look out for before they take any steps to mitigate the effects. They measure the inherent risk. KPIs, in contrast, measure residual risk after applying controls for weather such as an umbrella or raincoat. Routh explained that risk quantification seems to be working well in large organizations. It takes significant resources to spin up an internal risk quantification platform, so he recommends firms that choose that route go all in.

Routh detailed his three-pronged approach to identifying the top cyber risks.

1. Explore external sources for cyber threats (e.g. make a top-ten list)
2. Define the attack surface (e.g. count your devices, users, consumers, etc.)
3. Identify the top cyber risk using a consensus-based approach, rely on data, and prioritize investment decisions based on changes to risk

To conclude, Routh provided an example of how data-driven decisions about cybersecurity in a firm can lead to efficiency gains. He used enhanced authentication and getting rid of passwords for users as an example. First, it benefits the consumers by reducing friction and giving them a better digital experience. Second, the decision reduces account takeovers. Finally, adopting enhanced authentication lowers operation costs for the call centers that no longer spend time on password reset calls.
Panel: Next steps

Taylor Reynolds, the research director of MIT’s Internet Policy Research Initiative, moderated a session focused on summarizing the discussions over 1.5 days and proposing a way forward. He said the goal of the panel was to start down the road of identifying what are the most important risks that we need to measure that aren’t measured now and to look for ways that we can build a community to develop measurements and models around these risks.

Culture and technology: Focus on questions to address first

Nagarjuna Venna, a lecturer at MIT Sloan and co-founder of Bitsight, said figuring out the problem to solve is 80% of the challenge. He put forward that security is not a technical artifact, but a cultural one. This means that security outcomes are more dependent on culture than technology. His recommendation was focusing on getting the questions right first. Once we agree on questions, it will be easier to find solutions.

Threats are well established, but the attack surface is unique

Jim Routh, the former CISO of MassMutual and Aetna, explained how the threat landscape is well established, but the attack surface for every enterprise is unique. In that sense, work done on threats will be applicable to all and just needs to be adapted to an individual firm’s attack surface.

Learning from incidents

Routh said the most valuable learning comes from incidents that is then applied within the organization to improve security. He said it was typical for his firms to have around 225 incidents per year – about one per business day. There are plenty of opportunities to learn from incidents, so we should use them to make security improvements.

Continuous improvement using incident and loss data

Steve Bishop, the Research & Information Director at ORX, highlighted that loss data needs to be measured better, and that will require better collaboration within firms and across them. He linked back to early comments that we should focus on measuring what is important, not just what we can. The goal should be examining incidents, pulling out lessons learned, applying these lessons to metrics and monitoring, and improving continually. Jim Routh also provided an example of ransomware attacks. Early attacks focused on targets with relatively unsophisticated security measures, but then threat actors realized that large firms that typically have cyber insurance (and could pay ransoms) had antiquated and vulnerable backup systems. So the tactics changed and ransomware threat actors started targeting large firms and going directly after their backup systems.

Stitching existing pieces together

Aly Farooqui, the Chief Risk Office for IBM Cloud for Financial Services, emphasized that many of the pieces we need for better measurement already exist within silos among the companies and participants in the room. We would all benefit from a way to stitch the existing pieces
together. He provided background of the work IBM is doing with 115 banks on metrics to help de-risk the cloud. They built a coalition that worked for 7 months to develop a list of 61 KPIs and KRIs related to cloud security.

Standardization and the need for a common language

Martin Eling, a professor and director of the Institute of Insurance Economics at the University of St. Gallen, reiterated what others heightened during the conference. There is a need for standardization of metrics and a common language for working with cyber risk.

Addressing biases in existing data sets

Eling pointed out biases in existing data sets that inhibit our understanding and measurement of risk. These challenges mimic similar issues with biases in operational risk from 20 years ago.

Global data: Risks are global, but data sets are national

Eling emphasized that the cyber risks firms face are global, yet most data sets are done at a national level. This limits our understanding of the risks by only focusing on data from a single geographic region. Eling stated that most data we have comes from the US, so more data is needed to complement it from other countries and regions.

