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

28 March 2024
# Table of Contents

**Contents**

*Table of Contents* ............................................................................................................................................ 2  
*Context for the event* ..................................................................................................................................... 4  
*Keynote: Harriet Pearson* ............................................................................................................................... 4  
*Panel Discussion: Cyber Risk Officer (CRO) Session* ......................................................................................... 5  
  Importance of a Tabletop Exercise (TTX) ........................................................................................................ 5  
  Securing Data in Transit .................................................................................................................................... 5  
  Organizational Structure to Manage Risk ........................................................................................................ 6  
  Boosting Security Posture ............................................................................................................................... 6  
  Managing Third-Party Service Providers ......................................................................................................... 7  
  Building Risk Appetite .................................................................................................................................... 7  
  What Keeps the Panelists Up at Night ................................................................................................................ 7  
*Panel Discussion: Modeling Cyber Risk* ............................................................................................................ 7  
  Current Practices .............................................................................................................................................. 8  
  Modeling Approaches ...................................................................................................................................... 8  
  Remaining Challenges ..................................................................................................................................... 8  
*Keynote: James Wiener* ................................................................................................................................... 9  
*Panel Discussion: Financial stability* ................................................................................................................ 9  
  Cyber Resiliency ............................................................................................................................................... 10  
  Insuring Cyber Risk .......................................................................................................................................... 11  
  Future Threats .................................................................................................................................................. 11  
  Third-Party Risk .............................................................................................................................................. 11  
  Use of Modeling .............................................................................................................................................. 12  
*Keynote: Vinod Vaikuntanathan* ........................................................................................................................ 12  
*Welcome and Opening Remarks: Michael Barr* .................................................................................................. 13  
*Keynote: Arthur Lindo* ..................................................................................................................................... 13  
*Panel Discussion: Corporate Board Perspective* ............................................................................................... 14  
  Connect Cybersecurity Risks to Business Concerns ......................................................................................... 14  
  Governance over Management .......................................................................................................................... 14  
  How Board Members Can Provide Cyber Oversight ....................................................................................... 15  
  Implications of Generative AI .......................................................................................................................... 15
The Role of the Market in Evaluating Cybersecurity Risk ........................................ 16

Panel Discussion: Challenges for the Future ......................................................... 16

Current Trends ....................................................................................................... 16

Third-Party Risks .................................................................................................. 17

Long-Term View .................................................................................................... 17
MIT and the Federal Reserve System hosted a second joint conference on Measuring Cyber Risk in the Financial Services Sector on January 16-17, 2024, on MIT’s campus in Cambridge, Massachusetts. Over 400 participants attended the conference either in person or virtually.

Context for the event

The Federal Reserve Board of Governors, the Federal Reserve Bank of Richmond, and the Massachusetts Institute of Technology Internet Policy Research Initiative convened experts from industry, government, and academia for their second conference on efforts to measure and track cyber risk across the financial system. A common theme in the inaugural 2022 conference was that financial markets, financial services firms, researchers, and policymakers cannot manage risks that they cannot measure, and cyber risk remains difficult to quantify, despite the money spent to secure information networks. Data on cyberattacks, security failures, and losses are needed to effectively quantify and mitigate cyber risk. Today, however, these data are lacking, and without them, financial institutions and the financial system are vulnerable. The 2022 conference closed with a call for collaboration to develop a common set of metrics and reporting format to enable senior managers and boards of directors to assess and manage their organizations’ cyber risk. The 2024 conference built on the inaugural meeting and reviewed progress made.

Keynote: Harriet Pearson

Harriet Pearson, executive deputy superintendent and cybersecurity division head for the New York State Department of Financial Services, highlighted the value of data-driven actions through insights, engagement, and innovation.

