Testimony of:

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation
on behalf of the
Business Software Alliance

Hearing On:

"Draft Legislative Proposal on Cybersecurity"

Before the U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure
Protection and Security Technologies

December 6, 2011

Introduction

Chairman Lungren, Ranking Member Clarke and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation[1] and the Business Software Alliance (BSA)[2] as you consider this very important issue.

My name is Cheri McGuire and I am the Vice President of Global Government Affairs and Cybersecurity Policy at Symantec Corporation. I also serve as the current Chair of the Information Technology (IT) Sector Coordinating Council (SCC), which is one of 18 critical sectors identified by the President and the U.S. Department of Homeland Security (DHS) to work in partnership with the government on critical infrastructure protection (CIP) and cybersecurity policy and operational matters. I am also a member of the board for the IT Information Sharing and Analysis Center (ISAC), and serve as the principal IT Sector

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] The Business Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

representative to the Partnership for Critical Infrastructure Security (PCIS). Prior to joining Symantec in 2010, I served as Director for Critical Infrastructure and Cybersecurity in Microsoft's Trustworthy Computing Group, and before that, at the U.S. Department of Homeland Security (DHS), where I led the National Cyber Security Division and the U.S. Computer Emergency Readiness Team (US-CERT).

Symantec is the world's information security leader, with over 25 years of experience in developing Internet security technology. Today, we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing and spam. In short, if there is a class of threat on the Internet, Symantec knows about it.

At Symantec, we are committed to assuring the security, availability, and integrity of our customers' information and the protection of critical infrastructure is a top priority for us. We believe that CIP is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

We welcome the opportunity to provide comments as the Committee continues its important efforts to bolster the state of cybersecurity in the U.S. and abroad. In my testimony today, I will provide the Subcommittee with:

- our latest analysis of the threat landscape as detailed in the Symantec Internet Security Threat Report Volume XVI (ISTR XVI) and in the 2011 Norton Cybercrime Report;
- principles for improving our nation's cybersecurity;
- appropriate roles of industry and government in cybersecurity; and
- our views on your draft legislative proposal for cybersecurity.

Threat Landscape

Today, we rely on technology for virtually everything we do, from driving to and from work, to mobile banking, to securing our most critical systems that protect our nation such as our nuclear plants and electric grid. Our nation's critical infrastructure systems are constantly under attack, and the methods for attacking us are constantly evolving and becoming more sophisticated with each passing minute. It is our goal to ensure that we are thinking ten steps ahead of the attackers. Looking at the current threat landscape is not enough – we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report (ISTR) Volume XVI, we observed significant changes to the threat landscape in 2010.[3] The volume and sophistication of threat activity increased more than 19 percent over 2009, with Symantec identifying more than 286 million unique variations of malicious software or malware. These included threats to social networking sites and users, mobile devices, and phishing.

However, to understand the evolving threat landscape, we first need to look at who is behind the vast array of cyber attacks that we are seeing today. Attacks originate from a range of individuals and organizations, with a wide variety of motivations and intended consequences. Attackers can include hackers (both individual and organized gangs), cybercriminals (from petty operators to organized syndicates), cyber spies (industrial and nation state), and "hacktivists" (with a specific political or social agenda). Consequences can also take many forms, from stealing resources and information, to extorting money, to outright destruction of information systems.

It is also important to recognize that attackers have no boundaries when it comes to their intended victims. All organizations and individuals are potential targets. Corporate enterprises are often the object of targeted attacks not only to steal customer data and intellectual property, but also to disrupt business processes and commerce. Small businesses are often less resilient and the impacts of stolen bank accounts and business disruption can be catastrophic in a very short time frame. In addition, end-users or consumers are confronted with the financial and disruptive impacts of identity theft, scams, and system clean-ups, not to mention the lost productivity and frustration of restoring their accounts. Finally, governments are most often the victims of cyber sabotage, cyber espionage, and hactivism, all of which can have significant national security implications.

Over the years, we have observed an ominous change that has swept across the Internet. The threat landscape once dominated by worms and viruses developed by irresponsible hackers is now being ruled by a new breed of cybercriminals. As more people have access to technology, criminals leverage it for criminal purposes. In October, we released our 2011 Norton Cybercrime Report where we examined online behavior in 24 countries and interviewed nearly 20,000 consumers.[4] We calculated the cost of global cybercrime at $114 billion annually. We also calculated that lost time due to recovery and impact on personal lives was an additional $274 billion worldwide. Further, we found that more than two-thirds of online adults (69 percent) reported having been a victim of cybercrime in their lifetime. Every second, 14 adults become a victim of cybercrime, resulting in more than one million cybercrime victims every day.

