Prepared Testimony

Phillip J. Smith
Senior Vice President
Trustwave Holdings, Inc.

Hearing On

"Protecting Consumer Information: Can Data Breaches Be Prevented?"

Before The

U.S. House of Representatives
Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

Wednesday, February 5, 2014

2123 Rayburn House Office Building

Good morning, Chairman Terry and Ranking Member Schakowsky, Sub-Committee Members, staff, ladies and gentlemen. I want to thank you for requesting that I, on behalf of Trustwave, provide witness testimony on this important issue related to data breaches in our financial systems and more specifically, our payments industry.

By way of background, I am both a former Special Agent with the United States Secret Service and a Senior Trial Attorney in the Department of Justice's Terrorism and Violent Crime Section (now known as the Counterterrorism Section). My law enforcement experience in this area includes the investigation and prosecution of credit card fraud, access device fraud and counterfeiting. I left the Justice Department in July of 2000 to join Trustwave, a global information security and compliance services and technology company headquartered in Chicago. I currently serve on Trustwave's executive team as Senior Vice President of Government Solutions. In addition to early operational roles which include supervising our advanced research and ethical hacking practice, I served as General Counsel for the first 12 years with Trustwave.

Businesses and government agencies hire Trustwave to help them fight cybercrime, protect their sensitive data and reduce security risks**.** Trustwave has customers—ranging from some of the world's largest, multinational companies to small- and medium-sized businesses—in 96 countries. We specialize in a variety of areas: compliance and risk management, managed and cloud-based security services, as well as threat intelligence, ethical hacking and security research. We also train law enforcement on how to investigate network intrusion and data breach cases.

Today, I want to offer our observations and recommendations related to data breach and broader information security trends. It's important I note that as a company we do not comment or speculate on specific data breaches, and as such we will not be offering testimony today specifically related to specific companies involved in the latest string of data breaches. However, I believe our company's experience in investigating thousands of data breaches over the past few years, augmented by our ongoing security research and the threat intelligence gleaned from our large, global client footprint, will be of value to you and the industry as a whole.

I'd like to start with some of the macro-level trends we're seeing. In today's Internet-connected world, security is more complex than ever. Hackers are targeting businesses of all sizes and across all industries. There is a growing pool of attack vectors from which to choose, including what we now consider a basic business tool: the web, as well as emerging technologies like mobile devices and appliances (also known as "bring-your-own-device" or BYOD), social media and the cloud. Businesses also have huge amounts of information moving through their networks and applications and stored on their databases, meaning there is more data than ever to protect. Threats are growing more hostile and outpacing traditional security technologies like antivirus and firewalls. Budgets are also tight, and building and retaining a skilled security team can be challenging. According to a 2013 Frost & Sullivan Market Study, 56 percent of respondents believed there is a workforce shortage in the IT industry, compared to just two percent who believe there is a surplus. The gap is a result of simple economics—the demand has surpassed the supply. All of these factors leave in-house IT teams facing mounting pressures to ensure information security.

More specifically, I will also highlight:

- How cardholder data is being stolen through malware
- The value of the Payment Card Industry Data Security Standard (PCI DSS)
- Why businesses must go beyond PCI DSS compliance for increased security and technologies that can help.

Each year, our company publishes statistics and other observations from real-world data breach investigations in our **Trustwave Global Security Report**. The report is publicly available at www.trustwave.com/GSR. The focus of our report is around cybercrime. As our report states, attacks are carried out by professional criminals and most of them follow logical patterns of attack consisting of four common elements:

- **Infiltration** - Attackers must first find a way to penetrate an organization's environment
- **Propagation -** Pivoting from the initial point of entry to go after specific systems within an organization's network that contains sensitive data
- **Aggregation** - Identifying and collecting that sensitive data
- **Exfiltration** – Moving that data to a system (a computer or network) controlled by the attacker.