The New York State Department of Financial Services (DFS) was created on October 3, 2011, by merging the state Banking Department and Insurance Department. The financial services sector is a frequent target for cyberattacks, which cause significant financial loss for New York businesses and consumers. The DFS adopted the first-in-the-nation cybersecurity regulation in 2017. This regulation became a model for other federal and state regulations, including the Federal Trade Commission (FTC) Safeguards Rule, the National Association of Insurance Commissioners (NAIC) Model Law, and the Conference of State Bank Supervisors (CSBS) Nonbank Model Data Security Law. The DFS then investigated hundreds of cyber incidents and discussed industry practices with experts, concluding that most cyber incidents involve the same, well-known techniques. Their findings supported the idea that standard cyber controls are essential and could help defend against 90% of common attacks. The DFS adopted measures requiring covered entities to implement comprehensive cybersecurity programs based on their own risk assessments. Additional requirements set to take effect over a period of two years include new cybersecurity awareness training, monitoring privileged access, and an asset inventory policy.
Pearson explained that DFS values being equitable, innovative, transparent, and collaborative, and it uses data to drive its actions and propose regulations with a risk-based approach. Interested parties can subscribe to receive DFS cybersecurity updates at https://on.ny.gov/subscribenydfs.

Panel Discussion: Cyber Risk Officer (CRO) Session

- Moderator: Kristen Walters, Senior Managing Director and Chief Risk Officer, CPP Investments
- Betsy Brady, Managing Director, Cyber Risk, Bank of America
- Meyrick Douglas, Senior Vice President and Chief Risk Officer, Prudential Financial
- Mark Katzelnick, Chief Risk Officer, Fidelity Investments
- Ravi Varma, Chief Operational Risk Officer, EVP Enterprise Risk Management and Risk Oversight, American Express

The cyber risk officer (CRO) is responsible for building cyber resilience in an organization. Discussing best practices to measure and manage cyber risk, the panel recognized the need to have a data-driven approach but not become too buried in metrics when analyzing the data. The CRO should view threats through a business lens and identify the needed controls to calculate metrics over time. A firm can use quarterly metrics to stay accountable, and contextualizing metrics is critical because a large set of metrics can span different risk appetites. Thus, it is crucial to refine risk assessments in areas that have the greatest impact to ensure uninterrupted service for clients and customers.

Importance of a Tabletop Exercise (TTX)

The panel discussed the potential for smaller companies to underinvest in cybersecurity due to capital constraints. A tabletop exercise (TTX) can be a worthwhile expenditure for internal evaluation and to assess vendors. For instance, an annual simulation with the executive committee could identify important decisions that need to be made during a crisis and clarify critical communication channels to ensure all relevant parties are coordinating. Further, a TTX supports compliance with data governance and standards.

Securing Data in Transit

Firms should have a comprehensive inventory of data destinations and assess the need to transmit data. There is a demand for swift data delivery from customers and firms, but paid transmission of data carries risks. Firms should consider when data exits the internal network and ensure it does so securely and appropriately. The frameworks pertaining to data-risk management have evolved, placing an emphasis on usability, protection, and compliance.
Organizational Structure to Manage Risk

The panelists also discussed how their firms’ structures contribute to risk management. Betsy Brady, managing director of cyber risk for Bank of America, explained that the chief information security officer (CISO) oversees all security controls in the company in the first line. The second line assumes responsibility for reporting cyber risk appetite and collaborates closely with the first line on quantifiable metrics. This allows the second line to take a balanced approach, engaging in tool and technology evaluations as well as architectural developments. Brady highlighted that clear delineations of controls are crucial.

Mark Katzelnick, chief risk officer at Fidelity Investments, emphasized that the enterprise technology risk team produces models and offers testing, while another team focuses on cyber fraud in the second line. There is significant mobility between the first and second lines, and the third line encompasses audit. This enables the audit committee to report back to the board and engage in discussions about ongoing activities.

Ravi Varma, chief operational risk officer and EVP of enterprise risk management and risk oversight at American Express, described how the CISO reports to the chief information officer (CIO) as a first-line risk function. The second-line risk function focuses on risk appetite and oversight, distinct from operational and risk management functions. The challenge lies in fostering effective cross-pollination within the second-line function. Varma said that security analysts should transition into risk management roles rather than the reverse, making it challenging to find the proper skill sets when hiring.

