Prepared Testimony and
Statement for the Record of

Jeffrey E. Greene
Director of Government Affairs, North America & Senior Policy Counsel
Symantec Corporation

Hearing on

"The IRS Data Breach: Steps to Protect Americans' Personal Information"

Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

June 2, 2015

Chairman Johnson, Ranking Member Carper, my name is Jeff Greene, and I am the Director of Government Affairs for North America and Senior Policy Counsel at Symantec, where I focus on cybersecurity, the Internet of Things, and privacy issues. Prior to joining Symantec, I was Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues. I have also worked on the Committee on Homeland Security in the House of Representatives as a subcommittee staff director and as counsel to the Senate's Special Investigation into Hurricane Katrina. I recently served as the staff co-chair of the "Internet of Things" research subcommittee of the President's National Security Telecommunications Advisory Committee, and am a Senior Fellow at The George Washington University Center for Cyber & Homeland Security and a Senior Advisor at the Truman National Security Project. I also co-chair the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law.

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with 33 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of millions of attack sensors recording thousands of events per second, and we maintain 10 Security Response Centers around the globe. In addition, every day we process billions of e-mail messages and web requests across our 14 global data centers. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The hearing today not only is timely – given the recent high profile data breaches and other cyber attacks – but also is a critically important discussion that will help focus attention on what government, businesses, and individuals can do to protect themselves from similar attacks. In my testimony today, I will discuss:

- The current cyber threat landscape;
- Some common types of attacks;
- How breaches are happening, including the methods criminals are using to steal data; and
- Security measures to protect data and prevent breaches.

The Current Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on data breaches across the spectrum of industries. Breaches impact individuals whose identities have been stolen, the organizations that were compromised, and governments that are seeking ways to set data breach policies and to apprehend the perpetrators. Some of the organizations that suffered significant breaches over the past few years include Anthem Inc., the Internal Revenue Service, the State of South Carolina, Target, Neiman Marcus, Michael's, Home Depot, and Sony, just to name a few.

The recent theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches approached *one billion*. And this is just from known breaches, as many go unreported or undetected. Recent data breaches have touched all

parts of society and across the globe, from governments and businesses to celebrities and individuals' households.

While many assume that breaches are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a recent report from the Online Trust Alliance, 90 percent of last year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.[1] Moreover, some breaches are actually second generation activity – criminals leverage previously stolen personal information to compromise an individual's account.

Statistics from our 2015 Internet Security Threat Report demonstrate that the cyber threats we are facing on a day-to-day basis are growing. More than 348 million identities were exposed in 2014, a number that seems extraordinary until one considers that 550 million identities were exposed in 2013. Over the past two years, twelve breaches exposed more than 10 million identities each – and this does not include some of the major breaches we have heard about in 2015. These breaches expose PII such as names, birth dates, and government ID numbers. Some breaches also exposed other highly sensitive data, such as medical records or financial information.

While the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have damaging consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government.

The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – the criminals generally are looking for some type of financial gain, the hacktivists are seeking to promote or advance some cause, and the state actors can be engaged in espionage (traditional spycraft or economic) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Common Types of Attacks

Distributed Denial of Service ("DDoS")

Distributed denial-of-service (DDoS) attacks attempt to deny service to legitimate users by overwhelming the target with activity. The most common method is to flood a server with network traffic from multiple sources (hence "distributed"). These attacks are often conducted through

[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

"botnets" – armies of compromised computers that are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."[2]

DDoS attacks have grown larger year over year and in 2014 some attacks reached 400 gigabits per second, a previously unimaginable volume of data. This is roughly equivalent to blasting a network every second with the data stored on more than 10 DVDs. In the past few years we have seen attacks go from the equivalent of a garden hose to a fire hose to the outflow pipes of the Hoover dam. Even the most prepared networks can buckle under that volume of data the first time it is directed at them, which is why even some of our biggest financial institutions initially suffered outages when they were victims of a DDoS campaign. In addition to increasing in volume, the attacks are getting more sophisticated and varying the methods used, which makes them harder to mitigate. In 2014, attackers used new techniques to amplify the strength of an attack which made it easier for even the "average" attack to reach levels of volume that were unthinkable just years before.[3]

