ASA

Annie Searle & Associates LLC

Research Note

Can the U.S. Treasury Keep Your Money Safe?

Suggested Risk Strategies for the U.S. Finance Sector Protection Plan

Michael Callier

December 2015

Keywords: Financial Services Sector, Critical Infrastructure, U.S. Treasury Department, Risk Management

Abstract: The U.S. Department of the Treasury (the "Treasury Department") is responsible for facilitating collaboration between public and private entities, in order to strengthen the security and resilience of the U.S. financial services sector (FSS), a designated critical infrastructure. The threat of cyber-attacks, amplified by the private sector's general resistance to regulated breach incident information sharing and lack of FSS third-party vendor cyber security controls, pose significant risks to FSS security and resilience. This paper analyzes the above risks and recommends appropriate risk management strategies for each.

Introduction

Critical infrastructure provides essential services, jobs, and resources that underpin life in the US. Without them, US society would arguably fall into chaos. On February 12, 2013, President Obama called for an updated national plan to enhance the security and resilience of critical infrastructure against both physical and cyber threats.[1]

In response, the Department of Homeland Security (DHS) developed the National Infrastructure Protection Plan (NIPP). NIPP's mission is to "strengthen the security and resilience of the U.S. critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community."[2] Critical infrastructure community means Federal, State, regional, local, tribal, territorial, private sector, and other critical infrastructure partners and stakeholders.

NIPP identifies 16 sectors deemed critical to the U.S. infrastructure. Each critical sector has a Sector Specific Plan (SSP) and a Sector Specific Agency (SSA) responsible for implementing that

SSP. The Treasury Department is the SSA for the Financial Services Sector (FSS) and is responsible for deploying the FSS SSP to ensure that NIPP's stated objectives are met in the FSS.

The Threat Environment

The risk of data breach poses a threat to all critical infrastructure sectors but the FSS in particular. Verizon's Data Breach Report (2015) indicates that only the IT sector experienced more data breach incidents than FSS – a less than comforting statistic considering FSS's dependency on IT.[3] In terms of likelihood, data breach has become less a question of "if" and more a matter of "when." Forty-three percent of U.S. organizations experienced a data breach in 2014, up 10 percent from 2013.[4] A 2014 Ponemon Institute study found the probability of an organization experiencing a material breach involving a minimum of 10,000 records to be more than 22 percent.[5] More than one billion total records were breached in 2014, an increase of 78 percent over 2013.[6]

The impact of data breach incidents is also significant. Ponemon found that the U.S. average cost of data breach in 2014 was $201 per record with U.S. average cost of data breach at $5.85 million and a 15 percent annual increase in average cost around the world.

Gemalto (2015) also found that, although 25 percent of breaches were the result of accidental loss, 55 percent percent of attacks came from malicious outsiders.[7] The Internet is a critical infrastructure for FSS and the FSS SSP indicates that the FSS's greatest vulnerabilities exist through its interdependence on telecommunications and IT.

Treasury Department Challenges

In light of the existing cyber threat and FSS's dependency on the Internet, the Treasury Department faces at least two significant challenges to achieving its objectives.

A. Resistance to Information Sharing

In December 2012, the Obama administration initiated the U.S. government information sharing strategy through the National Strategy for Information Sharing and Safeguarding.[8] The PPD-21, Executive Order 13636 and the NIPP all followed, promulgating public/private partnerships as an element of strengthening critical infrastructure resilience and security. The federal government subsequently developed three information sharing bills, which are currently circulating through Congress: the Cybersecurity Information Sharing Act (CISA), the Protecting Cyber Networks Act (PNCA) and the National Cybersecurity Protection Advancement Act of 2015 (NCPAA). Collectively, these are the "Information Sharing Acts." In addition, both the Pentagon and DHS plan to open offices in Silicon Valley to further efforts at public/private partnership and information sharing.

According to Sorcher (2015), private industry remains wary of the government's efforts, particularly with regard to the Information Sharing Acts, due to their perceived unnecessary infringement on privacy rights.[9] According to a joint letter written by prominent security industry professionals, the threat data that security specialists use to resolve cyber incidents is far more narrow than the personal identifiable information that the bills targets as breach incident

data.[10] In addition, commercial enterprises prefer to avoid disclosing data breaches for fear of litigation and loss of consumer confidence. In fact, banks are not required to report breach incidents unless the bank concludes that the breach resulted in financial loss to customers.

B. Third-Party Vendor Vulnerabilities

In May 2014, the New York State Department of Financial Services (NYSDFS) published a report highlighting the continuing challenge facing the FSS due to its dependency on third-party service providers for critical banking functions.[11] According to the report, existing third-party cyber security controls are inadequate. Fewer than half of the organizations surveyed conduct onsite due diligence of vendors: only 46 percent required initial onsite due diligence of potential vendors and only 35 percent required periodic onsite due diligence of even high-risk vendors. The report also found that, although all surveyed institutions had written vendor management policies, the policies varied greatly. For example, 79 percent of respondents required that vendors maintain information security requirements but only 36 percent of respondents extended that requirement to subcontractors. In addition, 21 percent did not reserve the right to audit their vendors, and 44 percent did not require vendors to warrant the integrity of their data or products. Further, 30 percent of surveyed institutions did not require vendor notification in the event of a data breach. Only 38 percent of respondents used encryption for data "at rest" and 30 percent did not use multifactor authentication for at least some vendors to access sensitive information. Only 63 percent of respondents carried cyber insurance, and only 47 percent of those policies explicitly cover vendor data breach incidents. Finally, only half of institutions had vendor contracts that included indemnification clauses.

