Prepared Testimony and
Statement for the Record of

Jeff Greene
Senior Director, Global Government Affairs & Policy
Symantec Corporation

Hearing on

Securing Consumers' Credit Data in the Age of Digital Commerce

Before the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

November 1, 2017

Chairman Latta, Ranking Member Schakowsky, my name is Jeff Greene and I am the Senior Director, Global Government Affairs and Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and last year I supported the President's Commission on Enhancing National Cybersecurity. Prior to joining Symantec, I served as Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues.

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries and is comprised of more than 98 million attack sensors, which record thousands of events every second. We maintain nine Security Response Centers and six Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape. Symantec also provides identity theft protection to over 5 million Americans through LifeLock, a leading provider of identity theft protection and comprehensive remediation services for consumers.

Cybersecurity is the foundation of the age of digital commerce, and we are therefore pleased to see the Committee's continued focus on this subject, and appreciate the opportunity to provide our insights. The threat to consumers, and in particular their personal and credit data, is best understood in the context of the larger cyber threat landscape. In my testimony I will briefly discuss the broader cyber threat environment and then discuss securing enterprises and consumers against an evolving threat.

I. The Current and Emerging Cyber Threat Landscape - Overview

Cyber attacks reached new levels in the past year, which was marked by multi-million dollar virtual bank heists, explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, a record number of identities exposed in data breaches, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices. Yet while the attacks caused unprecedented levels of disruption and financial loss, perhaps the most striking change over the past year is that in many cases the attackers used very simple tools and tactics. During 2016, valuable Zero-day vulnerabilities and sophisticated malware was used more sparingly than in recent years. Instead, attackers increasingly attempted to hide in plain sight. They relied on straightforward approaches, such as spear-phishing emails and "living off the land" by using tools on hand, such as legitimate network administration software and operating system features. Yet despite this trend away from sophisticated attacks, the results were extraordinary, including:

- Over ***1.1 billion*** identities exposed in 2016;
- ***Power outages*** in the Ukraine;
- Over ***$800 million*** stolen through Business E-mail Compromise (BEC) scams over just a ***six month period***;
- ***$81 million*** stolen in one bank heist alone;
- A ***tripling*** of the average ransomware demand;
- Average time-to-attack for a newly connected Internet of Thing device down to ***two minutes;***
- And of course, the theft of over **145 million identities** from Equifax earlier this year.

Cyber attacks involving sabotage have traditionally been rare, but during 2016 we saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in the attacks on the Ukraine in January and again in December, resulting in power outages. Additionally, the disk-wiping Trojan Shamoon reappeared after a four-year absence and was used against multiple

organizations in Saudi Arabia. Previously, Shamoon was used in highly destructive attacks against Saudi and other Middle Eastern energy companies, and press reports linked it to Iran.

On the financial side, cyber criminals have broadened their targets. While in the past they mainly targeted individual bank customers, raiding accounts or stealing credit cards, over the past year we saw a new breed of attacker with bigger ambitions. We now see groups targeting the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. For instance, the Lazarus group stole $81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials. And while the attackers did make off with $81 million, it could have been much worse as they attempted numerous other transfers that were detected because a spelling error in a recipient's name raised suspicions that led to the transactions being suspended.

Criminals also target major corporations, and have found success stealing huge sums of money through relatively unsophisticated means. For instance, business email compromise (BEC) scams – which rely on little more than carefully composed spear-phishing emails – continue to cause major losses. Also known as CEO fraud or "whaling," BEC scams are a form of low-tech financial fraud where spoofed emails are sent to an organization's financial staff by scammers pretending to be the CEO or senior management. The scammers then request a large money transfer. These scams require little technical expertise but can reap huge financial rewards for the criminals – and significant losses for the companies involved. Earlier this year the FBI issued an alert noting that "[b]etween January 2015 and December 2016, there was a 2,370% increase in identified exposed losses" from BEC scams. The FBI estimated that over $5 billion was lost to BEC scams between October, 2013 and December, 2016.[1] In 2017, approximately 8,000 businesses have been targeted by BEC scams each month, and receive on average 5.2 BEC scam emails.[2]

