Prepared Statement

for the Record of

Ken Durbin, CISSP

Senior Strategist: Global Government Affairs & Cybersecurity

Symantec Corporation

Hearing on

"Assessing the State of Federal Cybersecurity Risk Determination"

Before the

United States House of Representatives

Committee on Homeland Security

Subcommittee Cybersecurity and Infrastructure Protection

July 25, 2018

Chairman Ratcliffe, Ranking Member Richmond, my name is Ken Durbin, CISSP, and I am a Senior Strategist for Symantec Global Government Affairs and Cybersecurity. I have been providing Solutions to the Public Sector for over 30 years. My focus on Compliance and Risk Management (CRM) and the Critical Infrastructure Sector has allowed me to gain insights into the challenge of balancing Compliance with the implementation of Cybersecurity Solutions. Additionally, I focus on the Standards, Mandates and Best Practices from NIST, OMB, DHS, SANS, etc. and their application to CRM. I spend a significant amount of my time on the NIST Cybersecurity Framework (CSF)[1], the DHS CDM Program and the emerging EU Global Data Protection Regulation (GDPR.)

Symantec Corporation is the world's leading cybersecurity company and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries, records events from 126.5 million attack sensors worldwide, and monitors threat activities in over 157 countries and territories. Additionally, 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. On our consumer side, we combined Norton Security with LifeLock's Identity and Fraud Protection to deliver a comprehensive cyber defense solution to a growing consumer base of nearly 4.5 million people.

In my testimony I will provide:

- an overview of the current threat landscape, including highlights of our 2018 Internet Security Threat Report (ISTR)[2]
- an assessment of the Federal Cybersecurity Risk Determination Report and Action Plan that was released in May
- high level recommendations on addressing some of challenges highlighted in the report.

The Threat Landscape

From the recent Thrip attack on satellite and telecommunications systems to the spread of WannaCry and Petya/NotPetya, to the rapid growth in coinminers, the past year has provided us with many reminders that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so. Symantec's annual ISTR provides a comprehensive view of the threat landscape, including insights into global threat activity, cyber criminal trends, and motivations for attackers. Below are some key highlights from this year's report and our recent work.

---

[1] NIST Cybersecurity Framework (CSF): Provides guidance to private companies on how best to prevent, detect, and respond to Cyber attacks.

[2] https://www.symantec.com/security-center/threat-report

Attackers are Evolving

Last month, we issued a report about a previously unknown attack group known as Thrip[3]. Thrip is a sophisticated attacker that used a technique we call "living off the land" – using operating system features or legitimate network administration tools to compromise victims' networks. Simply put, they use good programs to do bad things. These types of attacks are difficult to detect because malicious activity is disguised as normal system operations. This continued a trend we reported on in the ISTR, that attackers are relying less on malware and zero-day vulnerabilities. Instead, they are looking for new attack vectors that make less "noise" and can be hard for some defenders to detect.

When we discovered Thrip, they had already compromised satellite operators, telecommunications companies, and a defense contractor. We identified this malicious activity using an advanced hunting tool we call Targeted Attack Analytics, which crawls through massive data sets looking for minute indicators of malicious activity. When we find something – like Thrip – we update our protections to stop it in the future. Thrip was not the first living off the land attack, and it will not be the last, and defenders must evolve to stay ahead of the next attack.

Cryptojacking

During the past year, an astronomical rise in cryptocurrency values triggered a cryptojacking gold rush with cyber criminals attempting to cash in on a volatile market. This gave rise to a new category of malware called "coinminers" that attach to an individual's browser and utilizes their computers processing power to mine cryptocurrency. Detections of coinminers on endpoint computers increased by 8,500 percent in 2017. With a low barrier of entry – only requiring a couple lines of code to operate – cyber criminals are harnessing stolen processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency. Coinminers can slow devices, overheat batteries, and in some cases, render devices unusable. For enterprise organizations, coinminers can put corporate networks at risk of shutdown and inflate cloud CPU usage, adding cost. Macs are not immune either, with Symantec detecting an 80 percent increase in coinmining attacks against Mac OS. By leveraging browser-based attacks, criminals do not need to download malware to a victim's Mac or PC to carry out cyber attacks.

[3] https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets?om_ext_cid=biz_social_NAM_twitter_Asset%2BType%2B%2B-%2BBlog,Campaign%2B-%2BThreat%2BAlert

IoT

IoT devices continue to be ripe targets for exploitation. Symantec found a 600 percent increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine *en masse*.