With an estimated 431 million adult victims globally in the past year, and at an annual combined cost of $388 billion globally based on financial losses and time lost, cybercrime costs are significantly more than the global black market in marijuana, cocaine and heroin combined – which is estimated at $288 billion per year.

---

[3] Symantec Internet Security Threat Report XVI, April 2011. http://www.symantec.com/business/threatreport/index.jsp

[4] 2011 Norton Cybercrime Report. www.norton.com/cybercrimereport

It is not just our computers that we need to secure from cybercriminals. Today, a high percentage of consumers use their mobile phones to conduct nearly every aspect of their life, from basic communication to online shopping to mobile banking. Most of these phones are not secure. The Norton Cybercrime Report revealed that 10 percent of adults online have experienced cybercrime on their mobile phone. Further, we reported in the Symantec ISTR XVI that there were 42 percent more mobile vulnerabilities in 2010 compared to 2009 – a sign that cybercriminals are turning their efforts to the mobile space.

Recently, there has been an up-swing in press reports regarding cyber attacks and the "advanced persistent threat" or APT. While APT is one of the most overused terms in the security industry today, it is nevertheless something to be taken seriously. APTs covertly infiltrate systems and hide and wait for opportune moments to steal information or damage systems.

The APT is not one entity; rather it is many different and independent entities, with a tremendous range of motivations. Some of these motivations include financial gain, exfiltration (or theft) of sensitive and personal information, cyber espionage, and a new turn in the last 18 months, cyber sabotage as exemplified by the Stuxnet malware.

Another trait of the APT is to infiltrate a system, enterprise, or organization, but not immediately execute the ultimate mission. Often the APT will lie in wait, gaining intelligence, observing patterns, and use this information to glean information to further refine the ultimate attack.

The threats we are seeing are not new, they are just newly packaged. However, while the attacks are not new, they are becoming more targeted and the monetary losses have grown exponentially. Most indicators point to future cyber attacks as being more severe, more complex, and more difficult to prevent and address than current threats. Thus, it is even more vital that we have a cybersecurity policy that is flexible, fosters innovation, and enables us to stay ahead of those with bad intentions.

Principles for Improving our Nation's Cybersecurity

Symantec has been a long time proponent for improving our nation's cybersecurity. We have testified before Congress on the issue each of the last four years and have been a key stakeholder in the numerous legislative efforts and public-private partnerships to improve cyber research and development, cyber education, security standard setting, CIP, and more. We have also participated in various multi-industry efforts aimed at improving our cybersecurity policies. For example, as a member of the Business Software Alliance, we were part of a large coalition of cybersecurity stakeholders that authored a white paper on "Improving our Nation's Cybersecurity through Public Private Partnerships."[5] This paper laid

[5] March 8, 2011. "Improving our Nation's Cybersecurity through Public Private Partnerships: A White Paper." http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/cybersecurity_white_paper_publicprivatepartnership.ashx

out a number of principles, and we believe any cybersecurity legislation should stay true to the core principles associated with these key elements:

- Risk management standards, assessment, and incentives;
- Incident management;
- Information sharing and privacy;
- International engagement;
- Supply chain security;
- Innovation and research and development (R&D); and,
- Education and awareness.

For the purposes of my testimony, I will discuss a few of these in the context of your draft legislative proposal.

- **Information Sharing**

Any cybersecurity legislation must promote and improve information sharing. Information sharing is often referred to as *the* key to combating cyber threats. However, we must first recognize that information sharing is not an end goal, but rather a tool or mechanism to provide situational awareness, or visibility, so that appropriate protective and risk mitigation actions may be taken. In order for information sharing to be effective, information must be shared in a timely manner, must be shared with the right people or organizations, and must be shared with the understanding that so long as an entity shares information in good faith, it will not be faced with legal liability for sharing the information.

In order to achieve truly effective information sharing, there must be increased coordination between and among industry and government. In my roles both inside and outside of the government, and more recently as Chair of the IT Sector Coordinating Council and on the Board of the IT-ISAC, I have seen firsthand both successes and challenges in our current public-private partnership with respect to information sharing.

In particular, cybersecurity exercises have been one of the most successful public-private partnership and information sharing initiatives to date. The level of engagement and resources brought to bear from the government and industry to jointly plan, develop scenarios, define information sharing processes, and execute the exercises has been unprecedented. The lessons learned from these exercises have been invaluable to both industry and government. However, much work still needs to be done to address recommended actions associated with information sharing and realize improvements.

One way to improve information sharing is to provide the government with the proper tools and authority to effectively disseminate information. I have seen too many instances of the government releasing information on cyber threats, days and sometimes weeks, after the threat has been identified. In many of these cases, by the time the government releases the information, it has little use because the private sector has already identified and taken actions to mitigate the threat. There is no single solution that will eliminate these delays, but passing

legislation that sends a clear message to the government that sharing information with the private sector is both a priority and necessary to protect our infrastructure from cyber attacks will go a long way.

