U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks by Deputy Secretary Sarah Bloom Raskin at the American Bankers Association Summer Leadership Meeting

7/14/2015

As prepared for delivery

I. Introduction

Good morning. Thank you John for that kind introduction, and thanks for inviting me to speak at your Summer Leadership meeting in this irresistible city which occupies a special place in my heart. As John noted, I have had a number of jobs since I was Maryland's Commissioner of Financial Regulation, but nothing compares to being Maryland's banking commissioner right here in Charm City. Hollywood has worked hard to capture the feel of this place in shows like Homicide, The Wire, and House of Cards, but the magic of Baltimore will not be truly visible until someone makes a series about the Commissioner of Financial Regulation and the vivid and never-boring people—I was going to say characters—who run the banks from Easton to Baltimore to Chevy Chase that keep the wheels of commerce turning in the Free State.

I understand the purpose of this meeting is for you as banking industry leaders to think strategically about the future of banking. This future is intertwined with e-commerce and e-banking, so I want to focus on an issue that I have made a priority at the U.S. Treasury, and that is cybersecurity and cyber-resiliency as applied to banks and other entities in the financial sector.

Now, I state the obvious when I point out that the Internet and the gadgets we use to access it—personal computers, smart phones, and other devices—provide us with unprecedented connection to one another and the world. Think about this: in 2003, half a billion devices were connected to the Internet. By 2010, while the world's population had increased by about 8 percent, the number of devices connected to the Internet increased to 12.5 billion. (By the way, I'm convinced that most of them are in my household being used by my children.) By some estimates, in five years, 50 billion devices will be connected to the Internet.

This growth is profound and the access provided is immense. Our cultural and economic lives are increasingly propelled by the Internet. This is how the American people communicate with one another and engage in commerce, and this is where a vast amount of personal data is shared. This is also how the financial sector does business and how your banks interact with clients and customers. Modern society is dependent on digital networks, and this dependence offers not only unprecedented opportunities for universal education and networked human progress but unprecedented opportunities for cyber-mischief, cyber-vandalism, cyber-theft, cyber-sabotage, cyber-subversion, cyber-chaos, cyber-collapse, and cyber-warfare.

Cyber-attacks can be uniquely devastating for several reasons. In the first place, cyber-intrusions are intangible, inscrutable and often untraceable. Victims may not be aware that they have been targeted until months or years later. And the location of the breach on a network can take a very long time to determine. Cyber-attacks also threaten systemic exposure by invading and contaminating our vast interlocking digital network connections. Moreover, the purveyors of cyber-attacks have proven themselves to be devious, nimble, and relentless.

II. What a Difference Six Months Makes

So how do we promote cybersecurity in the new age of cyber-anxiety? Well, not to quote myself, but let me take us back six months: in early December of last year I spoke in Austin, Texas to a group of your colleagues at the Executive Leadership Cybersecurity Conference sponsored by the Texas Bankers' Association. Back then I shared a checklist of ten questions on cybersecurity for banks—covering three topics: (1) baseline protections, (2) information sharing, and (3) response and recovery. I recommended that CEOs and bank boards ask each of ten questions to better understand where their institutions stood in addressing their cybersecurity and cyber resiliency. My idea was, that armed with answers to those basic questions and diligent oversight of any needed follow-up, bank executives could help move the needle on their institutions' cybersecurity posture.

A lot has happened since then. Cyberattacks—and the harm caused by successful intrusions—have not abated but are rather drawing more intense public focus. A nation-state launched a destructive attack against Sony Entertainment Pictures, destroying systems and data, devaluing intellectual property by posting unreleased movies to the Internet, and embarrassing company executives by publicly releasing highly sensitive private information and communications.

Then, some of our nation's most prominent health insurers—Anthem, Premera, and CareFirst—were targets of attacks that stole their members' personal information. In addition to names, birthdates, and street and email addresses, in some cases the stolen information contained medical identification numbers, social security numbers, and employment data such as income. Experts characterized the breaches as especially worrisome because of the high black market value placed on private health data as tools for extortion, fraud, and identity theft.

And just last month, and again last week, the Office of Personnel Management in Washington announced a series of cybersecurity incidents and vulnerabilities affecting its systems and data that exposed sensitive information contained in personnel records and security-clearance files of millions of current and former federal employees and contractors.

