U.S. DEPARTMENT OF THE TREASURY

**Press Center**

# Remarks of Deputy Secretary Raskin at The Texas Bankers' Association Executive Leadership Cybersecurity Conference

12/3/2014

***Cybersecurity for Banks: 10 Questions for Executives and their Boards***

***As prepared for delivery***

**AUSTIN, TEXAS** - Thank you Commissioner Cooper, for your introduction, and for inviting me to speak on a topic that is with us now and that is going to remain with us for quite some time. The cyber threat is vast, and it relates to a vast number of topics -- everything from our country's national security and diplomatic relations to consumer protection and technological innovation. Cyber-incidents are not just increasing in number, but the types of incidents and the means for intrusion are growing at the same time.

We have seen this evolving threat play out in recent attacks against Target, Home Depot, and JPMorgan Chase, which, in the JPMorgan Chase case, resulted in hackers stealing the names and contact information of 83 million customers. We have learned from these attacks, that the prevalence of cyber risk creates a persistent and complex challenge for financial institutions spanning the sector, including financial institutions of all types and all sizes. We also know that for the American public, cyber risk can be not only confusing, but also potentially overwhelming.

This is why enhancing the nation's cybersecurity is a top policy priority for the President and the Treasury Department. Because the cyber threat transcends financial institution borders, and permeates all business sectors, the President has established a unified approach to strengthen and maintain critical infrastructure against cyber threats in 16 sectors, ranging from transportation and energy to communications and healthcare and financial services.[1]

For the financial services sector, Treasury serves as the day-to-day federal interface and coordinating agency with the Department of Homeland Security and other relevant federal agencies—including the regulatory, law enforcement, and intelligence communities. Treasury also collaborates with industry and state government agencies. Secretary Lew and I lead this effort for Treasury. Our ultimate goal is to instill confidence and show that the government—working in appropriate collaboration with the private sector—is defending the American public from damage caused by cyber attacks.

This is a tall task because there are many facets of what is necessary to reduce the threat and effect of cyber incidents. But today, I am focusing on just one area of this task: the cybersecurity of our nation's banks.

It is extraordinarily inspiring to see you all here gathered on this topic. You are smart to have come. Once again, we see here where cutting edge thought and innovation occur. In fact, several years ago, leadership in both government and industry in Texas recognized the importance of the cyber threat. Through a cooperative effort among the Texas Bankers Association, the Independent Bankers of Texas, Commissioner Cooper, and his impressive team at the Texas Department of Banking, timely and critical first steps have been taken by Texas to protect the financial system.

I was serving as Commissioner of Financial Regulation in Maryland in the spring of 2010 when the Texas Bankers launched the initial Electronic Crimes Task Force and led early work on corporate account takeovers.[2] The Conference of State Bank Supervisors organized a call with members, and Commissioner Cooper explained what Texas banks were experiencing. Within days of hearing Commissioner Cooper explain the problem, a Maryland bank reported to me that it had just been targeted in exactly the same fashion.

That nimbleness continues today through initiatives like the CSBS's Executive Leadership of Cybersecurity Initiative and the Multi-State Information Sharing and Analysis Center. These projects are a collaborative effort among many state entities, and from them we have learned the importance of tailoring and raising the cyber-threat message to the CEO. Understanding and dealing with the cyber threat has, due to your efforts, seeped from the IT shop and into the CEO shop. Responsibility is now shared. In fact, this new shared responsibility, among IT experts, the CEO, and the board of directors, has been the most noticeable trend in governance from my time in the industry, in state government, and in the federal government. Bankers rarely used to talk to me much about cybersecurity. Now, this is one topic that comes up every day.

With that recognition, I have sifted through the questions I've been hearing from bank CEOs in my conversations with them about cybersecurity and realized that it would be helpful to arm CEOs with a simple checklist of questions that could provide concrete steps that your banks can take—a roadmap of sorts—before an attack occurs. By asking these questions, obtaining the answers, and performing necessary follow-up, you can ensure more rapid detection, diagnosis, response, and recovery should a breach occur at your banks.

