Prepared Testimony and
Statement for the Record of

Jeffrey E. Greene
Senior Policy Counsel, Cybersecurity and Identity
Symantec Corporation

Hearing on

"Reporting Data Breaches:
Is Federal Legislation Needed to Protect Consumers?"

Before the

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

July 18, 2013

2123 Rayburn House Office Building

Chairman Terry, Ranking Member Schakowsky, distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Jeff Greene, and I am the Senior Policy Counsel for Cybersecurity and Identity at Symantec, where I focus on cybersecurity, identity management, and privacy issues. I currently serve as vice-chair of the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law and co-chair of the Supply Chain Working Group of the Information Technology Sector Coordinating Council. 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. Before that, I was Counsel to a Washington, D.C. law firm, where my practice focused on government contracts and contract fraud, as well as general civil and criminal investigations.

Symantec is the largest security software company in the world, with over 31 years of experience developing Internet security technology. We provide security, storage, and systems management solutions to help consumers and organizations secure and manage their information and identities. Our Global Intelligence Network (GIN) is comprised of more than 69 million attack sensors in over 200 countries, and records thousands of events per second. In addition, every day we process more than three billion e-mail messages and more than 1.4 billion web requests across our 14 global data centers.

These resources allow us to capture worldwide security intelligence data that gives our analysts a view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing, and spam. We welcome the opportunity to provide comments as the Subcommittee continues its important efforts to bolster the state of data security in the US. In my testimony today, I will discuss

- Some recent statistics on data breaches;
- How the breaches are happening, including the methods and tactics criminals currently use to steal data;
- Some basic security measures individuals and companies can employ; and
- Key elements to any legislative solution for addressing data breaches.

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 of a data breach is now higher than ever before. Some metrics:

- We estimate that there were 93 million identities exposed in 2012 (in 2011 there were 232 million)[1];
- The average breach involved data for 605,000 individuals (down from 1.1 million in 2011)[2];

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

- There were fewer massive data breaches in 2012, but there were more smaller ones[3];
- The median number of identities compromised per incident was 8,350 (more than 3x the 2011 median of 2,400)[4]; and
- Hacktivism – which was a major driver of breaches in 2011 – diminished as a factor in 2012;

Of course, these numbers are cumulative – once an 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 in 2011 and 2012 alone, the personal information of 325 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.

To be clear, 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 your control, you can do little more than hope that no one tries to monetize it either by using it themselves or selling it on the thriving black market. If your computer was compromised either as the source or as a result of a breach, until you are aware of it and are able to clean your system you are entirely at the mercy of the criminals. Your computer could be used to steal from you, or as part of a network of compromised computers that can send spam, take part in a denial of service attack, or try to infect other computers.

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

- In our 2012 Norton Cybercrime report, we put the global price tag of consumer cybercrime at $110 billion annually[5];
- We estimate that there are 556 million victims of consumer cybercrime per year (1.5 million victims per day, 18 per second)[6];
- On the business side, the Ponemon Institute estimates that in 2012, the cost to US companies was $188 per identity compromised[7];
- Ponemon's survey concluded that the average total organizational cost of a breach in 2012 was $5.4 million[8]; and
- Attackers are increasingly targeting smaller businesses, 71% of whom say their operations are somewhat or very dependent on the Internet.[9]

There is reason to be hopeful, however. The Ponemon survey found that an ounce of prevention is indeed worth a pound of cure. Strong security protocols before a breach and good incident

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *2012 Norton Cybercrime Report* (September 2012), 6. http://www.norton.com/2012cybercrimereport
[6] *Id.* at 23.
[7] *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
[8] *Id.* at 1.
[9] *Symantec 2012 National Small Business Study Fact Sheet*, National Cybersecurity Alliance & Symantec Corporation, 1. http://www.staysafeonline.org/stay-safe-online/resources/

management policies should a breach occur significantly decreased the average breach cost. Similarly, more consumers than ever are taking basic security measures such as deleting suspicious emails and using security software.

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 human error, system problems, and targeted attacks.

Company employees who violate data security policies still cause a large number of data breaches. Even today, employees work with sensitive information on unprotected servers, desktops, and laptops; in many ways, this is the natural result of a highly productive workforce. One of the most common types of data breach occurs when well-meaning insiders do not encrypt the sensitive data that they store, send, or copy. If a laptop is lost or stolen – or a hacker gains access to a network – these files are completely unprotected. And while most companies have policies that require encryption or other security precautions for sensitive data, many employees either ignore or do not know about 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 home 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 we sent is now lost and our company has had a data breach. Data breaches can also be caused by outright theft – a fired or disgruntled employee who steals sensitive information.

There is of course another cause for data breaches – targeted attacks. According to our 2013 Internet Security Threat Report (ISTR), 40% of data breaches were caused by hackers.[10] 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, trying to trick people into doing something that they would never do if fully cognizant 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 click on a link to a website that will then try to infect their computers or to open infected documents that will do the same. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many companies do not have up-to-date security or have it unevenly applied throughout their workforce.

Social media is an increasingly valuable tool for cyber criminals. 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 highly targeted attacks; it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his

[10] *ISTR XVIII*, 19.

or her guard down. The old cliché is true when it comes to cyber attacks: we have to be right 100% of the time while the attacker only has to get it right once.

In 2012, we also saw the rapid growth of "watering hole" attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals 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.[11] Cyber criminals 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.

All of these attacks have essentially one goal: to get control of the user's computer. In an intrusion into a company, once inside, attackers will typically conduct reconnaissance of the system and then move laterally within it until they find what they want to steal. In the case of an attack on an individual, the criminal will install malicious software ("malware") that allows them to steal information or otherwise take control of the computer for future use.

How to Protect Your Data

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 your email, your social media accounts, 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 your accounts.

Patch management is also critical. Do not delay installing patches, because the same patch that closes a vulnerability on your computer can be a roadmap for a criminal to exploit it and to compromise any unpatched computers. The reality is that a large percentage of computers around the world do not get patched regularly, and cyber criminals count on this. While so-called "zero days" – previously unknown critical vulnerabilities – get the most press, it is older, un-patched vulnerabilities that cause most systems to get compromised.

A modern security suite is essential too. While most people still commonly refer to security software as "anti-virus," good security needs to be much more than that. In the past, the same piece of malware would be delivered to thousands or even millions of computers. Today, cyber criminals can take the same malware and create unlimited unique variants that can slip past basic anti-virus software. Modern security software will monitor 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,

[11] *Id.* at 21.

which is a reputation-based security technology that puts files in context, using their age, frequency, location and more to expose threats that might otherwise be missed.

The move to the cloud presents both opportunities and challenges. Cloud done right is a huge boon for security – you are putting your data behind more secure walls and leveraging the knowledge and the resources of a broader community to protect yourself better. Cloud done wrong is a recipe for a data breach – you are putting all of your vital information in a place that is attractive to attackers yet poorly secured. The non-profit Cloud Security Alliance promotes the use of best practices for providing security in the cloud, and has published a matrix of security controls that provide a good baseline for any provider. Symantec is one of the largest cloud providers in the world, and we marry our cutting edge security technology with cloud services to create a secure on-line environment.

Mobile devices require security too, for as we conduct more of our online lives on mobile devices, the risks will increase accordingly. Cyber criminals will go where the money is, and we are already seeing them shift their focus to mobile. As we reported in the 2013 ISTR, there was a 58% increase in families of mobile malware over the previous year, and that trend shows no sign of slowing down.[12] Since the ISTR was released in April, we have seen further evidence of the shift to mobile attacks, as more malware that was originally designed for PCs has been adapted for use against mobile devices. As with PCs, the solutions are not complex: practice good hygiene and use security software where available.

Encryption is also key to protecting your data. Even the best security will not stop a determined attacker, and encrypting your sensitive data provides defense in breadth. Good encryption ensures that any data stolen will be useless to virtually all cyber criminals. 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 Breach Laws

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 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.

[12] *Id.* at 34.

2. Implementing pre-breach security measures should be central to 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 requiring reasonable security measures to ensure the confidentiality and integrity of sensitive personal information.

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." 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

The good news is that people are getting smarter. Our 2012 Norton Cybercrime Report showed that 89% of people will delete suspicious emails, 83% have basic antivirus, and 78% do not open attachments or links in unsolicited emails or texts.[13] That is a significant improvement from a few years ago, and a positive trend. Similarly, it is increasingly clear that strong security before a breach occurs and well-developed incident management policies to deploy after a breach can decrease the damage that a breach will cause to an organization.

The bad news is that the criminals know this, and they modify their techniques accordingly. That is why your hearing today and your focus on this important issue could not be more timely. Thank you again for the opportunity to testify, and I am happy to answer any questions you have.

[13] *2012 Norton Cybercrime Report*, 16.