New technology, however, is also a target for attackers, and in late 2016 we saw the first major incident originating from IoT devices, the Mirai botnet, which was composed of routers, digital video cameras, and security cameras. Weak security – in the form of default and hard-coded passwords – made these devices easy pickings for attackers. After compromising millions of devices, the attackers controlled a botnet big enough to carry out the largest DDoS attacks ever seen. Just over a year ago the combined power of these compromised devices led to brief outages at some of the most popular websites and online services in the world. Mirai's impact was further magnified when the developer released the source code for the malware, which led to copycat efforts by other groups.[3]

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we now see. Criminal gangs engaged in indiscriminate campaigns involving massive volumes of malicious emails that in some cases overwhelmed organizations by the sheer volume of ransomware-laden emails alone. Attackers are demanding more and more from victims, and the average ransom demand *more than tripled* in 2016, from $294 to $1,077. The number of new ransomware families also more than tripled to 101, from 30 in both 2014 and 2015. The volume of attacks increased as well. Detections were up 36% percent from 2015, and by December we were seeing almost twice the daily volume that we observed in January.

---

[1] FBI Public Service Announcement, *Business E-mail Compromise – E-mail Account Compromise the 5 Billion Dollar Scam, May 4, 2017;* https://www.ic3.gov/media/2017/170504.aspx#fn3

[2] ISTR Email Threats 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf

[3] See *Symantec Internet Security Threat Report,* XX!!, April 2017 pp. 68

Ransomware has become a jack-of-all-trades tool for cybercriminals. Originally, criminals targeted primarily individual users with ransomware, trying to extract a few hundred dollars per victim. This continues to this day – and ransomware is an incredibly profitable venture for cybercriminals. Unfortunately, we have seen attackers using ransomware in other, more troubling ways. First, criminals are now using ransomware as part of sophisticated, multi-staged attacks on corporations that seek tens of thousands of dollars (or more) in ransom. Second, some destructive attacks have been disguised as ransomware – the malware encrypts crucial data on the victim's computer, effectively destroying it, and no decryption key is held by the attacker. So while it appears to be ransomware to the victim, the intent was always destruction because the attacker has no ability to decrypt the data. Finally, we are seeing groups linked to nation states using ransomware to steal funds – specifically, the Wannacry outbreak in May, which we linked to the Lazarus group.

II. Methods Attackers Use to Compromise Systems - Inside the Attacker's Tool Kit

Successful attacks share a common factor – a compromised device. From this one computer, attackers often are able to move within a system until they achieve their ultimate goal. But the threshold question is how do they get that foothold – how do they make that initial compromise that allows them to infiltrate a system?

We frequently hear about the sophistication of various attackers and about "Advance Persistent Threats" or "APTs," but the discussion of cyber attacks – and of cyber defense – often ignores the psychology of the exploit. Most attacks rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

Spear phishing, or customized, targeted emails containing malware, are still the most common form of attack. Attackers harvest publicly available information and use it to craft an email designed to dupe a specific victim or group of victims. The goal is to get victims to open a document or click on a link to a website that will then try to infect their computers. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations and individuals do not have up-to-date security or properly patched operating systems or software. And many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

Social media is an increasingly valuable tool for cyber criminals in two different ways. First, it is particularly effective in direct attacks, as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. Thus, attackers target social media accounts and then use them to "like" or otherwise promote a posting that contains a malicious link. But social media is also widely used to conduct reconnaissance for spear phishing or other highly targeted attacks as it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his or her guard down.

One common web-based attack is known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. They do so by compromising legitimate websites that their targets are likely to visit and modifying them so that they will surreptitiously try to infect visitors. For example, one attacker targeted mobile application developers by compromising a site that was popular with them. Cybercriminals gained control of these websites through many of the same tactics described above – spear phishing and other social engineering attacks on the site managers, developers, or owners. Many of these websites were compromised through

known attack vectors, meaning that good security practices could have prevented them from being compromised.

III. Protecting Against an Evolving Threat

Cybersecurity is about managing risk, whether at the individual or the organizational level. Assessing one's risk and developing a plan is essential. For the individual, the Federal Trade Commission's website is an excellent starting point for doing so.[4] The website provides educational resources for how to better protect your identity and privacy online as well as helpful tools to help you report and recover if your personal information is ever stolen. Similarly, we offer many tools and reference materials on our Norton and LifeLock websites.