**THE GROWING CYBER THREAT**

Before launching into these 10 questions, let me underscore, again, the pervasiveness and the vastness of the cyber threat. Earlier this fall the accounting and consulting firm PricewaterhouseCoopers released the results of its annual global information security survey of corporate executives. That survey, which included 9,700 participants, reported almost 43 million ***detected*** cybersecurity incidents during the past year, a 48 percent increase over 2013.[3]

As to the average loss attributed to cybersecurity incidents, or the annual cost of cybercrime to the U.S. and the global economy, the estimates vary dramatically. [4] But what we can be sure of is that the financial costs are real and increasing; they stem from the disruption of business, erosion of customers, and the associated loss of revenue, from expenses incurred to secure systems, and appropriately notify customers. The non-financial costs include: reputational damage and loss of confidence, the competitive costs associated with the vast and monumental theft of intellectual property, and the loss of sensitive or confidential personal and business information.

Yet despite these potential costs, expenses, and losses, effectively focusing attention on cybersecurity remains a challenge. Part of the challenge is that cybersecurity is too often described in language only relevant to technical experts and is too often left in the hands of technology professionals without the watchful oversight of senior executives and boards.

It strikes me that when we think about cybersecurity we are still thinking that we have to communicate in ways that are obtuse, overly technical, and impossible to penetrate or understand without cyber experts in the room. Again, as my conversations with bank CEOs reflect, we need to recognize that cyber risk, like other potentially material operational risk, is something we already understand and already have the framework to understand, and it is a topic that falls squarely within the governance and oversight responsibilities of executive leaders and boards.

**10 QUESTIONS ON HOW TO RESPOND**

And so, to organize this work, at Treasury we have framed our thinking about cybersecurity and financial industry preparedness against cyber-attacks around three categories of activities: (1) baseline protections, (2) information sharing, and (3) response and recovery. These categories help us organize cybersecurity initiatives on a national level; the categories also help to topically organize the ten concrete questions your banks should ask.

**I. Baseline Protection**

The first set of questions to ask relates to a bank's baseline protections. A bank's baseline protections are the policies, procedures, and other controls that a bank has adopted to prevent penetration of their networks and systems, and to prevent damage assuming that there has been access.

This brings me to the first set of questions—four in particular—that I recommend you ask. Question one: Is cyber risk part of our current risk management framework? Banks should have risk management frameworks that are appropriately tailored to the cyber risks presented by their specific businesses and operations. Ideally, your cybersecurity risk management is part and parcel of your enterprise risk management framework, key components of which are technology, process, and people.

CEOs and boards of directors should identify the cyber threats presented by their particular activities and operations and match those threats to appropriate technology solutions. Then CEOs and boards should adopt policies, procedures, and other controls—like training and governance—to not only address identified cyber threats that their technology solutions cannot control, but also to reasonably anticipate possible breakdowns and overrides of that technology.

Finally, CEOs and boards should do their best to employ highly qualified people to monitor and continually reassess the effectiveness of the deployed technology and controls, including those technologies or controls which are not directly operated by the institution. When appropriately designed and executed, technology, process, and people form a risk management structure and the necessary first lines of defense against cyber-attacks.

Question two: Do we follow the NIST Cybersecurity Framework? The National Institute of Standards and Technology, or NIST as I have just referred to it, released the *Framework for Improving Critical Infrastructure Cybersecurity* in February.[5] The NIST Cyber Framework is a well-considered approach to strengthening the resilience of critical infrastructure. Banks should use the framework to reduce cybersecurity threats both within the bank and with outside vendors.

The framework is a risk-based approach to managing cybersecurity that can help identify your bank's cyber posture and determine its risk profile and tolerance. Importantly, the framework is not a technical document; it focuses on oversight process for management and governance. For example, it provides advice on how to develop organizational communication plans for responding to attacks, and provides a common language and set of practices, standards, and guidelines. And for organizations that have developed enterprise-risk management approaches, the NIST framework need not replace those approaches; instead the framework can be used to better inform and apply those established risk-management approaches when the risks and associated controls are cyber-related.