While the sophistication and peril of cyber-assaults have escalated, the good news is that both the government and society are beginning to address the threat with a serious investment of resources, creativity, and energy. We see the paradigm shifting in our struggle against cyber attacks in increased budgets, staffing, and planning. On a smaller scale I read an article earlier this summer about 250 middle-school Girl Scouts who attended a week-long cybersecurity and computer camp at Cal State San Bernardino. Under the guidance of cybersecurity engineers and instructors from Google, Facebook, and the Department of Homeland Security, the girls flew and learned how to down drones, and then used the same software programs to ward off hacking attacks. (Don't you just love this?) That program was one of more than three dozen jointly sponsored this summer by the National Science Foundation and National Security Agency. We are starting our girls young on the technology to cultivate the next cadre of skilled cybersecurity professionals.

The profoundly positive cultural change I want to remark upon is that cybersecurity and cyber resiliency have moved from the exclusive purview of IT professionals. It has progressed into executive suites and boardrooms, as well as into the classroom, summer camps, and, the Girl Scouts. We are often comfortable using the saying that we're not dealing with our parents' financial system or risk landscape anymore; but frankly, we are not even dealing with our children's cyberspace given the current rate of change in the cyber sphere. This is why executives and boards are increasingly focused on cyber-related threats, and risk committees are being tasked with overseeing cybersecurity and reviewing cyber-related strategies and spending.

So: in the spirit of better arming bank leaders for overseeing cybersecurity at their institutions, today I'd like to suggest ten follow-up questions—a sort of 2.0 for the ten questions I posed to the Texas Bankers' Association—that dive deeper into the topics I presented in December. These ten additional questions reflect what we have learned in the last six months from our cyber experiences and expand on the initial steps banks can take to enhance cyber resiliency; what I want to do for you today is add greater depth and detail to the 1.0 checklist. We'll think of the Texas speech as the introductory course and prerequisite for this, the intermediate course.

III. Follow-Up Questions

Here we go: last fall when discussing baseline protections, my checklist began by calling on CEOs to ask whether cyber risk was part of their banks' risk management framework. To probe deeper on exactly how cyber risk fits into your bank's control and governance infrastructure, question one today asks: Does our bank embed cybersecurity into our governance, control, and risk management systems?

Why is embedding cybersecurity into governance, control, and risk systems so important? Instead of making cybersecurity one of many perils that risk management systems at banks must monitor, manage, and mitigate, embedding cybersecurity into your business processes and activities, your control structures, and most importantly into your cultures can measurably increase the cybersecurity posture of institutions. Instead of grafting controls on top of existing infrastructure and processes and hoping they take, cybersecurity must be part of a bank's DNA.

To excel—really succeed—cybersecurity must become one of the fundamental building blocks of a bank's processes and activities so that security cannot be circumvented, removed, or defeated. Such an approach—much like establishing a culture of compliance or risk management—creates multiple levels of defense and redundancy so that a bank's cybersecurity is indelibly ingrained in its businesses, operations, and culture.

This is not simply a matter of technology; it's a matter of perspective.

To better determine whether your bank has embedded cybersecurity into its governance and control infrastructure, you need to ask follow-up questions on how the embedding was done, which leads to question two: Have we remained vigilant about systematically identifying our key assets, that is, those that provide high-value targets for malicious cyber actors?

One of the first steps in embedding cybersecurity into your bank's risk management framework is identifying your organization's crown jewels—the networks, systems, data, and other assets—that malicious cyber actors may try to exploit. Depending on your bank's specific business, key assets could include e-banking networks, the disruption of which could stop customers from initiating transactions. Key assets could also include your customers' personally identifiable information stored on your systems which, if exposed, violates privacy laws or expectations and could lead to substantial reputational harm to your bank.

But identifying high-value assets is just the first step, bringing us to question three: Have we tailored our security controls to the specific cyber risks presented by each key network, system, or set of sensitive data?

Once high-value assets are identified, banks need to determine the appropriate way to protect those assets. Remember: here, one-size does not fit all. Any solution should be necessary and appropriate, and most importantly, effective given the bank's particular business and regulatory environment. Depending on the asset, some thoughtful combination of technology, processes, and people will likely be needed.

If your key assets are networks and systems, new technology and security tools may address identified risk. But much like putting a fresh coat of paint on a house with a crumbling foundation, don't invest in purported technology solutions by rote before assessing the security of your bank's underlying network architecture. To be effective, banks should first remedy any architectural design flaws, and only then deploy new cybersecurity technology and tools.

