Prepared Testimony and
Statement for the Record of

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

Hearing on

"Cyber Threats: Law Enforcement and Private Sector Responses"

Before the

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Terrorism

May 8, 2013

226 Dirksen Senate Office Building

Chairman Whitehouse, Ranking Member Graham, and distinguished members of the Subcommittee, 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, including cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. In this capacity, I work extensively with industry and government organizations, including serving from 2010 to 2012 as Chair of the Information Technology Sector Coordinating Council (IT SCC) – 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 also serve as a board member of the Information Technology Industry Council, the TechAmerica Commercial Policy Board, and the US Information Technology Office (USITO) in China, and am a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Previously, I served in numerous positions at DHS, including as Acting Director and Deputy Director of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec is the largest security software company in the world, with over 31 years of experience in 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 Subommittee continues its important efforts to bolster the state of cybersecurity in the US and abroad. In my testimony today, I will provide the Subcommittee with:

- our latest analysis of the threat landscape as detailed in the just-released Symantec Internet Security Threat Report (ISTR), Volume 18;
- a summary of our cooperative engagements with law enforcement, both domestically and abroad; and
- some thoughts on how you can bolster the law enforcement community's important work in this area.

Today's Threat Landscape

We rely on technology for virtually every aspect of our lives, from driving to and from work, to mobile banking, to securing our most critical systems. As the use of technology increases so do the volume and sophistication of the threats. Criminals are constantly looking to exploit new vulnerabilities to steal money, intellectual property, and identities. At Symantec, it is our goal to ensure that we are thinking 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 and attack patterns.

In the latest Symantec ISTR, we identified the current trends in cybercrime and detailed how we see the landscape changing in 2013. Last year, we saw a significant increase in targeted attacks – up 42 percent

from 2011,[1] and it is almost certain that this trend will continue in the coming years. Large scale data breaches continued to be an issue, and last year approximately 93 million identities were exposed through hacking, theft, and simple error. That is 93 million people whose personal information is now potentially for sale on the black market – 93 million people who are at risk for credit card fraud, identity theft, and other illegal schemes.

Another trend in 2012 was the expansion of what we refer to as "watering hole attacks" – efforts by attackers to compromise legitimate websites so that every visitor to those websites runs the risk of infection. Criminals target sites that they believe their victims will frequent, and are often quite sophisticated in evading detection. In some cases, they insert malicious code onto the site only at key times of the day to evade security scans.

Once the criminals take over sites, they often use them to distribute so-called "ransomware," a type of malicious software that locks a user's computer and displays a screen purporting to be from a law enforcement agency. In the US, ransomware typically puts up a fake Federal Bureau of Investigation (FBI) notice that (1) informs the user that illegal content was found on his or her computer, and (2) offers to provide a code to unlock it if the user pays a "fine." *See* Figure 1. Unfortunately, payment of the "fine" usually does not unlock the computer.

Fig. 1 – Actual image used by common "Ransomware" to extort money from a victim. Note that in an effort to frighten the victim as much as possible, the ransomware accuses the victim of crimes involving child pornography and child abuse.

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

Networks of compromised, zombie computers that are controlled by criminal enterprises – also known as "botnets" – continue to be a problem. Botnets range in size from just dozens to millions. A computer becomes a "bot" when an attacker surreptitiously installs malware on the system that allows the criminal to remotely control it. Bots can be used to send spam, to try to infect other computers, or as pawns in massive denial of service attacks. We estimate that there were 3.4 million bot zombies in 2012, up from 3.1 million in 2011. Last year, one in seven (or 15 percent) of global bot-infected computers resided in the US.

We also saw a sharp rise in the threats to mobile devices. Last year, mobile malware increased by 58 percent, and 32 percent of all mobile threats attempted to steal personal information, such as e-mail addresses and phone numbers. Attacks on mobile devices will almost certainly continue to rise as we become ever more reliant on these devices to perform our daily activities, including working, banking, shopping, and social networking.

Another alarming finding was the rise of attacks on small and medium size businesses. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees, and the largest growth area for targeted attacks was aimed at businesses with fewer than 250 employees. Thirty-one percent of all attacks targeted them, up from 18 percent the year before. This likely stems from the fact that unlike large enterprises, smaller businesses often do not have the resources to establish adequate security protocols, making them an easier target for attackers. Yet many of these small companies subcontract or work for larger companies – and thus hold intellectual property and trade secrets coveted by attackers. As one of our security engineers likes to say, while every subcontractor may sign a strict non-disclosure agreement, the attacker who is sitting on that small company's system is not bound by it.