The 2013 Trustwave Global Security Report highlights data our experts analyzed from the more than **450 data breach/incident response investigations, thousands of penetration tests, millions of website and web application attacks and tens of billions of events** gathered through our security and risk assessments, managed security services and our other forms for threat intelligence including our advanced security research during 2012. The report reveals the threats and vulnerabilities businesses face. Specifically:

- The **retail industry was the top target** for data breaches in 2012 making up 45% of our investigations. Food & beverage was the second most targeted industry followed by the broader hospitality industry.
- **Cardholder data** was the primary data type targeted by attackers. There is a well-established underground marketplace for stolen payment card data.
- **Mobile malware increased 400%** in 2012. "Malware," which is short for "malicious software" is used to exploit vulnerabilities in computer systems, gather sensitive information, or gain access to private computer systems for a specific purpose—normally cybercrime.
- Out of more than 450 data breaches we investigated, the United States was the top victim location. **73% of victims were located in the U.S.**
- In 2012, almost all Point-Of-Sale (POS) breach investigations involved, what's known as, "targeted malware." That's when malware is designed for a specific computer system, business or computer user. **SQL (Structured Query Language) injection and remote access** made up 73% of the infiltration methods used by criminals. Other commonly used methods were **Blackhole exploit kits**, **malicious PDF files** (61% targeted Adobe Reader users) and "**memory scraping**." Criminals planted malware on users' machines by using all of these infiltration methods.
- It took businesses an average of **210 days to detect a breach**. Most victim organizations took more than 90 days to detect the intrusion, while 5% took more than three years to identify criminal activity.
- Only 24% of victim organizations detected the intrusion themselves. Most were informed by law enforcement or another regulatory body.
- **Web applications** emerged as the **most popular attack vector**; e-commerce sites being the most targeted asset.
- Users are continuously using weak passwords with "**Password1"** being the most common password of choice since it meets the bare minimum password requirement typically mandated by policies enforced by IT administrators. Weak default passwords and password requirements are a big problem.

How card data is being stolen

As I mentioned, most breaches follow the same patterns of attack: using infiltration, propagation, aggregation and exfiltration. Here's a breakdown of each step:

- **Infiltration—**Criminals get inside business systems by taking advantage of a variety of weaknesses—whether through web applications, social engineering, the web, zero-day vulnerabilities or remote access tools. For example, if a restaurant owner uses an IT service provider in the next state, the service provider might not be physically able to be in front of the restaurant's computer systems when action is required. So, using remote access tools, he accesses the restaurant's systems remotely. Attackers can enter the system using the same remote access tools but they also need a username and password. Oftentimes, businesses will not change their usernames and passwords when setting up their POS devices. This allows attackers to identify the POS default credentials or IT provider shared credentials and gain unauthorized access.
- **Propagation—**Once attackers gain access, they need to move from the point of infiltration to the systems that store, process, or transmit the desired data such as payment card data and other customer information. Since the attackers already have the administrative credentials, this step is often trivial.
- **Aggregation—**This is where the deployment of malware takes place. Attackers use custom malware, designed to identify cardholder data, and either encrypt or encode it, and place it in an output (or a dump) file. Custom malware does this automatically and without any visible service interruption to legitimate business activity.
- **Exfiltration—**Exfiltration can take place either automatically through the malware or the attackers will have to come back and get the data the same way they got in. Encrypted or encoded data is sent to a system controlled by the attacker. The stolen data moves undetected and is subsequently prepared to sell on the black market.

Payment Card Industry Security Standards Council (PCI SSC) and the Data Security Standard (PCI DSS)

The payments industry formed the Payment Card Industry Security Standards Council (PCI SSC) which is responsible for developing and administrating the Payment Card Industry Data Security Standard (PCI DSS) for any entity that stores, processes or transmits cardholder data. Here is our position on PCI DSS:

- The **PCI DSS plays a critical role** when it comes to data security.
- The standard has **increased awareness** surrounding data security.
- In today's environment, in which the threat landscape is more complex than ever and new business-improvement technologies are introduced everyday—keeping up with and complying with the standard simply isn't enough.
- A common misconception is that PCI was designed to be a catch-all for security. We believe the **PCI DSS serves as a baseline** for security, giving businesses guidelines for basic security controls to protect cardholder and personal data. Without PCI DSS, countless businesses would likely have fewer security controls (if any) than they do today.
- Organizations can improve their security posture by first understanding that the **PCI DSS is the floor, not the ceiling, when it comes to security**. While the PCI DSS helps businesses deploy some essential security controls, it doesn't cover security around every attack vector, such as security surrounding targeted malware, mobile devices and cloud technology.
- If organizations use a **defense-in-depth approach to security** consisting of multiple layers of defense, detection, response and ongoing testing, they can better protect themselves against attacks and inherently maintain compliance with the PCI DSS.
- Another standard for compliance, the **Payment Application Data Security Standard (PA-DSS)**, is also a good baseline. However, it does not include or require holistic manual penetration

testing against the entire Point-of-Sale platform (hardware, custom software and operating system)—testing we believe is important.