At Symantec, we also support an incentive-based approach to information sharing. There is no doubt that businesses can gain a competitive advantage by not disclosing information to their competitors. However, a well-incentivized program of collaboration can help offset the disadvantages and keep the information flowing freely.

At the same time, government does have an important role in fostering the effectiveness of information sharing. For example, government can increase voluntary information sharing through tax incentives, grant funding, and streamlining of regulatory procedures. We also need to address policies that discourage businesses who would be willing to share information but choose not to because of fear of prosecution. Therefore, liability protections are necessary to improve bi-directional information sharing.

As with any partnership, information sharing is founded upon and enabled by trust. That trust is weakened when government information sharing mandates are imposed on industry. Enhanced self-interest and a flexible approach are more likely to improve information sharing than government mandates to private industry.

- **Risk Assessment**

Effective and efficient cybersecurity cannot be accomplished under a "one size fits all" regime. Each system within our critical infrastructure and each cyber threat pose different risks. For example, a small mom-and-pop convenience store should not be required to implement the same policies or standards as a nuclear facility. Using a risk-based approach, as outlined in the National Infrastructure Protection Plan (NIPP)[6], provides a mechanism for the government and industry to assess risk and expend the necessary resources on areas that truly need it, rather than spending equal amounts of resources on both high and low risk targets. Thus, it is imperative that any cybersecurity legislation use a risk-based analysis system rather than a one size fits all regime. Leveraging existing regulatory and voluntary regimes to encourage cybersecurity risk assessments and the adoption of standards should be considered first in any proposals.

- **Innovation**

Any proposed legislation must also promote, not stifle, innovation. As I discussed earlier, threats are constantly evolving and so must the technology to mitigate those threats. Symantec has long been a supporter of a national cyber R&D strategy. Any cybersecurity innovation legislation must promote technology advancement so we can stay ahead of the curve. Cybersecurity policy should therefore maximize the ability of organizations to develop

[6] National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

and adopt the widest possible choice of cutting-edge cybersecurity solutions. An effective way to do this is through the creation and implementation of a National Cybersecurity R&D Plan.

Currently, we have a *federal* plan for cyber R&D, but industry must be part of the larger process, with prioritized, national-level objectives set jointly by public and private partners. The public-private partnership should be used to create a genuine *National* Cybersecurity R&D Plan that contains a detailed road map and specifies the respective roles of each partner. This would include input from industry, academia, and federal, state, and local governments. The plan and its implementation road map should be regularly reviewed by the partners to verify the action plan, determine progress and accountability, and adjust as necessary.

Roles of Industry and Government in Cybersecurity

In discussing public-private partnerships, we should first consider the various roles of industry and government with regard to defending critical infrastructure. The private sector's role is clearly defined to operate and protect their critical information networks. Just as a private citizen needs to lock the doors to their home, infrastructure owners and operators need to ensure that their network security environment is the most up to date to defend against the latest threats.

In addition, industry must continually tune their security environments to manage the level of risk associated with the information they are protecting, while at the same time working within the current economic pressures of doing more with less. Further, industry must move from a device-centric security model to one that is identity- and information-centric, with a focus on infrastructure that is secured and more importantly trustworthy. The new security paradigm of "data-centricity" is not only about protection of devices, but more importantly is about protecting the information.

While the defense of critical infrastructures and the networks they rely on rests with owners and operators, the government does play an important role in cybersecurity. As discussed above, government has the ability to create incentives that encourage the adoption of cybersecurity technologies. It can also assist with education, training and awareness to improve the first line of defense by empowering users. In addition, the government can serve as a facilitator for preparedness by sponsoring exercises and drills that include private industry. Further, it can raise the bar of security within the government by outlining minimum requirements for government procurement. Lastly, the government can support public-private partnerships and information sharing with industry to improve overall cybersecurity situational awareness.

While the government plays a number of roles in cybersecurity, one of the challenges is measuring the effectiveness of government CIP programs. To examine awareness, engagement, and readiness with regard to government CIP programs, Symantec conducts an annual global survey of critical infrastructure providers. Released in October, our 2011 Critical

Infrastructure Protection Survey, found a drop in awareness and engagement on a global basis.[7] We saw a marked decline in companies that are engaged in government CIP programs, with 37 percent in 2011, compared to 56 percent in 2010.

