U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research & Technology

HEARING CHARTER

Can Technology Protect Americans from International Cybercriminals?

Thursday, March 6, 2014
9:30 a.m. – 11:30 a.m.
2318 Rayburn House Office Building

Purpose

On March 4, 2014, the Subcommittees on Oversight and Research & Technology will hold a joint hearing titled, *Can Technology Protect Americans from International Cybercriminals?*

In light of the recent cyber-crimes against the University of Maryland database and the retail store Target and others over the past holiday season, this hearing will examine the current state of technology and standards to protect Americans from international cybercriminals. The hearing will also address the evolution of cyber-attacks against the U.S. industry from rogue hackers to sophisticated international crime syndicates and foreign governments, including the origination point of many of these crimes.

Witnesses

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Bob Russo**, General Manager, Payment Card Industry Security Standards Council, LLC
- **Mr. Randy Vanderhoof**, Executive Director, Smart Card Alliance
- **Mr. Justin Brookman**, Director, Consumer Privacy, Center for Democracy & Technology
- **Mr. Steven Chabinsky**, Senior Vice President of Legal Affairs, CrowdStrike, Inc.; Former Deputy Assistant Director, Federal Bureau of Investigation – Cyber Division

Background

The recent cyber-crimes perpetrated against retailers Target, Neiman Marcus, Easton-Bell Sports, Michaels and others, appear to be cases of 'RAM scraper,' which is a type of memory-scanning malicious software that enables cybercriminals to grab "unencrypted data during the split-second when it's vulnerable: while it's being processed at the register."[1] In the

[1] John Zorabedian, "Target, Neiman Marcus Card Data Thefts, RAM Scraper Malware, and You," Sophos Blog, January 24, 2014, available at: http://blogs.sophos.com/2014/01/24/target-neiman-marcus-card-data-thefts-ram-scraper-malware-and-you/; hereinafter Sophos Blog.

Target breach, the malware appears to have been "loaded into point-of-sale (POS) terminals, where the unencrypted credit card numbers were skimmed."[2] Under current Payment Card Industry-Data Security Standard (PCI-DSS) rules:

> *"[A]ll payment information must be encrypted when it is stored on the PoS system as well as when it is being transferred to back-end systems. While attackers can still steal the data from the hard drive, they can't do anything with it if it is encrypted, and the fact that the data is encrypted while traveling over the network means attackers can't sniff the traffic to steal anything.*
>
> *This means there is only a small window of opportunity—the instant when the PoS software is processing the information—for attackers to grab the data. The software has to temporarily decrypt the data in order to see the transaction information, and the malware seizes that moment to copy the information from memory."*[3]

After that, the data is "whisked off to be sorted into bundles and put up for sale on the black market, and printed onto phony cards used by crooks to buy goods at stores."[4]

In January, the FBI distributed a "confidential, three-page report to retail companies"[5] describing risks posed by RAM scraper malware that infects POS systems, including "cash registers and credit-card swiping machines found in store checkout aisles."[6] In this memo, the FBI said it has uncovered around twenty cases of cyber-attacks against retailers in the past year that utilized similar methods to those uncovered in the Target incident – with more expected in the near term.[7]

The "accessibility of the malware on underground forums, the affordability of the software, and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cybercrime attractive to a wide range of actors."[8]

These recent cyber-crimes against retailers raise concerns about whether and how Payment Card Industry-Data Security Standards were followed, or if these standards are adequate to ward off such cyber-attacks. If the voluntary standards are not sufficient, how might new technologies and processes defend against such cyber-attacks?

---

[2] Ibid.
[3] Fahmida Rashid, "How RAM Scraper Malware Stole Data From Target, Neiman Marcus," SecurityWatch, January 14, 2014, available at: http://securitywatch.pcmag.com/business-financial/319767-how-ram-scraper-malware-stole-data-from-target-neiman-marcus.
[4] Sophos Blog, *supra*, note 1.
[5] Jim Finkle and Mark Hosenball, "Exclusive: FBI Warns Retailers to Expect More Credit Card Breaches," Reuters, January 23, 2014, available at: http://www.reuters.com/article/2014/01/23/us-target-databreach-fbi-idUSBREA0M1UF20140123.
[6] Ibid.
[7] Ibid.
[8] Ibid.

