U.S. CHAMBER OF COMMERCE

Partnering With Law Enforcement to

Combat Cybercrime

keppler SPEAKERS

Based in the Washington, D.C. area, Keppler Speakers is the country's largest privately-held speakers bureau and has represented many of the most prestigious and celebrated speakers from the worlds of business, technology, world affairs, politics, entertainment, education, literature, sports, and leadership. With an expanding global client base that includes: Fortune 500 companies across industry sectors, national trade associations, colleges/universities, and performing arts centers, Keppler Speakers remains the preeminent resource for thought leaders across business and industry.

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business organization representing the interests of more than 3 million businesses of all sizes, sectors, and regions. Our members range from mom-and-pop shops and local chambers to leading industry associations and large corporations. They all share one thing—they count on the Chamber to be their voice in Washington, D.C.

I. Executive Summary

Effective partnerships between the business community and law enforcement are critical in defending U.S. national and economic security from cybercrime. Malicious actors continue to develop advanced attacks aimed at breaching systems and stealing data or holding information ransom, which can impact an organization's financial bottom line and damage its brand or reputation. With the rapid development of new technologies and Internet of Things (IoT) devices, businesses face new challenges when protecting their enterprises, products, and consumers. While there are many best practices and measures that should be implemented to secure digital assets, collaborating with law enforcement should be a top priority.

Cyber incidents to businesses of all sizes should be reported to law enforcement as soon as possible. Cooperation and information sharing with proper authorities both increases the likelihood of attribution for that business and, in many cases, can lead to further prevention by notifying other potential targets of the threat. However, if a business is not accustomed to working with law enforcement, this can lead to uncertainty as to which is agency is the appropriate contact and at which level of government.

Businesses can get ahead of this challenge by establishing relationships with law enforcement officers at the federal, state, and local levels before an incident occurs. The FBI and the Secret Service have field offices located in cities across all 50 states and dedicated task forces to partnering with industry. State police departments have formed cyber command centers designed to coordinate emergency response to critical cyber incidents. Local police departments are standing up cyber units and can help inform other agencies as required. Law enforcement agencies at all levels realize the significance of cyber threats posed by malicious actors and rely on partnering with businesses to combat these crimes on the federal, state, and local levels.

BEST PRACTICES FOR PARTNERING WITH LAW ENFORCEMENT

Cultivate trusted and bi-directional relationships with state and/or federal law enforcement and U.S. attorney points of contact.

Join a cyber information sharing organization like lnfraGard.

Develop, exercise, and update a cyber incident response plan.

Ensure legal counsel is familiar with the organizations cyber risk management and incident response plan and responsibilities interacting with government agents.

Contact law enforcement at any point during incident response for suspected criminal activity.

II. Introduction

Cybercrime poses an increasingly dangerous risk to U.S. national and economic security. In February 2018, the Council of Economic Advisers reported that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[i] And the global cost of these crimes is estimated to be more than $445 billion annually, according to the World Economic Forum.[ii]

While many attacks are aimed at big businesses that own large stores of customer or employee data, small and mid-size businesses face threats as well. The same holds true for specific industries. Financial institutions and health care providers are often targeted because of the high-volume of personally identifiable information they collect, but businesses in every industry are susceptible to significant attacks and need to be prepared to respond if they fall victim.

According to Keppler Speakers' Theresa Payton, Former White House CIO and CEO of world class cybersecurity consulting and intelligence operations firm, Fortalice Solutions, ***"The best time to engage law enforcement is before you have a digital disaster. Often times the first time a company is meeting their FBI cyber team is when they are knocking at their door to notify them their company is a victim of a data breach. Work early and often with law enforcement, they can often be another layer of offense alerting you to digital break-ins occurring across the globe and can provide practical steps to avoid becoming the next victim."***

Michael Daniel, President and CEO, Cyber Threat Alliance and former Cybersecurity Coordinator, The White House

With numerous agencies at all levels of government focused on preventing and responding to cyber incidents, small and mid-size businesses can become overwhelmed. By familiarizing themselves with law enforcement roles and responsibilities, businesses are better equipped to contact and work with the appropriate agency following an incident. This communication and collaborative working relationship between industry and government plays a crucial role in protecting the American business community from the newest cyber threats. Keppler Speakers' Michael Daniel, President and CEO of Cyber Threat Alliance added, ***"You don't want to be exchanging business cards on the day you discover a major intrusion or suffer an attack. You want to build those relationships ahead of time."***

