U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks By Deputy Secretary Sarah Bloom Raskin at the Cybersecurity Docket's Incident Response Forum 2016

3/31/2016

As Prepared for Delivery

WASHINGTON - Good morning. Thank you for inviting me to be the first speaker at the inaugural Incident Response Forum of the Cybersecurity Docket. I want to take a moment to underscore the importance of what you are launching here today, and that is to sponsor an event that focuses exclusively on response and recovery in the event of a cyberattack.

The topic at hand is critical to explore. And I'm pleased to be able to set the stage for your forum today, especially as it relates to response and recovery by the financial sector.

So far, the global economy and our financial infrastructure have been spared a cyber attack with far-reaching consequences to our financial system and our nation's economy. To be sure, we are concerned, and we need to prepare for cyber incidents that have such potential impact. But so far, by what I think has been in large part due to extraordinary preparation, coordination, and practice, we have avoided a catastrophe that freezes our financial system, our payment system, or our basic functioning of this critical infrastructure.

Hand in hand with the financial sector, as many of you know, we have discussed creating a cyber-resilient financial structure by focusing on three imperatives: First, we have discussed at length the importance of information sharing, which we emphasize is a necessary shield to attacks coming from the same IP addresses, from the same malware, from the same vectors.[1] When there is broad-based information sharing, in a timely and effective manner, we arm firms with information that permits them to more effectively employ their defenses.

Second, we have discussed—at length—baseline protections.[2] We stay apprised of attack methods and vectors that are actually being deployed and with this forensic analysis, we derive a constantly updated set of baseline protections that we recommend that firms deploy. From the breaches at Sony, JPMorgan Chase, and the federal government's Office of Personnel Management, we derive lessons about the importance of baseline protections such as multi-factor authentication, privileged access and carefully scheduled updates of patches.

The third imperative is the subject of today's conference. Today, under your leadership, we're going to discuss together what we can do once attacked, once intruded upon, once we are forced to perhaps shut down, to respond to the incident and then to recover from it in a way that minimizes both the short-term and long-term costs and damage.

As impossible as it may seem to know how to respond and recover when contemplated in the abstract, we know that there is nothing impossible about it. We can understand what it means to respond and recover, and we can do something. We have been through natural disasters and other physical emergencies; our financial system has had to respond to the likes of 9/11 and Hurricane Sandy. And from these disasters we have taken lessons about national preparedness. We know that the keys to effective response and recovery from physical threats are preparation, coordination, and practice. I offer to you today the argument that the key to effective response and recovery from virtual—or cyber—threats is nearly the same as the keys to effective response and recovery from natural disasters and other physical emergencies: the keys are preparation, coordination, and practice. When done correctly preparation, coordination, and practice together reduce the time that our financial infrastructure is frozen, with the potentially exacerbating and self-reinforcing negative effects regarding contagion and a loss of business, consumer, and market confidence. When done correctly, preparation, coordination, and practice will lead to a more efficient, effective, and sustainable response and recovery by the financial sector.

The variable that we want to minimize is time. The longer we take to respond and recover, the greater the damage to the firm, to the firm's customers, to the entire financial sector, and ultimately and possibly to the nation's economy and the global economy. How to minimize the variable of time, in the age of internet speed, is the challenge of effective response and recovery.

II. The Meaning of Response and Recovery in the Financial Sector

Looked at this way, when time is of the essence, preparation, coordination, and practice become the tools at our disposal. They are the tools we have to reduce response time and enhance nimbleness.

Let me paint a hypothetical scene: A cyber criminal infiltrates a bank using a ransomware payload that freezes files and data, and blocks the bank's ability to access its books and records and other critical business systems. While initially only impacting the individual bank, the interconnectedness of the financial sector—through payment systems or third-party vendors processing transactions, providing cloud-computing services, or operating mobile solutions—leads to actual or perceived contagion throughout the sector. First one by one, then at an accelerated pace, other institutions' files, data, and systems are likewise affected causing a crisis in confidence that one might imagine could threaten the financial stability of the United States and beyond. While this hasn't happened to date from a cyber-attack, the potential costs to our economic and national security could be real and substantial.

