FIREEYE RESPONSE TO THE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY RFI

DATE: SEPTEMBER 9, 2016

CONTACT: KLARA T. JORDAN, GOVERNMENT AFFAIRS MANAGER

EMAIL: KLARA.JORDAN@FIREEYE.COM

INPUT TO THE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

CONTENTS

Introduction

FireEye appreciates the opportunity to provide a response to the Commission on Enhancing National Cybersecurity's (the 'Commission') Request for Information issued on August 10, 2016. These comments are informed by FireEye's experience responding to and analyzing critical security incidents at hundreds of organizations each year and protecting more than 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000 on a daily basis. FireEye has unique insights into the value of tools and processes necessary to face evolving threats as a result of our over 10 years experience evaluating security programs maturity and readiness, being close to all the major cybersecurity breaches, running an Information Sharing Network, providing advanced warning from cutting-edge intelligence, and advanced detection to rapidly growing and diverse worldwide client base.

FireEye is providing comments in the following areas:

1. Cybersecurity metrics

2. Use of security-as-a-service (SECaaS) providers for small- and medium-sized organizations

3. Critical infrastructure cybersecurity; and

4. Cybersecurity insurance

We appreciate the opportunity to offer our recommendations to the next Administration. FireEye is proud of our contributions to protecting clients across the United States, both in the private or public sector. We look forward to future opportunities to engage in discussion on both the recommendations contained within this document, as well as other cybersecurity topics of interest – past, present, and future.

FireEye Recommendations for Enhancing National Cybersecurity

1. **FireEye recommends that the future Administration revises and significantly enhances FISMA metrics relating to respond and recover functions**.

   Given that 96 percent of typical defense-in-depth deployments have been breached, [1] and that attackers had free reign in breached environments for 146 days on average[2] the question is no longer whether an organization may be breached, but when and whether the organization has the requisite resources to mitigate the impacts of a breach. In light of the increasing inevitability of breaches and the potentially serious impact, the need for an effective incident response plan to manage risk after a breach becomes crucial. By detecting and identifying indicators of compromise early, organizations and government agencies may minimize the overall impacts of a breach—business disruption, loss of sensitive data, harm to data integrity, and damaged reputation. An incident response plan built and improved over time is one based on metrics for incident response processes. These metrics allow for measuring successes, progress and goal setting, and helping mature incident response capabilities of an organization.

   In the past decade, the Federal Government has seen an increase in the number and severity of breaches impacting its information, systems, and services. While the Federal Information Security Management Act (FISMA) metrics and the Federal adoption of NIST Cybersecurity Framework provide useful tools to measure some aspects of agencies' cybersecurity performance, they do not illustrate the efficiency and effectiveness of their ability to detect, contain, and remediate incidents.

   For example, currently FISMA metrics in the respond and recover section focus on the frequency of updates of incident response plan and the number of incidents reported to a SOC. These metrics provide little information on the efficiency of people, processes, and technology in the incident response area, which is a critical shortcoming.

   FireEye recommends that the future Administration revises and significantly enhances FISMA metrics relating to respond and recover functions to include metrics for dwell time and containment time of an incident. The dwell time refers to the time from the initial compromise through the point of notifying affected stakeholders. The containment time refers to the period between collecting live response data and the eventual remediation—either the time necessary to prevent the threat from communicating or moving laterally or full restoration of services. These tools would allow the OMB to track and measure how rapidly agencies are detecting, responding and containing breaches, whether they have the necessary tools to improve their incident response capabilities, and whether they are improving over time.

   These metrics enable measure the efficiency of the incident response plan, identify areas for improvement, and inform asset allocation in an effort to develop a more robust incident response capability. The enclosed reference document provides recommendations on how to break down these metrics into component parts and their individual benefits.

2. **FireEye recommends that the Administration incentivize the use security-as-a-service (SECaaS) providers for small- and medium-sized organizations.**

   Currently, cyberspace is characterized by a growing number of complex threats that are not only challenging to mitigate and eliminate, but also tough to detect. The security focus has shifted from attempting to prevent

[1] FireEye. "Maginot Revisited: More Real-World Results from Real-World Tests." January 2015.
[2] https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

breaches to correctly identifying and remediating attacks swiftly enough to contain and minimize any damage or loss. Advanced threat actors are successfully utilizing sophisticated and non-sophisticated tactics, techniques, and procedures to easily bypass conventional security deployments almost at-will and they engage in targeting individuals, not just in force-on-force engagements against government networks but increasingly small and medium sized businesses, which are at the core of the U.S. economy in terms of output, employment, and innovation.