In sum, whether they are attacking our computers, mobile phones or social networks, cyber-criminals are looking to profit by spying on us or stealing our information. Our best defense is strong security, education and awareness, and good computer hygiene.

Engagement with Law Enforcement

At Symantec, we partner with all levels of government, both here in the US and abroad. When requested, we work with law enforcement through traditional means, such as responding to subpoenas and warrants. In addition, 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. Of course, all of this work is done in keeping with both our strict privacy policies, and all applicable national and international privacy laws.

Symantec has a long and successful history of participation and leadership in various industry organizations, as well as public-private partnerships in the US and globally. Among these are the National Cyber-Forensics & Training Alliance (NCFTA), InfraGard, and INTERPOL. Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity and combatting cybercrime.

The NCFTA is a good example of how private industry and law enforcement partnerships can yield real world success. The NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners – from financial services and telecommunications to manufacturing and others – working with federal and international partners to provide real-time cyber threat intelligence to an actionable level in order to identify threats and actors, and provide intelligence to domestic and international law

enforcement to neutralize those threats. Through this partnership, hundreds of criminal investigations have been launched, which otherwise would not have been addressed, with successful prosecutions of more than 300 cyber criminals worldwide. In further support of these initiatives, the NCFTA has produced more than 400 cyber threat intelligence reports over the past three years alone. Through the NCFTA, Symantec is able to share crucial cyber threat information across a wide-ranging group of private industry and law enforcement entities at home and abroad.

InfraGard, of which Symantec serves on the National Board of Advisors, is another example of how law enforcement can partner with both private industry and individuals to share information on cyber threats. This successful partnership between the FBI and members of the private sector is focused on intrusions and vulnerabilities affecting 16 critical infrastructures. Comprised of a coalition of more than 55,000 private and public sector members, InfraGard promotes ongoing dialogue and timely communication between its members and the FBI. InfraGard members gain access to threat information that enables them to better protect their cyber and physical assets, as well as an avenue to share information with the government to help prevent terrorism and other crimes.

Cyberspace is a domain without borders, where crimes are often committed at a great distance. In effect, every computer in the US is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For this reason, Symantec works to maintain effective relationships and open communication lines with international law enforcement entities including INTERPOL, EUROPOL and individual national police forces, by making them aware of the latest technological trends, the evolution of the threat landscape and identifying some of the techniques that cybercriminals use to attack our customers. We also participated last fall in the first ever Industry Expert Meeting with the G8 High-Tech Crime Subgroup. The meeting was comprised of representatives of law enforcement, justice departments, and other governmental bodies of the G8 countries and private industry.

Unfortunately, both here in the US and around the world, there is a critical shortage of investigators, prosecutors, and judges who are adequately trained to handle complex cybercrime cases.

Recognizing this need, Symantec established the Norton Cybersecurity Institute (NCI) two years ago to help provide law enforcement with the skills to level the playing field with cybercriminals. Through the NCI, we have a number of initiatives whereby we work with law enforcement organizations and non-profit safety groups to provide training and technical expertise, and to help facilitate global cooperation. For example, through our partnership with the National Center for Justice and the Rule of Law (NCRLJ) and the US National Association of Attorneys General, Symantec has aided in training prosecutors in trying cybercrime cases as well as judges who adjudicate those cases.

This training can – and should – start when young lawyers are still in school. In March 2013, we sponsored a successful cyber moot court competition at UCLA School of Law. The competition helped the students develop their legal skills and introduced them to many of the difficult legal concepts surrounding cybercrime. Eleven law schools sent teams to compete – but more needs to be done.

It is important to remember that cybercrime is not victimless, and we do what we can to help the victims of cybercrime. We have partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make tools available to the public – for example, we offer free software that allows victims of ransomware and botnets to clean their systems.

Internationally, Symantec partners with various non-profit organizations, including the Canada-based Society for the Policing of Cyberspace (POLCYB), to provide training workshops to law enforcement officials and policymakers around the globe. Later this month, through our partnership with POLCYB, we are supporting a cybercrime workshop in Kiev, Ukraine to train law enforcement officials in the region. This is just one of several trainings offered annually to enhance public-private collaboration to identify and address gaps in cybercrime investigations and prosecutions. To date, we have partnered with POLCYB to train law enforcement officials and policy makers in more than 35 countries around the world.