Going beyond PCI Compliance for increased security

The following are steps businesses can take, whether through policies and procedures or technologies to help prevent malware attacks on their networks, applications and databases. We recommend:

- **Incident response preparedness—**Businesses should implement an incident response plan that includes advanced detection techniques, containment strategies and response scenarios. These elements will help them see, stop and respond to an attack. Incident response plans can drastically reduce the impact of a breach on a business so that it can get back quicker to "business-as-usual."
- **Security awareness training—**Businesses should regularly provide security awareness training to all employees, including contractors and temporary workers. Executives and business leaders are also prime targets, so training should be required for anyone who has access to private information. Training can help them follow security best practices to reduce the risk of infiltration.
- **Strong passwords—**If a criminal is going to access a system remotely, he must first know where the system is located (the IP address), the appropriate remote administration protocol and login credentials (username and password). That's why strong passwords play a vital role in helping prevent a breach. Strong passwords consist of a minimum of seven characters and should include a combination of upper and lower case letters, symbols and numbers. We recommend using "passphrases" such as "Myd0gisn@medBuck." Passphrases are both easier to remember and harder to crack.
- **Two-factor (or two-step) authentication—**Businesses should use two-factor authentication for employees who access the network. Two factor authentication forces users to verify their identity with information other than simply their username and password, like a special constantly-changing code sent to a user's mobile phone.
- **Business-wide security risk assessments and ongoing penetration testing—**Regular security risk assessments can help businesses identify where they store sensitive data and if that data is vulnerable to an attack. Frequent penetration testing, where ethical hackers use automated and manual tools to "break in" to business systems (at the request of that business), can help businesses identify and eliminate vulnerabilities that become the intrusion points of almost any breach.
- **Database scanning and security—**Databases hold a treasure trove of business data yet too often database security is overlooked. Businesses assume if their networks and applications are secure, so is their database. This assumption is false—and dangerous. Databases need constant vulnerability scanning and their own protection.
- **Certificates** and **firewalls—**Businesses should use certificates to further restrict remote access. Certificates help ensure the identities of both the server and user are trusted before granting the user access. Businesses should also install firewalls to help restrict any traffic that is not critical to their business.
- **Web application security—**Web applications are a high-value target for attackers because they are easily accessible over the Internet. Web applications are often a business's "front door" and are often connected to systems that contain private data. While monitoring 200,000 websites, our researchers found 16,000 attacks occurred on web applications per day. That is why businesses need to adopt protection that includes the ability to detect application vulnerabilities and prevent web application threats.
- **Advanced anti-malware protection—**Attackers often use compromised websites, or links to these sites in emails, as the point of entry to get malware on a business's network. A recent Osterman Research survey of security professionals showed that malware has infiltrated 74

percent of organizations through the web during the past year. To defend against these common attack vectors, businesses should deploy security "gateways." I must stress this is not anti-virus technology. Gateways specifically help protect businesses in real-time from threats like malware, zero-day vulnerabilities and data loss, and can help organizations use things like web and cloud applications securely.

