Prepared Testimony and
Statement for the Record of

Bill Wright
Director, Government Affairs & Senior Policy Counsel

Hearing on

"Promoting Security in Wireless Technology"

Before the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology

June 13, 2017

Chairman Blackburn, Ranking Member Doyle and members of the Committee, thank you for the opportunity to testify today on behalf of Symantec.

My name is Bill Wright and I am the Director of Government Affairs and Senior Policy Counsel at Symantec, managing a number of global cybercrime and cybersecurity operational relationships. I am responsible for Symantec's global partnership program agenda and government engagement strategy, which includes cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. In this capacity, I work extensively with industry, government agencies both at home and abroad. Prior to joining Symantec, I was a Staff Director for two U.S. Senate Subcommittees focused on homeland security, government IT and oversight and before that was a Senior Operations Officer at the National Counterterrorism Center Operations Center (NCTC).

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence NetworkTM tracks over 700,000 global adversaries and is comprised of more than 98 million attack sensors, which record thousands of events every second. This network monitors over 175 million endpoints located in over 157 countries and territories. In addition, we process more than 2 billion emails and over 2.4 billion web requests each day. We maintain nine Security Response Centers and six Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape. 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.

The cyber headlines of the past year have focused on sophisticated state sponsored attacks and global ransomware outbreaks. Cyber attacks are growing both in number and in sophistication. As we move to 5G technologies, billions of new devices will be connected to the Internet, transmitting massive amounts of information and substantially increasing the attack surface. While attacks against traditional desktops and servers have dominated the threat landscape in terms of numbers, there is a growing focus on other platforms, such as wireless networks, IoT, and mobile devices that attackers are now actively targeting.

Wireless devices are now an essential part of our daily lives, and it is essential that they, and the data they contain, remain safe and secure. Understanding the current threat environment is essential if we are going to craft good policy and effective defenses. We are therefore pleased to see the Committee's continued focus on this subject, and appreciate the opportunity to provide our insights.

In my testimony today, I will discuss:

- The Size and Scope of the Cyber Threat Landscape;
- Growing threats across new platforms;
- Mobile threats and best practices; and
- Public-Private Partnerships.

I. The Current and Emerging Cyber Threat Landscape - Overview

Cyber attacks reached new levels in 2016, a year marked by multi-million dollar virtual bank heists, explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, a record number of identities exposed in data breaches, and some of the biggest distributed

denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices. Yet while the attacks caused unprecedented levels of disruption and financial loss, perhaps the most striking feature of the 2016 attack landscape is that in many cases the attackers used very simple tools and tactics. During 2016, valuable Zero-day vulnerabilities and sophisticated malware was used more sparingly than in recent years. Instead, attackers increasingly attempted to hide in plain sight. They relied on straightforward approaches, such as spear-phishing emails and "living off the land" by using common tools, such as legitimate network administration software and operating system features. Yet despite this trend away from sophisticated attacks, the results were extraordinary, including:

- Over ***1.1 billion*** identities exposed;
- ***Power outages*** in the Ukraine;
- Over ***$800 million*** stolen through Business E-mail Compromise (BEC) scams over just a ***six month period***;
- ***$81 million*** stolen in one bank heist alone;
- A ***tripling*** of the average ransomware demand;
- Average time-to-attack for a newly connected Internet of Thing device down to ***two minutes***.

These shifting tactics demonstrate the resourcefulness of cyber criminals and attackers – but they also show that improved defenses and a concerted effort to address vulnerabilities can make a difference. Attackers are evolving and developing new attacks not because they want to, but because they have to do so. And that evolution comes with a financial cost to the attacker.

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we currently face. During 2016, criminal gangs engaged in indiscriminate campaigns involving massive volumes of malicious emails that in some cases overwhelmed organizations by the sheer volume of ransomware-laden emails alone. Attackers are demanding more and more from victims, and the average ransom demand *more than tripled* in 2016, from $294 to $1,077. The number of new ransomware families also more than tripled to 101, from 30 in both 2014 and 2015. The volume of attacks increased as well. Detections were up 36% percent from 2015, and by December we were seeing almost twice the daily volume that we observed in January.

2016 also saw the emergence of Ransomware-as-a-Service (RaaS). This involves malware developers creating ransomware kits, which can be used easily to create and customize new variants. Typically the developers provide the kits to attackers for a percentage of the proceeds. One example of RaaS is Shark (Ransom.SharkRaaS), which is distributed through its own website and allows users to customize the ransom amount and which files it encrypts. Payment is automated and sent directly to Shark's creators, who retain 20 percent and send the remainder on to the attackers. Our statistics show that, for the most part, attackers are concentrating their attacks on countries with developed, stable economies – 34% of the detections were in the US, and another 39% spread among the United Kingdom, Australia, Germany, Russia, the Netherlands, Canada, India, Italy.