This is not a fair fight and as most small and medium sized organizations possess neither the resources nor the expertise to defend against these threats. In particular, most small- and medium-sized businesses have limited resources and workforce to implement a comprehensive cybersecurity program; yet, they have extremely complex environments to manage. These organizations are unlikely to be able to fully leverage the recent efforts to improve cybersecurity through information-sharing. In particular, these organizations have limited resources and ability to monitor, process, contextualize, and take action on threat and vulnerability information that they receive from information-sharing forums and sources. Adding to the complexity is the proliferation of connected devices, the need to access data and applications at any place and time, large number of security alerts flowing from different appliances, and lack of interoperability between products, making it almost impossible to correlate findings and alerts and create any meaningful context. The burden of procuring, deploying, and maintaining security products raises costs and workforce requirements that many small- and medium- sized organizations can neither afford nor maintain.

To ensure that small- and medium-sized businesses are protected, FireEye recommends that the Administration incentivize the use of security-as-service (SECaaS) providers through the use of tax credits or liability caps. The National Institute for Standards and Technology (NIST) should also encourage and incorporate in the NIST Cybersecurity Framework the use of SECaaS as a risk-management best practice for small- and medium-sized businesses to achieve establishment of a new or augmentation of existing cybersecurity program. This option becomes increasingly attractive and implementable as organizations migrate to the cloud.

Use of SECaaS providers is an effective way for most organizations to address their security comprehensively—from threat protection, actionable intelligence, investigation and incident response to ensuring that the organization has the right technology in place to address its security needs. Having a seamless and scalable extension of organizations' security operations eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber-attacks.

3. **FireEye recommends systemic and technical improvements in critical infrastructure cybersecurity.**

In the past several years, a flood of vulnerabilities has impacted industrial control systems (ICS)—the technological backbone of electric grids, water supplies, and production lines. These vulnerabilities affect the reliable operation of sensors, programmable controllers, software and networking equipment used to automate and monitor the physical processes that keep our modern world running.

FireEye iSIGHT Intelligence teams analyzed 1,552 publicly disclosed ICS vulnerability disclosures, 34 percent of which remain unpatched and provide a significant opportunity for potential adversary exploitation. Through April 2016, at least five ICS-specific vulnerabilities have been exploited by nation states in the wild, a rate FireEye anticipates will increase in the future. [3] Currently, most security teams do not have an accurate understanding of control system assets, their locations, and functions and organizations operating these systems are missing the warnings and leaving their industrial environments exposed.

[3] https://www2.fireeye.com/rs/848-DID-242/images/ics-vulnerability-trend-report-final.pdf

Many of the current government efforts in the ICS area have been focused on information sharing. While information sharing is an important element of comprehensive cybersecurity strategy, it is not enough to counter current threats. Sharing threat information may be useful in improving detection and prevention and enhancing situational awareness, but because adversaries are able to easily modify malware and command and control infrastructure, the utility of this information is short lived and ephemeral. Current information-sharing initiatives for the ICS sector must be accompanied by long-term systemic and technical changes in ICS security.

Key areas to strengthen critical infrastructure and industrial control (ICS) cybersecurity include:

1. ICS security training

   FireEye recommends that the Department of Homeland Security (DHS) and the Department of Energy (DOE) extend cooperation with universities and the private sector to create and reinforce training programs in ICS security. The focus on education and awareness must span all aspects of the critical infrastructure lifecycle. There has been a focus on owners and operators of critical infrastructure, but FireEye views this as only part of the challenge. For example, cybersecurity courses should be available to students of engineering degrees and integrated within the curricula of their continuing education. Systems integrators and public utility commissioners should have access to cybersecurity education to empower them to effectively conduct their duties.

2. Increase visibility into ICS

   Current ICS installations may have little to no monitoring and logging capability, so “bump-in-the-wire” devices have to be deployed individually to gain visibility into activity in the network. While solutions for monitoring exist, but they are not widely available for a range of industrial networks.

   Monitoring and logging are important to allow asset owners to collect data about their networks and thus improve the visibility of activity on their networks. This data may be used to actively detect, respond, and contain threats and attacks to ICS. With no visibility, ICS asset owners are unable to proactively detect and identify threats before a potential attack occurs. Additionally, monitoring and logging provides data for forensic investigation after an attack.

   FireEye recommends that DARPA, through its Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program, extends the existing grants and cooperation with the industry to develop new and test and deploy existing programs for ICS monitoring and logging.