Irrespective of firm structure, there are shared approaches that all firms can adopt. Meyrick Douglas, senior vice president and chief risk officer of Prudential Financial, cautioned against operating on autopilot. In financial risk, the threat environment is continuously changing, and it is important to establish habits of recognizing metrics, incorporating external perspectives, and maintaining humility. Brady added that at Bank of America, there is a systematic process for threat intake to avoid constant firefighting. Since launching the intake process, the firm has assessed nearly 300 threats. Katzelnick shared that he engages third-party expertise to glean insights from others to identify areas for improvement.

Boosting Security Posture

The panel acknowledged the importance of staying current with emerging technologies like generative AI, quantum computing, and crypto. The panel also discussed modifications to cyber event reporting, such as the Security and Exchange Commission (SEC) requirement to report events within four days. Disseminating information about cyber events is crucial for a more comprehensive management of cyber risk. Panelists argued it is in the financial service industry’s best interest to remain interconnected.
Managing Third-Party Service Providers

At Bank of America, Brady relies on an inventory system for critical infrastructure and processing control to determine areas of protection. The firm also has an assessment program for third parties to validate their services. Katzelnick echoed that the same process occurs at Fidelity, managing access controls, privileged access, and frameworks.

Building Risk Appetite

Firms are naturally anxious about events with large outcomes and potential reputational risks. The panel emphasized the importance of addressing risks of exposure and funding to maintain information security. A firm’s risk appetite is determined not only by a budget, but also by where it receives the biggest “bang for its buck”. However, risk appetite can be limited due to a lack of quantification in cybersecurity. A risk appetite framework can articulate risk and offer a set of parameters from which to operate the company. Thoughtful discussion is needed around the nature of risks because metrics alone do not convey such details. An analysis can highlight where the firm is exposed to threats, and the board may want to receive more information based on qualitative indicators.

What Keeps the Panelists Up at Night

Katzelnick said both small and large events, including theft of intellectual property, are causes for concern. It remains a challenge to lock down critical assets. Douglas shared that reputational risk is a great concern because the financial industry is founded on trust, which takes a long time to build but may be lost quickly. Brady worried about finding the best people and upskilling talent. Varma echoed Brady and added that even the best operational and executive strategies can fail without the right people.

Panel Discussion: Modeling Cyber Risk

- Moderator: Lisa Ryu, Senior Associate Director, Supervision and Regulation, Board of Governors of the Federal Reserve System
- Gabriel Bassett, Director, Cyber Risk Advisory Services, Liberty Mutual
- Martin Eling, Professor, University of St. Gallen; Director, Institute of Insurance Economics
- David Severski, Senior Security Data Scientist, Cyentia
- Evan Wheeler, Senior Director, Technology Risk Management, Capital One

Measuring cyber risk requires data about security posture, control failures, and resulting financial impacts of security incidents. But the quantification and analysis of cyber risk is a
developing field, making consistent measurement a challenge. This panel discussed current methodologies used in evaluating cyber risk, emphasizing recent advances as well as gaps.

Current Practices

Lisa Ryu, senior associate director of supervision and regulation at the Fed Board of Governors, opened by introducing some of the key challenges to evaluating cyber risk, such as a lack of data and insufficient cyber-specific techniques compared to other risk areas. She then invited the panelists to discuss their current practices for measuring cyber risk despite these challenges. All panelists asserted that current approaches to measuring cyber risk are dissatisfactory. But Evan Wheeler, senior director of technology risk management for Capital One, said that existing techniques can work well to answer basic hygiene questions. Gabriel Bassett, director of cyber risk advisory services at Liberty Mutual, said that insurance doesn't look for perfection but improvements from basic correlations to move forward. Martin Eling, professor of economics at the University of St. Gallen, and David Severski, senior security data scientist at Cyentia, added that an important goal should be to better understand the insurability and impacts of cyber risk to effectively make a difference.

Modeling Approaches

Regarding current modeling approaches, Wheeler warned of the pitfalls of overcomplicating models to try to account for everything. That said, he noted that model structure is still vital to learn about what makes a difference. Performance can be crudely measured with back testing on historical data, although such data could become stale. Other pitfalls include difficulty determining whether an attack was avoided due to luck or successful risk avoidance, and modeling resilience versus threat. Bassett said that modelers can keep up with the pace of cybersecurity changes, and Eling said that a small number of parameters can often determine most of an organization's risk. Ryu noted that for most organizations, increased emphasis on basic, consistent controls can shore up defenses dramatically. For synthesizing data into new models, Bassett and Severski agreed that expert judgment should be incorporated into the decision-making process, but potential biases must be accounted for. This can be done by balancing human judgment with highly quantifiable models.

