Prepared Statement of Ron Bushar, Senior Vice President and Global Government CTO, FireEye Mandiant before the Cybersecurity, Infrastructure Protection, & Innovation Subcommittee of the U.S. House Committee on Homeland Security
September 1, 2021

Introduction

Thank you Chairwoman Clarke, Ranking Member Garbarino, and all the Members of the Subcommittee, for the opportunity to talk with you today about the importance of cyber incident reporting. FireEye Mandiant applauds your efforts to tackle this complex issue and appreciates the open dialogue we have enjoyed with you and your staff – public-private partnerships are critical to the success of any cyber incident reporting or disclosure program – both in its development and execution.

Background

My comments for today's hearing will focus primarily on the major tenets and benefits of a cyber incident reporting framework. Before I turn to this specific topic, let me share some background on myself and my company to establish context for my narrative.

I started my career in the United States Air Force as an officer in the Information Warfare Aggressor Squadron. For more than 20 years, I have worked in cyber defense operations, cybersecurity consulting, and incident response services in both the government and commercial sectors, including the Justice Department. In my current role at FireEye Mandiant, I lead a global team of cyber experts who deliver our unique platform of innovative security program capabilities and solutions to protect critical missions, infrastructure, and national security interests worldwide.

As I testify today, FireEye Mandiant employees are on the front lines of the cyberbattle, currently responding to over 150 active computer intrusions at some of the largest companies and organizations in the world. Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but we receive calls almost daily from organizations that have suffered a cybersecurity breach. For each security incident we respond to, it is our objective to determine what happened and what organizations can do to avoid similar incidents in the future. We also maintain over 200 intelligence analysts, located in more than 20 countries, speaking over 30 languages, who pursue attribution and identification of the threat actors via research and sources.

Incident Reporting Framework

FireEye Mandiant is encouraged by the draft legislation the Subcommittee has developed to improve cyber incident reporting. The "Cyber Incident Reporting for Critical Infrastructure Act of 2021" is a positive step forward in achieving important long-term goals of enabling early detection of malicious cyber attacks. It would also enhance the federal government's situational awareness to better partner with and assist private sector entities that become cyber attack

victims. This "whole of community" approach is critical to increasing capacity to prevent and deter future cyber attacks.

Any legislation on this matter should take into consideration the evolving cyber threat landscape; the increasingly sophisticated tactics, techniques, and procedures used by adversaries; and lessons learned from existing voluntary information sharing models, as established by the "Cybersecurity Information Sharing Act of 2015." Simply put, any reporting framework must be agile and include opportunities for the federal government to pivot or adjust its reporting requirements to keep pace with the threat environment and bad actors.

The U.S. government should consider a federal incident reporting program that goes beyond voluntary sharing of threat indicators as authorized under the 2015 law – it should also include mandatory disclosure requirements for cyber incidents. Major tenets of such a program should:

- Safeguard the protection and integrity of electronic and other types of data.
- Ensure confidential sharing.
- Encourage entities to adopt recognized cybersecurity standards and practices with a minimum threshold.
- Provide greater incentives for private sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation (e.g., confidentiality obligations).
- Protect privacy and civil rights.
- Provide outreach and technical assistance to entities that do not have cybersecurity expertise or capabilities.

FireEye Mandiant believes that strong cyber community protection is predicated on several key concepts. Lawmakers should consider the following additional components that we believe would constitute a robust and ultimately successful cyber incident reporting program:

Establish reasonable and effective timelines for reporting.
Reporting requirements should account for two key outcomes: 1) timely and relevant reporting of critical intelligence to relevant government authorities for assessment, correlation, and decision support and 2) reasonable latitude for the victim to determine the nature, extent, and potential impact of a breach. In the first instance, the timeliness and quality of the data reported to the government will largely determine how effective the response to and disruption of the attack will be. In the second instance, cyber attacks are often complex and require sophisticated analysis to understand the full scope of compromise.

Victims require support from external firms to fully analyze a breach and will likely be dealing with other business impacts and crisis management activities. Allowing for a reasonable amount of time to properly assess the situation before requiring reporting will limit false positives, redundant or contradictory information and prevent unnecessary data collection.

FireEye Mandiant encourages lawmakers to consider harmonizing reporting requirements with existing federal acquisition regulations and standards to provide for a consistent and streamlined regime that simplifies business processes and compliance.

Preserve existing trusted relationships and partnerships.
FireEye Mandiant strongly believes in the concept of a public-private partner approach to cyber security. Unlike most other domains of risk, cyber attacks and cyber crime are almost always predicated on the use, traversal, or compromise of privately owned infrastructure, even when the attacks are focused on government or national security assets. The private sector, especially critical infrastructure sector businesses, is both a key component of overall national cyber resiliency and a key source of intelligence on our adversaries' capabilities, intents, and activities in cyberspace.

Over the past decade, many Federal agencies, including the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the U.S. Secret Service, and the National Security Agency have built strong partnerships with key cyber security and critical infrastructure organizations through voluntary programs, outreach, and support. While we recognize that much more needs to be done, without these efforts and support functions, many private sector cyber attacks would have likely remained undetected for much longer and would have been much more severe. Under a new cyber incident reporting program, these trusted relationships and partnerships must be strengthened and enhanced to advance our common goals of reducing the frequency and severity of cyber attacks.

Ensure compliance is non-punitive.
A reporting program must encourage cooperation and strengthen trust between the public and private sector. A regulatory-based approach or a regime that focuses on punitive actions rather than mutual benefits would be counter to the goal of creating a strong national partnership model to counter the increasing cyber threats we are facing.

As previously suggested, although mandatory reporting is necessary, the focus should be on supporting organizations to achieve compliance, not punishment for non-compliance. Fines and other financial or legal punishments do not properly reflect the truth that, barring gross negligence or willful misconduct, organizations that suffer a cyber attack are victims of a crime. Mechanisms to compel collection of critical information when necessary, such as subpoenas, better align to the general concept of criminal investigation and response.

Require information to flow back into the community.
Information sharing must be bi-directional. An incident reporting framework should allow for a consistent flow of two-way information sharing between the public and private sectors to help maximize the ability to resolve and consider attribution. Organizations that invest significant effort into collecting, analyzing, and sharing cyber attack technical information require feedback on the usefulness and value of what they have provided. They also benefit from data that can only be provided by the government to enhance their own security posture and help to hone their threat detection and response functions.

Benefits

Finally, I would like to highlight several clear benefits to broader cyber incident reporting and bi-directional information sharing. Timely reporting of incidents, within and across sectors, allows

for earlier detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or national security implications.

Technical indicators, along with contextual information related to attacks, provide a more robust dataset to conduct faster and more accurate attribution and adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a timeframe that has a higher probability of successful countermeasures or deterrence.

Cyber incident information also allows for cross correlation and collaboration with international partners, thereby enabling a multilateral response to state-sponsored or state- sanctioned cyber criminals that often originate overseas and travel through an allied nation's infrastructure.

Lastly, robust and centralized collection of incident information provides the government with a much more accurate cyber risk picture and enables more effective and efficient investments and support before, during, and after major cyber attacks.

Conclusion

On behalf of FireEye Mandiant, thank you for the opportunity to testify before the Subcommittee. We are committed to working with our public and private sector partners to safeguard the Nation from cyber attacks by sharing cyber threat information, lessons learned, and best practices, including through the newly established Joint Cyber Defense Collaborative at the Cybersecurity and Infrastructure Security Agency.

We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyberspace and to build better resiliency into our networks. I look forward to your questions.