The NIST framework also provides firms with a tool to evaluate vendors and other third-parties that have access to their networks, systems, and data; which leads us to question number three: Do we know the cyber risks that our vendors and third-party service providers expose us to, and do we know the rigor of their cybersecurity controls?

Third-party vendors—and any other third parties with access to a firm's networks, systems, and data—can present a significant cybersecurity hazard. As you know, given the nature of modern IT services, many banks do not own or operate their systems for payment services or other back-office processes. This means that personnel with access to your networks, systems, and data may not even be employed by your bank.

As such, it is imperative that you understand the security safeguards that your vendors and other relevant third-parties have in place. At a minimum, this means four things: (1) knowing all vendors and third-parties with access to your systems and data, (2) ensuring that those third parties have appropriate protections to safeguard your systems and data, (3) conducting ongoing monitoring to ensure adherence to protections, and (4) documenting protections and related obligations in your contracts.

Question number four: do we have cyber risk insurance? And if we do, what does it cover and exclude? Is our coverage adequate based on our cyber risk exposure? While the cyber insurance market is relatively new, it is growing. More than fifty carriers now offer some type of cyber insurance coverage.

Unlike the past, now *some form* of cyber coverage exists for organizations of all sizes, from small, family-owned shops to Fortune 500 companies. Policyholders can now find coverage to match a broad array of cyber risks, ranging from liability and costs associated with data breaches to business interruption losses and even tangible property damage caused by cyber events.

Cyber insurance cannot protect your institutions from a cyber incident any more than flood insurance can save your house from a storm surge or D&O insurance can prevent a lawsuit. But what cyber risk insurance can do is provide some measure of financial support in case of a data breach or cyber incident. And, significantly, cyber risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls. Qualifying for cyber risk insurance can provide useful information for assessing your bank's risk level and identifying cybersecurity tools and best practices that you may be lacking.

I have been asking our insurance and cyber experts at Treasury to think about how to encourage an environment where market forces create insurance products that enhance cybersecurity for businesses.[6] Ideally, we can imagine the growth of the cyber insurance market as a mechanism that bolsters cyber hygiene for banks across the board.

Which leads us to the fifth question you should ask: do we engage in basic cyber hygiene? Here I am referring to ensuring that your bank engages in fundamental practices to bolster the security and resilience of your networks and systems. What exactly does this mean? Things like: Knowing all the devices connected to your networks. Knowing what is running—or attempting to run—on your networks. Knowing who has administrative permissions to change, bypass, or override system configurations and then reducing that number to only those who need those privileges. And also: patching software on a timely basis, and conducting continuous, automated vulnerability assessments and remediation. The Center for Internet Security, working with others including the Department of Homeland Security, launched the Cyber Hygiene Campaign in April.[7] By some estimates, engaging in basic cyber hygiene will prevent 80 percent of all known attacks.[8] This is the basic "blocking and tackling" that doesn't take a computer wizard to understand.

**II. Information Sharing**

These are five questions to ask about your bank's baseline protections. Now let's move to a second category of questions, namely, information sharing. By information sharing, I'm referring to the sharing of timely, actionable information regarding cyber vulnerabilities, threats, and incidents with a view toward limiting attacks and stopping contagion across systems, networks, and other institutions. We know that the most effective defenses do not happen in isolation. Instead, the banks most sophisticated in cyber defense are those that play an active role in the information-sharing community, which leads us to the sixth question you should be asking at your banks: Do we share incident information with industry groups? If so, when and how does this occur?

When bad actors attack one bank, it is possible—and increasingly likely—that those actors or others will use the same or similar methods to target other institutions. We saw this play out earlier this year during the attack on JP Morgan Chase's systems. That attack was not limited to JP Morgan Chase, but reportedly targeted other institutions as well.

Sharing knowledge of vulnerabilities, threats, and incidents allows banks to benefit from the experience of others. This benefit is more acute today, when banks act as correspondents and comprise an interconnected system; and when an intrusion at one bank may quickly enable an intrusion at another.