- **Augment in-house security expertise—**Since security has become a more time-consuming, skills-specific, sometimes daunting task for many in-house IT teams, more businesses are augmenting their staff by partnering with an outside team of security experts that helps ensure more effective security tools are installed and running properly in order to prevent a data compromise. Managed security services help IT professionals maintain a higher state of security so they can focus on their primary jobs of IT projects that generate revenue for their employers.
- **End-to-end encryption—**Persistently encrypting cardholder data can help render data unreadable to unauthorized third parties, such as attackers, who try to steal sensitive information, such as credit card numbers. Encryption is another layer of defense against these malicious hackers or an unauthorized third party because even if the data is accessed they would be unable to read it. We believe this emerging technology, along with other security controls, shows great promise.
- **"Chip and PIN"—**Chip and PIN helps authenticate transactions and helps prove that the cardholder is the person requesting the transaction. In this scenario, the combination of an embedded microchip on a payment card and a PIN code replaces the traditional combination of the magnetic stripe data and signature. Layering this authentication method with other layers of security, such as end-to-end encryption can greatly reduce the risk of a card data compromise for brick and mortar merchants, or really anywhere that a card is present for the transaction.
- **Segmentation—**Currently the PCI DSS does not require businesses to segment or separate their systems that contain cardholder data. We recommend businesses go beyond PCI and separate their systems that contain critical data to make it more difficult for a criminal to access the target network. When businesses segment their systems, it causes the attacker to have to circumvent a second set of security controls.
- **Mobile device payment systems—**To conduct payment card transactions, some merchants may be using mobile devices that are consumer grade products with an attached card reader. These devices are designed for ease-of-use but sometimes contain serious security vulnerabilities. While the PCI DSS doesn't address these kinds of mobile devices, the standard does apply to any merchant that stores, processes, and transmits cardholder data, so the onus is on business leaders to make sure these devices comply.
- **Third-party vendor security checks—**When partnering with third-party IT providers, we recommend businesses require their provider use or do many of the items I've already discussed. Additionally, we recommend they have detailed and locked-down security policies, perform ongoing and regular penetration testing, demonstrate appropriate remote access controls, ensure software and hardware vendors are consistently patched and updated for security vulnerabilities, and that data is isolated from other customers in a shared, cloud environment.

Conclusion

I would like to thank Chairman Terry and Ranking Member Schakowsky, Sub-Committee Members, and staff for the opportunity to appear today on this important issue facing our businesses, our payment systems and our citizens. I brought several copies of the 2013 Trustwave Global Security Report and included a link to download the report as well as other information related to today's security threat landscape. We encourage the Members and their staff to review this information. I would be more than happy to address any questions related to my testimony.

Additional Information

2013 Trustwave Global Security Report
http://www.trustwave.com/GSR

Infographic: New data reveals extent of the malware problem
Trustwave Blog & Osterman Research
https://www.trustwave.com/trustednews/2014/01/infographic-new-data-reveals-extent-malware-problem#sthash.CrkMGzlU.dpbs

How security professionals are dealing with web, email and social threats
Trustwave Blog & Osterman Research
https://www.trustwave.com/trustednews/2014/01/trustwave-qa-how-security-professionals-are-dealing-web-email#sthash.zJghIaIj.dpuf

Two million stolen passwords: How to protect yourself
Trustwave Blog
https://www.trustwave.com/trustednews/2013/12/two_million_stolen_passwords_how_to_protect_yourself#sthash.AA1LaupH.dpuf

Inside a hacker's playbook: 10 targeted techniques that will break your security
Trustwave E-book
https://www2.trustwave.com/cpn-hackers-playbook-2013-sm.html

Infographic: The high cost of BYOD
Trustwave Blog
https://www.trustwave.com/trustednews/2013/04/infographic-the-high-cost-byod#sthash.WRSY7hZq.dpbs

Infographic: Keep the bad stuff out and the good stuff in
Trustwave Blog
https://www.trustwave.com/trustednews/2013/03/keep-the-bad-stuff-out-keep-the-good-stuff-in#sthash.yNtU3ckc.dpbs

Trustwave Reveals Increase in Cyber Attacks Targeting Retailers, Mobile Devices and E-Commerce
Trustwave Blog
https://www.trustwave.com/trustednews/2013/02/trustwave-reveals-increase-cyber-attacks-targeting-retailers-mobile#sthash.9S5zNEcG.dpuf

Executive Guide for Law Enforcement
Trustwave
https://www.trustwave.com/leoguide

Media Inquiries
Abby Ross
Media Relations
Trustwave
aross@trustwave.com
312-873-7648

Other Inquiries
Cas Purdy
Corporate Communications
Trustwave
cpurdy@trustwave.com
312-470-8703