For organizations of any size, the National Institute of Standards and Technology's Cyber Security Framework[5], developed by industry and government in 2014 and in which Symantec was an active contributor, provides a solid structure for risk management. It lays out five core cybersecurity functions (Identify, Protect, Detect, Respond and Recover) that all organizations can use to plan for managing cyber events and protecting against data breaches, as well as useful references to international standards. As detailed below, good security starts with the basics and includes measures specific to one's needs.

a. Protecting the Enterprise

Attacks are getting more sophisticated, but so too are security tools. Security still starts with basic measures such as strong passwords and up-to-date patch management. But while these steps may stop some older, simpler exploits, they will be little more than a speed bump for even a moderately sophisticated attack – and will do little to slow a determined, targeted attack.

Effective protection requires a modern security suite that is being fully utilized. An attack requires access, and attackers are increasingly relying on stolen credentials to gain their footholds. Deploying effective multi-factor authentication is essential to denying access to the would-be attacker. To block advanced threats and zero day attacks, sophisticated machine learning and advanced exploit detection and prevention technologies are necessary. This includes tools for detecting encrypted malware, as attackers are increasingly using encryption in an effort to bypass common security tools. Automated security tools learn how to identify attacks, even ones that have never been seen before. It is also increasingly critical to use big data analytics to evaluate global software patterns to create real-time intelligence. Today these analytics are able to identify and block entirely new attacks by evaluating how they are distributed and their relationships with other devices and other files.

Data protection is equally important, and a comprehensive security program includes data loss prevention (DLP) tools that index, track, and control the access to and movement of huge volumes of data across an organization. Perhaps most importantly, DLP tools will prevent that data from moving outside an organization. Organizations should also use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key.

Device-specific protections are also important. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. In the IoT world, there are authentication, encryption, and endpoint protection tools that are designed to run on

[4] http://www.consumer.ftc.gov/topics/privacy-identity
[5] http://www.nist.gov/cyberframework/

small and low power devices. These tools can protect everything from a connected vehicle to the small sensors built into a bridge or that monitor critical machinery.

Good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving, and security must as well.

b. Protecting the Individual

Consumers need to secure both their devices (computers, tablets, phones, anything "connected") and their identities. Device security used to be relatively simple –access and password management, patching and updating software, and employing modern security tools. These are still the pillars of good security, and there is significant overlap with the enterprise security steps laid out above. Individuals, like enterprises should employ multi-factor authentication whenever it is available, and in particular on financial or highly personal accounts. Individual security also includes caution when opening attachments, going to unknown links, or enabling macros in common software platforms. While this may seem like old news, the unfortunate reality is that criminals are always coming up with new ways to trick their victims into visiting a bad site, opening a malicious attachment, or otherwise unwittingly facilitating an attack.

The good news is that individuals *can* protect their computers and devices. Many scams directed at individuals take advantage of older, known vulnerabilities and tactics, and will not work on computers (or phones or tablets) that are updated and protected by modern security tools. Connected devices such add a new dimension to home security, but they too can be protected. First and foremost, consumers should make sure that they change any preset, default passwords on *anything* that connects to the internet. Finally, we all should stop and think before we purchase a connected device, or before we connect an internet-enabled device that we have purchased. Still, there will be some devices that simply cannot be secured – either because they lack the power to run security tools or because it is simply unavailable. For these home devices, we developed Norton Core™, the first router designed specifically to secure IoT devices, whether a connected appliance or a digital video recorder.[6]

Recent events have made clear, however, that individuals can be victimized by cyber criminals even if they have taken every possible step to protect their devices. And just as consumers can secure their devices, there are things that we all can do to protect ourselves against identity theft. A first step is to check your credit reports to look for accounts or activity that you do not recognize, which could indicate identity theft. You can do this for free by visiting annualcreditreport.com. Another option is to consider placing a fraud alert on your files, which warns creditors that you may be a victim of identity theft. If you do so, creditors are required to make a reasonable effort to verify that anyone seeking credit in your name is, in fact, you. You can also place a credit freeze on your credit files, which means that potential creditors cannot access your credit report. This makes it less likely an identity thief can open new accounts in your name. Finally, on a regular basis you should monitor your existing credit card and bank accounts and watch for charges or activity you do not recognize. The Federal Trade Commission offers other tips for protecting yourself after a data breach on its website.