For key assets like customers' personally identifiable information and other sensitive information from clients, banks might decide to segregate and add enhanced security around that information. The extra security could mean encrypting sensitive data throughout its lifecycle, not only when that sensitive data is in transit but when it is at rest. It could also mean taking data off line—effectively putting it in cold storage—or implementing a policy to only request and maintain sensitive information that the bank absolutely needs from a business or regulatory perspective. This would include maintaining information only for the time required to conduct business, perform operations, and meet regulatory obligations, and then responsibly disposing of the data. In fact, some predict that in the not so distant future centralizing and hoarding customer data will become a liability rather than the perceived asset it is today.

After identifying high-value assets and tailoring specific controls to address particular cyber risks presented to those assets, we come to question four: How do we prioritize the implementing of enhanced controls around key networks, systems, and sensitive data?

Why is the answer to this question so important? Because the reality for most banks is that resources are not limitless. Therefore, the most effective banks systemically prioritize their cybersecurity controls so that the most significant exposures are addressed first, with the remaining exposures tackled in an order that considers factors like importance, degree of difficulty, and cost. The National Institute of Standards and Technology's cybersecurity framework, or the NIST Framework, can help organizations set their priorities. This framework provides a risk-based approach for organizations to assess their cyber posture and determine their risk profile and tolerance. This type of information proves invaluable when prioritizing which cyber defenses to solidify.

On a related note, as many of you may have heard, the Federal Financial Institutions Examination Council (FFIEC) recently rolled out a cybersecurity assessment tool, which is designed to complement the NIST framework. This tool can help banks better inform their cybersecurity controls and priorities. It was conceived to provide banks with a replicable and measurable process for assessing cyber risk levels along with the maturity of their related risk management processes. As such, question five emphasizes the value of the FFIEC tool and asks: Have we reviewed the FFIEC Cybersecurity Assessment Tool and appropriately incorporated it into our approach to cyber risk management?

The next two questions focus on how people themselves can help embed cybersecurity into governance, control, and risk management systems. Question six asks: Have we designated specific professionals to be responsible for our cybersecurity strategy and provided them with the authority, resources, and access they need to effectively perform their work?

Designating specific individuals responsible for a bank's overall cybersecurity strategy is important because it establishes responsibility and accountability. A bank's organizational structure will dictate which individuals and teams to designate. And, while a bank's IT team will play a crucial role for key parts of the strategy, your business, operational, risk, HR, and legal teams may play an equally important role depending on your structure.

The specified individuals should be given the authority and resources that they need to drive the cybersecurity strategy forward. Those individuals must also have access to executive management—and the board when necessary—so that the bank's senior leadership can effectively oversee the implementation and execution of the strategy.

This leads to question seven: Have we trained our personnel on our cybersecurity policies? Probably more important than any single technology or process improvement, banks should instill a culture of cybersecurity in their workforce, whether employees or contractors, directors or officers. This is because from what we see, people are the weakest link to cybersecurity.

Given the prevalence of phishing and other social engineering techniques—where hackers trick individuals into divulging their usernames and passwords or installing malicious software—the difference between success and failure increasingly depends on whether someone in your organization thinks about cybersecurity when deciding whether to click on an email attachment or hyperlink. It cannot be overstated how important it is for a bank's personnel to protect their usernames, passwords, and other credentials that provide system access. By using stolen or misappropriated credentials to impersonate others, hackers can circumvent firewalls and other technology protecting the perimeter of your networks and systems. Once in, if networks and systems are not appropriately segmented, hackers may have unfettered access. This is why education and training—what I've been calling cyber literacy—is vital.

The most effective cybersecurity training not only reviews a bank's cybersecurity policies but also explains the reasons behind the policies using real-life scenarios that resonate with people. The more tailored that training is to a person's actual duties, and risks posed by those duties, the better. Ultimately, cybersecurity education should instill a healthy dose of on-line skepticism and, when done right, turns people from an organization's weakest link into its strongest defense.

Switching gears, the next two questions relate to cyber risk insurance. We've been watching the evolution of the market for cyber risk insurance. Question eight asks: How do we ensure that our insurance coverage matches our cyber-related risks?

To date, no standard policy or terms exists. Standalone policies, however, typically protect against technology and data breaches and cover related liability and damages. The policies may also cover business interruption losses and incident response in the aftermath of an intrusion, such as the hiring of lawyers, consultants, and public relation firms, providing credit monitoring, and establishing call centers. But typically standalone cyber insurance policies do not cover bodily injury or property damage from a cyberattack. Ask yourself what the range of losses you may face could be; and seek out coverage for them.