Industry to industry partnerships also work. One example is the model that helped to bring down the Bamital botnet, a major takedown that happened earlier this year. This effort was the culmination of a multi-year investigation, in partnership with Microsoft and law enforcement, to dismantle the botnet. The Bamital botnet had taken over millions of computers for criminal activities such as identity theft and click fraud, threatening the $12.7 billion online advertising industry. This successful takedown demonstrates what can be done when private industry and law enforcement join forces to go after cybercriminal networks.

Current and Future Law Enforcement Efforts

Investigating and prosecuting cybercrime poses no less a challenge than does defending against cyber attacks. It is technically challenging, and requires a level of expertise and training that many police agencies and prosecutors are beginning to develop. It is also resource intensive – the time and money required to see a case from inception through to a successful conviction is often substantial. The criminals know this, and often count on it.

In the face of these obstacles, the amount of progress that has been made is impressive. Not too long ago, numerous cultural and organizational barriers prevented federal agencies from coordinating on the investigation and prosecution of international cyber criminals. Those barriers have come down, and today we see that kind of cross-agency coordination on a regular basis. John Boles, the Deputy Assistant Director of the FBI's Cyber Division, had it right when he told a House Subcommittee this past March that federal agencies "are coordinating at an unprecedented level."

The disruption of an Estonian cyber gang using the "DNSChanger" malware is an excellent example of the kind of real-world results that can come from this coordination. Dubbed "Operation Ghost Click," the criminals surreptitiously installed malware that changed the settings on a computer that control how it routes to websites, essentially hijacking a victim's searches and directing web browsers to ads that generated revenue for the criminals from phantom "clicks." The malware also prevented the victims from finding resources that might alert them to the infection. Working with the Estonian authorities, in 2011 the FBI arrested six members of the gang and shut down their operations.

But the effort did not stop with the arrests. Because simply shutting down the criminals' command servers would have effectively disconnected millions of unknowing victims from the Internet, the FBI worked with the DHS, the Courts, and the private sector to put in place infrastructure so that victims could still access the Internet safely and clean their machines of the infection. This type of effort was unprecedented: not only was a major criminal ring interrupted, but the government worked across agency lines and with the private sector to minimize the impact on the victims.

Operation Coreflood is another example of how effective legal tools can be when they are employed creatively. Coreflood was a piece of malware that infected and took over as many as two million

computers, creating a massive botnet. In this case, the FBI worked with private sector partners and obtained a court order that allowed them to commandeer the command and control servers, identify the infected computers, and send a command to each of them telling the malware to shut down.

Unfortunately, these examples highlight just how much still needs to be done. For while Ghost Click and Coreflood were successes for law enforcement, there are undoubtedly more – and larger – criminal rings operating today. This should not be taken as a criticism, however; the relative dearth of cases like these is not because the government does not want to pursue them, or because the criminals are not out there. The investigators and prosecutors are willing, and the private sector is eager to help. But unfortunately, cybercrime cases require a highly technical understanding of how computers and the Internet work. They are also time intensive – the Ghost Click investigation took more than two years, and the effort to disinfect affected computers took almost another year. There are simply not enough investigators, prosecutors, or judges who can handle them well, and the FBI, the Secret Service, and state and local law enforcement agencies need more personnel dedicated to fighting cybercrime.

And while the Courts proved helpful in those two cases, there is no doubt that law governing cybercrime needs to be modernized. In the US, we need to look at laws such as the Electronic Communications Privacy Act, which was written before most Americans had heard of email or the Internet and when cell phones were the size of bricks. This is no less true overseas. While Estonia had modern laws that allowed the US Government to work with them on Operation Ghost Click, most countries laws are playing catch up with the state of modern technology.

CONCLUSION

The threat landscape is constantly changing, and cyber criminals will not stop seeking new victims and new ways to compromise computers and networks. There is still much work to be done, but in one important way we have made progress: at all levels, government recognizes the imperative for collaboration to fight cybercrime and is working to fill the gaps in our law enforcement system.

At Symantec, we are committed to improving online security across the globe, and will continue to work collaboratively with governments 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.