Technology

Chip and PIN or EMV (Europay, MasterCard and Visa) Cards

EMV cards contain a computer chip which is a microprocessor embedded in the card that is tamper- and copy-resistant and provides stronger security and protection against fraud by generating a different cryptographic authentication every time it is used. These cards, therefore, are also referred to as "chip cards" or "smart cards."

The payments industry and retailers have been working together toward a goal of updating credit and debit card security by October 2015. After that date, there will be a liability shift for whoever is utilizing the least secure technology for consumers. In other words:

> *"[I]f a merchant is still using the old system, they can still run a transaction with a swipe and a signature. But they will be liable for any fraudulent transactions if the customer has a chip card. And the same goes the other way – if the merchant has a new terminal, but the bank hasn't issued a chip and PIN card to the customer, the bank would be liable."*[9]

While EMV or chip and PIN cards are not the silver bullet to prevent all cyber-crimes, this technology has been shown to prevent many such crimes.

Key Participants and Considerations

National Institute of Standards and Technology (NIST)

NIST develops guidelines, standards and technology to help protect domestic IT systems and infrastructure from cyber-attacks and threats to the confidentiality, integrity, and availability of their information and services through initiatives such as the Framework for Improving Critical Infrastructure Cybersecurity, National Strategy for Trusted Identities in Cyberspace (NSTIC), and the National Vulnerability Database (NVD). NIST's work supports smart card development and applications in the federal and private sectors as well as standards established by the payment card industry for the private sector.

Payment Card Industry Security Standards Council (PCI SSC)

Created in 2006, the PCI SSC is a global open body responsible for the "development, management, education, and awareness of the PCI Security Standards,"[10] and for maintaining and promoting the Payment Card Industry security standards. The Council was created by the five major payment card brands: Visa, MasterCard, American Express, Discover and JCB International.

---

[9] Tom Gara, "October 2015: The End of the Swipe-and-Sign Credit Card," The Wall Street Journal, February 6, 2014, available at: http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/.

[10] PCI Security Standards Council, available at: https://www.pcisecuritystandards.org/organization_info/index.php.

Vulnerabilities in merchants' card-processing systems can appear anywhere including "point of sale devices; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmissions of cardholder data to service providers."[11] The PCI Data Security Standard (DSS) applies to "all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with PCI DSS."[12] However, the Council does not enforce penalties for non-compliance; that is left to each individual payment card brand.

Smart Card Alliance

Established in 2001, the Smart Card Alliance is a "multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests heavily in education on the appropriate uses of technology for identification, payment and other applications and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity."[13]

The Alliance is made up of over 200 members from around the world, including "participants from financial, government, enterprise, transportation, mobile telecommunications, healthcare, and retail industries."[14] Through a combination of educational, industry and member-driven efforts, the Alliance focuses on providing the public with information about smart cards, how they work, and the future of this technology.

Center for Democracy & Technology (CDT)

CDT's mission is "to conceptualize and implement public policies that will keep the Internet open, innovative, and free."[15] Principles of the Center include:

- **Preserving the Unique Nature of the Internet**: The open, decentralized, and user-controlled nature of the Internet creates unprecedented opportunities for innovation, democratic participation and human development.
- **Enhancing Freedom of Expression**: CDT fights for the right of individuals to communicate, publish and access an unprecedented array of information on the Internet. We oppose governmental censorship and other threats to the free flow of information. We believe that technology tools—not government controls—are the best way to allow families and individuals to make choices about the information they receive on the Internet.
- **Protecting Privacy**: Maintaining privacy on the Internet requires a mix of laws, corporate policies and technology tools giving people control of their personal information.