As you are likely aware, last month the Federal Financial Institutions Examination Council released observations from a cybersecurity assessment that its members performed last summer at more than 500 community institutions. The purpose of this assessment was to evaluate those institutions' preparedness for mitigating cyber risks.

A key recommendation from that work was that regulated financial institutions should participate in cyber risk information sharing.[9] As the council noted, participating in information-sharing forums "is an important element of a financial institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents."[10]

The primary information-sharing center for the financial services sector is the Financial Services Information Sharing and Analysis Center, known as the FS-ISAC. Treasury has also set up an internal group to partner with the information-sharing center, which is the Financial Service Cyber Intelligence Group. This group is staffed by Treasury employees who scour law enforcement and intelligence reports to find relevant information unavailable elsewhere. That team then provides declassified threat and vulnerability information to the information-sharing center, which disseminates the information to its approximately 4,000 members. The center also disseminates threat alerts received from commercial sources, law enforcement, other members, and government agencies.

**III. Response and Recovery**

We've talked about the questions to ask about your banks' baseline protections, and the questions to ask about how you share data. The third and final category of questions relates to response and recovery. Given the sheer number and continual morphing of assaults, we know that a goal of avoiding every attack is currently "pie-in-the-sky," so instead we have to increasingly focus our efforts on making response and recovery more efficient, effective, and predictable.

In this regard, the Treasury coordinates with homeland security, law enforcement, financial regulators, and relevant financial institutions. This work informs the development of the last four recommended questions in my set of ten. They are devoted to response and recovery following cyber incidents.

Question number seven sets the stage for response and recovery. I urge you to ask: do we have a cyber-incident playbook and who is the point person for managing response and recovery? Whether it is a stand-alone document or part of a larger business continuity and disaster recovery plan, your bank should consider having a detailed, documented plan that designates who is responsible for leading the response-and-recovery efforts; and that individual, as well as the entire organization, should know his or her authority. The person you choose to lead this effort should have exceptional organizational and communication skills because he or she will quarterback internal and external interactions.

Which leads us to question eight, relating to what happens as part of the response during a cyber incident. Question eight: What roles do senior leaders and the board play in managing and overseeing the cyber incident response? The CEO and the board have to understand what their respective roles will be in the event of a significant cyber incident at the bank or in an adjacent sector such as energy or telecommunications that might significantly affect the bank. This means clearly understanding when and which matters get escalated to the CEO. It also means understanding whether the full board or a committee—like risk or audit—is initially tasked to oversee the response from a governance perspective. Attacks can create confusion and fear, but the damage can be vastly minimized if leaders clearly understand their roles in response and attack mitigation.

To practice those roles, it makes sense for banks to participate in cyber exercises that simulate a cyber intrusion. These exercises allow CEOs, directors, and other key players to figure out how they will navigate the pressures and problems that come from the intrusion.

The Treasury is developing an exercise regime designed to test communication and decision-making during cyber incidents, an effort that will involve institutions from across the financial sector as well as departments and agencies throughout government. Likewise many trade associations regularly organize cybersecurity exercises, like the one scheduled for this afternoon. Think of these exercises as complicated fire drills; proactive engagement with regulators and law enforcement through these exercises helps to better prepare your banks for actual attacks.

Question nine covers another essential aspect of responding to cyber incidents: when and how do we engage with law enforcement after a breach? It is important to remember that most cybersecurity breaches are crimes, some of which are crimes in progress. As such, your cyber-incident playbook should contemplate when, based on the data gathered, you should reach out to law enforcement. Because many of you may not have had reason to reach out to federal law enforcement agencies who specialize in cyber-crimes, we recommend that financial institution leaders—at banks of all sizes—cultivate relationships with local U.S. Secret Service and FBI field offices. These teams are spread out across the country, and have personnel dedicated to cybersecurity. This relationship-building should start now if it hasn't already, before a cyber event is unfolding. If you need help making those connections, our team will facilitate those introductions.

