Remarks by
Thomas J. Curry
Comptroller of the Currency
Before the
New England Council
Boston, Massachusetts
May 16, 2014

It's a pleasure to be with you back home in Boston. I was here just six weeks ago for a conference we sponsored jointly with Boston University, commemorating the 150th anniversary of the creation of the OCC. We spent the day engaged in discussions of the future of the industry, with a particular focus on how we might avert the types of breakdowns that led to the financial crisis in 2008. As you might imagine, the panel discussions focused on issues like derivatives, mortgage-backed securities and whether some banks might be too big and too complex to be managed. Those are all important concerns, and I suspect some of them would be of interest to this group as well. But I want to spend my time today talking about a different challenge, one that affects virtually every business and every individual in America, and, indeed, the world. That issue is cybersecurity, and I'd like to tell you what we are doing in the bank regulatory community to meet the challenge of cyberattacks.

First, let me say that there are few issues more important to me, to the OCC, and to our country's economic and national security than the risk posed by the increasing sophistication and growing number of cyberattacks. Not so many years ago, hacking was largely the domain of bright amateurs who were mainly interested in exploring data networks or demonstrating their hacking skills to their peers. Today, though, it's the province of an array of terrorists, organized criminals and so-called "hacktivists" intent on doing real harm. These groups have grown into a dangerous assortment of threats capable of launching coordinated attacks from almost anywhere in the world.

Over the years, we have seen a steady increase in malicious activity in the banking sector, from Distributed Denial of Service attacks to account takeovers, ATM cash out schemes, and the attacks on retailers that allowed criminals to steal credit card data and other confidential customer information. If we needed a wake-up call, the holiday data breaches involving Target and Neiman Marcus gave us one. With hundreds of millions of credit cards potentially compromised, people all over the country and from all walks of life suddenly had reason to worry that their financial accounts and information might have been exposed. And banks that may have thought that risks from breaches stopped at the perimeter of their firewalls were reminded that the vulnerabilities of others can damage their business and erode the trust of their customers. As technologies are leveraged in new ways, such as mobile payments, we will almost certainly continue to see cyberattacks evolve with them.

Cyber-threats to our banks and to public confidence are a special concern for me as a banking regulator. We're long past the time when retail payments were made with cash through face-to-face transactions inside a bank branch or with paper checks that cashiers verified by checking a driver's license. Instead, we now live in a world where consumers use their cellphones to deposit checks, pay bills over the Internet, and make purchases at the mall by swiping a credit card or flashing a smartphone app. For most consumers, those payment mechanisms are a routine part of their life, and they probably don't give much thought to what goes on behind the scenes to provide security for payment and settlement systems.

In fact, quite a lot is going on behind the scenes. The national banks and federal savings associations supervised by the OCC are devoting enormous amounts of time and resources to address cyber threats. Our large banks in particular have stepped up spending on people and systems. But they are being challenged every day by threats that keep coming, in ever more pernicious form.

In part, that's because banks are increasingly interconnected, not only to each other but also to their customers, their suppliers, and to other critical infrastructures. The third parties banks increasingly rely upon to support their systems and business activities often have further connections to other institutions and servicers. Each new relationship and every new connection provides potential access points to all of the connected networks, any one of which can provide access to the system. These interconnected networks are potentially vulnerable to attacks that may affect multiple organizations at one time. Moreover, while banks have generally done a good job of thwarting the attacks on their own systems, they have no direct control over the systems used by third parties.

As regulators, we have long been concerned about the relationships between banks and third parties, and not just because of cyber threats. We've unfortunately found it necessary to take enforcement actions against some of our large institutions for problems brought on by poorly-managed third-party relationships, from debt collection companies to telemarketers. Most recently, banking regulators took enforcement action against a technology service provider for deficiencies that prevented it from restoring service to banks in the aftermath of Superstorm Sandy.

That episode illustrates one of our major concerns about banks' involvement with third parties: the extent to which service providers are consolidating and leaving more financial institutions dependent upon a single vendor. As a result, deficiencies at one vendor have the potential to affect a large number of banks simultaneously.

A second, and related, trend that concerns us is the increased reliance by banks on foreign vendors, including foreign-based subcontractors, to support critical activities. The reliance on foreign vendors presents special challenges. Banks need to consider the legal and regulatory implications of where their data is stored or transmitted, and make sure that their interests and those of their customers are protected.

