Prepared Testimony and
Statement for the Record of

Jeff Greene
Senior Director, Global Government Affairs & Policy
Symantec Corporation

Hearing on

"The Current State of DHS Private Sector Engagement for Cybersecurity"

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

March 9, 2017

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Committee, my name is Jeff Greene and I am the Senior Director, Global Government Affairs and Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and recently supported the President's Commission on Enhancing National Cybersecurity. Prior to joining Symantec, I served as Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues.

Symantec Corporation is the world's leading cybersecurity company. We help organizations, governments and people secure their most important data wherever it resides. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on our Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing us to see and protect against the most advanced threats. We maintain nine Security Response Centers and six Security Operations Centers around the globe and every day we scan 30 percent of the world's enterprise email traffic and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts a unique view of the cyber threat landscape.

No government or company can go it alone in this environment, and we are happy to see the subcommittee focusing on how the private sector engages with DHS and other government agencies to help defend against growing cyber threats. Lasting improvements in cybersecurity require the combined efforts of government and industry together. In my testimony today, I will discuss:

- The current and emerging threat landscape;
- DHS and Private Sector Engagement; and
- How we partner with our industry counterparts to stop cyber attacks.

I. The Current and Emerging Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on massive data breaches and cyber espionage across the spectrum of industries and governments. These headlines remind us that no organization or government entity is impervious when targeted by a motivated and skilled attacker. Yet while the focus on data breaches and the personal information exposed is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and that can have damaging consequences. There is a wide set of tools available to the cyber-attacker, and the incidents we see today include increasingly sophisticated forms of ransomware, massive distributed denial of service (DDoS) attacks by "Internet of Things" (IoT) devices, sophisticated (and potentially destructive) intrusions into critical infrastructure systems, and the weaponization of personal information. The economic impact to an organization can be immediate, through the theft of money or the payment of ransom, 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, nation states, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – criminals generally are looking for some type of financial gain, hacktivists are seeking to promote or advance some cause, and 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.

Attack methods vary, and the only constant is that the techniques are always evolving and improving. Spear phishing, or customized, targeted emails containing malware or malicious links, is the most common form of attack. Many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach. Social media is an increasingly valuable tool to criminals as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. We have also seen the rapid growth of targeted web-based attacks, known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals lie in wait on legitimate websites that they compromise and use to try to infect visitors. Most of these attacks rely on social engineering – simply put, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychological as they are technological.

One particularly concerning trend is the recent use of IoT devices in DDoS attacks. By taking advantage of poor security and design practices, criminals were able to compromise hundreds of thousands, if not millions, of devices and aggregate them as a single army of zombie devices – the world's first major IoT botnet, known as Mirai. In October 2016, cybercriminals used the Mirai botnet to launch a massive DDoS Attack on DNS provider Dyn, which disrupted some of the Internet's biggest websites, including Spotify, Twitter, PayPal, Reddit and others. Mirai's "bots" were primarily compromised webcams and digital video recorders, but also included routers and other Internet connected devices. This attack was quickly followed by at least two others, each record-breaking in its size.

How did these IoT-based attacks happen? Very easily, unfortunately. The average IoT device is scanned for vulnerabilities *just two minutes after it is connected*, and when one is found that device is promptly compromised. The most common method is simple – criminals take advantage of pre-programmed, default usernames and passwords and simply log onto devices and commandeer them. With the explosion of insecure Internet-connected devices hitting the market, this type of attack will only continue to grow and become more effective.

II. DHS and Private Sector Engagement

The Department of Homeland Security has made considerable progress in recent years engaging with the private sector, especially in the area of information sharing. The Cyber Information Sharing and Collaboration Program (CISCP) is DHS's primary structure for private companies to share information about incidents, cyber threats and known vulnerabilities. This information is then shared among participating industry partners in an anonymized fashion to help secure their own networks. In addition, CISCP convenes cybersecurity practitioners at quarterly Advanced Technical Threat Exchanges (ATTE). We have been active in these exchanges, and late last year presented our research on ransomware, which included an in-depth analysis of new infection trends and payload execution. We provided a list of specific indicators that participants could use to further research and ensure their own systems were protected. We have also presented on how companies and governments can leverage threat intelligence to reduce "Indicator of Compromise (IoC) noise." Beyond the technical information shared, the ATTEs are helpful in building trusted relationships and contacts between government and private industry, and even within the private sector itself. These exchanges often lead to follow-on collaboration and, in some cases, joint research.

