FINANCIAL SERVICES ROUNDTABLE

TESTIMONY OF TIM PAWLENTY

Chief Executive Officer, The Financial Services Roundtable

The Permanent Select Committee on Intelligence

Hearing entitled, "The Growing Cyber Threat and its Impact on American Business"

March 19, 2015

Chairman Nunes, Ranking Member Schiff and Members of the Committee, thank you for the opportunity to appear before you today to address the important topic of cybersecurity and the further steps needed to better protect our nation's cyber infrastructure, the financial sector's cyber infrastructure, and the information – both personal and proprietary – that the sector holds in its care.

The Financial Services Roundtable ("FSR") represents many of the country's largest financial service companies. Our members include leading banking, insurance, asset management, finance, and payment companies. Cybersecurity has been a key focus area for FSR and our companies for decades. Since 1996, FSR's technology policy division, BITS, has played an important leadership role in addressing cybersecurity, fraud reduction, vendor management, payments and emerging technology issues.

It is important to note the leadership of this Committee has often been at the forefront of cybersecurity policy development, including efforts to pass cyber threat information sharing legislation during the past two sessions of Congress. The Committee's leadership in this regard has been important and appreciated.

My testimony today will address the following topics: the current cyber threat environment; the high priority of cybersecurity to the financial industry; steps Congress can take to bolster cybersecurity; and the importance of protecting consumer data and ensuring consumer trust.

The Cyber Threat Environment

Cyber risks grow daily as attacks increase in number, pace, and complexity. Attacks are no longer perpetrated mostly by individual "hacktivists" or fraudsters. Attacks are now more typically perpetrated by organized crime syndicates, nation-states and nation-state supported actors. The nature of the threat has evolved from webpage defacement and fraud, to large-scale distributed denial of service (DDoS) attacks and attacks aimed at the integrity of the financial system through data manipulation or destruction.

According to Symantec's 2014 "Internet Security Threat Report," the number of targeted spear-phishing campaigns rose by 91 percent in 2013.[1] In recent years, nation-state actors and organized criminals have attacked Estonian, Georgian, and Ukrainian telecommunications systems[2], European power plants[3], U.S. public utilities[4], health care providers[5], retailers of all

[1] Symantec Corporation, "Internet Security Threat Report 2014," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, (April 2014).

[2] Reuters, "Ukraine: Cyberattack on communications, MPs phones blocked," http://www.cnbc.com/id/101465198, (March 4, 2014).

[3] Symantec Security Response, "Dragonfly: Western Energy Companies Under Sabotage Threat," http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, (June 30, 2014).

[4] ICS-CERT Monitor, "Internet Accessible Control Systems At Risk," https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf, (January-April 2014).

[5] Abelson, Reed and Matthew Goldstein, "Millions of Anthem Customers Targeted in Cyberattack," http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (February 5, 2015).

sizes and many other entities[6]. A recent report reveals that of the estimated $2-3 trillion generated annually from the "internet economy," cybercrime alone extracts between 15 to 20 percent of that total value.[7]

In response, the private sector has dramatically increased cybersecurity spending, with one financial services firm now reportedly spending $250 million per year.[8] Notwithstanding that response, detection and response systems need improvement. The most recent Verizon Data Breach Investigation Report revealed that only about 20 percent of breached organizations discover the attack through their own internal processes.[9] Nearly 80 percent of organizations learned of breaches from third parties, including law enforcement.[10] This statistic highlights the need for appropriate collaboration between public and private entities.

Cybersecurity: An Industry Priority

Senior executives at FSR member companies have long been concerned about cybersecurity issues and those issues have become key priorities for CEOs and boards of directors. In addition to efforts at the company level, the industry overall has also been working collectively to coordinate cyber defense efforts.

FSR member companies participated in the recent White House Cybersecurity Summit, and the financial services sector continues to lead efforts to address many of the topics raised during the summit including: cyber threat information sharing, payments security, and increased public-private sector collaboration.

On March 18, FSR convened the 6th Annual Joint Associations Cybersecurity Summit, which was attended by representatives of seven partner associations (FSR, Financial Services Sector Coordinating Council (FSSCC), the Financial Services Information Sharing and Analysis Center (FS-ISAC), American Bankers Association (ABA), Independent Community Bankers of America (ICBA), Securities Industry and Financial Markets Association (SIFMA), The Clearing House (TCH)), senior executives from 22 financial services companies, and officials from 9 government agencies. We discussed cyber-related regulatory efforts, strategies for defending against future cyber attacks with key leaders from government and the financial services sector, and key deliverables of the Joint Associations Cybersecurity Action Plan.

Other examples of financial service sector collaboration and coordination regarding cybersecurity include:

---

[6] Symantec Corporation, "Internet Security Threat Report 2014," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, (April 2014).

[7] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II,http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, (June 2014).

[8] U.S. Department of Treasury, "Remarks of Secretary Jacob J. Lew at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor," http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx, (July 16, 2014).

[9] Verizon Enterprise, "2014 Verizon Data Breach Investigations Report," http://www.verizonenterprise.com/DBIR/2014/ (March 2014).

[10] Ibid.

