Department of Justice

STATEMENT OF
HOWARD S. MARSHALL
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
HOUSE COMMITTEE ON SMALL BUSINESS
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SMALL BUSINESS INFORMATION SHARING:
COMBATING FOREIGN CYBER THREATS"

PRESENTED
JANUARY 30, 2018

STATEMENT OF
HOWARD S. MARSHALL
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
HOUSE COMMITTEE ON SMALL BUSINESS
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SMALL BUSINESS INFORMATION SHARING: COMBATING FOREIGN CYBER THREATS"

PRESENTED
JANUARY 30, 2018

Chairman Chabot, Ranking Member Velázquez, and members of the committee, thank you for the invitation to provide remarks on the FBI's role in helping small businesses defend against cyber threats. We consider engagement with the private sector to be a significant factor in our mission to identify, pursue, and defeat nefarious cyber criminals and enemies of the United States.

As the committee is well aware, the growing number and sophistication of cyber threats poses a critical risk to U.S. businesses, and the impact of a successful attack can be devastating to small businesses in particular. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Some of the more prevalent or rising cyber threats to small businesses include the following.

Business E-mail Compromise

Business E-mail Compromise ("BEC") is a scam targeting businesses working with foreign suppliers or businesses that regularly perform wire transfer payments. By compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques, criminals are able to conduct unauthorized transfers of funds. Notably, BEC scams have been reported in all 50 States and have resulted in hundreds of millions of dollars in losses to U.S. businesses and individuals.

The victims of BEC scams range from small businesses to large corporations across a variety of services. The BEC threat is highly adaptable and constantly evolving, but criminals have been particularly active in targeting small to large companies and individuals which may transfer high-dollar funds or sensitive records in the course of business. BEC compromises can be facilitated through a variety of vectors, including social engineering, phishing scams that lure

victims to click on malware brute force cracking of e-mail passwords, or the obtaining of e-mail credentials online. An actor will use one or more of these vectors to steal the victim's credentials, impersonate a person with authority to request payments or records, and obtain access to data and e-mail for the purposes of theft; or to impersonate a legitimate vendor or business contact to trick the victim into paying an invoice or transferring payroll records to the actor's account.

The sophistication of BEC actors varies. In general, transnational organized crime groups may invest more time and resources in high-dollar targets. On the other hand, less sophisticated actors, who likely account for the majority of attempts, steal smaller sums using spoofed e-mails sent in bulk or through e-mail contact with a presumably vulnerable target. Unfortunately, both types of actors can be successful if victims are not vigilant. Popular BEC targets include third-party payroll companies, parties involved in real estate transactions (including buyers, sellers, realtors, and title companies), firms offering legal services, and import and export companies.

When we engage with the private sector, we encourage companies to take certain precautions to safeguard their systems, records, and data. We recommend that businesses require a secondary, independent verification of any payment requests or changes to existing beneficiary accounts; that they use complicated passwords or long passphrases for company and personal e-mail accounts, change passwords regularly, and not use the same password for multiple accounts; implement two-factor authentication; and that they utilize commercial antivirus and anti-spyware products. We also recommend they avoid doing formal business on free web-based e-mail accounts; establish a company domain name and limit formal communications to company e-mail accounts; and, if possible, create intrusion detection system filters that flag e-mails with extensions that are similar to company e-mail.

Ransomware

Ransomware is a type of malware used to encrypt an individual's or organization's files and documents, making them unreadable until a ransom is paid. Ransomware targets both human and technical weaknesses in organizations and individual networks to deny the availability of critical data or systems. Ransomware is a simple and proven model that continues to yield profits for cyber criminals. The attacks are difficult to attribute, and they do not require "money mule" networks (i.e., people involved in transferring illegally obtained money on behalf of someone else) to cash out. Malicious cyber actors are increasingly using virtual currency, such as bitcoin, to facilitate their crimes. Mixers, tumblers, and other anonymizing services create challenges for tracing and attribution. While these services use different mechanisms and approaches, they obfuscate the source and destination of funds by mixing funding streams, adding extra layers, or combining transactions.

In short, ransomware actors are using more sophisticated tools that allow the malware to propagate faster, and the campaigns are becoming bigger and causing more damage. For these reasons, we can expect ransomware to remain a significant threat to businesses in the U.S. and worldwide. Popular targets include hospitals, law firms, and businesses needing immediate

access to their data. Two typical infection methods include clicking on malicious phishing e-mail links and visiting infected websites. Remote Desktop Protocol, a program that allows one computer to remotely operate another, can also be used as a vector.

Once a machine is infected, typically all files on local and attached drives are encrypted and effectively locked away from the user. The criminal notifies the victim they must pay a ransom in order to receive a digital key to unlock and retrieve their files. It is important to note that even if a ransom is paid, there is no guarantee the business or individual will obtain their files from the cyber criminal.