According to a survey by Neustar, 60 percent of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once.[4] The most affected sectors were the gaming, media, and software industries. The purpose of most attacks is to disrupt, not to destroy. Cybercriminals can rent DDoS attack services on the black market for as little as $5, allowing them to conduct a short, minutes-long DDoS attack against any chosen target (fig. 1).[5] If successful, even such a short attack is enough to garner attention – or to distract an organization's security team, as another recent use of DDoS attacks has been to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing credit card information.

Fig. 1. Example of a DDoS service for hire – this one is directed at online gamers.

[2] "Bots and Botnets – A Growing Threat," *Symantec,* http://us.norton.com/botnet/
[3] Symantec, "*Security Response: The Continued Rise of DDoS Attacks,*" October 21, 2014, Pg. 25.
[4] Neustar, "*2014, The Danger Deepens: Neustar Annual DDoS Attacks and Impact Report,*" June 2014, Pg. 3.
[5] Symantec, "*Security Response: The Continued Rise of DDoS Attacks,*" October 21, 2014, Pg. 12.

Targeted Attacks

Targeted attacks are another tool in the cybercriminal's tool box, and the attached graphic illustrates some common attack methods as well as the economics of cybercrime (see *Path of A Cybercriminal*, attached on page 12). Some attacks are directed at a company's servers and systems, where attackers search for unpatched vulnerabilities on websites or undefended connections to the internet. But most rely on social engineering, tricking people into clicking on a link, opening a file, or taking some other action that will allow an attacker to compromise their device. They can be targeted at almost any level, even at an entire sector of the economy or a group of similar organizations or companies. They also can target a particular company or a unit within the company (*e.g.*, research and development or finance) or even a specific person.

Most of the data breaches and other attacks that have been in the news were the result of a targeted attack, but the goal of the attacker can vary greatly. One constant is that after attackers select a target they will set out to gain access to the systems they want to compromise and once inside there are few limits on what they can do if the system is not well-protected. The malware used today is largely commoditized, and while we still see some that is custom-crafted, most of the attacks rely on attack kits that are sold on the cyber black market. But even these commodity attack kits are highly sophisticated and are designed to avoid detection – some even come with guarantees from the criminal seller that they will not be stopped by common security measures. This makes it all the more important – but also more challenging – to stay ahead of them.

Scams, Blackmail, and other Cyber Theft

Like most crime, cyber attacks are often financially motivated, and some of the most common (and most successful) involve getting victims to pay out money, whether through trickery or direct threats. One early and widely successful attack of this type was known as "scareware" (fig. 2). Scareware is a form of malware that will open a window on your device that claims your system is infected, and offer to "clean" it for a fee. Some forms of scareware open pop-ups falsely claiming to be from major security companies (including Symantec), and if a user clicks in the window they are taken to a fake website that can look very much like that of the real company. Of course, in most cases the only infection on your computer is the scareware itself. Victims who fall for the scam are lucky if they only lose the $20 or $30 "cost" for the fake software, but most are out much more as they typically provide credit card information to pay the scammer in the mistaken belief they are purchasing legitimate security software. Not only did they authorize a payment to the scammer, but they also provided financial information that could then be sold on the criminal underground. And by allowing the scammer to install the supposed cleaning software on their device, they give the criminal the ability to install additional malware and potentially steal more financial information or turn their system into a zombie soldier in a botnet.

Fig. 2. An example of Scareware. The pop-ups proclaim that the victim's computer is infected, and often cannot be closed.

First widely seen in 2007, scareware began to diminish in 2011 after users became alerted to the scams and they became much less effective. Nevertheless, criminals have made millions from this type of scam.