Remaining Challenges

One major question in this field is how to define cyber risk and other related metrics like control maturity, which Ryu invited the panelists to discuss. Eling defined cyber risk as a subset of operational risk, but he said there are still unique problems that make cyber risk difficult to measure, such as non-financial losses. Severski said that the complexity of cyber risk makes it difficult to properly define, considering the variety of attack vectors, the contrast between small risk with sizable data versus large risk without data, and indirect costs. Even with data, it is still difficult to quantify the benefits of singular controls or the aggregate level of security for an organization. Bassett and Wheeler concurred that external reports of cyber incidents provide frustratingly little insight into the internal workings of an attack or the performance of controls.
Although there are many challenges to modeling cyber risk accurately, especially when it comes to the ever-present threat of large attacks, most cyber events can be understood and managed with foundational controls and contingencies. Further research must be done on the effects of regulatory mechanisms and developing better standards for quantifying and sharing cyber risk between organizations so that everyone can improve their understanding of cyber impacts. However, successes should not be overlooked. Due to the nature of the data and skew in the news, Bassett pointed out that there is a greater focus on failures. Taking the time to note and build up previously successful designs is also important. Ryu observed that these goals will require a collaborative effort.

Keynote: James Wiener

James Wiener, partner and vice chairman in Oliver Wyman's financial services practice and former chief risk officer and chief executive officer of BNY Mellon, shared his perspective on cybersecurity risk measurement and how it informs organizational risk management. He emphasized the interconnectedness between cyber risk and technology risk, stating that an organization cannot implement effective cyber controls without a modern technology infrastructure. This view fueled the massive investments of BNY Mellon in technology and infrastructure modernization, focused on the following areas:
- Automation of IT assets
- Infrastructure management and protection
- Identity and access management
- Data protection
- Threat and vulnerability detection
- Reporting and monitoring

Wiener recognized that even with technology modernization, all cyber controls can be improved to better withstand state actors. Additionally, while there isn’t a robust quantification framework to measure an organization’s overall cyber risk, measuring the individual components that impact cyber risk is critical. Wiener emphasized that metrics related to high cyber risk exposure are generally stable and can effectively guide investment strategy. Lastly, there is a need for real-time data on the cyber threat environment, which could be acquired through an expanded public-private partnership.

Panel Discussion: Financial stability

- Moderator: Martin Boer, Senior Director of Regulatory Affairs, Institute of International Finance
- Gerald Glombicki, Senior Director, Insurance, Fitch Ratings
- Ron Green, Mastercard Fellow, Mastercard
The panel examined the broader financial sector in discussing systemic cyber risk and financial stability. The panelists represent various aspects of the financial sector: a bank, a payment company, a credit rating agency, and the U.S. Treasury.

**Cyber Resiliency**

Martin Boer, senior director of regulatory affairs for the Institute of International Finance, asked panelists to define cyber resiliency and their approaches to achieving and maintaining it. Richard Ifft, lead senior insurance regulatory policy analyst – TRIP for the U.S. Treasury Federal Insurance Office, explained that his organization is not a regulatory body, but it does keep an eye on the insurance sector. Insurance companies are vital to increasing cyber resilience. Katheryn Rosen, managing director and global head of regional information security and supervisory engagement for JP Morgan Chase, noted that large banks are critical infrastructure to the United States. JP Morgan’s approach to cyber resilience considers the nature of the business, the threat environment that the business faces, the possible contagion effect of an attack, and the regulatory requirements for each location they operate in. The first step is to identify the essential services of the business and the critical points of failure. Rosen spoke about the creation of a “Firm Wide Simulation Utility,” whose goal is to think about end-to-end scenarios that are both plausible and disruptive, as well as the possible impacts to all essential services. After-action reports, which summarize the findings of a simulation and identify areas of improvement, are also important to the program. Third parties that work with the business need to take a cyber resilience approach as well.