Perhaps most importantly, we are concerned about third-party access to sensitive bank or customer data. For an industry in which reputation means everything, a single data breach involving confidential customer information can be extremely costly. Banks are particularly vulnerable to events that erode trust. Once an institution's reputation is damaged, it can take years to repair.

All of these risks are manageable. But they must be managed. What concerns me most is that risk management practices haven't always kept pace with the risks institutions take on. Some banks that historically have been regarded as well-managed have found themselves in trouble because they underestimated the risk in third-party relationships and didn't have the right controls and oversight in place. As a result, they faced credit losses, compliance problems, litigation exposure, and damage to their reputations.

Recognizing the importance of managing third-party relationships, the OCC issued updated guidance last October that focuses on risk management practices for critical activities throughout the lifecycle of the third-party relationship. It also stresses the important role of the board of directors and management in overseeing these activities. We expect the board and management to ensure that risks are identified and well understood, that appropriate risk management practices are in place, that clear accountability for day-to-day management of these relationships is established, and that independent reviews of these relationships are conducted periodically.

Third-party vendors are especially important to community banks, many of which outsource their back-office operations to technology service providers and which often don't have the resources that our largest institutions can devote to cybersecurity. And while the largest institutions might be the most tempting targets for the bad guys, what we've learned from other sectors and are now seeing in the financial sector is that as the larger financial institutions improve their defenses, hackers are likely to direct more of their attention to community banks.

We at the OCC and the other banking agencies are doing everything possible to support our smaller banks and thrifts in this area. We've arranged briefings for banks, held webinars, and provided support through the supervisory process.

In addition, we've utilized the Federal Financial Institutions Examination Council, or FFIEC, which brings together all of the banking agencies at the federal and state level, to raise public awareness about cyber-threats and to promote information-sharing on cybersecurity among banks. As its current chairman, I asked the FFIEC to create a working group on cybersecurity issues. That group is up and running, and it's already having an impact on how we do business. The group has met with intelligence, law enforcement and homeland security to share information, and it's exploring additional action we can take to help banks of all sizes shore up their defenses.

We also worked through the FFIEC to get out an alert on the OpenSSL vulnerability, which you probably know as the Heartbleed bug. While this vulnerability received widespread media coverage, we wanted to get specific information out to the industry, and the FFIEC alert was the result. By the way, if you'll permit me to pause momentarily for a public service announcement, I hope each of you took the news about Heartbleed as an occasion to change the passwords on your social media and email accounts after being notified that a patch for this vulnerability had been installed. In fact, changing passwords regularly and using complex passwords that don't build on common words or the names of your family is one of the steps that every person can take to keep their personal information secure, and I would encourage you to devote some time and energy to this practice.

Let me close by emphasizing the importance of collaboration in meeting the cybersecurity challenge. This isn't a problem that any one agency or institution can solve on its own. To deal effectively with cyber threats, institutions both large and small need to communicate, not only with each other but also with relevant government agencies. Fortunately, some excellent mechanisms are in place to facilitate information-sharing.

For example, the Financial Services Information Sharing and Analysis Center, which includes the OCC and other public sector agencies as members, is an information-sharing non-profit organization run by financial institutions. Another body, the Financial Services Sector Coordinating Council, brings together private sector firms and trade associations across banking, financial markets, and insurance. These organizations meet regularly with the regulators to discuss emerging issues and best practices and to support cooperative efforts to deal with critical infrastructure issues facing the financial sector.

Sharing best practices, techniques and strategies, and collective responses to wide-scale events helps banks focus their resources on the most significant areas of concern. In an increasingly interconnected economy, information-sharing is vital, and not only for banks. The more we work together, the stronger and safer we all become.

In my time as Comptroller of the Currency, I have tried to emphasize the importance of collaboration and cooperation in all aspects of our mission. Nowhere is collaboration more important than in the realm of cybersecurity, where the threat transcends agency jurisdictions and industry boundaries. We can succeed in safeguarding our data networks and our economic security, but only if all of us work together in a collegial and collaborative way for the good of our country.

Thank you for giving me this time today. I'd be happy now to take some of your questions.