Kevin Stiroh: Thoughts on cybersecurity from a supervisory perspective

Remarks by Mr Kevin Stiroh, Executive Vice President of the Financial Institution Supervision Group of the Federal Reserve Bank of New York, at SIPA's Cyber Risk to Financial Stability: State-of-the-Field Conference 2019, Federal Reserve Bank of New York, New York City, 12 April 2019.

* * *

As prepared for delivery

Good morning and welcome to the Federal Reserve Bank of New York. We are very happy to be hosting this conference on "Cyber Risk to Financial Stability" for the Columbia School of International and Public Affairs (SIPA).[1]

One of the advantages of a talk on cybersecurity is that there is not a motivation problem—you don't need to convince anyone that this is a fundamental risk for financial firms, the financial system, and the broader economy. There is strong consensus on that point. As a result, we can use our time more productively to talk about the substantive issues around things like identification, protection, detection, response, and recovery, the implications for financial stability, and the important work that needs to be done.

The focus of today's conference is on the link between cyber threats and financial stability. This is clearly an important topic and there is a growing field of research that explores issues around transmission channels, amplifiers, and behavioral dynamics. As a few specific examples, recent papers map out the link from cyber risk to financial stability through a range of transmission channels such as interconnectedness, confidence, and data integrity, and a related paper focuses on the potential dynamics of a cyber-triggered run.[2] I think these frameworks and perspectives offer a very useful point of departure for macroprudential policy discussions. For today, however, I'm going to shift from a macroprudential view to a microprudential one and offer some thoughts on cyber risks from a supervisor's perspective. These are not independent views, so I hope my perspective adds to the broader discussion today.

Before proceeding, I'd like to emphasize that these are my views and do not necessarily reflect those of the Federal Reserve Bank of New York or the Federal Reserve System.

As you may know, the supervisory program for the largest banks that was implemented after the financial crisis looks at both individual firm safety and soundness and the potential impact that distress at a large bank can have on broader financial markets or the economy.[3] More specifically, this framework expresses two complementary goals for the supervision of systemically important firms: (1) Enhanced resiliency of the firm to lower the probability of failure or inability to serve as an intermediary and (2) Reduced impact on the financial system or economy in the event failure or material weakness does in fact occur. This is one way to link microprudential issues to the macroprudential concerns.

From a supervisory perspective, cyber risk can be viewed through the lens of operational resiliency where a cyber attack threatens the ability of a firm to provide critical financial services. An effective risk management framework with appropriate governance and controls is one way to mitigate those risks. Just as capital and liquidity promote financial resilience, strong governance and controls support operational resilience. The governance and controls portion of the large bank assessment framework includes an evaluation of risk management capabilities including independent risk management and controls and planning for the ongoing resiliency of a firm.[4]

As I indicated earlier, cyber risks are well-known and firms are expending considerable

resources and management bandwidth to address them in terms of technology, process and personnel. U.S. banks and other financial firms are projecting higher spending on cybersecurity each year as they face bigger threats and more attacks.[5] Cumulatively, we have seen estimates as high as $1 trillion for global spend on cybersecurity through 2021.[6]

One area of supervisory focus is on maintaining resilience of core business services. For cybersecurity, this includes continued progress on preventive and detective efforts. It also includes things like a comprehensive process to assess cyber-related capabilities; identification of gaps in business resilience requirements such as recovery time objectives; risk monitoring and testing programs; and management reporting to facilitate appropriate prioritization. Moreover, bank resiliency increasingly depends on the resiliency of third-party service providers.

In this sense, our approach to cybersecurity is embedded in the broader supervisory and risk management frameworks. As such, we see notable similarities to other shocks that could impact a firm's operational resiliency, safety and soundness, and ability to continue to provide financial services in a sustainable way. From a process perspective, for example we expect firms to leverage traditional approaches to risk identification, measurement, mitigation, monitoring and reporting. In terms of governance, we expect effective oversight from Boards of Directors. There are also similarities to risk management of information technology with a focus on things like change management and information security controls, asset management, and the software development lifecycle.

There are, however, important differentiators that distinguish cyber risk from other operational shocks such as those related to natural events or human error. These differentiators provide a useful map for risk managers and supervisors who must adapt to these evolving risks.