III. Recent Interconnected Threats Mean that Response and Recovery Require Coordination

Nothing at this scale has happened to test our skills at response and recovery.

A. DDoS attacks

At what scale have threats occurred and how has our ability to respond and recover been tested? Some of the earliest attention on cyber-attacks in the financial sector has been on large-scale Distributed Denial of Service (or DDoS) attacks. Over a one-and-a half year period ending in May of 2013, these attacks targeted the U.S. financial sector. As described in the indictment announced last week by the Department of Justice, seven Iranian hackers infected thousands of computers with malicious software, creating armies of computer code—or botnets—that they could control upon command. Then the hackers directed the botnets to overwhelm the Internet-accessible servers of approximately 46 financial-sector corporations. Customers were unable to access their online accounts or the websites of affected corporations during the attacks, although no customer data or funds were compromised.

B. Theft and misuse of customer data

DDoS attacks limit access by customers and depositors. Beyond DDoS attacks, we have seen next a series of large-scale intrusions that have gone beyond loss of access. We have seen intrusions that have involved the theft and misuse of customer data. Over the past several years, retailers have had financial information on well over 100 million credit and debit card accounts stolen. Hackers have also infiltrated networks and systems at banks and broker-dealers, stealing email addresses and other account data and later using that information in subsequent stock manipulations. Law firms are targets as well for the confidential information that their clients entrust to them; information such as trade secrets, negotiation strategies for deals, and details on undisclosed mergers and acquisitions.

And theft of consumer data is not limited to the financial sector. Health insurers and governmental agencies are targets as well; the type of information stolen ranges from customer street and email addresses to medical identification and social security numbers to fingerprints and detailed biographical data.

C. Destruction of systems and data

Transcending denials of access and transcending the theft and misuse of customer data, attackers also exploit vulnerabilities that can lead to the destruction of systems and data. North Korea launched a digital attack against Sony Pictures that destroyed company systems and wiped out data after which it took months for the company to recover. Late last year we also had the first known power blackouts resulting from digital attacks.

For several hours, nearly a quarter of a million Ukrainians were plunged into darkness as the result of a synchronized, coordinated multi-pronged cyberattack.[3] The affected utilities said that hackers, working remotely, stole credentials from system operators and entered several of their networks and systems. After extensive reconnaissance, the hackers learned how to cut power on electric distribution equipment by switching breakers, and they installed malware on the systems that operators used to control those breakers.

Then, over a 30-minute period, the hackers flipped the breakers to cut power on the distribution equipment, detonated the malware on the control systems, and flooded a utility's call center with telephone traffic, preventing real customers from reporting outages. Once set off, the malware deleted selected files and rendered inoperable control systems. Without control systems properly functioning, operators could not automatically restart equipment, forcing them to rely on time-consuming manual processes. .

IV. How to Return to Normal Functioning Effectively

In such cases, how do we return to normal functioning? How do we minimize the time for this return? How do we ensure that we are not prematurely returning to normal operations? How do we optimize the timing of this return in the face of incomplete and imperfect information? The government and financial sector have three tools at our collective disposal: preparation, coordination, and practice.

Since I started at Treasury just over two years ago, the government and financial sector have made substantial progress with these three response and recovery tools.

A. How Governments Assist in Response and Recovery

Let's start with the use of these tools by governments. Governments possess unique capabilities regarding preparation, coordination, and practice as tools for responding to cyber incidents. Last month as part of the **national action plan on cybersecurity**, the Administration announced the roll out of a national cyber incident coordination policy.[4]

Intended to be scalable, flexible, and cooperative in approach, a national cyber incident coordination policy is intended to clarify the specific roles, responsibilities, and authorities of government agencies individually and collectively during significant cyber incidents. Such a coordination policy would outline the role of network defenders — like the Department of Homeland Security — in helping to address and remediate vulnerabilities and evaluate and restore systems and services. It would describe what to expect from law enforcement when identifying, pursuing, and taking action against malicious actors; as well as the role of the intelligence community in analyzing threat trends to facilitate degrading or mitigating adversary capabilities.