Another notable example of effective information sharing through the CISCP program came in October of last year when Symantec published a report exposing a hacking group that was trying to steal money from banks by exploiting the financial based SWIFT messaging system used to identify electronic transactions in the global financial system. In one of the highest-profile attacks of the year, attackers used this same method to steal $81 million from the Bangladesh Central Bank. Similar to the Bangladesh attack, Symantec found a previously unknown malware variant (called Odinaff) being used against financial institutions. This particular malware can delete customer logs of SWIFT transactions, allowing attackers to hide their tracks. We passed along our in-depth, technical research to CISCP managers along with a list of indicators including hashes, command and control nodes, and domains. The CISCP team then used our indicators to create an Indicator Bulletin (IB) and pushed it out to all CISCP participants for their use.

The quality of DHS's analysis reports can vary. Many reports include substantive analysis and actionable information, while some have fallen short. In those instances, many of the IoCs included in the report were unvetted, and companies that used them without proper care saw a high volume of false positives. In some cases the IoCs proved to be unrelated to the threat itself. To its credit, DHS is generally responsive to industry concerns and has on occasion issued updated reports with more information.

The importance of carefully vetting indicators is of increased importance as DHS moves to Automated Indicator Sharing (AIS). The AIS program allows the two-way exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. This means that as soon as a company or a federal agency identifies a threat, that indicator is shared in real time with all of the AIS participants. However, with an emphasis on velocity and volume, appropriate context and more vigor in vetting is necessary. Added context allows recipients to understand how to use an IoC or how to calibrate their internal response. To be sure, DHS and its partner agencies are in a difficult spot – the private sector is demanding both timely *and* vetted information, and this balance is not easy to strike. Industry has conveyed these concerns to DHS, which has worked to improve both its analysis and the quality of the indicators.

Another program DHS has implemented to engage with industry is the Critical Infrastructure Cyber Community or C³. The C³ is a voluntary program that helps critical infrastructure operators improve their cybersecurity and actively encourages the adoption of the Framework for Improving Critical Infrastructure Cybersecurity, commonly known as the NIST Cybersecurity Framework (CSF). The CSF was developed in collaboration with the private sector, and Symantec was part of that effort. We began using the CSF when it was still in draft form and was one of the first companies to map our internal security to it. We support DHS's efforts to encourage use of the CSF, both for companies with existing cybersecurity programs and for those who are building one from scratch.

In addition to the Department's formal programs, we work with DHS informally. For instance, just last week, we hosted a group of ten cyber threat analysts at our Herndon Security Operations Center to discuss specific threats and to explore potential areas to coordinate in the future. Among other topics, we discussed Shamoon, a family of destructive malware that we have tracked for years. Shamoon was used in attacks against the Saudi energy sector in 2012[1] and recently we have been tracking a fresh wave of attacks hitting the Middle East.[2] The opportunity to sit face-to-face and discuss threats often

[1] *The Shamoon Attacks*, Symantec Security Response, 8/16/12; https://www.symantec.com/connect/blogs/shamoon-attacks

[2] *Shamoon: Multi-staged destructive attacks limited to specific targets*, Symantec Security Response, 2/27/17; https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets

alleviates another concern among many private sector security companies, that too often the information flows just one way – from industry to the government. In-person exchanges often lead to a more complete and bilateral interchange of ideas.