Once scareware began to be less effective, criminals turned to "ransomware," which has grown significantly since 2012. Ransomware is another type of deception where the malware locks the victim's device and displays a screen that purports to be from a law enforcement entity local to the user. The lock screen states that there is illegal content on the computer – everything from pirated movies to child pornography – and instructs the victim to pay a "fine" for their "crime" (fig. 3). The criminals claim that the victim's device will be unlocked once the "fine" is paid, but in reality the device frequently remains locked. Both of these types of attacks can be removed from your computer and we offer instructions and free tools on our Norton.com website to assist victims in doing so. Unfortunately, some of the more sophisticated variants can require some expertise to remediate.

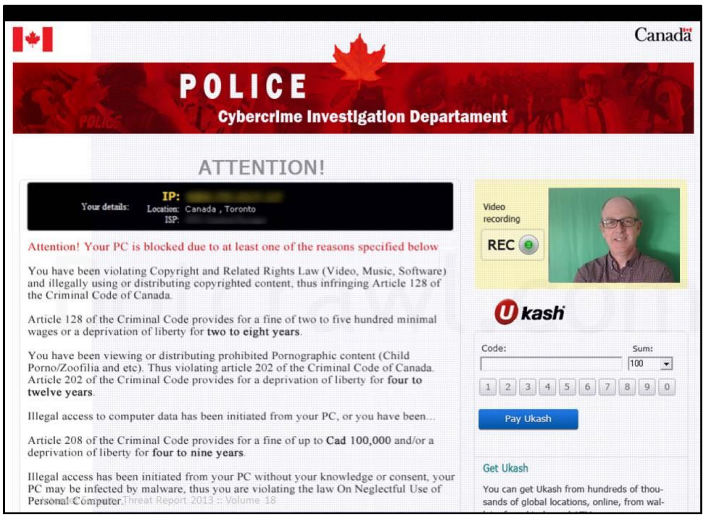


Fig. 3. This ransomware targeted victims in Canada; victims in other countries would see logos of law enforcement local to them. It used built-in webcams to take a victim's picture to further frighten them.

Criminals have now moved beyond even ransomware and are using a more insidious and harmful form of malware known as "ransomcrypt." While scareware and ransomware are more classic confidence schemes, ransomcrypt is straight-up blackmail: pay a ransom or your computer will be erased (fig. 4). And unlike scareware and ransomware, there is often no easy way to get rid of it – the criminals use high-grade encryption technology to scramble the victim's computer, and only they have the key to unlock it. Unless the system is backed up, the victim faces the difficult choice of paying the criminals or losing all the data, and earlier this year a police department in Maine paid a ransom in order to regain control of its data.[6] The police chief said "[w]e needed our programs to get back online."[7]

Fig. 4. This is a screenshot of Cryptolocker, a sophisticated piece of ransomcrypt that was disrupted in summer 2014 by an international takedown effort, in which Symantec participated.

This is not meant to suggest that the criminals are unstoppable; in fact, in June 2014 we were part of a team that helped take down Cryptolocker, a prevalent form of ransomcrypt. Symantec assisted the FBI and several other international law enforcement agencies to mount a major operation during which authorities seized a large portion of the infrastructure that had been used by the cybercriminals. As a result of Symantec's research into the threat, we were able to provide technical insights into their operation and impact. Since the operation, the Cryptolocker infection rate has dropped to near zero. But other forms are still out there, and the fight goes on.

Threats to Critical Infrastructure

Critical infrastructure such as the power grid, water systems, and mass transit are also at risk. As more of these devices become connected and are controlled remotely, attackers have more opportunities to try to exploit them. In June 2014, we notified and provided detailed Indicators of Compromise (IoC) to more than 40 national computer security incident response teams around the world about a new threat

[6] Stephanie Mlot, "Maine Police Pay Ransomware Demand in Bitcoin," *PCmag*, April 14, 2015, http://www.pcmag.com/article2/0,2817,2481356,00.asp

[7] *Id.*

we named *DragonFly*.[8] This was an ongoing cyber espionage campaign against a range of targets, mainly in the energy sector, which gave attackers control over computers that they could have used to damage or destroy critical machinery and disrupt energy supplies in affected countries. Among the targets of *Dragonfly* were energy grid operators, electricity generation firms, petroleum pipeline operators, and industrial equipment providers – the majority of which were located in the U.S., Spain, France, Italy, Germany, Turkey, and Poland. Quick and detailed notification was critical in mitigating the threat.

This was not the first campaign targeted at the energy sector. In 2012, cyber attackers mounted a campaign against Saudi Arabia's national oil firm Saudi Aramco, which destroyed approximately 30,000 computers and took its network off line for days. The infected computers were rendered unusable and displayed the image of a burning American flag. Though operations were not impacted, there was speculation in the press that oil production was the ultimate target. Shortly after the Saudi Aramco attack, a Qatari producer of liquefied natural gas, RasGas, suffered a similar attack which damaged its networks and took down its website. Other sectors have seen attacks too. In the manufacturing sector, late last year the German Government disclosed that a cyber attack on a steel plant had resulted in the failure of multiple components and, according to one report, "massive physical damage."[9]

In the U.S. we have yet to see major destructive attacks on critical infrastructure. However, there have been widespread reports that foreign actors have sought to gain a foothold on the networks of U.S. critical infrastructure providers.[10] And we have seen the actual compromise of one water treatment facility in South Houston, Texas (fig. 5), though the attacker did not alter any controls or settings and claimed to be trying to bring attention to the vulnerabilities that exist in critical infrastructure. This particular facility was not following security best practices and was still using default passwords that were widely known. There are undoubtedly many other critical systems that are similarly exposed.

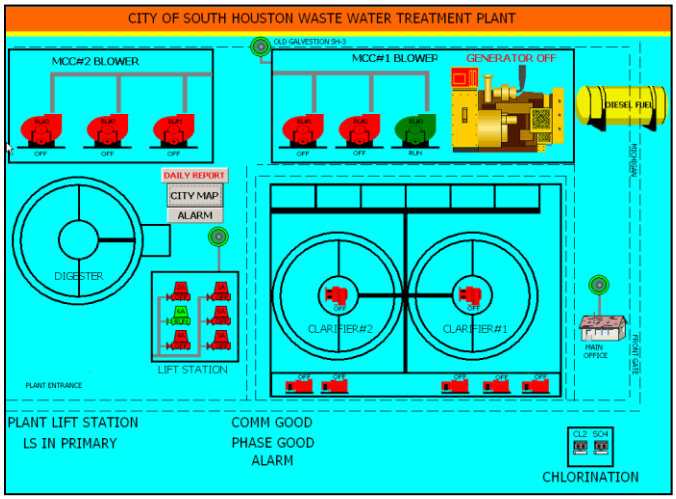


Fig. 5. Screenshot a hacker posted of the graphical user interface of the South Houston Waste Water Treatment Plant. He accessed this through use of an unchanged default user name and password.

[8] Symantec, "*Security Response: Dragonfly: Western Energy Companies under Sabotage,*" June 30, 2014. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[9] SANS Industrial Control Systems (ICS), "*German Steel Mill Cyber Attack,*" December 30, 2014, Pg.1.

[10] Pierluigi Paganini, "The US energy industry is constantly under cyber attacks," *Security* Affairs, November 14, 2014 http://securityaffairs.co/wordpress/30328/cyber-crime/cyber-attacks-energy-industry.html

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

All of the attacks outlined above started with 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, is 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. The old cliché is true when it comes to cyber attacks: we have to get it right 100 percent of the time while the attacker only has to do so once.

Beginning in 2012, we saw the rapid growth of a new type of targeted web-based attack, 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 victims 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. In another case, we saw employees from 500 different companies in the same industry visit one compromised site in just 24 hours, each running the risk of infection.[11] 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.

[11] Symantec, "*Internet Security Threat Report, Volume XVIII,*" April 16, 2013, Pg. 21.

