U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

The Expanding Cyber Threat

Tuesday, January 27, 2015
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

Purpose

On Tuesday, January 27, 2015, the Research and Technology Subcommittee will hear from private sector and government experts about issues related to cybersecurity, including impacts to critical infrastructure, cyber hardware and software, and personal security and privacy stemming from cyber threats, attacks and breaches in order to inform the Committee's legislative work. The Committee's jurisdiction includes research and development related to cybersecurity at the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security's Science and Technology Directorate (DHS S&T).

Witnesses

- **Ms. Cheri McGuire**, Vice President, Global Government Affairs & Cybersecurity Policy, Symantec Corporation
- **Dr. James Kurose**, Assistant Director, Computer and Information Science and Engineering (CISE) Directorate, National Science Foundation.
- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Dr. Eric A. Fischer**, Senior Specialist in Science and Technology, Congressional Research Service
- **Mr. Dean Garfield**, President and CEO, Information Technology Industry Council

Overview

Information technology (IT) is continuously evolving, leading to markedly increased connectivity and productivity for industry, government and personal use. The benefits provided by these advancements have led to the widespread use and incorporation of information technologies across major sectors of the economy. This level of connectivity and the dependence of our critical infrastructure systems on IT have also increased the vulnerability of these systems. Reports of cyber criminals, "hacktivists" and nation-states accessing sensitive information and disrupting services in both the public and private domains have risen steadily, heightening concerns over the adequacy of our cybersecurity measures.

Cybersecurity related concerns range from spearfishing attempts and spam, to malware, to illegal or illicit activity on the darknet (private networks using non-standard protocols not connected to the internet). More and more cases of successful cyber-attacks are being reported. Financial information, medical records, any and all personal data maintained on computer systems by individuals or by organizations large and small are vulnerable. Mobile, wireless technology presents new opportunities for cyber-attacks. As more devices communicate with one another, from security systems to thermostats, the "Internet of Things" presents a growing target. Social media sites and advertisements also present opportunities for cybersecurity breaches. A number of companies with cybersecurity services compile data and have made predictions about cyber threats. "[I]n 2014, Proofpoint found a 650% increase in social media spam compared to 2013."[1]

During the 113th Congress, the Science, Space, and Technology Committee held a number of hearings on issues related to cybersecurity including a February 2013 hearing, *Cybersecurity Research and Development: Challenges and Solutions*[2]*;* a January 2014 hearing, *Healthcare.gov: Consequences of Stolen Identity*[3]*;* and a March 2014 hearing, *Can Technology Protect Americans from International Cybercriminals.*[4] Each hearing explored a different aspect of cybersecurity concerns facing Americans today.

High-profile cyber breaches in recent months include: Target and Home Depot financial transaction systems, Apple's iCloud systems, Sony, and the U.S. Central Command. The number and changing nature of threats serves to underscore the importance of safeguarding information technology and systems.

According to the U.S. Government Accountability Office, "[f]ederal agencies have significant weaknesses in information security controls that continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support their operations, assets, and personnel."[5] In fiscal year 2014, the federal government spent more than $81 billion on information technology.[6] "Federal agencies spend a significant part of their annual IT funding on cybersecurity, which currently constitutes more than one in every eight dollars of agency IT budgets."[7]

Cybersecurity research and development efforts include working on the prevention of cyber-attacks, detecting attacks as they are occurring, responding to attacks effectively, mitigating severity, recovering quickly, and identifying responsible parties. Research and development provides a better understanding of weaknesses in systems and networks and of how to protect those systems and networks.