To guard against the ransomware threat, we encourage businesses to schedule regular data backups to drives not connected to their network. These drives can be used to restore a system to the backup version without paying the ransom to the perpetrator. Additional guidance from the FBI for guarding against ransomware is available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

Criminal Data Breach Activity

Cyber criminals are continuously looking for vulnerabilities in the networks of U.S. businesses of all sizes, as well as prominent public and private sector officials. Cyber criminals are looking for entry into any network that contains personal or financial information of employees or customers that can be monetized or posted online. Some actors also seek to encrypt corporate data so it can be ransomed. Vectors can range from the use of phishing e-mails in order to steal login credentials to crafting malware to exploit sensitive, vulnerable systems.

Business networks often contain financial information such as credit card and bank account information, as well as personally identifiable information such as names and social security numbers. Consequently, we encourage businesses to apply a variety of best practices to secure their network architecture, network activity, and user data as much as possible in order to make it more difficult for an adversary to compromise their infrastructure.

Internet of Things

Internet of Things ("IoT") devices and embedded systems are becoming widespread in business, government, and home networks. They provide low-cost, real-time monitoring and automation services to users. The information these devices collect provides billions of data sets useful in analyzing productivity, marketing, consumer and market trends, and user behavior and demographics. However, IoT devices could be compromised by cyber actors taking advantage of lax security standards and inherent device connectivity to increase the impact of cyber attacks, or as a pivot point into personal or corporate networks. Increased connectivity through IoT devices will only increase the potential attack surface for networks, as cybersecurity is largely under-prioritized from device design through implementation.

In September 2016, an IoT botnet was used to conduct one of the largest Distributed-Denial-of-Service ("DDoS") attacks ever recorded. Similar attacks have since taken place. These attacks have resulted in widespread Internet outages and are very costly to victims. The source code for multiple IoT malware variants are publicly available, making it easy for cyber actors to create their own IoT botnet. Since October 2017, new IoT malware variants are targeting and exploiting firmware vulnerabilities, increasing the number of devices vulnerable to compromise. Individuals and businesses can prevent their devices from being compromised by changing default user name and passwords, ensuring device firmware is up to date, implementing strong firewall rules, and by turning off or rebooting devices when not in use. The FBI has issued guidance on securing IoT devices through Public Service Announcements, published on the Internet Crime Complaint Center's ("IC3") website at www.ic3.gov. In addition, guidance from the Department of Justice for securing IoT devices is available at https://www.justice.gov/criminal-ccips/page/file/984001/download. Other agencies are working to address this challenge as well, notably, the Department of Commerce's National Institute of Standards and Technology, which is in the process of collaborating with businesses, academia, and government stakeholders to develop standards, guidelines, and related tools to improve the cybersecurity of IoT devices.

FBI Cyber Private Sector Engagement

In light of these and other cyber threats to U.S. businesses, the FBI has made private sector engagement a key component of our strategy for combatting cyber threats. Recognizing the ever-changing landscape of cyber threats, the FBI is enhancing the way it communicates with private industry. Traditionally, the FBI used information developed through its investigations, shared by intelligence community partners, or provided by other law enforcement agencies to understand the threat posed by nation states and criminal actors. However, we are now also looking to integrate private industry information into our intelligence cycle to enhance our ability to identify and respond to both emerging and ongoing threats. We also utilize our intelligence to prioritize sector engagement and potential vulnerabilities. Private industry has unique insight into their own networks and may have information as to why their company, or their sector, may be an attractive target for malicious cyber activity. Companies may also be able to share intelligence on the types of attempted attacks they experience. We believe it is important the FBI integrate this type of data into its own intelligence cycle. As we move forward to enhance our sector-specific analysis capabilities, we are looking to private industry to help us gain a better understanding of their companies and their respective sectors. This type of information sharing enables us to provide more specific, actionable, and timely information to our industry partners so they can protect their systems in a proactive manner.

In fiscal year 2017, FBI Cyber Division reorganized its analytic and outreach resources to focus on this intelligence-driven approach to FBI engagement with critical infrastructure entities on cyber threats. FBI Cyber Division has published Intelligence Directed Queries that direct field offices to address collection needs in cyber space when engaging with sector partners.

In addition, the FBI disseminates information regarding specific threats to the private sector through various reporting mechanisms. Public Service Announcements ("PSAs"), published by the Internet Crime Complaint Center ("IC3") on www.ic3.gov, provide timely and practical information to U.S. businesses and individuals on the latest threats and scams. Each PSA typically contains information about a threat, warnings signs and indicators businesses should look for, precautions organizations should take to protect their data and networks, and steps for mitigation in the event of a compromise. We have released nearly 70 of these announcements over the past five years, including seven in 2017 that addressed such topics as Business E-mail Compromise, IoT vulnerabilities, and tactics being used by nefarious actors to launch DDoS attacks.

We also offer several other types of reports to the private sector, including Private Industry Notifications ("PINs"), which provide contextual information about ongoing or emerging cyber threats, and FBI Liaison Alert System ("FLASH") reports, which provide technical indicators gleaned through investigations or intelligence. These communication methods facilitate the sharing of information with a broad audience or specific sector and are intended to provide recipients with actionable intelligence to aid in victim notifications, threat neutralization, and other investigative efforts. In some instances, the FBI may work with other government agencies to release joint products for private industry. These joint products my include Joint Intelligence or Indicator Bulletins ("JIB"), Joint Analysis Reports ("JAR"), or other miscellaneous products.