Given how Mastercard operates in many countries around the world, Mastercard Fellow Ron Green stressed the importance of different sizes of testing, especially for countries and companies that have much smaller budgets for cyber resiliency. He discussed the transition from "little T" testing, where each application is tested independently, to "big T" testing, which tests the applications together. Tabletop exercises (TTX) are also important to engage executive leadership in the cybersecurity landscape, especially to identify and justify areas of improvement. The next step is to include law enforcement, public relations, law firms, customers, and other partners in those tests. Green emphasized the importance of public-private partnerships, as many of the firms are facing the same adversaries. Gerald Glombicki, senior director of insurance for Fitch Ratings, stated that cyber resiliency is both hard and expensive to achieve. It requires an understanding from every aspect of the business about cyber risk and incident response plans. Cyber regulation only represents the bare minimum that companies should meet, and firms need to cultivate a culture of cyber resilience.
Insuring Cyber Risk

On the topic of how insurance companies are working to manage high-severity cyber risks, Ifft stated that there is a need to evaluate whether the market is focused on catastrophic cyber risk, which differs from attritional cyber risk. Glombicki commented that investors are already pricing risks relative to bonds in the insurance linked security (ILS) market, with cyber making up $500 million of the $4.5 billion market.

Future Threats

Turning to future technologies, like quantum computers, Rosen stressed the importance of cross-border collaboration on regulations. Enhanced awareness campaigns are needed, since the changes brought about by quantum computing aren’t likely to be large-scale for another 10 years. Keeping the public informed and publishing roadmaps is the best course of action. Actions being taken today include the formation of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States, the National Institute of Standards and Technology (NIST) developing the new standards for post-quantum security, and the World Economic Forum publishing a high-level roadmap for what financial service firms need to do today. Rosen stated that the G7 and G20 need to also be engaged in these conversations, and regulators need to be prepared because they have so much data.

On the topic of making regulations more consistent, Rosen expressed the difficulty of knowing the timing, details, and even the destination for incident reporting. Although the Financial Stability Board (FSB) has done some work to create a template for reporting, countries within the FSB are also developing their own standards, complicating incident reporting for international businesses. Security operations are inhibited by efforts to create network boundaries at country borders for national security reasons. Data localization also causes problems, compounded by utilization of the cloud.

Third-Party Risk

Boer discussed the rising importance of third-party risk, and asked how risk should be managed between a firm and their third-party providers. Green stated that every firm should be responsible for understanding their third and parties and making sure their providers can meet their requirements. Even if the regulatory body is the same across firms, there can be small differences between the regulations for each firm, which can raise the complexity of meeting all requirements. This inhibits a firm’s ability to secure the business, as managers devote more time to checking off boxes. Rosen commented that people who can perform such complex reporting are in high demand because it takes up so much of a firm’s time. Green added that countries try to top their neighbors in terms of reporting, leading to an arms race rather than harmonization.

The panel was asked if third parties should be supervised or regulated to improve resiliency. Green mentioned that ratings and similar oversight could help improve the maturity of third
parties, but it isn’t guaranteed to improve their resiliency. Rosen stated that third parties need to be supervised and regulated to help resiliency, and banks have to make private contracts with their third parties to meet resiliency requirements. A firm’s third parties need to be told to operate in a specific way so that the firm can meet their regulatory requirements.

Use of Modeling

The panel addressed a final question about how modeling can help firms make better decisions. Glombicki stated that because different users require different answers, it ultimately boils down to model maturity. Rosen mentioned that changing administrations often leads to a restart of relationships due to the different approaches of sharing information, transparency, and building institutions that work. Work needs to be done to establish a foundation that doesn’t change. Boer brought the discussion to a global scope; each jurisdiction has its own ideas and justifications for why they have specific requirements. As a result, while each jurisdiction makes itself stronger, the overall system becomes weaker, which impacts overall financial stability. Green stated that adversaries do not care about national boundaries as they operate and attack.

Keynote: Vinod Vaikuntanathan

System designers often consider data as existing in one of three states. There is data at rest, which is when the data is stored in a database. There is data in transit, which is when the data is being moved between machines. Finally, there is data in use, which is when the data is an input to an actively running computation. Classical cryptography focuses on protecting data in the first two cases, where encryption schemes and signature schemes protect the privacy and integrity of data at rest and in transit. Fully homomorphic encryption (FHE) completes this picture by protecting data in use. FHE is a form of encryption that allows computations to be performed over data while the data remains encrypted. This technology can also be used to securely pool data that is too sensitive to store in the open, such as medical or financial data. There are numerous applications for FHE across a variety of industries, such as matching ad views to purchase data, identifying trends across patients with rare diseases, and connecting persons of interest across different law-enforcement agencies.

Vinod Vaikuntanathan, cryptographer and professor of computer science at MIT, discussed a project using FHE to securely pool information about vulnerabilities and cyber events to answer several important questions. This included MIT’s SCRAM project for determining the current risk profile of broad categories of firms, understanding the effectiveness of various controls, and calculating the ROI for cybersecurity spending (scram.mit.edu). The FHE constructions that Vaikuntanathan used have the added benefit of relying on the same underlying security assumptions that NIST has announced as the basis for post-quantum cryptography. This means that even in the unlikely event that a large-scale quantum machine capable of breaking current number-theoretic assumptions is created, this FHE construction will remain secure.
Vaikuntanathan said that the main goal was to understand what computations would be most useful to the participants of the study in order to write FHE kernels to support these tasks. The longer-term goal is to develop a full software stack so that developers without expertise in advanced cryptography can still write applications that safely compute using sensitive data.

Welcome and Opening Remarks: Michael Barr

Michael Barr, vice chair for supervision of the Board of Governors of the Federal Reserve System, gave the opening address for the second day of the conference. He spoke about various critical needs and considerations that financial institutions and the present community should focus on going forward. As the cyber threat landscape evolves, cybersecurity preparedness becomes increasingly essential for all institutions. This includes not just cyber defense, but also resilience in the forms of well-maintained business continuity plans and risk management. In particular, there are gaps in banks’ management of cyber risk introduced by third-party service providers. New guidance on such third-party risk has been recently adopted by the Federal Reserve and other bank regulatory agencies. Barr noted that forums such as this conference are essential to gauge how the community thinks about and measures risk in financial markets. International cooperation on cyber risk is also necessary to support the globalized financial system. Barr said that it was clear that more research needs to be done on the spillover effects of attacks. More work on quantifying cyber risk is also needed. Quantifying cyber risk is still in a nascent stage largely due to a lack of data. Better avenues for interconnectedness and incident reporting will improve data and the collective ability to respond to threats.

Keynote: Arthur Lindo

Arthur Lindo, deputy director for policy in the Federal Reserve Board of Governors Division of Supervision and Regulation, spoke about the importance of effective governance for cybersecurity and the future of measuring cyber risk and cyber resilience. Collaboration between the private and public sectors is needed to develop harmonized security standards. Lindo noted that while efforts are underway to develop these standards, continued vigilance is needed to uphold those standards across the sector. Adversaries’ capabilities continue to evolve, increasing the need to identify the best uses of finite cybersecurity resources. Lindo stressed the importance of identifying the most critical resources for both individual entities and the financial sector as a whole. Guides, such as those published by the Cybersecurity and Infrastructure Security Agency, can help firms of all sizes take steps to improve their cybersecurity. Lindo called for expanding the scope of data collection and cyber risk measurement. There is a need to consider the human factor when measuring the
adequacy of cybersecurity measures and to improve the current frameworks on disclosures. Lastly, Lindo discussed areas for further work, including developing quantitative measures of cyber risk and resilience and analyzing the impact of people on cyber risk and resiliency. Continued dialogues, collaborations, and partnerships are needed to further improve financial sector resilience.

Panel Discussion: Corporate Board Perspective

- **Moderator:** Andrew Lo, Professor of Finance and Director of the Laboratory for Financial Engineering, MIT
- **Larry Clinton,** Internet Security Alliance; NACD fellow
- **Patricia Mosser,** Senior Research Scholar, Columbia SIPA; Director, Nomura Holdings
- **Corey Thomas,** Chairman and CEO, Rapid 7; Chair, Board of Directors, Federal Reserve Bank of Boston

This panel focused on cyber risk measurement and management from the corporate board member’s perspective, discussing how a board can address cyber risk within their range of responsibilities and communicate effectively with the firm.