It would set forth expectations for private institutions as well as the entities — such as Internet and technology service providers — and the advisers that support them.

In short, once adopted, such a coordination policy will enable government agencies and the private sector to better understand what to anticipate from each other and one another. It will be a tool for more effective coordination and efficient responses during a significant cyber incident; having it in place will be a mechanism to reduce the time it takes to restore normal operations.

B. Treasury's Role in Response and Recovery

Obviously, this national cyber incident coordination policy will be only one tool. The Department of the Treasury also assists the financial sector in their attempts to reduce response and recovery times.

Treasury serves as the day-to-day federal interface and coordinating agency for cybersecurity in the financial services industry. We are the hub of the wheel, providing know-how on the financial services sector, its operations and interconnectedness, and its cyber-related risks to the homeland security, law enforcement, and intelligence communities.

These coordination efforts include providing expert Treasury personnel to help identify, pursue, and take action against malicious actors around the globe through the FBI-led National Cyber Investigative Joint Task Force. We also help staff DHS's 24-7 cyber situational awareness and incident management center, the National Cybersecurity and Communications Integration Center. By providing financial-sector knowledge to this center, we are helping others better understand how attackers could exploit structural and other vulnerabilities at financial firms to create contagion within the U.S. financial system.

We also work extensively with federal and state financial and banking regulators directly and as the chair of the *Financial and Banking Information Infrastructure Committee. Here, too, we are driving* to enhance incident response preparation and coordination.

During a significant cyber incident, the financial regulatory community now recognizes that it must quickly and effectively coordinate with one another, with law enforcement, and with the national security agencies. The more opportunities the regulators have to prepare, coordinate, and practice with the financial regulatory community, the greater the chance we will have to enhance recovery.

Treasury is working with the financial industry and government partners to update and streamline the sector's incident response playbook. This way, all parties throughout the government and private sector can better anticipate how each will respond to a significant cyber incident.

And to test our collective preparedness, Treasury, working in partnership with DHS, DOJ, and financial regulators, as well as the private sector, has completed five large-scale cybersecurity table-top exercises in little over a year. This is how we practice. These exercises pre-game various coordination mechanisms around information sharing, communication, escalation, and incident response protocols.

Earlier this month, Treasury along with relevant government agencies tested a fast-moving exercise scenario that involved not just actual contagion, but perceived contagion across the U.S. financial system.

C. The Role of the Private Sector in Enhancing Response and Recovery

The work to make any organization more effectively responsive to a cyber attack takes place well before an incident occurs. This preparation includes creating robust and agile cyber incident playbooks which identify key players, actions, and timelines. Such preparation includes continuous monitoring, by both automated systems and highly-skilled technicians. Such preparation includes establishing well-worn linkages between your CIO, your CISO, and your business and executive leadership. In the fog of an attack, you will want to be familiar and trust your team—you will need practice translating the technical jargon and high-level strategy for one another.

How does one build such a cyber incident playbook?

Whether stand-alone documents or part of larger business continuity and disaster recovery plans, these playbooks are most useful as preparation tools when they are informed by existing sector-specific response protocols as well as by the national cyber incident coordination policy once it is released. These playbooks should minimize response and recovery lags by describing the basics of who does what, when, and who reports to whom when a cyber incident happens.

As to the "who," the playbook should designate the person responsible for leading the command-and-control of the response-and-recovery efforts; and that individual, as well as the entire organization, should know his or her authority. The person chosen to lead should have exceptional organizational and communication skills because he or she will be quarterbacking internal and external interactions. The playbook should also identify other key internal and external leaders—including those from the legal, communications, and executive teams—and their specific responsibilities during a cyber incident. These individuals also need understudies—back-ups—and those back-ups also need to be designated in the playbook if for whatever reason a quarterback can't perform his or her duties.

As to the "what," the playbook should cover anticipated incidents based on the firm's individual risks. Depending on the firm, those risks could include: network intrusions, data or system corruption, malware infections, loss of customer personally identifiable information, theft of intellectual property, or distributed denial of service or ransomware attacks.