[1] http://www.proofpoint.com/threatinsight/posts/cybersecurity-predictions-for-2015.php

[2] http://science.house.gov/hearing/subcommittee-technology-and-subcommittee-research-joint-hearing-cyber-rd-challenges-and

[3] http://science.house.gov/hearing/full-committee-hearing-healthcaregov-consequences-stolen-identity

[4] http://science.house.gov/hearing/subcommittee-oversight-and-subcommittee-research-and-technology-joint-hearing-can-technology

[5] http://www.gao.gov/key_issues/cybersecurity/issue_summary#t=0

[6] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/omb_presidents_it_budget_for_fy_2015_summary_chart.pdf

[7] http://www.fas.org/sgp/crs/misc/R43831.pdf

The National Science Foundation

The National Science Foundation (NSF) is the principal agency supporting unclassified cybersecurity research and development as well as technical education. The NSF Directorate for Computer and Information Science and Engineering (CISE) promotes the progress of computer and information sciences, advances the development and use of cyberinfrastructure and leads the Foundation's Secure and Trustworthy Cyberspace investment to build a knowledge base in cybersecurity and a cyber-secure society. NSF has made investments in cybersecurity education and workforce. The Scholarship for Service program, recently codified in *The Cybersecurity Enhancement Act* (PL 113-274), provides awards to increase the number of students entering the computer security and information assurance fields, and to increase the capacity of institutions of higher education to produce professionals in these fields. NSF also offers Advanced Technological Education (ATE) grants educating technicians for high-technology fields with a focus on two-year colleges.

CISE was funded at $894 million in fiscal year 2014 (FY14), the President's budget request was just over $893 million for FY 15. Scholarship for Service received $45 million for FY14 and the FY15 request included $25 million. ATE funding levels of nearly $125 million in FY14 were maintained in the FY15 request.

The National Institute of Standards and Technology

The National Institute of Standards and Technology's (NIST) core cybersecurity focus areas include: research, development, and specification; secure system and component configuration; and assessment and assurance of security properties of products and systems. In 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* stemming from a 2013 Executive Order (more details below). Title III of the E-Government Act (PL 107-347), the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with developing cybersecurity standards, guidelines, and associated methods and techniques for use by the Federal Government. In April 2011, the Administration tasked NIST with leading the National Strategy for Trusted Identities in Cyberspace (NSTIC), an initiative focused on establishing identity solutions and privacy-enhancing technologies to improve the security and convenience of sensitive online transactions.

NIST's Information Technology Laboratory (ITL) leads the organization's cybersecurity related responsibilities. ITL is a part of NIST's six laboratory units under the Science and Technical Research Services (STRS) appropriations line item. In FY14 ITL was funded at over $109 million, the FY15 request was $111 million.

In December 2014, *The Cybersecurity Enhancement Act of 2015* (PL 113-274) passed the House and Senate and was signed into law. The new law strengthens the efforts of NSF and NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development. PL 113-274 coordinates research and related activities conducted across the Federal agencies to better address evolving cyber threats.

The Department of Homeland Security Science and Technology Directorate

In fiscal year 2011, the DHS Science and Technology Directorate (S&T) established the Cyber Security Division (CSD) within S&T's Homeland Security Advanced Research Projects Agency (HSARPA). CSD works to enhance the security and resilience of the nation's critical information infrastructure and the Internet. CSD develops and delivers new technologies, tools and techniques to enable DHS and the U.S. to defend, mitigate and secure current and future systems, networks and infrastructure against cyber-attacks. CSD serves a wide range of customers and partners within DHS and at other federal agencies, state and municipal administrations and first responders, and private sector organizations.

In FY14 DHS S&T was funded at $1.2 billion, the FY15 request was nearly $1.1 billion for the Directorate. HSARPA and CSD fall under the Research, Development and Innovation line item for DHS S&T which in FY 14 was funded at $462 million and in FY15 the Administration requested nearly $434 million.

Executive Order on Improving Critical Infrastructure and Framework for Improving Critical Infrastructure Cybersecurity

In February 2013, President Obama issued an executive order (EO 13636) on cybersecurity for critical infrastructure.[8] Among other provisions, the EO encouraged information sharing between public and private sectors and directed NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST was instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework.

In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* in response to the EO. NIST worked in collaboration with industry stakeholders to establish a three-pronged *Framework* that includes a Core, Profile and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[9]

[8] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[9] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf