Prepared Testimony and
Statement for the Record of

Fran Rosch
Senior Vice President
Security Products and Services, Endpoint and Mobility
Symantec Corporation

Hearing on

"Privacy in the Digital Age:
Preventing Data Breaches and Combating Cybercrime"

Before the

U.S. Senate
Committee on the Judiciary

February 4, 2014

226 Dirksen Senate Office Building

Chairman Leahy, Ranking Member Grassley, distinguished members of the Committee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Fran Rosch, and I am the Senior Vice President, Security Products and Services, Endpoint and Mobility at Symantec. In this role I drive the development and execution of Symantec and Norton's endpoint and mobile management and protection strategy. I joined Symantec in 2010 through the acquisition of VeriSign's security business, and during my twelve-year career with VeriSign I worked with the company's largest customers to design and deploy effective security solutions to solve business challenges.

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. Symantec is the largest security software company in the world, with over 31 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 and information in any environment – 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, and we maintain 10 Security Response Centers. These sensors record thousands of events per second. In addition, every day we process billions of e-mail messages and web requests across our 14 global data centers. These resources allow us to capture worldwide security intelligence data that give our analysts a unique view of the entire Internet threat landscape.

The hearing today is not only timely – given the recent high profile data breaches – but it is a critically important discussion that will help focus attention on what businesses can do to protect themselves from similar attacks. Symantec welcomes the opportunity to provide comments to the Committee as it looks at how to prevent data breaches, combat cybercrime, and protect privacy.

In my testimony today, I will discuss:

- The need for basic computer hygiene;
- Recent statistics on data breaches;
- How breaches are happening, including the methods criminals are using to steal data;
- Security measures to protect data and prevent breaches; and
- Key elements for data breach legislation.

Computer Hygiene as a Basic Layer of Defense

Preventing data breaches and protecting privacy starts with basic computer hygiene such as having security software installed, good patch management practices, using strong passwords, and not responding to suspicious emails. But that is just the start, because sophisticated, well-funded attackers are persistent and highly skilled. Anti-virus software (AV) should be part of any security program and will stop known malicious software (malware), but it is just one element. Today, even moderately sophisticated pieces of malware have unique signatures and can slip past systems that are using only AV software. Thus, strong security is layered security – in addition to basic computer hygiene and AV software, organizations need comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, and data loss prevention tools. These advanced tools look not just for known threats, but they can check the reputation of any file that is loaded on a computer and look for other behavior that could indicate the presence of previously unknown malware.

The kinds of attacks on point-of-sale (PoS) devices that this hearing is looking at are not new, but it does appear the pace is increasing. The increase in successful attacks brings with it media attention and citizen concern, but it is critically important that the public conversation we are now having *not* just be about one attack or one company. Every retailer is at risk, and over time we often learn that the most widely reported victim was not the one hit hardest. So the conversation should be about breaches – plural – not just one breach; it should be about how they are happening, how government can go after the sophisticated criminal enterprises that steal the data, and what organizations can do to prevent and minimize the risk of a successful attack.

Data Breaches by the Numbers

For organizations that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk associated with a data breach is now higher than ever before. Simply put, stealing data is big business; most major breaches are part of sophisticated criminal enterprises that trade on stolen identities and credit card numbers. The cost impacts of and the metrics associated with worldwide data breaches are significant.

In 2013, we estimate that the identities of over 435 million people were exposed, and that number is rising as new reports surface. For comparison, our estimate for 2012 was 93 million, and for 2011 was 232 million.[1] In fact, a recent report by the Online Trust Alliance indicates that of the top ten breaches in history, 40% occurred in 2013.[2] Of course, the total number of identities exposed is cumulative – once a person's identity has been exposed, it does not get "unexposed" when the calendar changes. So in the most basic of terms, as a result of breaches over the past three years, the personal information of up to 750 million individuals is or could be for sale on the criminal black market to be used for identity theft, credit card fraud, and countless other illegal activities.

It is important to remember that not every one of these victims will have his or her identity stolen or bank account raided. In fact, a low percentage of them will actually suffer that kind of direct loss. But every one of them is at risk for it because once your personal information is outside of your control your options are limited. You can start credit monitoring and get new credit cards, but to a large degree your best hope is that the information becomes stale before someone tries to use it themselves or sell it on the thriving black market.