Qualitative Risk Assessment and Risk Management Strategy

A1: Resistance to Information Sharing

The risk level for this threat is medium because, if the risk happens, the Treasury Department can still help to strengthen the security and resilience of the FSS infrastructure through existing channels like FBIIC and FSSCC,[i] although its public/private collaboration and integration would be less effective. Since the Edward Snowden event, the cyber security private community has distanced itself from Washington. So long as the Information Sharing Acts reach for private information beyond that necessary to address data breach incidents, the distrust is likely to continue.

---

[i] FBIIC stands for the Financial Banking Information Infrastructure Committee. FBIIC is comprised of 17 financial sector regulatory agencies and is responsible for encouraging coordination and communication between financial regulators, promoting public-private partnerships, and enhancing overall FSS resilience. FSSCC stands for the Financial Services Coordinating Council for Infrastructure Protection and Homeland Security. FSSCC is comprised of FSS private entities and helps to identify the need for sector protective programs and resilience strategies. The FSSCC collaborates with the FBIIC to support sector resilience efforts and also deploys independent efforts when its members identify industry security needs.

A2: Recommended Risk Strategy:

Tolerate/Transfer. The Treasury Department does not have authority to compel information sharing in its role as FSS SSA. Therefore, it can only continue to tolerate lack of information sharing with the private sector and continue its efforts through the FBIIC/FSSCC partnership until Congress passes some form of the Information Sharing Acts and state regulators, like the NYFDSF, enact disclosure requirements that the Treasury Department can rely on to compel desired information sharing.

B1: Third-Party Vendor Vulnerabilities

The risk level for this threat is high because of the high likelihood of breach (indicated above) and, if it happens, the impact will be to weaken security and resilience in the FSS, including consumer confidence, as did the JP Morgan breach. Still further, it is not just the cost of breach remediation that threatens FSS security and resilience but also consumer lawsuits (including class actions) and commercial disputes between companies and their third-party vendors. Target has already incurred breach costs of $162 million (a total of $252 million with insurance payout offset of $90 million) and paid $19 million in settlement funds to MasterCard.[12] Any additional litigation damages will only add to Target's already sizeable breach costs, not to mention reputational damage.[13] Financial institutions face the same threat for breach incidents caused by their third-party vendors and, conversely, harm that they may cause to their third-party vendors.

B2: Recommended Risk Strategy: Treat. The Treasury Department should leverage FBIIC to encourage state agencies, like NYSDFS, to enact regulatory standards that require constituent FSS entities to: (1) conduct onsite due diligence for all potential third-party vendors and periodic onsite due diligence for third-party vendors (or at least for high-risk vendors); (2) require both vendors and vendor subcontractors to maintain at least NIST Framework Implementation Tier 3; (3) execute written agreements with all relevant third-party vendors and ensure that such agreements reserve the right to audit vendors, require vendors to warrant the integrity of their data or products and include indemnity provisions in favor of the bank; (4) use encryption for all data, including data at rest, and require third-party vendors to do the same; (5) require that vendors use multifactor identification protocols to access bank network and information; and (6) require banks to carry cyber insurance that explicitly covers vendor data breach incidents.

References

[1] "Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21)." The White House. 12 Feb. 2013. Accessed Jun. 2015 <www.whitehouse.gov>.

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity. U.S. Department of Homeland Security. Mar. 2013. Accessed Jun. 2015 <www.dhs.gov>.

The Comprehensive National Cybersecurity Initiative. The White House. Mar. 2010. Accessed Jun. 2015 <www.whitehouse.gov>.

[2] *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. U.S. Department of Homeland Security.

Jan. 2014. Accessed Jun. 2015 <www.dhs.gov>.

[3] *2015 Data Breach Investigation Report*. Verizon Enterprise Solutions. May 2015. Accessed Jun. 2015 <www.verizonenterprise.com>.

[4] Weise, Elizabeth. "43% of Companies Had a Data Breach in the Past Year." USA Today. 24 Sep. 2014. Accessed Jun. 2015 <www.usatoday.com>.

[5] *2014 Cost of Data Breach Study: Global Analysis*. Ponemon Institute LLC. May 2014. Accessed Jun. 2015 <www.ibm.com>.

[6] Warren, Zach. "Gemalto Reports That More Than One Billion Total Records Were Breached." *Inside Counsel.* 17 Feb. 2015. Accessed Jun. 2015 <www.insidecounsel.com>.

[7] Ibid.

[8] *National Strategy for Information Sharing and Safeguarding*. The White House. Dec. 2012. Accessed Jun. 2015 <www.whitehouse.gov>.

[9] Sorcher, Sara. "At Cybersecurity Gathering, the White House Steps up Charm Offensive." *The Christian Science Monitor.* 24 Apr. 2015. Accessed Jun. 2015 <www.csmonitor.com>.

[10] Granick, Jennifer. "Technologists Oppose CISA/Information Sharing Bills." The Center for Internet and Society, Stanford Law School. 16 Apr. 2015. Accessed Jun. 2015 <www.cyberlaw.standford.edu>.

[11] *Update on Cyber Security in the Banking Sector: Third Party Service Providers*. Department of Financial Services, New York State. Apr. 2015. Accessed Jun. 2015 <www.dfs.ny.gov>.

[12] Hill, Mitzi L. "Companies Target Each Other In Data Breach Disputes." *Business Insurance.* 26 Apr. 2015. Accessed Jun. 2015 <www.businessinsurance.com>.

[13] Lunden, Ingrid, "Target Says Credit Card Data Breach Cost It $162M In 2013-14" *TechCrunch*. 25 Feb. 2015. Accessed Jun. 2015 <www.techcrunch.com>.