The world of cyber espionage experienced a notable shift towards more overt activity in 2016, much of which was designed to destabilize and disrupt targeted organizations and countries. We saw:

- a January attack against the Ukrainian power grid;
- an attack on the World Anti-Doping Agency and subsequent release of test results;
- a widespread, destructive attack on computers in Saudi Arabia; and

- a second attack against the Ukrainian power grid in December.

In years past, any one of these events would have been the biggest story of the year. But in 2016, we also saw an attack on the US Presidential election, an operation that the Intelligence Community (IC) attributed to Russia. Cyber attacks involving sabotage have traditionally been rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in the attacks on the Ukraine in January and again in December, resulting in power outages. Additionally, a disk-wiping trojan known as Shamoon reappeared after a four-year absence and was used against multiple organizations in Saudi Arabia. Previously, Shamoon was used in highly destructive attacks against Saudi and other Middle Eastern energy companies, and press reports linked it to Iran.

In 2016, cyber criminals expanded their focus from individual bank customers to the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. Two groups targeted the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network and stole SWIFT credentials. They used those credentials to initiate fraudulent transactions and covered their tracks by doctoring the banks' printed confirmation messages to delay discovery of the transfers. One group began its attack at the start of a long weekend to reduce the likelihood of a quick discovery.

Good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving and adapting, and security must as well.

II. Growing threats Across New Platforms

And while ransomware and financial fraud groups continue to pose the biggest threat to individual users, other threats are beginning to emerge. It was only a matter of time before attacks on IoT devices began to gain momentum, and during 2016 Symantec witnessed a twofold increase in attempted attacks against IoT devices. 2016 also saw the first major incident originating from IoT devices, the Mirai botnet, which was composed of routers, digital video cameras, and security cameras. Weak security – in the form of default and hard-coded passwords – made these devices easy pickings for attackers. After compromising millions of devices, the attackers controlled a botnet big enough to carry out the largest DDoS attacks ever seen. In October, the combined power of these compromised devices led to brief outages at some of the most popular websites and online services in the world. Mirai's impact was further magnified when the developer released the source code for the malware, which led to copycat efforts by other groups.[1]

Though there is no single way to fix a complex problem like this, risk-based baseline security standards are part of the solution. Of course, manufacturers should take the lead role in the security of the products that they are sending to market. They should provide consumers a level of transparency in the security of connected devices so that consumers can make informed decisions. This also allows security to become an inherent feature of a device, which would allow premium manufacturers to differentiate their products based on security.

As cloud usage by both enterprises and consumers has become mainstream, attackers have increased their focus on it. While cloud attacks are still in their infancy, last year we saw the first widespread outage of cloud services as a result of a denial of service (DoS) campaign, serving as a warning for how susceptible cloud services are to malicious activity. Widespread adoption of cloud applications in

[1] See *Symantec Internet Security Threat Report,* XXII, April 2017 pp. 68

corporations, coupled with risky user behavior that the corporation may not even be aware of, creates new opportunities for cloud-based attacks.

Part of this is because many organizations simply do not understand how much they rely on the cloud. At the end of 2016, the average enterprise organization was using 928 cloud apps, up from 841 earlier in the year. However, our research found that most CIOs believed that their organizations were using only 30 to 40 cloud apps. Attackers, on the other hand, grasp the opportunity for mischief and crime in the cloud - during 2015, we identified more than 3 million malicious apps that were in fact malware, which was nearly 30% of all apps that were analyzed. Most of these malicious apps were from third party app stores.[2]

III. Mobile Threats

With billions of smartphones and tablets and tens billions of Internet-connected devices coming on line, the focus of Internet security must shift from the desktop to the pocket, the purse, and the home. Today more than half of the world's population uses a smartphone and more than half of the world's web traffic now originates from mobile phones.[3] In the United States, these trends are even higher. People are using their mobile devices in nearly every aspect of their lives – from accessing their bank accounts, to sensitive health and business activity, to conducting e-commerce. The lines are quickly blurring between what constitutes a work device and a personal device. Our mobile devices are filled with valuable personal and business related data, and more often than not, the information stored on a mobile device is worth far more than the device itself.

Unfortunately, the very attributes that make mobile devices attractive to consumers also make them an enticing target for cybercriminals. Criminals use a number of techniques to steal or otherwise monetize your information including, phishing, malware, and ransomware. These threats are evolving and becoming more sophisticated. Cybercriminals are bound only by their imagination.