[i] The Council of Economic Advisers, February 2018, *The Cost of Malicious Cyber Activity*, https://bit.ly/2FiyUyy
[ii] World Economic Forum. *Cybercrime*. 2018. https://www.weforum.org/projects/cybercrime

III. Roles and Responsibilities of U.S. Law Enforcement

In 2016, the Obama administration issued Presidential Policy Directive 41-*United States Cyber Incident Coordination* (PPD-41)[iii] outlining the roles and responsibilities of federal agencies when responding to any significant cyber incident affecting government or private sector entities. The directive organizes the federal response into three concurrent lines of effort: threat response, asset response, and intelligence support.

The FBI leads on threat response which includes law enforcement and national security investigative activities. DHS leads asset response efforts and provides technical assistance to organizations to better protect their assets, mitigate vulnerabilities, and reduce the effects of cyber incidents. Intelligence support and related activities enable the sharing of situational threat information and are headed by the Office of the Director of National Intelligence. These efforts, collectively, help organizations respond to and recover from significant cyber incidents.

PPD-41 also required DHS to finish updating the National Cyber Incident Response Plan (NCIRP). The plan was developed as a strategic framework for understanding how the federal government and other national partners provide resources and support in responding to and recovering from a significant cyber incident that puts critical infrastructure at risk. The NCIRP is a product of close collaboration between the government and private sector and was designed to sync with industry standards and best practices for cyber risk management set forth by the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[iv] The NCIRP builds off of PPD-41 to expand on the roles of the federal government, the private sector, and state, local, tribal, and territorial governments in each concurrent line of effort.

Although all three lines of effort are critical to managing cyber incidents effectively, this paper focuses on helping businesses support law enforcement's leadership in the threat response line of effort. Daniel said, ***"Along with adopting the National Institute of Standards and Technology's Cybersecurity Framework and developing an internal cyber incident response plan, knowing how to engage with law enforcement should form a key element of any organization's efforts to manage their cyber risk effectively."***

Theresa Payton, CEO, Fortalice Solutions and former Chief Information Officer, The White House

When asked if there is any danger of the victim company's name being revealed by law enforcement to the media, Payton responded, ***"If you have a data breach that requires public disclosure, that's another matter. If you are the victim of a cybercrime that does not require public disclosure such as ransomware, extortionware, or malware that does not lead to credit card data being stolen, you can ask to remain anonymous. I have worked with the FBI on several cases and the victims' identities have remained anonymous."***

[iii] PPD-41: *U.S. Cyber Incident Coordination.* https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident

[iv] *Framework for Improving Critical Infrastructure Cybersecurity, version 1.0.* National Institute of Standards and Technology, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Department of Justice and Federal Bureau of Investigation

The FBI is the primary federal agency responsible for investigating cybercrime. The agency leads threat response efforts as outlined in PPD-41 and is tasked with investigating cyberattacks on U.S. entities and providing attribution. Through its Cyber Division at headquarters in Washington, D.C. the FBI investigates computer intrusion cases involving counterterrorism, counterintelligence, or other criminal matters with national security implications.

With 56 field offices located in major cities across the U.S. and Puerto Rico, the FBI is well positioned to respond to major cybercrimes by working with the affected organization on-site.[v] There are cyber teams in each of these field offices experienced in working with the business community to protect from cybercrimes, such as the theft of intellectual property or personal information. And when a crime occurs, the FBI teams work with employees to investigate and collect digital evidence. By working with businesses to recover from an attack, the agency is able to connect like incidents and identify others that may be vulnerable to the threat. This coordination between private industry and law enforcement is critical in combating cybercrime.

NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE

The FBI collaborates with other federal law enforcement agencies to investigate cyber threats. The National Cyber Investigative Joint Task Force (NCIJTF) is a multiagency partnership, led by the FBI, focused on sharing information and supplying intelligence to support global cyber investigations.[vi] The task force is made up of more than 20 agencies from the Department of Defense, the intelligence community, and law enforcement. The NCIJTF uses its collective authorities to help arrest and prosecute cybercriminals seeking to cause harm to U.S. national and economic security.