---

[11] PCI DSS Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard, Version 2.0 (October 2010).
[12] Ibid.
[13] Smart Card Alliance, available at: http://www.smartcardalliance.org/pages/alliance.
[14] Ibid.
[15] Center for Democracy & Technology, available at: https://www.cdt.org/about.

- **Limiting Government Surveillance**: CDT advocates for stronger legal standards controlling government surveillance, to keep pace with the growing exposure of personal information as digital media have become central to our lives.[16]

International Crime Syndicates

The Target retailer hack has been traced back to a "17-year-old hacker from St. Petersburg named Sergey Taraspov. He allegedly wrote the program and then sold it for $2,000 on a Russian website. At least 40 different criminals, most from the former Soviet Union, used this software to attack American retailers."[17]

Russia and Russian-speaking countries have typically been responsible for increasingly sophisticated cyber-attacks around the world. With an estimated "annual turnover of more than $2 billion a year, the Russian cybercrime industry is the source of at least a third of all viruses, Trojans, and other malicious software, or malware, sent around the world." There are many reasons why Russia "is the leading producer of malicious software,"[18] including inadequate salaries for computer engineers and an unlimited supply of "organized crime with strong ties to the government, which tends to look the other way when it comes to cybercrime."[19] Most Russian hackers are not prosecuted if they focus their crimes against other countries.

Two years ago, former FBI Director Robert Mueller made the following comment at the annual RSA cyber security conference, "Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country."[20]

Related Legislation

On March 14, 2013, the Committee passed H.R. 756, the Cybersecurity Enhancement Act and H.R. 967, the Advancing America's Networking and Information Technology Research and Development Act by voice votes. On April 16th, the House overwhelmingly and in a bipartisan manner passed both bills. However, since then, the Senate has taken no action on these bills.

H.R. 756 the Cybersecurity Enhancement Act

H.R. 756 coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create

---

[16] Ibid.
[17] Ben Plesser, "Skilled, Cheap Russian Hackers Power American Cybercrime," NBC News, February 5, 2014, available at: http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371. Feb 5, 2014
[18] Ibid.
[19] Ibid.
[20] Stacy Cowley, "FBI Director: Cybercrime Will Eclipse Terrorism," CNNMoney, March 2, 2012, available at: http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/.

new technologies and standards that better protect America's information technology systems. To improve America's cybersecurity abilities, this bill strengthens activities in four areas:

1) Strategic planning for cybersecurity research and development needs across the federal government;
2) Basic research at NSF, which we know is important to increasing security over the long-term;
3) NSF scholarships to improve the quality of the cybersecurity workforce; and
4) Improved research, development and public outreach organized by NIST related to cybersecurity.

H.R. 967, the Advancing America's Networking and Information Technology Research and Development Act

H.R. 967 provides the coordinated R&D efforts necessary to improve cyber and data security nationwide. The bill convenes an interagency working group to identify cloud computing research gaps and examine the potential for using the cloud for federally funded research. The bill also formally codifies and stresses the role of the National Coordination Office (NCO) and implements several recommendations from the President's Council of Advisors on Science and Technology (PCAST) 2007 and 2010 assessments, including:

1) Improving program planning and coordination through strategic planning and an Advisory Council with appropriate policy and technical expertise;
2) Rebalancing portfolios to focus less on short-term goals and more on large-scale, long-term, interdisciplinary research with the potential to make significant contributions to society and U.S. competitiveness;
3) Codifying the National Coordination Office's (NCO) creation of a workshop to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems with participants from universities, industry, and federal laboratories.

Key Questions

- What is the relationship between the federal government and the private sector on issues related to cybersecurity?
- How can the federal government best help and support the private sector to protect its sensitive data?
- How will a transition to EMV chip cards likely impact cyber-attacks against U.S. industries?
- How have the nature and origin of cyber-attacks against the U.S. industry evolved over the past couple of decades?
- Do federal law enforcement agencies have the technology resources and tools they need in their pursuit of international cybercriminals?
- Can new technologies better protect Americans from international cybercriminals?