The cost of these breaches is very real and is borne directly by both consumers and organizations:

- In our 2013 Norton Report, we estimated the global price tag of consumer cybercrime was $113 billion annually;[3]
- We estimate that there are 378 million victims of consumer cybercrime per year (1 million victims per day, 12 per second);[4]
- The Ponemon Institute estimates that in 2012, the cost to US companies was $188 per identity

[1] *Symantec Internet Security Threat Report* XVIII (April 2013), 17. http://www.symantec.com/security_response/publications/threatreport.jsp

[2] *2014 OTA Data Breach Guide*, 4. https://otalliance.org/breach.html

[3] *2013 Norton Cybercrime Report* (October 2013), 8. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[4] *Id.* at 10.

compromised;[5]

- Ponemon's survey concluded that the average total cost of a breach in 2012 was $5.4 million;[6] and
- Attackers are increasingly targeting smaller businesses, 71% of which say their operations are somewhat or very dependent on the Internet.[7]

The Ponemon survey also found that an ounce of prevention is worth a pound of cure. Strong security protocols before a breach and good incident management policies can dramatically cut the cost of a breach. Similarly, more consumers than ever are taking basic security measures such as using security software and deleting suspicious emails.

How Data Breaches are Occurring

While the continuing onslaught of data breaches is well documented, what is less understood is why data breaches happen and what can be done to prevent them. The main causes for breaches are targeted attacks and human error.

Targeted attacks are indeed an increasing cause of data breaches. According to our 2013 Internet Security Threat Report (ISTR), 40% of data breaches were caused by hackers.[8] Some are direct attacks on a company's servers, where attackers search for unpatched vulnerabilities on websites or undefended connections to the Internet. But most rely on social engineering – in the simplest of terms, tricking people into doing something they would not do if fully aware of the consequences of their actions. Email is still a major attack vector and can take the form of broad mailings ("phishing") or highly targeted messages ("spear phishing"). More and more we see the latter variety, with publicly available information used to craft an email designed to dupe a specific victim or group of victims. The goal of both varieties is to get victims to open an infected file or go to a malicious or compromised website. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations do not have up-to-date security, do not make full use of the security tools available to them, or have it unevenly applied throughout their enterprise.

Another major cause of breaches is a lack of basic computer hygiene practices, often in the form of company employees who do not follow data security policies. Even today – despite the recent focus on the loss of personal information – a large segment of the workforce handles sensitive information on unprotected mobile devices, servers, desktops, and laptops. Ironically, in many ways this is the natural result of a highly productive workforce. One of the most common types of data breach occurs when sensitive data that an employee stores, sends, or copies is not encrypted. If a laptop is lost or stolen – or a hacker gains access to a network – these files are left unprotected. And while most large companies have policies requiring encryption or other security precautions for sensitive data, many employees either do not have the tools available or they ignore or are unaware of the policies.

Email, web mail, and removable storage devices are another major source of breaches. Most of us at one time or another have emailed something to our personal email address from our office so that we can work on it later. If our email accounts or home computers are compromised, or if we misplace the thumb drive we use to

[5] *Cost of Data Breach Study: Global Analysis*, Ponemon Institute (May 2013), 1. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

[6] *Id.* at 1.

[7] *Symantec 2012 National Small Business Study Fact Sheet,* National Cybersecurity Alliance & Symantec Corporation, 1. http://www.staysafeonline.org/stay-safe-online/resources/

[8] *ISTR XVIII*, 19.

transport files, any sensitive, unencrypted data we sent is now lost and our company has had a data breach. Data breaches also can occur through outright theft, often by a fired or disgruntled employee.

Cybercriminals are also targeting the places where we “live and play” online in order to get at sensitive personal data. Social media is an increasingly sinister tool for cybercriminals. 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; 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 be right 100% of the time in protecting ourselves, while the attacker only has to get it right once.

We are also seeing the rapid growth of “watering hole” attacks on Internet sites. 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 deliver malware to every visitor. For example, one attacker targeted mobile app developers by compromising a site that was popular with them. In another case, we saw employees from 500 different companies visit one compromised site in just 24 hours, each running the risk of infection.[9] Cybercriminals gain 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, and sensitive data on users systems would have been protected.

All of these attacks have essentially one goal: to get control of the user’s computer, because once they have gained this foothold they can use the system for virtually any criminal purpose (including stealing data). When infiltrating a company, once inside, attackers typically will conduct reconnaissance of the system and then move laterally within it until they find what they want to take. In the case of a retailer, this can include compromising PoS devices and stealing information in bulk from them. In the case of an attack on an individual, the criminal will install malware that allows them to steal information or otherwise take control of the computer for future use.

Protecting Data and Preventing Breaches

Basic Security Steps - i.e., Closing the Door.