Other Government Partnerships

Partnerships can lead to concrete results. One recent example came in December 2016, when Symantec concluded a decade-long research campaign that helped unearth an international cybercriminal gang dubbed "Bayrob." The group is responsible for stealing up to $35 million from victims through auto auction scams, credit card fraud and computer intrusions. Through our research, we discovered multiple versions of Bayrob malware, collected voluminous intelligence data, and tracked Bayrob as it morphed from online fraud to a botnet consisting of over 300,000 computers used primarily for cryptocurrency mining. Over time, Symantec's research team gained deep technical insight into Bayrob's operations and its malicious activities, including its recruitment of money mules. These investigations and countermeasures were crucial in assisting the Federal Bureau of Investigation (FBI) and authorities in Romania in building their case to arrest three of Bayrob's key actors and extradite them to the U.S.

Indeed, in recent years we have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world. In July 2015, a New York judge sentenced Alexander Yucel, the creator of the "Black Shades" Trojan to five years in prison and the forfeiture of $200,000. Yucel was swept up by the FBI and Europol last year along with dozens of other individuals in the US and abroad. Symantec worked closely with the FBI in this coordinated takedown effort, sharing information that allowed the agency to track down those suspected of involvement. In June 2015, Ercan "Segate" Findikoglu, who prosecutors say orchestrated one of the biggest cyber bank heists in American history, was extradited to the US to stand trial for stealing more than $55 million by hacking bank computers and withdrawing millions in cash from ATMs.

Additionally, government and private sector cooperation has led to takedown operations against prominent financial fraud botnets. In June of 2014, the FBI, the United Kingdom (UK) National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet Gameover Zeus and the ransomware network Cryptolocker. Gameover Zeus was the largest financial fraud botnet in operation in 2014 and is often described as one of the most technically sophisticated variants of the ubiquitous Zeus malware. Symantec provided technical insights into the operation and impact of both Gameover Zeus and Cryptolocker, and worked with a broad industry coalition and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.

III. Private Sector Partnerships to Enhance Cybersecurity – the Cyber Threat Alliance

While DHS continues to engage industry, the private sector is not just waiting on the government to solve the problem. Industry partnerships have proven to be highly effective in fighting cybercrime. The Cyber Threat Alliance (CTA) is an excellent example of the private sector banding together to improve the overall safety and security of the Internet. In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the CTA to work together to share threat information. Since that time, Cisco and Checkpoint have joined the CTA as founding members. The goal of the CTA is to better distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers.

Prior industry sharing efforts were often limited to the exchange of malware samples, and the CTA sought to change that. Over the past three years the CTA has consistently shared more actionable threat intelligence such as information on "zero day" vulnerabilities, command and control server information, mobile threats, and indicators of compromise related to advanced threats. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations. In short, the CTA is not about one vendor trying to gain advantage — we are all contributing and sharing with the community.

Because of the success of the CTA, the founding members decided to take it to the next level and earlier this year formally incorporated it as a non-profit organization. Working together, CTA members have developed a new platform designed to automate intelligence sharing in near-real time. Through this effort we hope to solve some of the problems created by isolated and manual approaches to cyber threat intelligence. The new CTA has three purposes:

1. To share threat information in order to improve defenses against advanced cyber adversaries across member organizations and their customers;
2. To advance the cybersecurity of critical information technology infrastructures; and
3. To increase the security, availability, integrity, and efficiency of information systems.

CTA is also committed to engaging in discussions around policy initiatives that will improve cybersecurity for individuals and governments. As CTA moves forward with its mission, it intends to explore how to best partner with US and international government organizations in furtherance of its mission.

Conclusion

As the Members of this Subcommittee know better than most, we still face significant challenges in our efforts to improve cybersecurity and fight cybercrime. Cybersecurity is a team sport and effective public private partnerships with DHS and other government agencies are essential. DHS and industry have made notable progress over the last several years – trust has improved – but there is still room for growth. Attackers are always evolving, becoming more sophisticated, and both government and industry recognize the imperative for cooperation to fight cybercrime. At Symantec, we are committed to improving Internet security across the globe, and will continue to work collaboratively with industry and government partners like DHS 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.