   FireEye also recommends that the North American Electric Reliability Corporation (NERC) provides more specific network security monitoring requirements for power grid cybersecurity as part of NERC CIP 007-6 R4 compliance. In their current iteration the standards do not provide recommendations on the types of logs to collect or placement of network sensors which is a critical shortcoming. Logs along with strategically placed sensors provide the context around what attacks may occur. Context is critical for understanding an attack lifecycle as it provides information about the nature, scope, and risk associated with indicators of attack. Context enables prioritization and decision making, allowing defenders to respond faster and more effectively.

3. Extend collaboration between DHS-ICS CERT and the private sector in ICS incident response

   Currently, ICS-CERT partners with members of the control system community to develop and vet recommended practices and provide guidance in support of ICS-CERT incident response capability.

FireEye recommends that DHS extends this collaboration to private sector entities that provide incident response services in ICS spaces in areas such as training and technical collaboration. Many of the incident response providers have expertise in investigating large-scale intrusions performed by the most advanced threat groups across industries. Extended collaboration would allow introducing new tools and expertise to incident response and would be particularly beneficial in cases of widespread incidents affecting multiple victims or multiple sectors.

4. Develop and deliver secure ICS protocols

Industrial Control Systems protocols are vital for the functioning of the ICS systems. These computer-to-computer protocols send controls and read values like temperature, volts, amps, and provide information whether a system valve is open or closed. These protocols have been historically weak and lack basic security controls, which are common in corporate IT networks, such as authentication or encryption. Many of the secure ICS devices remain vulnerable because of deficiencies in ICS protocols.

FireEye recommends that ICS user groups and public groups such as the Distributed Network Protocol (DNP3) user group conduct research into existing ICS protocols and identify which measures may be deployed to secure them and provide recommendation on new designs for protocols.

5. Develop secure ICS devices

Many of today's devices have poor password security, hard-coded passwords, insecure management protocols or no device driver signing. Some of these weaknesses demonstrated their detrimental consequences in cases such as Stuxnet[4] or Havex[5].

FireEye recommends that the next Administration encourages DARPA and Department of Energy national labs' research into development of secure devices. Areas for research include security development lifecycle in the code development and testing, security features such as authentication and secure passwords and accounts, signed software and firmware, and secure protocols such as SSH, HTTPS and secure ICS protocols such as secure DNP3, OPC-UA.

4. **FireEye recommends further developments in cyber insurance to mitigate organizations' risk exposure.**

The rapid growth of online businesses, increasing number of breaches, and new compliance and regulatory rules around security are all growing concerns for businesses. Risk managers, chief financial officers, and general counsels all care about managing risk and how to improve and transfer risks for their organization. Cyber insurance provides an opportunity for organization to mitigate risk exposure by offsetting costs involved with recovery after a breach and is an effective tool in developing best practices in risk management.

Current obstacles to mature cyber insurance market such as lack of data, lack of methodology around visibility into the risk, the reluctance of insurers to cover cyber risk beyond data breaches, all discourage more effective risk management for exposures.

1. Recommendations for insurance companies

[4] Lagner, Ralph. "To Kill A Centrifuge." The Lagner Group. 20 Nov. 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf 18 May 2015.

[5] Wilhoit, Kyle. "Havex, It's Down With OPC." FireEye. 17 July 2014. https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html 18 May 2015.

Currently, insurance companies lack visibility in the scope of their clients' risk posture. They are not widely using risk assessment tools that provide them with a comprehensive understanding of client's risk and determine which coverage is appropriate for each client.

FireEye recommends that underwriters use risk assessment tools to measure the cyber risk for the company. Such tools may provide high-level evaluation of an organization's risk level and profile based on its technology, processes and people to facilitate the identification, classification, and analysis of cyber risk for insurance underwriting. An independent third-party assessment focused on threats to company or the sector, exposure levels, asset management processes, state of technology, processes and people deployed for detection, analysis, response and containment of advanced cyber-attack would provide a comprehensive picture of risk the insurance company is to underwrite.

2. Recommendations for the future Administration

Insurance companies are reluctant to take the risk of insuring cyber-related events that go beyond data breaches, although a major cyber event could have a serious impact on lives, the economy, and the everyday functioning of society.

FireEye recommends that the Administration updates and clarifies the Terrorism Risk Insurance Act (TRIA) for the program to explicitly cover large-scale cyber-attacks and for such attacks to qualify to trigger TRIA coverage. Clarifying the application of TRIA to these events would encourage the development of additional capacity in the cyber insurance market and encourage better cybersecurity posture.