Beyond loss data linked to lessons learned

Jeffrey Gerlach, a Vice President in the Richmond Fed, said we need better data on incidents that go beyond simple loss data and connect to threats and lessons learned. He emphasized the need for data on “near misses” that typically fall outside of data collections but are still offer valuable lessons for firms and the industry.

Determining an organization’s risk tolerance threshold / risk appetite

Reynolds put forward a question about how firms determine their risk tolerance threshold. He said that many firms say they struggle to develop these metrics. The discussion uncovered several insights.

- **Risk appetite can vary by audience**: Farooqui explained that risk appetite varies across an organization depending on the audience. For example, the governance board will likely have a different perspective than other groups within the organization such as line 2 and line 3 who are responding to different needs. Jack Jones said that organizations do not have just one risk appetite. For example, organizations may have different appetites for data breach versus an outage event. Jones suggested solving locally and then building up from there. Venna countered that it is possible to get a reasonable view from the top down without talking to companies and used Log4j as an example. He also mentioned that Israel and Belgium are both doing a good job with the top-down approach to risk measurement.

- **Risk appetites are not used well yet**: Bishop explained that it isn’t clear if risk appetite measures are being used well in businesses, but there is an opportunity to take what we have learned from other risk lines such as credit risk and apply it to cyber.
- **Solvency capital ratios in Europe**: Eling talked about the solvency capital ratio used in Europe to determine whether insurers and banks will be able to meet their obligations to policyholders. It can be used as a risk appetite measure for scenario modeling.

- **Need to quantify risk appetite measures**: Jack Jones said the industry needs to clarify what we mean by quantification. Is it done with an interval scale (1 to 5 score), because if so, it is not the type of quantification we need.

- **Call for transparency**: Jim Routh explained that most security information is shared internally in organizations on a need-to-know basis, but that implies that people in the organization don’t know where the defects are. He called for more transparency in organizations as a model to move forward. Steve Bishop agreed. He said that we should encourage transparency both internally and externally. Aly Farooqui agreed and said sharing and transparency would help firms understand “what good looks like”. Nedim Baruh also agreed on the need for more transparency and said this was a lesson learned from work on operational risk where they put a premium on transparency and understanding on the models in use. Martin Eling also said collaboration and communication are the key, both internally and across organizations.

- **Calls for sharing data**: Many of the participants called for more data sharing on risks. Ryan Harris from the St Louis Federal Reserve Bank argued that all firms have risk appetites, KPIs and KRIs, and that sharing them does not give away a firm’s competitive advantage. Nedim Baruh agreed and said there is no competitive advantage in risk measurement and models. Parameterization, factors, controls, and calibration may be different, but the methods and models are similar and should be shared. This would unlock significant value for the entire industry. Jim Routh said he had never had a bad experience with sharing information with the ISACs. He said, “there is no competition when it comes to cybersecurity in the financial service industry; there never has been and there never will be”.

- **Better business impact measures**: Chase Englund from the Federal Reserve Board asked about the need for better business impacts data to measure resilience. As an example, outage times are often measured in hours, but they lack information about the decrease of production from the shutdown that is needed to calculate losses.

**Collaboration recommendations coming out of this meeting**

- **Initial questions to answer**: Jeff Gerlach said we need a stronger focus on the questions we want answered by a collaboration. Ni Kenney suggested that we think about cyber risk management in three dimensions: 1) How can we prevent incidents 2) If controls break, how to maintain operational resilience 3) Try to understand the exposure to the organization in the case of a large event to set aside the right amounts of capital. With those in mind, we can plan a way forward out of this meeting with the following questions:
  - 1. What data do we need?
  - 2. How fast do we need the data?
  - 3. How can we provide insights back to the industry?
- **Set clear objectives and a framework**: Steve Bishop recommended setting clear objectives and developing a framework for the way a collaboration will operate. He also said the group needs a platform for operations. This is how ORX began 20 years ago and has been very successful.

- **Don’t lose the momentum**: Jeff Gerlach emphasized that we do not want to lose the momentum built during this meeting. On the Federal Reserve side, there is significant interest. Both Tom Barkin and Tammy Hornsby-Fink came in person to participate, and Barkin is behind the work along with other senior leaders.