Targeted Attack Groups

The number of targeted attack groups is on the rise with Symantec now tracking 140 organized groups. Last year, 71 percent of all targeted attacks started with spear phishing – the oldest trick in the book – to infect their victims. As targeted attack groups continue to leverage tried and true tactics to infiltrate organizations, the use of zero-day threats is falling out of favor. Only 27 percent of targeted attack groups have been known to use zero-day vulnerabilities at any point in the past. The security industry has long discussed what type of destruction might be possible with cyber attacks. This conversation has now moved beyond the theoretical, with one in ten targeted attack groups using malware designed to disrupt.

Supply Chain Attacks

Symantec identified a 200 percent increase in attackers injecting malware implants into the software supply chain in 2017. That's equivalent to one attack every month as compared to four attacks the previous year. Hijacking software updates provides attackers with an entry point for compromising well-guarded networks. The Petya outbreak was the most notable example of a supply chain attack. After using Ukrainian accounting software as the point of entry, Petya used a variety of methods to spread laterally across corporate networks to deploy their malicious payload.

Ransomware for Profit

In 2016, the profitability of ransomware led to a crowded market. In 2017, the market made a correction, lowering the average ransom cost to $522 and signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cashing in while cryptocurrency values are high. Additionally, while the number of ransomware families decreased, the number of ransomware variants increased by 46 percent, indicating that criminal groups are innovating less but are still very productive.

Assessment of the Federal Cybersecurity Risk Determination Report and Action Plan

The Office of Management and Budget (OMB), in response to Presidential Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* produced a report that provides a tough but fair assessment of the current state of the Executive Branch's Cybersecurity Posture. The EO and the report builds upon the efforts of

previous administrations and works within existing frameworks, including FISMA[4], FITARA[5], CDM[6], and CSF. While none of these are perfect, OMB sees their value and seeks to improve them. The EO held OMB to a tight timeline in which to produce the report and OMB held agencies to a similarly aggressive timeline. This alone sent a strong message, both about the seriousness of the situation and about the Administration's commitment to improving the Executive Branch's Cybersecurity posture.

As a threshold matter, I would like to commend the Administration and OMB for recognizing the value of the CSF as a tool to improve the current state of the Executive Branch's Risk Management efforts. The CSF's power is its ability to take a complex set of cybersecurity data and present them in a clear, logical and simplified way such that one does not need to be a cyber expert to gain valuable insight and make important decisions. For example: An agency now needs to collect data from over 200 FISMA controls across 10 Control Families to evaluate cybersecurity readiness. That same data can be consolidated into the five CSF Functions (Identify, Protect, Detect, Respond, and Recover) for a clearer view into their cyber readiness.

Recommendation #1: Increase Cybersecurity Threat Awareness

To highlight the need for increasing cybersecurity threat awareness, the report points out that "38% of Federal cyber incidents did not have an identified attack vector." This equates to 11,802 cyber incidents that "led to the compromise of information or system functionality in FY 2016." To improve this situation the report recommends implementing the Cyber Threat Framework (CTF) with the idea that it will help prioritize and manage cybersecurity risks. The CTF was developed to enable consistent characterization and categorization of cyber threat events, in other words, to provide a common lexicon to describe and understand threats. This, of course is a worthwhile pursuit, but it is not clear how the CTF would have helped protect against the 11,802 cyber events that compromised information and systems.

I recommend that, along with implementing the CTF, OMB put a strong emphasis on cybersecurity solutions that can automate the detection and remediation of cyber events. Automated cybersecurity solutions that can communicate between strategic control points hunting for indicators of compromise (IoCs) will help to reduce the number of unidentified attacks, and reduce the burden caused by the shortage of qualified cyber professionals.