The middle of an attack is never a great time to learn unexpected things about your own organization. In advance of an attack, firms should identify their most sensitive and highly valued processes or assets—processes or assets critical to the functioning of the organization and those that pose the most risk if they should falter. Should these be compromised, firms should have specific plans for how they will secure these processes or assets in order to minimize damage physically, financially, and reputationally.

The playbook should also cover "when" the response team should act: what to do in the initial minutes, hours, and first few days of an incident and during the process of returning to normal. The specific steps may vary depending on the type of incident. But generally, response starts with containing and mitigating the incident, and then moves to eliminating incident artifacts — such as removing malware, disabling breached accounts, and mitigating vulnerabilities that were exploited. The recovery ends when systems are restored to normal operations and vulnerabilities for similar incidents are remediated.

As to "who reports to whom," to be effective, playbooks should cover when to get executive management and the board involved. The CEO and the board have to understand what their respective roles will be in the event of a significant cyber incident or a cyber attack on critical infrastructure on which the firm relies, such as energy or telecommunications. 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 — will initially oversee the response from a governance perspective.

The playbook should also cover when to call law enforcement to trigger coordination with the government. That initial contact may be to a field office of the FBI or U.S. Secret Service. Regardless of where that original connection is made — through law enforcement or DHS's National Cybersecurity and Communications Integration Center or a sector-specific agency, such as Treasury—knowing ahead of time that all relevant federal agencies will be rapidly notified will facilitate a unified and coordinated federal response, enhancing recovery and minimizing damage.

Playbooks should also cover when and how to notify customers, counterparties, and shareholders. Transparency and consistency are important. To instill trust and confidence, notification messages should avoid technical jargon and legalese and provide clear and consistent information. Public companies have additional considerations regarding the timing and content of their disclosure if the breach is considered material information. Ideally, a firm would have draft messages already vetted by its lawyers based on the firm's risk profile.

Finally, to be most effective, playbooks should be regularly updated to reflect the changing nature of the firm's risk profile. And firms should practice their playbooks. Internally this means that practice occurs with executive management all the way up to the board; externally this means that practice occurs through exercises with other firms and the government. Practicing this coordination will speed up response and recovery efforts.

V. Conclusion

Given the increasing number and morphing nature of cyber assaults, we must prepare for the eventuality of significant cyber incidents. By deploying the tools of preparation, coordination, and practice, the government, the financial sector, and their advisors can exponentially accelerate cyber response and can recover in a way that does not prolong the opportunity for damage—damage not only to the firms that compose our nation's financial infrastructure, but also damage to the people of our country who rely on this financial infrastructure. With this preparation, if and when a significant cyber incident occurs, we will be better equipped to respond and recover with level heads, and carry on with the business of returning to normal functioning.

Thank you.

###

---

[1] See: Sarah Bloom Raskin, *"Enhancing Cyber Resilience in the Financial Sector,"* Remarks at City Week, London, March 25, 2015, available at: https://www.treasury.gov/press-center/press-releases/Pages/jl10008.aspx; Sarah Bloom Raskin, *"Cybersecurity for Small and Mid-Size Banks: 10 Questions for Executives and Their Boards,"* Remarks at the Texas Bankers' Association Executive Leadership Cybersecurity Conference, Austin, December 3, 2014, available at: https://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx.

[2] See: Sarah Bloom Raskin, *"Frontiers of Financial Sector Cybersecurity,"* Remarks at The Clearing House Annual Conference, New York City, November 17, 2015, available at: https://www.treasury.gov/press-center/press-releases/Pages/jl0276.aspx; Sarah Bloom Raskin, *"Cybersecurity for Banks Version 2.0: 10 Follow-up Questions for Executives and their Boards,"* Remarks at the American Bankers Association Summer Leadership Meeting, Baltimore, July 14, 2015, available at: https://www.treasury.gov/press-center/press-releases/Pages/jl0112.aspx; Sarah Bloom Raskin, Remarks at The Center For Strategic And International Studies Strategic Technologies Program, Washington, D.C., September 10, 2015, available at: https://www.treasury.gov/press-center/press-releases/Pages/jl0158.aspx.

[3] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01; https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[4] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.