INFRAGARD

Businesses in critical infrastructure sectors are urged to connect with the FBI through InfraGard.[vii] This partnership allows a platform for the timely, accurate exchange of the latest information needed to defend critical infrastructure from impending attacks. The program has 84 chapters nationwide with more than 50,000 members. Regular meetings are held at each chapter, led by an FBI agent and the local governing board, to discuss threats impacting the business community. To join InfraGard, visit www.infragard.org or contact your local FBI field office.

We asked Theresa Payton if spending time at Infragard is worth it and she adamantly said, ***"Yes, it is worth making time on your calendar for the Infragard meetings! As vice president of the Carolinas Infragard chapter in Charlotte, I can tell you first hand that joining Infragard is worth your time. Real threat information sharing for physical security issues, fraud issues, and cybersecurity issues are discussed at the meetings. You can learn best practices from other companies and learn strategies to protect your company better. The resources provided are unmatched anyplace else."***

[v] Federal Bureau of Investigation. *Addressing Threats to the Nation's Cybersecurity.* https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view
[vi] Federal Bureau of Investigation. *National Cyber Investigative Joint Task Force.* https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force
[vii] InfraGard Quick Facts. March 15, 2017. https://www.infragard.org/Content/InfraGardQuickFacts.pdf

INTERNET CRIME COMPLAINT CENTER

It is essential that businesses report cyberattacks to proper authorities. The FBI makes it easy to do this through the Internet Crime Complaint Center (IC3), a reliable mechanism to submit information on suspected internet crimes.[viii] The IC3 Unit operates under the Cyber Division's Cyber Operations Section V and is made up of individuals who are experts at preventing and detecting cybercrime. Businesses are encouraged to report a wide range of complaints through the IC3, including ransomware, business email compromise, phishing, economic espionage, and extortion. Since the creation of the IC3, the center has received more than 3 million reported complaints. Representatives from financial institutions, retailers, internet providers, and many other industries have formed alliances with the IC3 to facilitate more effective information sharing. The IC3 regularly shares public service announcements on the latest cyber trends to alert businesses. To learn more, visit www.ic3.gov.

CYBER ACTION TEAM

Another asset the FBI can deploy when a rapid response is needed for a significant cyberattack is the Cyber Action Team (CAT).[ix] This team is composed of a group of cyber experts who are prepared to be on-site at a major attack within 48 hours to help move a case forward quickly. The CAT is essential in collecting and investigating cases with time-sensitive evidence requiring immediate action. The team consists of about 50 special agents and computer scientists with expertise in computer languages, forensic investigation, and malware analysis.

FBI GUIDANCE ON RANSOMWARE

Ransomware is one of the biggest threats facing businesses today. The number of ransomware detections rose 36% in 2016, up 123,000 detections from the previous year.[x] Cybercriminals use this type of malware to lock data on a victim's system and then demand a ransom to release the information. Because of the increasing frequency and sophistication of ransomware attacks on businesses, the FBI has made it policy not to support paying ransom as it does not always result in the retrieval of the encrypted information. In many cases, paying a ransom will even lead the malicious actor to target more businesses. Rather than pay the ransom, the FBI recommends employee education and awareness, access controls, and the regular backing up of data to a secure, separate network.

"Ransomware is a real and present danger," says Payton who added that ***"According to the Cisco 2017 Annual Cybersecurity Report, ransomware is growing at a yearly rate of 350% and according to Steve Morgan's at Cybersecurity Ventures, the resulting damages from ransomware rose 15X in 2 years!"***

[viii] Federal Bureau of Investigation. *Internet Crime Complaint Center Brochure.* https://www.ic3.gov/media/IC3-Brochure.pdf

[ix] Federal Bureau of Investigation. *The Cyber Action Team: Rapidly Responding to Major Computer Intrusions.* May 4, 2015. https://www.fbi.gov/news/stories/the-cyber-action-team

[x] *Internet Security Threat Report.* Symantec Corporation, April 2017. Volume 22. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Department of Homeland Security and U.S. Secret Service

Under PPD-41, DHS is the lead department for providing asset response to victims through its National Protection and Programs Directorate. While these response efforts typically involve providing technical assistance to an affected organization, mitigating vulnerabilities, and reducing impacts of the attack, the U.S. Secret Service plays a significant role in threat response and working with U.S. businesses to investigate and protect against incidents in their respective jurisdictions.[xi]

Since the agency's creation in 1865 it primarily focused on investigating and preventing counterfeiting. However, with the rapid development of modern technology, the Secret Service's mission has evolved to include protecting financial systems in the U.S. from computer-based crimes. Today, the agency holds the crucial responsibility of securing critical banking and finance infrastructure from cyber incidents.

