STATEMENT OF
MICHAEL CARANO
EXECUTIVE DIRECTOR
CHICAGOFIRST

BEFORE THE

SUBCOMMITTEES ON INFORMATION TECHNOLOGY
AND GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

June 20, 2016

Introduction

Chairman Hurd, Ranking Member Kelly and distinguished Members of the Committee, on behalf of ChicagoFIRST members, I thank you for the opportunity to appear before you to discuss Federal efforts to improve cybersecurity.

The Chicago financial services industry is one of the most diverse in the United States and one of the largest employers in the City of Chicago. Its participants include securities and futures exchanges, large and small banks, securities and futures clearinghouses and cash operations of the Federal Reserve Bank of Chicago. Because of its diversity and importance to Chicago, disruption of these markets would seriously affect the city, as well as key financial operations nationally and globally.

ChicagoFIRST provides a collaborative forum for financial and critical infrastructure firms to promote individual and collective emergency preparedness and resiliency through local, regional and national public private partnerships.

The operational partnership offers 24/7 situational awareness and networking opportunities with members and public sector representatives through workgroups, roundtables, workshops and exercises. In these trusted venues, members share best practices, identify challenges and engage in collaborative solution-based discussions addressing risk management, emergency preparedness, response and resilience.

Through longstanding relationships with the public sector, ChicagoFIRST takes a leadership role at the local, state and federal levels, representing issues of importance to members. A nonprofit association formed in 2003, 29 individual firms constitute ChicagoFIRST's membership, govern its operations, fund its activities and manage its staff.

Overview

ChicagoFIRST members support government efforts to improve our nation's cybersecurity through the Cybersecurity National Action Plan and the Cybersecurity Act of 2015. ChicagoFIRST's Cybersecurity Work Group developed a consensus view of the local cybersecurity landscape for this testimony.

Cyber criminals have a financial incentive to gain access to bank and credit card accounts, while nation-state actors seek to harm our collective economic interests. E-mail phishing remains a popular tool for illegitimate access to personal accounts and critical infrastructure systems. We're also concerned about the new types of fraud using mobile payments and digital wallets, and the increase in attempts to gain access to wholesale inter-bank payments mechanisms like SWIFT.

Establishing a bipartisan commission to recommend cybersecurity best practices and the development of a privacy council to establish standards for how the government protects Americans' sensitive information are both positive steps to prepare the nation for the inevitable cyber-attacks to come. In this testimony, ChicagoFIRST members chose to focus on five areas: Education, Data Sharing, Cross Sector Coordination, Cyber Security Frameworks and Information Privacy.

Public Education

ChicagoFIRST members believe new high-profile public education campaigns are a vital component in the ongoing efforts to combat cybercrime because people of all ages, from toddlers to senior citizens, use networked computers. While many employers provide cyber education to protect company systems and customer data, public education is equally important to safeguard personal data and systems. For example, everyone needs to recognize the characteristics of increasingly sophisticated phishing attempts in order to thwart these attacks. With the proliferation of remote access to corporate systems as more employees work remotely, the security of home networks and computers is becoming more important to overall national security.

K-12 education programs, such as Science, Technology, Engineering and Mathematics (STEM) workshops designed to assist teachers in providing cyber security education, can play an important role in building cyber security awareness in children and teens. Early education is necessary as children now carry state-of-the-art mobile devices hosting applications that are increasingly susceptible to attacks and are connected to home networks that may have access to personal financial information. As teenagers begin to use e-mail for school or professional reasons, they require additional education on the dangers of phishing, malicious links and unexpected documents in e-mail.

To counteract ransomware and destructive malware, the public at large needs to better understand the importance of backing up the data on their computers and other devices, and the options they have for accomplishing those backups. Moreover, civilians need to know the significance of having a firewall with sufficient restrictions, maintaining up-to-

date anti-virus protection and selecting restrictive social media privacy settings for their families.

A framework for minimum cyber education requirements may be useful to provide guidance to various age groups based on the technology they are most likely to use. Educational messaging must be frequent to instill the learning and to account for the evolving threat vectors. ChicagoFIRST members also believe there needs to be consistency in cybersecurity terminology and definitions used by government, educators, and private industry so that messaging is clear and consistent in public and private education efforts.

