Keynote Speech

by

Beth Dugan
Deputy Comptroller for Operational Risk

at

The Clearing House's First Operational Risk Colloquium

February 11, 2015
Washington, D.C.

Thank you. It's an honor to be invited to speak here today, not least because this is The Clearing House's inaugural Operational Risk Colloquium. The Clearing House has had a long and important role in the American banking system. You've supported its smooth functioning in benign times, and you've played significant stabilizing roles in times of stress. And you've provided a forum for discussion of some of the most important challenges facing the banking industry.

The cliché "Great minds think alike" isn't always true, otherwise there wouldn't be innovation. However, I think it's safe to say that The Clearing House and the OCC have a common view on the importance of addressing cyber threats and vulnerabilities, and the risks they pose to banks and the banking system. Virtually every issue of The Clearing House's quarterly journal, *Banking Perspective*, has had an article that addressed this topic, and sometimes multiple articles. The OCC shares your concern and focus. The topic of cyber threats was prominent in the OCC's 2014 *Annual Report*—in fact it was the first of the four main themes the Comptroller addressed—and it was a key risk theme in our Fall 2014 *Semiannual Perspective on Risk*. And if you'll bear with me, I'd like to make a few comments on this topic,

as well as address some of the other operational risks the OCC has on its radar, and how these risks are inter-related.

As the Deputy Comptroller for Operational Risk, I can tell you without hesitation that the risks to banks from cyber threats and vulnerabilities are significant. The severity of cyber threats is escalating rapidly and attackers are exhibiting an increasing ability to exploit vulnerabilities in commonly used infrastructure. While the impact on financial service firms has been relatively limited so far, as we see from experience in other industry sectors there is a growing possibility for materially severe attacks on banks or the infrastructure on which they depend. Let me give you some examples of what we are seeing broadly across the landscape.

- Attackers are demonstrating a growing proficiency in compromising credentials and systems through social engineering using targeted e-mails, and by corrupting legitimate Web sites with malware. Cyber criminals are using these techniques to install malware that harvests bank employee, third party, and customer credentials including usernames, passwords, and other information such as e-mail addresses.
- Attackers are becoming more adept at crafting attacks that encrypt data or mobile devices—including those of banking customers. Once the data or device is encrypted, the criminals extort the users or the organization by demanding a payment to retrieve data or release access to the device.
- The severity of damage to compromised business systems is escalating. Some attacks have exploited gaps in systems and business processes at foreign financial institutions and other organizations to install malware that erases, corrupts, or encrypts data on a large scale. At non-financial organizations, malware has wiped data and rendered computer hardware unusable by destroying operating systems.

- Infrastructure vulnerabilities are being identified on an almost daily basis, and these vulnerabilities are being exploited more quickly than ever before. For example, within hours after the public announcement of vulnerabilities in the Bourne-again shell (Bash) system and Open SSL software—two systems widely used—cybercriminals were broadly sharing tools to identify and exploit the vulnerability.

Addressing the risks that cyber threats pose to individual banks and to the banking system have been a top priority for the Comptroller and the Federal Financial Institutions Examination Council, or FFIEC. In his capacity as chair of the FFIEC, Comptroller Curry called for—and the other council members concurred in—the creation of the Cybersecurity and Critical Infrastructure Working Group. A key initiative was the interagency Cybersecurity Assessment conducted last summer, which used a new pilot examination work program to assess the cybersecurity preparedness of more than 500 community institutions. That pilot assessment resulted in two FFIEC documents. One summarized the general observations from the work done, posed key questions for financial institution management to consider, and provided a list of resources. The other encouraged financial institutions to become members of the Financial Services Information Sharing and Analysis Center, or FS-ISAC, to facilitate monitoring and awareness of cyber threats and vulnerabilities. I would categorize these as early attempts to increase awareness of threats and best practices. The FFIEC and OCC will be doing more in both of those categories in the months ahead.