We are also seeing an increasing number of "second generation" compromises – where attackers use personal information that was previously stolen or harvested off the internet to access data or even establish new online accounts. Twenty or more years ago criminals would use stolen social security numbers or other information to open fraudulent credit cards; today that same information can be used to verify – fraudulently – a person's identity to access information held by companies or governments. As the personal information of more people is stolen and sometimes coupled with other information posted on social media or elsewhere, systems that use Knowledge Based Authentication (KBA) are increasingly under attack. This is particularly true with static KBA – which uses fixed questions and information provided by a user, and is often drawn from a set of queries that have become well-known to attackers.

Dynamic KBA, which connects some identifying information with data drawn from a wider data-set that is not supplied by a user, provides a higher level of security. However, it is still most effective when paired with additional authentication, which can include behavioral analytics or additional factors such as a text message, a smart card, biometrics, or a token or mobile application with a changing numeric password. To make it even more secure, some systems require an out-of-band communication such as a phone call or even standard mail before allowing an account to be opened. Of course, additional security measures can also slow the verification process, which can frustrate users.

The information that is stolen through these types of attacks can be used for immediate gain, though it is often used in more sophisticated criminal scams such as tax fraud. But the lesson is plain: no matter how innocuous a piece of data may seem to you, criminals are constantly devising new ways to monetize it once it is stolen.

Security Measures

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.[12] 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.com website.

For organizations of any size, the National Institute of Standards and Technology's Cyber Security Framework[13], 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.

- *Basic Security Steps*

Poor basic computer hygiene practices are a major cause of breaches. While good practices will stop most attacks – which often exploit known vulnerabilities – too many organizations do not keep their

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

systems updated. Indeed, security starts with the basics. Though criminals' tactics are continually evolving, good cyber hygiene is still the simplest and most cost-effective first step. Strong passwords remain the foundation of good security – on home and work devices, email, social media accounts, or whatever you use to communicate (or really anything you log into). And these passwords must be different, because using a single password means that a breach of one account exposes all of your accounts. Using two factor authentication significantly increases the security of a login.

Patch management is also vital. Individuals and organizations should not delay installing patches, or software or hardware updates, because the same patch that closes a vulnerability can be a roadmap for a criminal to exploit and compromise any unpatched devices. The reality is that a large percentage of computers around the world, including some in large organizations, do not get patched regularly, and cybercriminals count on this. While so-called "zero day exploits" – previously unknown critical vulnerabilities – get the most press, it is older, unpatched vulnerabilities that cause most systems to get compromised.

Additionally, we all need to exercise caution on social media. Cybercriminals target the places where we "live and play" online in order to get at sensitive personal data, and are increasingly using social media to launch attacks. It is particularly effective in direct attacks, as people tend to trust things that appear to come from a friend's social media feed. But social media is also widely used to conduct reconnaissance for spear phishing or other targeted attacks. Exercising some care in how we use social media can make the attacker's job harder.

- *Modern Security Software*

Poor or insufficiently deployed security can also lead to a breach, and a modern security suite that is being fully utilized is also essential. While most people still commonly refer to security software as "anti-virus" or AV, advanced security protection is much more than that. In the past, the same piece of malware would be delivered to thousands or even millions of computers. Today, cybercriminals can take the same malware and create unlimited unique variants that can slip past basic AV software. If all your security software does is check for signatures (or digital fingerprints) of known malware, you are by definition not protected against even moderately sophisticated attacks. Put differently, a check-the-box security program that only includes installation of basic AV software may give you piece of mind – but that is about all it will give you.

Modern security software does much more than look for known malware: it monitors your system, watching for unusual internet traffic, activity, or system processes that could be indicative of malicious activity. At Symantec we also use what we call *Insight* and *SONAR*, which are reputation-based and behavior-based heuristic security technologies. Insight is a reputation-based technology that uses our Global Intelligence Network to put files in context, using their age, frequency, location and other characteristics to expose emerging threats that might otherwise be missed. If a computer is trying to execute a file that we have never seen anywhere in the world and that comes from an unknown source, there is a high probability that it is malicious – and Insight will either warn the user or block it. SONAR is behavior-based protection that uses proactive local monitoring to identify and block suspicious processes on computers.