The FBI believes it is critical to maintain strong relationships with private sector organizations to allow for the successful responses to cyber attacks. One example of an effective public/private relationship is the National Cyber-Forensics and Training Alliance ("NCFTA"), a nonprofit 501(3)(c) corporation focused on identifying, mitigating, and neutralizing cybercrime threats globally. Working hand in hand with private industry, law enforcement, and academia, the NCFTA's mission is to provide a neutral, trusted environment that enables two-way information sharing, collaboration, and training. The NCFTA works directly with 136 member organizations from the banking, retail, critical infrastructure, healthcare, and government sectors. NCFTA recently expanded from its headquarters location in Pittsburgh and is now operating additional offices in New York City and Los Angeles.

The FBI Cyber Division regularly coordinates initiatives for engagement with private sector partners to prevent threats and ultimately close intelligence gaps. In recent years, we have launched public awareness campaigns or "open houses" to educate businesses on serious cyber threats. In 2016, the FBI collaborated with the Department of Homeland Security ("DHS"), U.S. Secret Service ("USSS"), Department of Health and Human Services ("HHS"), and the National Council of Information Sharing and Analysis Centers ("NC-ISACs") to host conferences and workshops at FBI and USSS field offices across the country to educate businesses on the ransomware threat. The FBI and USSS jointly hosted these workshops in 14 key cities, targeting small, medium, and large organizations. Over 5,700 individuals were briefed during this campaign.

Similarly, in 2017, the FBI collaborated with DHS, USSS, and NC-ISAC to host workshops on the BEC threat in strategically identified locations across the country. These workshops were launched in October of 2017 to coincide with National Cyber Security Awareness Month and continued into early fiscal year 2018. Nearly 2,500 business leaders were briefed during this campaign.

The FBI Cyber Division continues to engage directly with businesses in other ways as well. The FBI Cyber Division either hosts or participates in briefings, conferences, workshops, and other meetings providing strategic-level information to key executives throughout industry. These briefings include both classified and unclassified discussions regarding cyber threats. Over the past five years, the FBI Cyber Division has completed nearly 2,800 such engagements, not counting the many informal contacts and interactions we have with businesses on a regular basis.

In addition, the FBI leverages its unique, decentralized field office model to ensure it can engage effectively with small and local businesses across the country and work side-by-side with State and local law enforcement for the furtherance of cyber investigations. The FBI is made up of 56 field offices spanning all 50 States and U.S. territories, each with a multi-agency Cyber Task Force ("CTF") modeled after the successful Joint Terrorism Task Force program. The task forces bring together cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians from various Federal, State, and local agencies present within the office's territory. Our field-centric business model allows us to develop relationships with local businesses, companies and organizations, putting us in an ideal position to engage with potential victims of cyber attacks and crimes. Cyber-trained special agents are in each field office, providing locally available expertise to deploy to victim sites immediately upon notice of an incident. Computer scientists and intelligence analysts are also stationed in field offices to support incident response efforts and provide intelligence collection and analysis as well as technical assistance and capability.

The Bureau has had success with operating joint investigations with local law enforcement through our Cyber TFOs to dismantle large criminal enterprises engaging in computer intrusion and cyber-enabled crimes. Additionally, the Bureau works with local law enforcement on various Internet fraud matters through our Operation Wellspring platform, through which we package complaints from the Internet Crime Complaint Center ("IC3") and provide them to local law enforcement to work independently or in coordination with their local FBI field office.

Recognizing small businesses often engage State and local law enforcement as a first line of defense during a cyber incident, the Bureau offers our State and local partners access to FBI cyber training, including private sector training that offers certifications in the cyber security industry. The FBI's Cyber Division—working with the International Association of Chiefs of Police ("IACP") and cyber experts from Carnegie Mellon University—has developed the Cyber Investigator Certification Program ("CICP"). This self-guided, online training program is

available free of charge to all local, State, Tribal, territorial, and Federal law enforcement personnel and provides training in how to conduct effective cyber investigations.

When a small business has been victimized by a cybercrime and reaches out to the FBI for assistance, we coordinate with the individual business to determine the best course of action to address the incident. The FBI's approach in working with potential or actual victims of cyber intrusions or attacks is to first and foremost, and to the best of our ability, use our processes to protect the victim from being re-victimized, and to provide confidentiality and discretion during the investigative process. No matter what course of action is deemed appropriate, the FBI views a company that has been attacked as a victim and will protect investigative information appropriately. Our goal in each instance to work with the business side by side to investigate the systems and data at play in the incident. We will work with the victim to determine attribution, which can lead to prosecution of the subject. Through its work with other government agencies, the FBI and Department of Justice can provide information that can be used to initiate indictments, affect arrests, generate demarches, or produce international sanctions against those who conduct cyber attacks or aggressive actions against entities in the United States.

We at the FBI appreciate this committee's efforts in making cyber threats to small businesses a focus and to committing to improving how we can work together to better defend U.S. business from cyber adversaries. We thank you for the opportunity to speak about our cyber outreach efforts; we look forward to discussing these issues in greater detail and answering any questions you may have.