ELECTRONIC CRIMES TASK FORCES

One way the Secret Service works to protect the integrity of U.S. financial systems is through its national network of Electronic Crimes Task Forces (ECTFs).[xii] These task forces aim to increase resources for federal, state, and local law enforcement by enhancing partnerships with the business community to amplify its efforts to combat cybercrime.

With a shared purpose of preventing, detecting, and mitigating attacks on critical financial infrastructure, ECTFs support investigations that will have a significant economic or community impact, involve transnational or multijurisdictional organized criminal groups, or use schemes deploying new technology. ECTFs have conducted investigations into an array of crimes such as online counterfeit currency, bank fraud, computer intrusions and cyberattacks, phishing, identify theft, and malware proliferation.

The first ECTF was formed in New York in 1995. Since then, the network of task forces has grown to nearly 30 ECTFs located in major cities across the U.S. For more information on the U.S. Secret Service Electronic Crimes Task Forces, visit www.secretservice.gov/ectf or contact your local Secret Service field office.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

DHS also operates the National Cybersecurity and Communications Integration Center (NCCIC) to share information and situational awareness on emerging cyber threats. The NCCIC serves as a national nexus for the integration of cybersecurity and communication between law enforcement, the federal government, and the intelligence community. Sharing information with both the public and private sector, the NCCIC seeks to create awareness of known vulnerabilities, cyber incidents, and mitigation strategies. Through these efforts, DHS is able to reduce the likelihood and severity of cyberattacks that have the potential to significantly compromise critical infrastructure.[xiii]

[xi] U.S. Secret Service. *The Investigative Mission.* https://www.secretservice.gov/investigation/
[xii] United States Secret Service. *Electronic Crimes Task Forces.* https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf
[xiii] U.S. Department of Homeland Security. *National Cybersecurity and Communications Integration Center.* June 2017. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

Under the banner of the NCCIC there are four branches providing the authorities, capabilities, and partnerships that facilitate an all-encompassing approach to national cybersecurity. These branches include the NCCIC Operations and Integration (NO&I); the U.S. Computer Emergency Readiness Team (US-CERT); the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and the National Coordinating Center for Communications (NCC). To learn more about the NCCIC, please visit www.dhs.gov/national-cybersecurity-and-communications-integration-center.

IV. State, Local, Tribal, and Territorial Government Roles and Responsibilities

Governments at the state, local, tribal, and territorial levels (SLTT) have developed their own capabilities and initiatives to respond to cyberattacks in the public and private sectors. Many of these governments have implemented criminal statutes prohibiting the unauthorized access of a computer system or have taken on an increased role in cyber incident response activities. While SLTT governments vary enormously in their abilities to prevent and respond to cyber incidents, the most important thing law enforcement agencies at these levels can do is serve as a liaison between their business community and federal law enforcement.

It is often a challenge for small businesses to create relationships with or gain access to federal law enforcement resources. However, SLTT law enforcement agencies have established channels through which they can share information with federal law enforcement and connect businesses with the appropriate agencies. One major step in this sharing of information was achieved through the *Cybersecurity Information Sharing Act of 2015*, which provided legal protections for sharing information among the federal government, SLTT governments, and the private sector.[xiv]

Working to facilitate communication between businesses and federal law enforcement is a critical responsibility of law enforcement at the state and local level. Other initiatives that SLTT governments can implement to reduce cybercrime follow.

State Police Cybercrime Units

"It has been my honor to be able to provide cyber and intelligence training to groups such as the U.S. Marshals and to the Carolinas Sherriff's conference. What the business community should know is that you have local talent at the ready to assist you." Says Payton. Almost all 50 states in the U.S. now have divisions or units within their state police departments dedicated to fighting cybercrime. These units consist of state police detectives, civilian analysts, and others who support cyber investigations with seizure, acquisition, and analysis of digital forensic evidence. Each of the personnel within these cybercrime divisions undergoes special training on network intrusion crimes and their impacts on government

[xiv] U.S. Department of Homeland Security: *National Cyber Incident Response Plan.* December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

and businesses. State police teams investigate and provide support on a range of cybercrimes such as data theft, cyber stalking, insider threats, and social networking account intrusions. Many states have also developed corporate outreach services that aim to educate corporate entities of vulnerabilities to their organizations.