Professional Education

Cybersecurity leaders are deeply concerned about the availability of competent candidates to fill the growing number of information security roles at private sector firms. We support efforts to further develop cyber curriculums at higher education institutions and to promote the field of study with qualified students and individuals seeking a career change. Private sector employers are expressing the need to clearly define a career path for cyber security workers and to fill that pipeline with capable staff. Maintaining an adequate depth of talent at individual firms has become increasingly difficult because information security employees tend to switch jobs for increased salary as they obtain new levels of proficiency and the demand for experienced staff continues to outpace supply.

In dealing with the supply shortage for cyber security professionals, some employers are encouraging staff from other areas of IT to consider a career change in exchange for training in cyber security. For example, Help Desk and Quality and Assurance testing staff often have analytical and diagnostic skills that transfer well into a cyber security role. Similarly, IT Generalists that have a broad view of many roles in a typical IT organization (e.g. development, server support, data center operations) may be a good information security candidate. Given the institutionalized cyber recruitment efforts of Nation-State actors with bad intent, it is vital that our own cyber education and recruitment efforts bring the most capable talent into the field, whether directly from college or as a career change, in both public sector agencies and private sector critical infrastructure firms.

Data Sharing

The financial services sector discovers new cyber threats on a daily basis and shares this threat intelligence through a variety of channels including the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Federal Bureau of Investigation, the United States Secret Service and industry groups that publish vulnerability information on specific products or systems. The FS-ISAC in particular has become an invaluable tool for receiving the latest threat information based on the day-to-day experiences of peer firms. In addition, firms collect their own system log, asset and vulnerability data. The vast amount of data available presents the problem of correlating

threat intelligence, vulnerability reports, company assets and logs to determine the high priority threats at a particular company. The lack of a method or commercial tools to produce actionable information from this data may be an opportunity for a public private research effort on how critical infrastructure institutions can better correlate threat data and improve the speed of response and remediation efforts.

Some firms are concerned about the timeliness of cyber threat information from the FBI. For example, it often takes a month for the FBI to declassify and provide the private sector with information on destructive malware, which creates a window of risk for critical infrastructure firms. ChicagoFIRST members would appreciate government efforts to expedite the release of vulnerability information through trusted channels or intermediaries so that firms can take mitigating actions as soon as possible. FS-ISAC members are able to report problems anonymously for the benefit of other members, which reduces any reputational, legal or financial risk that might occur with a disclosure while allowing for immediate mitigation steps by other firms. This type of anonymity in disclosures may also be useful for other industries so information can be shared rapidly without retribution for acknowledging known vulnerabilities or incidents.

Cross Sector Coordination

Financial services, power and telecommunications have a great degree of interdependency upon each other. The Financial Services Sector Coordinating Council (FSSCC) has long worked with the energy and communication sectors to jointly share information and identify vulnerabilities and restoration priorities for major events. This collaboration continues with emergency response planning and exercises to improve our collective capabilities to respond to regional disasters. Looking forward, cross sector emergency planning, testing and response should continue to be emphasized at all levels of government to ensure individual sector response plans are not developed within industry silos.

Cybersecurity Frameworks

ChicagoFIRST members recognize that assessing cyber risk is a critical component of an effective program to safeguard individual firms and our interconnected sector as a whole. While larger institutions have embraced the NIST Framework for Improving Critical Infrastructure Cybersecurity, some community banks have found the Federal Financial Institutions Examination Councils (FFIEC) Cybersecurity Assessment Tool to be a more straightforward means for assessing their environments. The two assessments are not harmonized to the extent that a financial institution that completes one assessment could understand its risk posture under the other. In working with regulators, financial institutions need options for compliance based on the scale and risk profile of their institution. Maintaining assessments under multiple frameworks to meet often divergent requirements of state, federal and international regulators is not sustainable given cyber security human capital resource constraints. Harmonization and alignment of the assessment frameworks is a possible solution to reducing the regulatory burden while maintaining confidence that institutions are taking prudent steps to mitigate cyber risks.