While the findings of this survey are somewhat alarming, it is not that surprising. Many survey respondents reported limitations on staffing and resources which help explain why critical infrastructure providers have had to prioritize and focus their efforts on more day-to-day cyber threats. However, given the increase in targeted attacks, such as Stuxnet, Duqu, and Nitro, against critical infrastructure providers, businesses and governments around the world should be aggressive in their efforts to promote and coordinate protection of critical cyber networks. Given the survey results, we have several recommendations for governments to promote CIP programs to owners and operators in order to raise awareness:

- Governments should continue to put forth the resources to establish government critical infrastructure programs.
    - The majority of critical infrastructure providers confirm that they are aware of government critical infrastructure programs.
    - Furthermore, a majority of critical infrastructure providers support efforts by the government to develop protection programs.

- Governments should partner with industry associations and private enterprise groups to disseminate information to raise awareness of government CIP organizations and plans, with specifics about how a response would work in the face of a national cyber attack, what the roles of government would be, who the specific contacts are for various industries at a regional and national level, and how government and private business would share information in the event of an emergency.

- Governments should emphasize to critical infrastructure providers and enterprises that their information be stored, backed up, organized, prioritized, and that proper identity and access control processes are in place.

<u>Views on Draft Legislative Proposal for Cybersecurity</u>

Symantec was pleased to review the draft bill that has been circulated by you, Mr. Chairman. The draft legislation is a positive step forward in developing a national cybersecurity policy that helps fulfill the core principles I discussed above.

- **National Cybersecurity Authority**

To accomplish the goal of improving cybersecurity, we believe there needs to be improved coordination between and among entities. Currently, there are several government agencies

[7] Symantec's Critical Infrastructure Protection Survey is the result of research conducted in August and September 2011 by Applied Research, which surveyed C-level, IT professionals in SMBs and enterprises in 14 industries specifically designated as critical infrastructure industries. The survey included 3,475 organizations from 37 countries in North America, Europe, Middle East and Africa, Asia Pacific, and Latin America. http://www.symantec.com/about/news/release/article.jsp?prid=20111030_01

working on various aspects of cybersecurity, though there is no designated lead. Thus, we are supportive of the bill's designation of a single entity as the "National Cybersecurity Authority." We must be mindful, however, that we do not create an additional level of bureaucracy.

- **Risk Assessment and Standards**

We support the bill's inclusion of a risk-based approach to cybersecurity. Requiring the Secretary of Homeland Security – in collaboration with industry – to identify risks within our cybersecurity infrastructure ensures that we do not overburden small businesses with unnecessary security requirements, while ensuring that our chemical facilities, dams and electric grid are appropriately protected. We are also supportive of using existing internationally recognized consensus-developed risk-based performance standards, including those developed by the National Institute of Standards and Technology (NIST). In addition, we support the bill's instruction to the Secretary to develop market-based incentives designed to encourage the use of such standards.

We are also especially pleased that the legislation directs DHS to take into account how our national cybersecurity strategy and implementation policies will enhance economic prosperity. Keeping this goal in mind will help to prevent burdensome regulatory policies from being implemented. It also appropriately emphasizes the need to maximize market-based incentives and public-private partnerships for improved cybersecurity.

- **Information Sharing**

Finally, we support the bill's emphasis on promoting information sharing. The bill clearly articulates that the government must share real-time, actionable information with critical infrastructure owners and operators.

We also understand the motivation to create a National Information Sharing Organization, or the NISO. The current system of SCCs and ISACs was developed to facilitate bi-directional information sharing between and among government and private industry. These entities have been successful in facilitating information sharing within industry, and have had varying levels of success in industry to government sharing. However, improvements must be made with regard to how well the government shares threat information with private industry.

We believe that one of the reasons the government is reluctant to share real-time actionable information is because there is no mandate to do so. The mandate within the structure of the NISO that the government must share information is a strong step in the right direction. However, questions remain about how we will continue to utilize the existing entities under the proposed NISO framework. We believe this is important given the significant time and resources that companies have invested in the SCCs and ISACs. We look forward to working with the Committee to address these important issues.

Conclusion

In conclusion, if we are to successfully mitigate today's multi-dimensional threats more effectively – and use public-private partnerships and information sharing as tools – we must incorporate a comprehensive approach for risk, resiliency and collaboration to improve critical infrastructure and cybersecurity. The U.S. public-private partnership has encountered both successes and challenges over the years, but it is clear that we must continue to work together to leverage the best that industry and government bring to the table and confront the challenges directly. Recognizing there is no silver bullet for cybersecurity, we must shift the dialogue from "solving" the cybersecurity problem, to "managing the risk" associated with it.

On behalf of Symantec and the Businesses Software Alliance, we commend you and your staff's efforts in crafting this legislation that appropriately focuses on risk management, information sharing, and technology innovation. We look forward to working with you in the future as the bill moves through the Congress. I look forward to answering any questions you may have.