Mobile Malware: The number of malware detections on mobile devices doubled in 2016 to more than 18 million. Cybercriminals continue to employ mobile malware primarily for financial theft and fraud, using tried and true monetization methods, such as stealing user account credentials (i.e. banking), sending premium text messages, advertisement click-fraud, and ransomware. Infections can occur in a number of ways – from downloading a malicious applications to visiting an infected website. Malware targeting financial institutions and their customers have focused on mobile users more often in the last year. In response, financial institutions have increased their security measures in their interactions with customers and also on their own backend systems. However, cybercriminals are adapting and mimicking the customer's behavior as closely as possible and attacking the institution themselves. Since the introduction of mobile banking apps and two-factor authentication (2FA), cyber criminals have had to look for ways to either bypass 2FA using social engineering or by attacking the mobile device itself. 2FA is an added security authentication tool that requires not only a password and username but also something that only the user would know or have access to.[4]

[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[3] https://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview
[4] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

Mobile Ransomware: Ransomware has dominated the threat landscape for the last two years and has achieved mainstream notoriety with the May 12th global outbreak of the WannaCry Ransomware. WannaCry hit more than 300,00 victims in 150 countries, and crippled Britain's National Health Services and other critical sectors.[5] Criminals are taking lessons they learned from traditional ransomware attacks on PCs and applying them to mobile platforms. Like its PC counterpart, mobile ransomware infects your device and encrypts sensitive data, and then demands payment, often via Bitcoin, in exchange for unlocking or returning you data. Mobile ransomware most often masquerades itself as a legitimate app, usually in a third party app store. In many ways, mobile devices are more integrated into our daily lives than our PCs ever were, and as a result mobile ransomware can have a devastating impact on consumers and business alike.

Mobile Phishing: The popularity of mobile devices has made them a frequent target of traditional web-based attacks, especially phishing.[6] Phishing is another example of how tried and true PC-based attacks have been adapted to mobile platforms. Phishing is not a new attack, and is rooted in social engineering – aiming to trick the user into doing something they would never do if they were fully aware of the dangers. In a traditional, PC based phishing attack if a criminal wanted to steal your banking credentials he would compose an email or a social media posting to lure the victim to a fake website, designed to look legitimate. There, the unwitting victim would use his log-on credentials, passing them onto the cybercriminal. However, mobile users are far less likely to log into their bank through a web browser, so the savvy criminal phishes through malicious apps. Mobile apps are self-contained tools and enjoy a higher level of trust. While phishing apps are a new take on an old theme, they are highly effective at stealing your information.

Public-Private Partnerships

The growing challenge of securing the mobile environment will require more than just increased user awareness. It will take participation from all of the mobile communication stakeholders – ISPs, device manufacturers, software developers, security vendors, government, consumers, and enterprises to help secure the mobile ecosystem. Symantec partners closely with governments to help identify threat trends, share threat information, develop innovative security tools, and publish best practices.

Some partnership programs are formal, such as the Cyber Information Sharing and Collaboration Program (CISCP). This is DHS's primary structure for private companies to share information about incidents, cyber threats and known vulnerabilities. For example, last October, we used the CISCP program to share a report we published that exposed one of the groups that was trying to steal money from banks by exploiting the SWIFT messaging system. Through CISCP, 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.

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

[5] https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
[6] http://www.csoonline.com/article/3103296/mobile-security/mobile-phishing-same-attacks-different-hooks.html

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. They are currently in federal custody awaiting trial.

The private sector is also working together to counter cybercrime and industry partnerships have proven 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, including mobile threats. 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.[7]

Conclusion

At Symantec, we work hard to educate consumers by providing guidelines to protect personal data on the Internet. There are a number of basic things that consumers can do to protect themselves from common mobile threats. First and foremost, both consumers and employers should begin treating mobile devices like the small, powerful, computers that they are, including:

- Regularly patch and update your software.
- Do not download apps from unfamiliar sites.
- Use different passwords for different apps.
- Pay close attention to the permissions being requested by apps.
- Install security on your mobile devices.
- Make frequent backups of important data.
- Be vigilant for phishing schemes.

Effectively defending networks and devices will require continuous innovation. As our wireless networks move to 5G technologies, we will be connecting more and more devices to the Internet and transferring previously unimaginable amounts of data. The trust in the Internet will hinge on how secure that data, those devices, and those networks can be made. We are pleased to assist the Committee as it examines these issues.

[7] https://cyberthreatalliance.org