Connect Cybersecurity Risks to Business Concerns

Larry Clinton, leader of the Internet Security Alliance and NACD fellow, previously developed principles to guide board members on cyber risk oversight. He explained that a goal of the principles was to communicate cyber risk in a non-technical, coherent manner. Clinton emphasized that board members are not typically interested in learning technology, so cybersecurity risks must be embedded in business concerns, such as connecting cybersecurity issues to supply chain problems. Board members need an understanding of cybersecurity that will remain relatively stable and guide overarching thinking.

Governance over Management

Patricia Mosser, director of the MPA Program in Economic Policy Management at Columbia SIPA and board member of Nomura Holdings, described how board members need to be equipped with the appropriate tools to determine strategic priorities. Board members require information on vulnerabilities and awareness of the evolution of the threat landscape, but they cannot be expected to collect this information themselves or to develop detailed plans to address cyber risk given the rapid pace of change. The board’s role is to continue asking the “uncomfortable questions” regarding operational resilience and behaving as an advisory body.

Corey Thomas, chairman and CEO of Rapid 7 and chair of the board of directors of the Federal Reserve Bank of Boston, recognized the emotional and psychological pressures that board members feel as a response to the speedy rate of change in technology and the lack of
harmonization across regulators. Thomas reiterated that it is crucial that boards not do management’s job.

How Board Members Can Provide Cyber Oversight

- **Request that the management team complete a sophisticated cyber risk assessment**
  - Clinton emphasized that this risk assessment should include empirical and economic analysis to understand what risks to accept, mitigate, reject, or transfer. This assessment is distinct from determining regulatory compliance.
  - Panel moderator Andrew Lo, professor of finance and director of the Laboratory for Financial Engineering at MIT, followed up with a question asking how organizations of different sizes should approach assessments, which can vary widely in cost. Thomas responded that assessment of the fundamentals, and implementation of essential controls outlined in NIST (for example), are very cost effective.

- **Share information regarding cyber risk to improve understanding of the threat landscape**
  - Clinton particularly directed this advice at large banks with a more sophisticated understanding of cyber risk, emphasizing the need for a collaborative model given the interconnectedness of the environment. Clinton reiterated that the board holds an affirmative responsibility to understand cyber risk not just on an entity basis but on an ecosystem basis.
  - Lo asked how board members should deal with countries that do not share the same sensibilities regarding collaboration or behave as international bad actors. Mosser recalled her experience as a board member of a Japanese company, and recognized the difficulty of geopolitical tensions that raise uncertainty in business strategy and cybersecurity risk. Mosser stressed that limited sharing across borders increases cyber risk, and that even though there are increasing calls for more information sharing, board members must assume that certain countries and sectors will remain unwilling.

Implications of Generative AI

- **Lo specifically asked Thomas to address a recent tagline from his company, Rapid 7, that the “AI race is with your enemies.”** He asked for his thoughts on the combination of AI and cyber risk efforts. Thomas emphasized that board members cannot be so alarmist regarding AI risk that they miss current or potential risk that can be addressed with basic cyber controls. Generative AI continues to evolve the cyberthreat landscape. It can enable attackers to identify weak points faster or conduct more convincing phishing attacks. Defenders need to leverage AI to eliminate this attacker advantage. Cyber maturity in the past 10 years has steadily increased, but regulatory agencies can help focus organizations on addressing the fundamentals.
The Role of the Market in Evaluating Cybersecurity Risk

- Clinton explained how the macroeconomics of cybersecurity provide a fabulous business model for bad actors because there is virtually no law enforcement. He advocated for the development of a macroeconomic model of the economics of cybersecurity to better understand the impacts of policies. Mosser concurred with the need for more careful economic analysis, particularly regarding the network effects of a cyberattack.
- Thomas said harmonizing regulatory standards is critical. The combination of regulation and data from the cyber insurance market can provide a baseline to compare the cybersecurity postures of organizations. Once this threshold is established, markets can reinforce good behavior because investors can assess this information.
- Lo proposed that with data gained from MIT’s SCRAM project, it is possible to create a new market of cyber intrusion swaps, which is a bet on the likelihood that a company will be a target of an intrusion of a particular severity. With enough data, capital markets can price tradeable cyber insurance, as opposed to relying on the reserves of cyber insurance companies.