Consumers can also obtain credit monitoring services and identity theft protection. Credit monitoring tracks changes to one or more your credit reports, including applications for a new credit card or a loan and can detect suspicious activity. Identity theft protection adds additional layers of protection, typically providing credit file monitoring at one or more of the three credit reporting agencies and sometimes a credit score from one agency or more. Services may include alerts if your personally identifiable information is used in ways that may not show up on your credit report such as commission

[6] *See https://us.norton.com/core*

of a crime or employment fraud. Identity theft protection may also provide restoration services that help victims resolve a variety of identity theft issues.

If you do believe that you are the victim of identity theft, you need to take action. Below are some steps to consider for some of the more common forms of identity theft:

1. If you spot unfamiliar transactions on a bank or credit card account, you could be the victim of **financial identity theft**. Contact your bank or credit card company immediately.
   - If someone has unauthorized access to your bank account, you will of course want to close that account and open a new one with a new account number. You will also want to work with the bank to resolve any fraudulent transactions.
   - If someone has stolen your credit card number, you should contact the issuer to alert them to the fraudulent charges and ask them to close the account and issue you a new card.

2. **Governmental identity theft** occurs when someone fraudulently shares your personal information with the government. One example is tax-related identity theft – for instance, an imposter uses your Social Security number and other personal information to file an income tax return in your name, hoping to obtain a fraudulent tax refund.

   - If you discover that you are a victim of tax-related identity theft, you will need to alert the IRS, the Federal Trade Commission and your local police department (you may need a police report to resolve the issue).
   - You should also contact one of the three major credit reporting agencies to place a "fraud alert" on your credit report, making it more difficult for criminals to open accounts in your name. The credit reporting agency you contact will contact the other two agencies.
   - The IRS also advises these additional steps:
     - Respond immediately to any IRS notice.
     - Complete the IRS Identity Theft Affidavit, Form 14039.

   Another example of governmental ID theft is employment fraud, when someone uses your Social Security number to obtain employment. If you are a victim of employment fraud, the Identity Theft Resource Center (ITRC) suggests that you file a police report and call the Social Security Administration (SSA) in your area. SSA forms can help you correct the fraudulent activity that is now part of your records. You will also need to inform the Internal Revenue Service and your state's internal revenue department, assuming you have a state income tax.

   And if someone is using your Social Security number for tax-related identity theft or employment fraud, they may also be using it for other purposes. It is a good idea to review your credit reports for any fraudulent activity.

3. It is possible also for an identity thief to assume your identity to see a doctor or visit an emergency room. This is called **medical identity theft**. Since your healthcare data could become mingled with your imposter's data, this crime could even threaten your health. The ITRC offers several recommendations, including:

   - Ask for copies of your medical records from the providers where your identity may have been used fraudulently.
   - Ask those same health care providers for a list of those with whom they have shared your protected health information – it may have the same errors.
   - Reach out to any medical facilities asking you for payment for services you did not receive. Tell them this is a case of identity theft or mistaken identity and ask what service was provided.

- File a police report in your local jurisdiction.

Unfortunately, there are numerous other types of identity fraud, and both the FTC and the ITRC provide resources and information for victims.

Conclusion

Citizens are increasingly aware of the cyber risk and the need to take precautions to secure their data and protect their privacy. While we cannot prevent every cyber attack or every data breach, applying cybersecurity best practices and using risk management principles to protect data appropriately can significantly reduce the attack surface and the impacts we see today. Every time someone patches a computer or mobile device, changes a password, or utilizes a modern security suite, he or she is making it more difficult for cybercriminals to operate. Like any other illicit activity, cybercrime will never be completely eliminated, but it can be fought – cybersecurity is a proverbial journey, not a destination. Understanding the threat, how it is changing, and where it is going, is essential if we are going to stay on track in this journey.