One obvious differentiator of cybersecurity risk is around motivation. While there are exceptions, we don't usually think of a credit or market risk event or a natural disaster happening with intentionality by a determined adversary. Asset quality or market prices may change unexpectedly and weather events may prove disruptive, but they lack intent to harm. By contrast, cyber events, by definition, involve an intention to steal, disrupt, or destroy. According to one recent survey, the biggest drivers of cyber attacks were access to information followed by financial profit.[7] Cybercriminals are increasingly motivated by data theft, rather than solely direct monetary theft. In addition, the adversary is likely to evolve and may even actively respond during an attack making it necessary to have a dynamic response to this more complex threat.

Motivation also impacts the varied nature of the threat landscape. Cyber events are driven by nation states, organized crime, and political activists. As result, the threat landscape changes not only with opportunity, data and technology, but also in response to global and domestic politics. One study highlights that cyber incidents from nation states are on the rise.[8] These types of cyber attacks have no physical boundaries as a malicious actor can successfully launch an attack on an institution located in another part of the world. All of these factors impact how an institution will choose to prepare and respond.

A second critical differentiator is the nature of disruption including potential impacts on data confidentiality, integrity, and availability. Cyber attacks that involved data corruption or destructive malware are unique to a cyber threat and can have an immediate and devastating impact. The question of data integrity has emerged as a critical factor in a cyber attack and introduces additional risk management challenges. For example, the ability to respond and recover may be disrupted if there is data destruction or corruption in a scenario that is also likely to include considerable uncertainty. Even if a firm can recover from a data corruption cyber-attack, when would customers and clients trust them as a counterparty? Issues around confidence and interconnectedness are ways that a cyber event can have broader macroprudential implications.

A third differentiator relates to the skill and human capital needed to build the most successful

defenses. Cyber security requires a different set of skills and abilities including systems development and acquisition lifecycles; general enterprise architecture and IT governance; and IT service management sub-disciplines such as asset management, and configuration management. Even within the technology fields, cybersecurity efforts involve specialized disciplines that are not usually addressed by general IT specialists related to perimeter defense, endpoint security, and authentication. Acquiring and retaining the critical talent for these activities is a growing challenge.

All of these issues present unique challenges from a risk management perspective. Moreover, the fragmented regulatory landscape for cyber risk and lack of mature metrics and measurement tools add difficulty. This is true both for the firm's second and third lines of defense and Boards of Directors' oversight, as well as for supervisors approaching this from an external perspective.

As I mentioned at the beginning of this talk, these issues are well-known and both the private sector and the public sector are actively working toward solutions to these difficult problems. I expect we'll see continued evolution of the risk management framework as the broader fintech ecosystem develops and cyber defenses co-evolve with new threats. Challenging and complex issues include the most effective strategies around prevention, detection and response; communication protocols internally, and with clients, vendors, and the official sector; business continuity plans and contingency exercises; and the role of Boards of Directors. Supervisors can contribute to this debate by continuing to emphasize the critical importance of a strong risk culture with the appropriate governance and controls framework.

To conclude, I believe that resiliency to a cyber event is an area where the incentives of the private and public sector are closely aligned. Microprudential and macroprudential objectives are reinforcing. As a result, there is an imperative to collaborate, share information, and learn from one another about threats, responses, and best-practice approaches. Conferences like this one that bring together the private sector, the public sector and academics are a critical component to that necessary dialogue.

Thank you for your attention.

---

[1] I thank Danny Brando, Bill Brodows, Dianne Dobbeck, Jackie McCormack and Danielle Vacarr for help preparing these remarks.

[2] Jason Healy, Patricia Mosser, Katheryn Rosen and Alexander Wortman, The Ties that Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability, Columbia SIPA, December 2018 and The Future of Financial Stability and Cyber Risks, The Brookings Institution, October 2018. Darrell Duffie and Joshua Younger, "Cyber Runs," February 13, 2019. See also Office of Financial Research, Cybersecurity and Financial Stability: Risks and Resilience, 17–01, February 5, 2017 and Financial Stability Oversight Council, 2018 Annual Report, 2018.

[3] Federal Reserve Board, SR 19–3, Consolidated Supervision Framework for Large Financial Institutions, December 2012.

[4] Federal Reserve Board, SR 19–3, Large Financial Institution Rating System, February 2019.

[5] Thales, Thales Data Threat Report 2018 – Financial Services Edition, December 2018.

[6] Cybersecurity Ventures, 2018 Cybersecurity Market Report, May 2017.

[7] Positive Technologies, Cybersecurity Threatscape 2018: Tends and Forecasts, March 2019.

[8] Crowdstrike, 2019 Global Threat Report: Adversary Tradecraft and The Importance of Speed, February 2019.