- Creating the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999 in response to Presidential Decision Directive 63, which is arguably the most robust sector cyber threat information sharing entity in existence [11], The FS-ISAC has steadily grown in membership and capabilities, and it has significantly helped the sector respond to cybersecurity challenges.
- Creating the Financial Services Sector Coordinating Council (FSSCC) in 2002. The FSSCC was established at the request of the U.S. Treasury Department (in accordance with Presidential Decision Directive 63) following the September 11, 2001 attacks. The FSSCC works closely with the Treasury Department and other federal financial sector regulatory agencies to foster government and industry information exchange and study of cybersecurity issues.
- Creating the annual Joint Associations Cybersecurity Summit described above.
- Funding and launching "Soltra Edge" as a joint venture of the FS-ISAC and the Depository Trust and Clearing Corporation. Soltra Edge is a software solution that dramatically enhances cyber threat information sharing capabilities so that trusted, actionable intelligence from disparate sources can be uniformly and quickly disseminated nearly in real time. This improved capability helps companies more timely identify and address cybersecurity threats. Soltra Edge software takes only a few minutes to download and the basic license is free so the solution is accessible to financial institutions of all sizes. We anticipate the technology behind Soltra Edge will be adopted by other critical sectors.
- Creating the Merchant and Financial Associations Cybersecurity Partnership which brought together 19 associations representing the merchant/retail community and financial services sector. The partnership was designed to: share best practices, improve cyber threat information sharing, enhance security of payments, identify and support certain cybersecurity legislation, and better rationalize data breach notification standards.
- Coordinating the financial services industry's efforts during the development of the voluntary NIST Cybersecurity Framework. The development and use of the NIST Cybersecurity Framework was successful due, in part, to process transparency and incorporation of industry input.
- Expanding and improving critical relationships with law enforcement agencies. In 2014, the FSR, FBI and U.S. Secret Service co-hosted a major event addressing cyber crime. The event provided a visible example of the growing collaboration between financial services companies and law enforcement agencies.
- Securing the top-level domains .BANK and .INSURANCE. We combined efforts with the American Bankers Association and leading financial service companies to create a financial services sector-owned, operated and governed fTLD registry. The .BANK and .INSURANCE domains will offer far more than a less generic alternative to .COM and .ORG legacy domains. The new domains will have robust operational requirements including: eligibility requirements, verification, name selection standards, and security-focused technical requirements such as Domain Name Security Extensions (DNSSEC), encryption standards, email authentication requirements designed to reduce phishing and spoofing activities, and more.

[11] The Bush Administration updated Presidential Policy Directive 63 in 2003 with Homeland Security Presidential Directive 7, which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.

Notwithstanding these industry efforts, more needs to be done and Congress needs to act.

Steps Congress Can Take to Bolster Cybersecurity

As noted above, the financial services sector has made progress regarding cyber threat information sharing, but such efforts are significantly constrained by fear of legal liability and potential disclosure, even if such cyber threat information is shared in good faith and for an appropriate purpose.

To encourage better cyber threat information sharing within and between sectors as well as between industry and government, legislation providing sensible "Good Samaritan" protections is needed. Such legislation should:

- Facilitate real-time cyber threat information sharing to enable institutions and government to act quickly;
- Provide a reasonable level of liability protection for good faith cyber threat information sharing;
- Provide targeted protections from public disclosures, such as exemptions from certain Freedom of Information Act requests;
- Facilitate appropriate declassification of pertinent cyber threat information and expedite issuance of clearances to selected and approved industry executives; and
- Include appropriate levels of privacy protections.

Securing Sensitive Data: GLBA as a Model for Other Industries

Data security legislation to help prevent data breaches also continues to be a top priority for FSR, and we urge Congress to act swiftly on this critical issue.

Section 501(b) of Title V of the Gramm-Leach-Bliley Act (GLBA), enacted by Congress in 1999, directed regulators to establish standards for financial institutions to protect customer information. Pursuant to the GLBA, Federal and State regulators imposed wide-ranging information security requirements for regulated financial institutions. Bank regulators, for example, have imposed the most detailed requirements mandating strong internal procedures, vigorous threat and risk assessments, ongoing testing and evaluation of security systems, and required reporting to senior management and directors.

Among the obligations to secure systems and protect data under GLBA, financial institutions must:

- Develop and maintain an effective information security program tailored to the complexity of its operations;
- Oversee service providers with access to customer information, including requiring service providers to protect the security and confidentiality of information;

- Train staff to prepare and implement information security programs;
- Test key controls, systems, and procedures and adjust key controls and security programs to reflect results of such ongoing risk assessments;
- Safeguard the proper disposal of customer information; and
- Update systems and procedures taking into account, for example, technology changes, emerging internal or external threats to information, changing business arrangements (e.g., mergers and acquisitions), personnel changes, and more.

Protecting sensitive information and maintaining consumer confidence and trust is critical for the financial sector, and it is vitally important for other sectors as well. We encourage policymakers to pass legislation ensuring all sectors have an obligation to properly protect customer information. We simultaneously encourage Congress to note the rapid pace of innovation in security technology and avoid mandating specific technologies or applications which could soon become outdated or obsolete.

Conclusion

Each week, more businesses and customers fall victim to cyber attacks. The private sector is obviously waging a battle against attacks which are clearly launched by organized crime, other nations, or hostile entities supported by other nations. While the financial sector is an example of strong and frequent cyber collaboration and investment, we cannot fight this battle alone. As outlined in these remarks, Congress needs to act. In addition, these issues will need to be more aggressively and effectively addressed as part of America's larger foreign policy and security initiatives.

Thank you for the opportunity to appear before this Committee. We look forward to continuing to work with you to address these important issues.