While the Cybersecurity Assessment was conducted at community institutions, the lessons we learned have real implications for banks of all sizes. First, the key questions for community bank board and management are equally relevant for your own boards and senior

management. I hope they're asking those questions right now. Second, many of those community banks are your correspondent clients. You have a stake in their well-being because they are connected to your systems, and because they are your customers. Finally, banks of all sizes are being targeted. That is why it is important that banks of all sizes stay better informed and prepared by participating in forums like the FS-ISAC. Hundreds of financial institutions have become FS-ISAC members since the FFIEC released its statement, and we hear that they add another five to ten new members every day.

The agencies' encouragement of information sharing by financial institutions mirrors a project that The Clearing House helped launch a year ago this month: a partnership between trade associations representing the merchant and financial services industries to explore paths to increased information sharing, better card security, and maintaining the trust of customers. There even have been recent proposals for legislation that would enable and encourage greater sharing of information on cyber threats.

So, yes, great minds sometimes do think alike. And it's increasingly important that those great minds collaborate more in their response to cyber risks. That's because financial institutions—and other industry sectors—are interconnected, not only through the infrastructure upon which they rely, but also as a result of third-party relationships that have become increasingly important to bank business models as contributors to revenue and technical expertise, as well as a means to manage expense.

Unfortunately, for many firms, their best efforts at maintaining awareness, monitoring their systems and environments, and implementing controls and mitigants will not be enough. Increasingly, the question is not "What more can we do to prevent or mitigate this risk?" It is becoming "What is our response when the risk is realized?"

Financial institutions' exposure to cyber threats and vulnerabilities has increased as a result of every third party and customer link into their systems. Risk grows with the competitive pressure to make those systems even more open and responsive in response to the demand for connectivity and integration, and the complexity and interconnections of the infrastructure on which these linkages depend. It's for this reason that resiliency is taking on a new importance.

We used to call it "business continuity" or "contingency planning." And we used to think of it as restoring and resuming operations after a fire or natural disaster or technology disruption. However, the levels of connectivity and dependence—both internally and externally—have changed. As a result, our approach to business resiliency needs to change as well. Let me give you a couple of examples of how the risks—and the required responses—are different. Natural disasters, fires, and utility failures don't have motivations and aren't persistent. That's not true for cyber attackers. They do have motives. Sometimes motives involve money. Sometimes attacks are state sponsored or political in nature. Whatever the motivation, these attackers are persistent in their intent to bring systems down or cause harm. Moreover, the cyber threats are scalable, evolving, and global in nature. Historically, having physically separate but fully redundant primary and secondary sites that mirror data in near real-time has been the approach to continuity of operations. But cyber threats potentially have the capacity to compromise both sites simultaneously, which could result in a complete loss of operational capability.

Physical threats still matter, but interconnectedness, new concentrations in service providers—including financial market infrastructure firms—and the changing nature of cyber threats call for new and creative thinking about resiliency. The OCC has been doing more than just talking about the changed environment of threats and vulnerabilities. For example, our 2013 guidance bulletin on risk management of third-party relationships re-emphasized the importance

of understanding and managing risks associated with third parties, which may also include subcontractors. Part and parcel of managing third-party relationships is ensuring that planning for resiliency involves not just operations performed internally, but the operations of those connected with your bank that perform critical business activities. The federal banking regulators think the resilience of technology service providers is vital to the industry, and it's long been an area of focus in our interagency program for supervising the largest firms that provide processing services to banks.

Financial institutions need to expand their disruption scenarios to consider the impacts of cyber threats not only to themselves and their critical systems and operations, but also from and to their third-party relationships, their customers, and the critical infrastructure components on which they depend. For example, recovery and restoration plans need to be re-evaluated for technology environments that present different or new risks. In certain technology architectural approaches—such as those that use real-time, mirrored-data replication and cloud-based services and data storage—there are no longer a physical or logical separation of production and backup systems and data. Disruption scenarios also should contemplate threats from knowledgeable insiders, cyber-attacks that simultaneously target production and backup data for corruption or destruction, disruption of communications and core infrastructure, and simultaneous attacks on the bank and critical service providers. Banks also need more robust incident management and response plans for notifying **all** stakeholders when an event occurs, including regulators, law enforcement, and those information sharing networks I spoke about earlier. After all, there is potential for significant negative consequences to the bank's reputation and strategy, in addition to the direct financial costs and operational disruption. Financial institutions need to establish

relationships with cyber-attack response resources, law enforcement, regulators, and others in advance for rapid activation and dissemination of information related to the event.

