Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on

"Getting It Right on Data Breach and Notification Legislation in the 114th Congress"

Before the

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

February 5, 2015

253 Russell Senate Office Building

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

My name is Cheri McGuire and I am the Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, which includes cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. I lead a team of professionals spanning the U.S., Canada, Europe, and Asia, and represent the company in key policy organizations. In this capacity, I work extensively with industry and government organizations, and currently serve on the World Economic Forum Global Agenda Council on Cybersecurity, as well as on the boards of the Information Technology Industry Council, the US Information Technology Office (USITO) in China, and the National Cyber Security Alliance. From 2010 to 2012, I was Chair of the Information Technology Sector Coordinating Council – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. I am also a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

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 over 32 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, 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 – but also is a critically important discussion that will help focus attention on what businesses can do to protect themselves from similar attacks and how Congress can craft effective data breach legislation. Symantec welcomes the opportunity to provide comments to the Committee as it looks at how to prevent and respond to data breaches.

In my testimony today, I will discuss:

- The current cyber threat landscape;
- 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.

The Current Cyber Threat Landscape

Most of the recent headlines about cyber attacks have focused on data breaches across the spectrum of industries, which have become an all too common occurrence. Breaches impact individuals whose identities have been stolen, the organizations with systems that have been penetrated, and governments that are seeking ways to set data breach policies and to apprehend the perpetrators. Organizations that suffered significant breaches over the past few years include the State of South Carolina, Target, Neiman Marcus, Michael's, Home Depot, and Sony, just to name a few.

The theft of personally identifiable information (PII) over this timeframe is simply unprecedented – over just the past two years alone, the number of identities exposed through breaches will likely approach *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 individual's 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]

In addition, the statistics from our 2014 Internet Security Threat Report are clear that the cyber threats we are facing on a day to day basis are growing. More than 550 million identities were exposed in 2013, which was an increase of 62% over the prior year, and the top eight breaches exposed more than 10 million identities each. These breaches often exposed real names, birth dates and/or government ID numbers (e.g. social security numbers). Some records 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 dangerous 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.

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

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.

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. Targeted attacks remain a major cause. 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.

Another major cause of breaches is a lack of basic computer hygiene practices. 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 or patched systems, do not make full use of the security tools available to them, or have security unevenly applied throughout their enterprise. 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.

Email, web mail, and removable storage devices are another 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 transport files, any sensitive, unencrypted data is now lost and our organization suffers a data breach. And of course, breaches 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 can provide 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 percent of the time in protecting ourselves, while the attacker only has to get it right once.

Security Measures to Protect Data and Prevent Breaches

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.[2] The website provides educational resources for how to better

[2] http://www.consumer.ftc.gov/topics/privacy-identity

protect your identity and privacy online as well as helpful tools to help you report and recover if your personal information is ever stolen.

For organizations of any size, the NIST Cyber Security Framework[3], 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*

When it comes to security, it 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 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 vital. Individuals and organizations should not delay installing patches, or software 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.

- *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

[3] http://www.nist.gov/cyberframework/

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.[4] 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. 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.

Data loss Prevention (DLP) tools are also important in keeping your most valuable data safe and securely 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

[4] *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

can help stop the theft of sensitive data by alerting the system manager before the data is exfiltrated, or moved outside the system.

Key Elements for Data Breach Legislation

In the U.S. 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 apply to 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. Breaches are much less costly for companies that are proactive in applying security. New legislation should not simply require notification of consumers in the event 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.

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, businesses, and governments.

Conclusion

Data breaches are continuing at an unprecedented pace, putting consumers at risk and damaging the public's trust in the Internet. 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. Moreover, legislation cannot stop breaches from happening, but smart data breach legislation can help businesses and governments respond effectively and efficiently, and empower consumers with accurate and timely information. 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.