But even when cyber insurance coverage matches a bank's cyber risk, proposed exclusions in the policy must be carefully scrutinized, which brings us to question nine: Does our cyber risk insurance impose "minimum required practices," which may lead to denial of coverage if not followed?

Some cyber insurance policies have "minimum required practices" exclusions. These exclusions require a policyholder to maintain the cybersecurity procedures and controls identified in its application as a condition for coverage. These exclusions policies are typically negotiable, but you have to know what practices you can and cannot adhere to before the policy is issued. If a bank's cyber insurance policy has this type of exclusion, the cybersecurity controls identified in the application process need to be appropriately maintained.

In other words: when it comes to cyber risk, banks should understand the coverage afforded by, and excluded from, the entirety of their insurance program, including the conditions and exclusions of their cyber risk insurance policy.

Now, my last recommended question for CEOs and boards to ask relates to basic cyber hygiene, those fundamental practices that bolster the security and resilience of networks and systems. I've saved this question for last, not because it is the least important, but because it may be the most important of the ten given that engaging in basic cyber hygiene may prevent 80 percent of all known incidents.

In my initial checklist I called for bank executives to ask whether their institutions engage in basic cyber hygiene. To elaborate, question ten urges you to ask about four specific forms. As part of cyber hygiene: (1) Do we require multi-step identity checks—known as "multi-factor authentication"—before allowing access to our networks, systems, and data? (2) Have we restricted special, high-level access to only those who need it? (3) Are we doing regular maintenance and consistently patching our software? (4) And are we effectively scanning our systems for malicious activity?

Last month, the federal government launched a 30-day cybersecurity sprint to accelerate progress being made to enhance its cybersecurity. Each of these four basic steps—increasing multi-factor authentication, limiting high-level system access, patching, and scanning for vulnerabilities—are part of that sprint. In the aftermath of the large-scale cyber incidents, we have learned that taking one or more of these four steps would have made a real difference in limiting the scope of, and damage caused by, cyber incidents.

Why is multi-factor identification so important? Usernames and passwords are too easy to guess or steal. To verify the identity of a user, multi-factor authentication typically combines something the user knows (like a password) with something only the user should have (like a smart card or phone).

Users with special, high-level access, known as "privileged users," are typically your IT professionals with administrative rights to do things like install software, configure systems, and grant access to other users. Privileged users usually also have access to data and services that run on the systems they manage. Given potential threats posed by the access and rights afforded privileged users, banks should consider tightening controls around these individuals. Such controls may include limiting the number of privileged users to only those absolutely necessary to run your business, operations, and systems. Controls may also restrict the systems that privileged users can access and functions they can perform, may restrict the length of time they can be logged in, and could impose regular reviews of access logs.

As to patching software, we know that the vast majority of cyber intrusions that take advantage of system weaknesses can be found and fixed. Yet we also know that malicious cyber actors are aware of these vulnerabilities, meaning vulnerabilities need to be addressed swiftly so they aren't exploited. This is why patching should occur on a regular and systematic basis.

Finally, scan your systems using indicators—such as rogue IP addresses or malware hashes—which are virtual fingerprints that can help find intruders in your systems. This is critical because we know that malicious cyber actors often use the same or similar methods to target multiple institutions. Private security firms, the Department of Homeland Security, and the Financial Services Information Sharing and Analysis Center all disseminate these indicators and other useful cybersecurity information. I urge you to use these resources to better protect your systems.

IV. Conclusion

There you have it: Cybersecurity 2.0. I'll end with this observation: cyber risk and the challenges posed by cybersecurity seem daunting and insurmountable. If only there were a simple, single solution. Perhaps one day we will see such a single solution emerge. But for now, we are where we are. Fortunately, I'm reminded that extraordinary things can, and often do, happen through perseverance, in small, consistent increments. As the American soldier Creighton Abrams more colorfully analogized: "When eating an elephant, take one bite at a time."

We are confronting this challenge the only way we can, and that is one step at a time—from our work in the government and in financial institutions of all sizes, to, for the next generation, cybersecurity camps and tech savvy Girl Scout troops. Fundamentally, I'm optimistic that in the face of enormous challenges, confronting the barriers to improved cybersecurity and resilience is a significant opportunity because the space to improve is still vast, and within such space we can do extraordinary things.

Thank you.

###