Fusion Centers

When asked the value of the Fusion Centers, Payton replied ***"The Fusion Centers are designed to provide real time analysis and information sharing for the greater good of the U.S. government and U.S businesses. Often times these fusion centers have reach to their counterparts across the globe, which is vital to shutting down attacks before they spread from one country to another."*** Throughout the U.S. there are 79 fusion centers operated by state or local entities designed to analyze, gather, and share threat information between federal, state, local, tribal, territorial, and private sector partners.[xv] These information sharing hubs allow government, law enforcement, and industry at all levels to plug into a system that provides access to the dissemination of threat indicators that cannot be provided by any single entity. Independent from federal agencies or partners, fusion centers are highly collaborative partnerships that can provide stakeholders with a view of the cyber threat landscape specific to their state or locality. As a major channel of communication between state and local leadership and interested parties, fusion centers can help law enforcement at all levels secure vulnerabilities to government and business alike. For a list of fusion centers, visit www.dhs.gov/fusion-center-locations-and-contact-information.

V. Best Practices and Tips for Successful Law Enforcement Engagement

While interacting with law enforcement before, during, and after an attack is critical to an organization's cyber resiliency and security, there are steps that every organization can take ahead of time to ensure these interactions are as efficient and successful as possible. Three of the most important steps are identifying your organization's most valuable information, developing an actionable cyber incident response plan, and consulting with legal counsel.[xvi]

Every business is different and as so leaders must determine what assets and data are most critical to the continuity of their organization. For some this might mean placing the utmost importance on protecting intellectual property or trade secrets, while for others it may mean guaranteeing security of data such as customer information. Identifying these "crown jewels" and assets that require the most protection is a vital first step in defending your organization from a cyberattack and will help reduce response times when working with law enforcement.

[xv] U.S. Department of Homeland Security: *State and Major Urban Area Fusion Centers.* June 26, 2017. https://www.dhs.gov/state-and-major-urban-area-fusion-centers

[xvi] U.S. Department of Justice. *Best Practices for Victim Response and Reporting of Cyber Incidents.* April 2015. https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

Business leaders also need to develop an actionable cyber incident response plan that their organization can follow to help contain the attack, mitigate the effects, and preserve digital evidence. A successful plan sets guidance for employees to follow including, what data is of highest value; who has responsibilities related to public communications, access to information technology, and remaining legal questions; and procedures for engaging with law enforcement. It is crucial that management establishes an incident response plan ahead of time so that they are not trying to create emergency procedures during the attack.

Cyber incidents, such as the theft of intellectual property or personally identifiable information, also raise important legal questions for a business. You should consult with either an in-house or outside legal counsel, preferably one who specializes in data privacy or security, who can advise you on federal and state laws that may come into play. Working closely with legal counsel before an attack to develop your cyber incident response plan and during an attack to engage with law enforcement can lead to more efficient decision making and help your organization become more resilient.

VI. Conclusion

Partnership between the business community and law enforcement is key to combating cybercrime and deterring malicious cyber activity in the U.S. and around the globe. ***"The federal government must ensure that deterrence works in the digital domain,"*** said Nate Fick, CEO of Endgame. ***"Cyber conflicts often pit the vast resources of nation-states against those of private companies. Businesses can only be reasonably expected to agree to increased cybersecurity regulation if they have confidence in the government to perform its basic function of protecting its citizens."***

As criminals continue their assault on business networks, attacks will grow in frequency and sophistication. It is the responsibility of businesses large and small to report these attacks and share relevant information with appropriate law enforcement agencies. Michael Daniel added, ***"Although many people think the U.S. Government sees everything that happens on the internet, that's just not true; unless businesses report these crimes, law enforcement will probably never know they have occurred. And if they don't know about the crimes, they can't help you."*** By effectively sharing threat information, a business can help others in the private and public sectors increase their cyber resiliency. While there are many opportunities for an organization to plug in with law enforcement at different levels of government, whether through an anonymized federal reporting mechanism or a state information sharing center, businesses need to make sure they are communicating with law enforcement before, during, and after a major cyber incident occurs.