- *Tailoring Security to the Device*

Security should also be specific to the device being protected. For example, modern Point of Sale (PoS) systems, which were linked to a number of major data breaches, are at their core just computers running mainstream operating systems. Because a user on such a device typically does not browse the web, send emails, or open shared drives, the functionally of the machine and the files that actually need to be on it are limited. This allows businesses to reduce the attack surface by locking down the system and using application control tools, as well as controlling which devices and applications are allowed to access the network. Doing so can render many strains of malware useless because they would not be allowed to run on the devices. In addition, payment card system infrastructure is highly complex and threats can be introduced at any number of points within the system. Last year we released a report, *Attacks on Point of Sale Systems*, that provides an overview of the methods that attackers may use to gain entry into a system.[14] It also describes the steps that retailers and other organizations can use to protect PoS systems and mitigate the risk of an attack.

- *Encrypting and Monitoring Data*

Encryption also is key to protecting your most valuable data. Even the best security will not stop a determined attacker, and encrypting your sensitive data provides defense in breadth, or across many platforms. Encryption ensures that any data stolen will be useless to virtually all cybercriminals. The bottom line in computer security is no different from physical security – nothing is perfect. We can make it hard, indeed very hard, for an attacker, but if well-resourced and persistent criminals want to compromise a particular company or site, with time they are probably going to find a way to do it. Good security means not just doing the utmost to keep them out, but also to recognize that you must take steps to limit any damage they can do should they get in. Data loss prevention (DLP) tools are also important in keeping your most valuable data safe on your system. The latest DLP technology allows the user to monitor, protect and manage confidential data wherever it is stored and used – across endpoints, mobile devices, networks, and storage systems. It can help stop the theft of sensitive data by alerting the system manager before the data is exfiltrated.

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 their 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. For example, the criminals did not stop using the scareware described above because they wanted to – they quit when it stopped working. At Symantec, we are committed to improving online security and we look forward to continuing to work with government and industry on ways to do so. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

[14] *Special Report on Attacks on Point of Sale Systems*, Symantec Security Response (February 2014). http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf

PATH OF A CYBER ATTACKER

1

Attacker
A person who uses computers to gain unauthorized access to data.

Technical Abilities
Ranges from **Novice** "Script Kiddies" (Typically youth without skill who rely on readily available code tools) to **Expert** Malware Coders

Motivations
- Money
- Risk vs. Reward
- Political

2

Attacker Shops Virtual Underground Markets
These underground markets are growing in size, complexity, are geographically spread out and are masked from the public eye with cryptographic features in the "darknet."

3

Attacker Employs Tools
Attacker uses tools to steal data such as: personal information; account information; and credit card data. Victims range from individual users to multinational companies and Governments.

4

Attacker Sells Stolen Data on Underground Market:

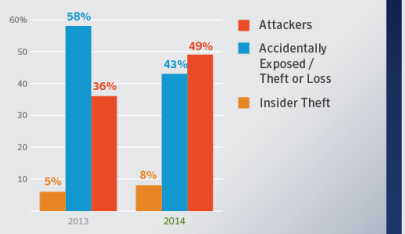
1,000 Stolen Email Addresses	$.50 to $10
Credit Card Details	$.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to 15$
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

5

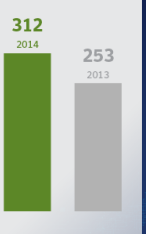
Attacker Uses Money Mule to Transfer Stolen Funds
Money Mule Shaves off small percentage for self.

6

Attacker Now Has Laundered Money to Invest in More Powerful Hacking Tools



Top Causes of Data Breach
Source: Symantec



Total Breaches
Source: Symantec

Source: Symantec, 2015 Internet Security Threat Report, Volume 20

ISTR20
INTERNET SECURITY THREAT REPORT

Symantec.

The 2015 Internet Security Threat Report (ISTR) provides an overview and analysis of the year in global threat activity. It is compiled using data from the Symantec™ Global Intelligence Network, which our global cybersecurity experts use to identify, analyze, and provide commentary on emerging trends in the threat landscape.

04/15 21350013