Finally, I don't have to tell you that community and regional banks are crucial to the communities they support. Your presence and stature in your communities instills a confidence in our financial structure on which our country's macroeconomic stability depends. This is why the tenth question you should ask at your banks is this: after a cyber incident, when and how do we inform our customers, investors, and the general public? Transparency is key. To instill trust and confidence, the messages you communicate should avoid technical jargon and legalese and provide clear and consistent information. In addition, for those organizations that are public companies, you will have additional considerations regarding the timing and content of your disclosure if the breach is considered material information. These are some reasons why having draft messages for various scenarios is an important part of your bank's playbook, given the possibility that events may be serious and fast-moving.

**CONCLUSION**

Now, though these recommendations have inadvertently taken the form of a David Letterman countdown (but without the humor!), your work of course won't end with a punch line or after simply asking yourselves and your institutions these ten questions. Maintaining preparedness and cyber hygiene requires constant vigilance, even after cyber risks and controls become embedded in your bank's enterprise risk management framework. Cyber threats are constantly evolving, and so too must our vigilance and safeguarding efforts.

The entire financial sector—organizations of all sizes and leaders at all levels—should take initiative across the board in cybersecurity, and I commend your Association's leadership in this area to date.

That spirit of cooperation extends to the federal level and I want to extend my thanks to Commissioner Cooper and also to Phillip Hinkle for their efforts. We are pleased to have Phillip serving on the Financial and Banking Information Infrastructure Committee, a committee of regulators focused on cyber, and to have him chair an important working group.

As a former state commissioner, I remain impressed by how the states model the very best in nimbleness and collaboration; and as Deputy Secretary, I am glad to have you as a partner. I hope what I highlighted today serves both as motivation and as a guidepost for your continued role in strengthening your firms, customers, and communities against cyber threats. I wish you all a successful and productive conference. Thank you.

###

[1] This was done pursuant to Executive Order 13636 and Presidential Policy Directive 21.

[2] *See e.g.* Texas Bankers Electronic Crimes Task Force, *What is Corporate Account Takeovers?* at http://www.ectf.dod.texas.gover/aboutcato.htm; American Bankers Association, *The Small Business Guide to Corporate Account Takeover* at http://www.aba.com/Tools/Function/fraud/pages /coporateaccounttakeoversmallbusiness.aspx (a corporate account takeover is a type of fraud where criminals obtain control of a business's bank account by stealing passwords and other validation credentials and then use those credentials to make unauthorized transactions, including, for example, initiating fraudulent wire and ACH transactions into accounts controlled by the criminals).

[3] PwC, *Managing Cyber Risk in an Interconnected World: Key Finding from The Global State of Information Security Survey 2015,* at 7 (Sept. 30, 2014).

[4] *See id.* at 10 (survey reported average loss attributed to cybersecurity incidents at $2.7 million—a 34 percent increase from 2013—but noted a 92 percent increase in entities reporting losses of $20 million or more); Ponemon Institute, *2014 Cost of Cyber Crime Study: United States*, at 3 (Oct. 2014) (noting that financial loss from cyber attacks in the U.S. at surveyed organizations ranged from $1.6 million to $61 million annually per company); Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (June 2014) (study estimated annual cost of cybercrime to the global economy as likely to exceed $400 billion, and could range from $375 billion to $575 billion).

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[6] On Nov. 20, 2014, the U.S. Department of the Treasury held a Cyber Risk Insurance Roundtable.

[7] Press Release, *The Center for Internet Security and Council on CyberSecurity Launch a Nationwide Campaign for Basic Cyber Hygiene in Support of NIST Framework Adoption* (Apr. 3, 2014), http://www.counciloncybersecurity.org/press/1-the-center-for-internet-security-and-council-on-cybersecurity-launch-a-nationwide-campaign-for-basic-cyber-hygiene-in-support-of-nist-framework-adoption.

[8] *Id*.

[9] Federal Financial Institutions Examination Council, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*, at 1 (Nov. 4, 2014), https://www.ffiec.gov/cybersecurity.htm.

[10] Federal Financial Institutions Examination Council, *FFIEC Cybersecurity Assessment: General Observations*, (Nov. 2014), http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.