Changes to a financial institution's need for resiliency, however, often require changes to the board and senior management's approach to strategic planning and organizational culture. In this new environment, with its different and rapidly evolving risks, strategic planning cannot just be an exercise in projecting loan growth and profitability. New products and distribution channels, new technology platforms and applications, and changing use and connectivity with third parties all have an impact on the risk-reward equation. The board and management should have sound processes to ensure that the risks of business model change, new products or services, and new utilization of third-party relationships—individually and collectively—are assessed and clearly understood; that internal control and mitigation strategies are identified, implemented, and sustainable; and that the resulting risk level is consistent with the organization's risk appetite.

The importance of a financial institution's risk management and oversight can't be overemphasized. It starts with board and senior management awareness, which set the all-important "tone at the top." Routine discussion of cyber threats and vulnerabilities, risk assessments, and mitigation and incident response strategies is the foundation for a sound security culture. Training and awareness programs that are current and frequent reinforce the culture of awareness and monitoring, and can turn every employee into the first line of defense. And, if you will pardon a football metaphor, you want your defense to stop the attack at the line of scrimmage, and not down field.

Frankly, the quality of risk management and organizational culture have been topics for discussion by industry, media, and the regulatory community. Heading into the recent financial

crisis there were clear weaknesses. For some, discussion of those weaknesses has only now begun in earnest, but Comptroller Curry has been addressing the issue for some time. More recently, in his article in the 2014 fall issue of "Banking Perspectives" he stated: "What troubles me is not that some individuals made bad decisions, but that the business practices that have caused problems were made possible by weaknesses in the organization's risk management and risk culture." He reinforced that point at The Clearing House Association's last annual conference, when he said: "…a strong risk culture that promotes responsible business practices is important not just for its own sake, but is essential to safety and soundness."

And so, the OCC issued its Heightened Standards guidelines in the fall of last year to clearly articulate regulatory expectations for its largest, most complex banks. While the Heightened Standards don't mention cyber or operational risk or resiliency specifically, the elements regarding governance framework, roles and responsibilities, risk appetite, risk data aggregation and reporting, talent management, and expectations for the board are all relevant. Given the importance of the cyber threats and their potential impact, they must be a priority and addressed within a firm's risk governance framework and culture.

Underlying all that I've talked about so far is a theme of relentless change, in financial institutions and the industry more generally as well as in the operating environment. Your firms are likely going through a period of significant change and the pace of that change may be more rapid than before. For some it may involve a significant transformation of your business model, processes, products, and markets. The drivers of change may be the overall economic environment, competition (such as from nonbanks), a need to modernize technology systems or business processes for efficiency and profitability, or even recent regulatory developments. In periods of high velocity and volume of change, execution risk increases because resources and

capacity are strained, and there is a temptation to short cut or by-pass established change processes. At times like these, second and third lines of defense charged with monitoring change can be overwhelmed. These are also periods when attention can be diverted from risk assessment and monitoring as well as controls. In this environment, financial institutions may lower their guard against cyber threats, too.

Finally, there is complexity. Your business models, product-service mix, delivery channels, organizational structures, and technology systems—and the overall environment of threats and vulnerabilities in which these operate—are enormously complex. Many of you are trying to simplify, rationalize, streamline. Dealing with complexity is always a hard task. As H.L. Mencken once said, "Complex problems have simple, easy to understand, wrong answers." Nevertheless, it's important for the nation's banks to be proactive, to think clearly and comprehensively about the risks and the range of responses, and—finally—to make good decisions.

These are all topics of today's colloquium: sifting through the competing priorities in order to find the best approaches and tools for identifying, assessing, and managing operational risk; understanding how strategic choices can result not only in traditional operational losses but also exposure to significant legal expense and regulatory fines; and quantifying loss experience and forward-looking measures of risk into an appropriate level of capital that can be allocated to business activities for effective decision-making and the pricing of business activities. These are challenging topics, and we may not discover the answers today. But events such as this, which bring together leading practitioners to have honest and thoughtful discussions, are essential to helping answer that question in the same way that information sharing about cyber threats is essential, because working together we are stronger.

Thank you.