I applaud OMBs efforts to develop a Risk-Based-Budgeting process to help direct IT purchases towards products, solutions, and services that will have a direct impact on reducing identified risk. OMB may want to consider taking this effort one step further to address one long-standing

[4] Federal Information Security Management Act: Requires Government agencies to implement security systems to protect information and information systems.
[5] Federal Information Technology Acquisition Reform Act: Changed the way the Federal Government buys and manages its computer technology
[6] Continuous Diagnostics and Mitigation: Four phase program that monitors what is on a network, who is on a network, what is happening on a network, and how data is protected for Federal agencies.

issue around Agency IG Report Recommendations. IG Reports regularly contain risk-based recommendations that are carryovers from previous years reports, and often they remain unresolved due to budget or staffing issues. Adding IG recommendations as line items in an agencies budget request could be a way to ensure the recommendations receive adequate prioritization. Additionally, DHS has modified the CDM Program to allow agencies to submit Requests for Service (RFS) to fulfill specific needs. Known as CDM DEFEND, this may be another vehicle to address risk-based procurement.

Recommendation #2: Standardize IT and Cybersecurity Capabilities

This recommendation harkens back to the massive GSA "Desktop" Contracts of the 1980's and 1990's. For the most part those contracts mandated a standardized PC platform with specific software preinstalled. (The original contract required a Zenith 286 with DOS, Harvard Graphics, Lotus123 and WordStar.) This did have some of the same advantages spelled out in the report, including consistent software versions, ease of patching, known configurations, and simplified troubleshooting. The downside was that even if a competitor of Zenith had a better PC it was next to impossible to justify not using the Desktop Contract.

I believe the Continuous Diagnostics and Mitigation (CDM) concept achieves the goals set forth in this recommendation by focusing on standardized *capabilities* rather than a standardized vendor. However, in order to be effective in meeting this goal, the CDM Program will need move faster - five years after CDM was launched Phase 1 has still not been fully deployed. DHS has taken steps to accelerate the program, launching CDM DEFEND, which utilizes the GSA Alliant Contract and extends the period of performance of awarded Task Orders.

Recommendation #3: Consolidate Agency SOCs

Redundant Security Operation Centers (SOCs) working in silos are ineffective when trying to defend an enterprise. Consolidating SOCs and coordinating their efforts will improve overall incident detection and response. OMB states that only 47% of agencies can detect encrypted exfiltration incidents, and only 27% have the ability to detect an exfiltration attempt. Consolidation is part of the solution but detecting the exfiltration of data by a SOC across an agency, especially a federated agency requires more than consolidation. A SOC must have the right tools in place to tag and monitor the activity of sensitive data on an endpoint, server, data center, in storage or in the cloud. A SOC also needs the ability to look into encrypted traffic and scan for sensitive data and malware. If a SOC does detect a data exfiltration threat, the SOC needs to have a solution in place to mitigate the threat, preferably utilizing automation.

Recommendation #4: Drive Accountability Across Agencies

I would like to focus on the "data-level-protections" aspect of this recommendation. OMB acknowledges the call from industry, privacy advocates and the GAO for an increased focus on data level protections. However, the government *must* expand the scope of data level *protection* to include data level *prevention* as well. Far too often we see the government equate data level protection with the encryption of data, both in transit and at rest. Encryption is important, but its focus is limited to data "protection." This thinking needs to be expanded to include *prevention* – specifically "data loss prevention" (DLP) capabilities that prevent the misuse of data in the first place. DLP solutions can discover where sensitive data lives, categorize the data based on its sensitivity and control who has access to the data. DLP can also enforce policies that describe what can be done with data. For example; DLP can block data from being copied to a thumb drive, emailed to a personal email account, block access to data from certain locations or during certain times. DLP can even automatically encrypt data before its transmitted even if the end user forgot to encrypt it themselves.

CDM is slated to address Data Protection in Phase 4 of the Program. I recommend that DHS advance Data Protection so it is implemented concurrently with ongoing and planned CDM Task Orders. This would have the added benefit of maximizing the effort undertaken by agencies during the OMB mandated Cyber Sprint of 2015 and its follow-on components. Under the Cyber Sprint agencies were to identify their "high-value" assets but were not provided with solutions to protect those assets. The Data Protection capabilities of CDM, along with CDMs funding would go a long way toward protecting high-value assets in a timely manner.

Conclusion

This committee understands as well as anyone that cyber threats are growing in number and complexity at an alarming pace and that government agencies continue to be an attractive target. The OMB report takes a clear-eyed and unbiased look at the current state of our cybersecurity preparedness and does not shy away from pointing out areas that need significant improvement, and makes recommendations that build upon proven efforts of previous administrations. I hope my ideas can build on OMBs recommendations and maximize their ability to improve our governments cybersecurity posture. Thank you for the opportunity to testify before this committee, and I would be happy to take any questions you may have.