Panel Discussion: Challenges for the Future

- Moderator: Daniel Weitzner, Senior Research Scientist, CSAIL, MIT; Founder of the MIT Internet Policy Research Initiative
- Joel Brenner, Senior Research Fellow, MIT; Former Senior Counsel, National Security Administration
- Maya Bundt, Former Swiss Re; Board member, Baloise Group, Valient, APG SG; Executive board member, Cyber Peace Institute
- John Horn, Director, Cybersecurity Practice, Datos Insights

The panel focused on aspects of cyber risk that are currently overlooked.

Current Trends

Daniel Weitzner, senior research scientist for MIT’s CSAIL and founder of the MIT Internet Policy Research Initiative, observed that cyber risk management has matured notably. The actual risk of a catastrophic failure seems to empirically be quite low. Joel Brenner, senior research fellow at MIT, explained that big attacks are quite hard to execute for anyone other than nation-state actors. An attack at that level is essentially equivalent to an act of war, and there isn’t a sophisticated nation-state that thinks it can currently win a war against the United States. This is a major deterrent for these attacks. It’s not that the attacks aren’t possible, just that the consequences would be too severe.

Maya Bundt, formerly of Swiss Re, expressed similar concerns from the reinsurance view. The reinsurance industry is very worried about exactly this eventuality; they don’t want to wait until war is declared. Setting these serious but low-probability events aside, she argued that the
focus should be on the small, “death by a thousand cuts”-type of risk that accumulates over years.

Third-Party Risks

Weitzner then led the discussion to third-party risk, which is both difficult to assess and can easily get quite large. John Horn, director of cybersecurity practice at Datos Insights, explained that the main source of mitigation for this type of risk is redundancy (i.e. having multiple options for third-party suppliers in case one goes down). This is potentially sufficient for some types of third-party risk, such as supply-chain risk, but it doesn’t really address other serious sources. A major example is the Target hack, which was via a vulnerability in their HVAC supplier. It doesn’t really seem like redundancy solves the problem in this case. Bundt said that reinsurance has a lot of data on this but is also worried because regulation is mainly focused on supply chain resiliency and not so much on other ways that third-party providers can put the larger system at risk. Brenner was very skeptical that regulation can solve the problem, since no third-party provider will willingly accept the liability for their clients’ systems. Horn was also skeptical about further regulation.

Weitzner pressed this a bit further by asking how people currently measure third-party risk. Bundt talked about the growth in the cyber insurance market and how insurance companies have been trying to build these risks into their models. However, insurance companies are far from any solutions; they’ve just identified the problem of systemic and unmitigated third-party risk. Brenner also thought that insurance could provide most of the solutions by insuring more specific incidents like data loss or business interruption.

Long-Term View

Weitzner concluded by asking the panel what they think will be important over the next five years. Brenner mentioned digital identity as a major focus. Bundt answered that risk models are very important to develop further. Horn pointed out that these systems are fundamentally unsecure, perhaps suggesting that future system designs should take security as a primary design principle rather than an afterthought. He then said that gathering more data to better measure risk is very important. He added that the government, including the National Security Agency, doesn’t have the answers here. Everyone needs to share more data to figure this out together.

Concluding remarks

Market pricing of cybersecurity risk is emerging, with instruments such as insurance-linked securities and the potential for new instruments such as cybersecurity breach swaps. Markets
need data to price risk, though, and both Jeff Gerlach of the Federal Reserve Bank of Richmond and Daniel Weitzner from MIT, both conference organizers, called on the group to work together over the next year and come back to the next conference with new data and shared risked models. To make this happen, MIT will launch a consortium of financial service firms to create models and metrics corresponding to a set of core cyber risks identified and prioritized by the group. Academics and risk modeling teams from banks will work together to develop a standardized set of indicators, models, and definitions for cyber risk to guide corporate governance and management, enabling senior managers, executives, and boards of directors to define risk appetite, measure progress internally, mark-to-market risk, and benchmark against peers.