Recent FFIEC regulatory guidance has emphasized the assessment of key vendors and business partners for cyber risk. These third-party risk assessments are often developed by individual firms to assess their business partners without following any framework or standards for areas of inquiry. Financial service providers, insurance companies and financial utilities are facing a burden of answering these free-form inquiries in increasing numbers as more firms respond to the guidance to assess their vendors. Conversely, individual firms are grappling with how to effectively assess their vendors, which could number in the hundreds for a larger institution. Standardized cyber risk declarations may be a method to streamline these vendor assessment processes.

Information Privacy

ChicagoFIRST members expressed support for the continued de-emphasis of social security numbers as a personal identifier. Banks remain concerned about synthetic identity theft fraud using the social security numbers of minors. The Social Security Administration has no validation structure that includes birthday, so this type of identity fraud can be difficult to detect.

Non-public personal information breach response continues to be challenging as a result of the 47 divergent state and territorial data breach response requirements. We support continuing efforts to define a national standard for breach response that balances consumer protections with efficient notification.

Conclusion

ChicagoFIRST member firms appreciate the opportunity to provide a regional view of cybersecurity threats, legislation and executive actions. We fully support the continued public private collaboration on preparedness, mitigation, response and recovery efforts at all levels of government.

We place great emphasis on the public's awareness of cyber threats, how they can avoid the consequences of attacks as well as the need to advance the field of information security through education and career development efforts. While financial services threat intelligence data sharing has matured to a great extent, there is a need to ensure there are timely and safe mechanisms to share information between the public and private sectors and between critical infrastructure sectors. Likewise, cross sector planning and response coordination is vital as multiple sectors are often deeply connected at the regional level. Finally, we support the effort to create consistent privacy laws across the states and harmonize assessment frameworks to avoid burdensome and duplicative work.

ChicagoFIRST looks forward to continued work with all of our government partners to enhance our Nation's cybersecurity resilience.

ChicagoFIRST Members

Aon
Ariel Investments
Bank of America
BMO Harris Bank*
BP
Chicago Board Options Exchange*
Chicago Trading Company*
CME Group
CNA*
Commonwealth Edison
Enova Financial
Federal Home Loan Bank of Chicago
Federal Reserve Bank of Chicago*
Fiserv*
Goldman Sachs
Guggenheim Partners
Harbor Funds*
Jackson National Asset Management*
Lockton
MB Financial Bank
Mesirow Financial
Mizuho Securities
Northern Trust Bank
Options Clearing Corporation*
PPM America
PrivateBank*
Synchrony Financial*
United Airlines
William Blair & Company*

Members denoted by an asterisk participated in the ChicagoFIRST Cyber Work Group meeting to provide input to this testimony.

Michael Carano
ChicagoFIRST, Executive Director

Mr. Michael Carano is the Executive Director of ChicagoFIRST, a non-profit association of mid-western private sector firms that coordinates critical infrastructure protection among its members and in partnership with government agencies at the city, county, state, and federal levels. Mr. Carano co-chairs the Chicago Public Private Task Force with the Executive Director of the Chicago Office of Emergency Management and Communications. He also serves on the steering committee for the United States Secret Service Electronic Crimes Task Force in Chicago and the executive committee of the Financial Services Sector Coordinating Council based in Washington DC.

Prior to joining ChicagoFIRST, Mr. Carano worked for Cook County, the second largest county in the nation, to develop a comprehensive Continuity of Government program encompassing crisis management, business process recovery and technology recovery. Mr. Carano also served as both Chief Continuity Officer and Chief Privacy Officer for Netherlands-based ABN Amro Bank, which included LaSalle Bank in the United States, and he led an independent consultant firm focused on business continuity and information privacy.

As an Assistant Vice President for the Federal Reserve Bank of Chicago, Mr. Carano developed post 9/11 business continuity strategies and collaborated with government agencies, financial institutions and exchanges to improve the resilience of the financial sector. He joined the Federal Reserve as a software developer and advanced to management while providing technology services for high-value electronic payment and inter-bank settlement systems.

Mr. Carano holds an MBA from the University of Chicago, information technology degrees from Loyola University and Southern Illinois University, and he is a Certified Business Continuity Professional, Certified Information Privacy Professional, a Project Management Professional, and earned a Critical Infrastructure Protection Certification from Texas A&M.