When it comes to security, it starts with the basics. Though criminals’ tactics are continually evolving, good cyber hygiene, as discussed previously, 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 a second authentication factor (whether through a text message, a smart card, biometrics, or a token with a changing numeric password) significantly increases the security of a login.

Patch management is also critical. Individuals and organizations should not delay installing patches, or software updates, because the same patch that closes a vulnerability on one computer can be a roadmap for a

[9] *Id.* at 21.

criminal to exploit that vulnerability 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.

Modern Security Software – i.e., Bolting the Doors and Windows

But 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 computer, 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 – i.e., Locking Your Valuables in a Safe

Security should also be specific to the device being protected, and in some ways PoS devices have advantages over other systems. For while a modern PoS system is typically at its core just a computer running a mainstream operating system, the functions it needs to perform can be narrowly defined. 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. The special report we released yesterday, *Attacks on Point of Sales Systems*, provides an overview of the methods that attackers may use to gain entry into a system.[10] It also describes the steps that retailers and other organizations can use to protect PoS systems and mitigate the risk of an attack.

[10] *Special Report on Attacks on Point of Sales 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

Encrypting Data – i.e., Hiding Family Treasures in a Secret Compartment in your Safe

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. Good 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 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.

Responding to a Breach

The criminal organizations that carry out many of the major targeted attacks are well funded, sophisticated, and persistent. In the face of this onslaught, even the most security conscious organizations can have a data breach. Every organization needs to be prepared to manage the effects of one, because deploying an effective incident management plan after a breach can help mitigate the damage of the data loss. Organizations need to be prepared to react on several different fronts, beginning with an incident response team that represents all functional groups within an organization and a response plan that has been exercised before an incident has occurred. Lastly, organizations need to be prepared to bring in law enforcement and, as expeditiously as possible, notify anyone impacted and communicate timely information to them.

In the longer term, effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving overall cybersecurity and combatting cybercrime. At Symantec, we participate in various industry organizations, as well as public-private partnerships in the US and globally with all levels of government. We share high-level cybercrime and cyber threat trends and information on a voluntary basis through a number of different fora to help protect our customers and their networks. Among our partners are the National Cyber-Forensics and Training Alliance (NCFTA), which includes more than 80 industry partners and law enforcement from around the world, and the Information Technology (IT) Information Sharing and Analysis Center (ISAC), which is comprised of 27 leading IT vendors and contributes to cyber risk management of the other 15 critical infrastructure sectors through the National Council of ISACs.

Data Breach Legislation

In the United States today, there are at least 48 state-specific data breach notification laws. This creates an enormous compliance burden, particularly for smaller companies, and does little to actually protect consumers. Symantec supports a national standard for data breach notification, built on three principles:

1. Data security legislation should apply equally to all. The scope of any legislation should include all entities that collect, maintain, or sell significant numbers of records containing sensitive personal information. Requirements should impact government and the private sector equally, and should include educational institutions and charitable organizations as well. By the same token, any new legislation should consider existing federal regulations that govern data breach for some sectors and not create duplicative, additional, or conflicting rules.

2. Implementing pre-breach security measures should be a part of any legislation. As the Ponemon survey demonstrates, breaches are much less costly for companies that are proactive. New legislation should not simply require notification of consumers in case of a data breach, but should seek to minimize the likelihood of a breach by pushing organizations to take reasonable security measures to ensure the confidentiality and integrity of sensitive personal information. Numerous standards, best practices, and guidelines already exist to help organizations establish a cybersecurity program or improve an existing one. The Cybersecurity Framework that NIST will issue next week is the result of a lengthy and successful public-private partnership and if it is consistent with the drafts we have seen will be a flexible, scalable tool that organizations of all sizes and sophistication levels can use to secure their environments and protect critical infrastructure.

3. The use of encryption or other security measures that render data unreadable and unusable should be a key element in establishing the threshold for the need for notification. Any notification scheme should minimize "false positives" – notices to individuals who are later shown *not* to have been impacted by a breach because their data was rendered unusable before it was stolen. A clear reference to the "usability" of information should be considered when determining whether notification is required in case of a breach. Promoting the use of encryption as a best practice would significantly reduce the number of "false positives," thus reducing the burden on consumers and business.

Conclusion

This hearing is a key part of an important conversation that we need to have as a nation. Data breaches and cyber threats are a part of every American’s day-to-day lives, and will be even more so in the years to come. We will never be able to prevent every data breach or every cyber attack, but working together, industry and government can make it increasingly more difficult – and more expensive – for cybercriminals to succeed.