Cyber incidents: How best to work with law enforcement

Received (in revised form): 22nd May, 2017

David H. Laufman

serves as Chief of the Counterintelligence and Export Control Section (CES) in the National Security Division at the US Department of Justice (DOJ). CES has supervisory responsibility within DOJ for the investigation and prosecution of offences concerning US export controls and economic sanctions, atomic energy and counterproliferation, espionage, economic espionage, foreign agent registration and disclosure, and cyber intrusions and attacks by nation states and their proxies. He previously served both as a federal prosecutor and at DOJ's highest operational and policy levels. As Chief of Staff to the Deputy Attorney General from 2001 to 2003, he assisted in the day-to-day management of DOJ and helped to coordinate DOJ's responses to the terrorist attacks on 11th September, 2001. From 2003 to 2007, he served as Assistant US Attorney in the Eastern District of Virginia, where he prosecuted terrorism, export control and other national security offences. From 2010 to 2011, he served as a Special Trial Attorney to the Fraud Section at DOJ, where, on detail from the Special Inspector General for Iraq Reconstruction (SIGIR), he investigated and prosecuted procurement fraud and corruption related to US economic assistance to Iraq. He also has extensive experience in the field of economic sanctions. From 2000 to 2001, he served as Staff Director and Deputy Chief Counsel to the Judicial Review Commission on Foreign Asset Control, a congressionally mandated body that examined the administration of US laws governing the imposition of economic sanctions by the Office of Foreign Assets Control of the US Department of the Treasury. While serving as Chief of Staff to the Deputy Attorney General from 2001 to 2003, he also served as DOJ's representative to the National Security Council's Policy Coordinating Committee on Terrorist Financing, a sensitive inter-agency body that formulated intelligence, law enforcement policy and tactics regarding the designation of individuals and organisations suspected of financing Al-Qaeda and other terrorist organisations.

Chief, Counterintelligence and Export Control Section, National Security Division, US Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, USA
Tel: +1 202-233-0986; E-mail: nsd.public@usdoj.gov

Sean Newell

is a Deputy Chief with the US Department of Justice (DOJ) National Security Division (NSD), Counterintelligence and Export Control Section (CES), where he manages DOJ's strategic and tactical efforts to investigate, disrupt and deter malicious cyber activities conducted by nation states and their proxies, including their targeting of the private sector and critical infrastructure. Most notably, he is a member of the prosecution teams that obtained the May 2014 indictment of five members of China's People's Liberation Army in United States v. Wang Dong *et al.*, the January 2016 indictment of seven Iranians who participated in the distributed denial-of-serivce attack (DDoS) attacks against the US financial sector in United States v. Ahmed Fathi *et al.*, and the February 2017 indictment of two officers in the Russian Federal Security Service (FSB) and two criminal hackers for their role in the intrusion into Yahoo, Inc. and the resulting theft of information regarding over 500m Yahoo accounts in United States v. Dmitry Dokuchaev *et al.* He also represents the DOJ on inter-agency policy committees concerning cyber security.

Deputy Chief, Counterintelligence and Export Control Section, National Security Division, US Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, USA
Tel: +1 202-233-0986; E-mail: nsd.public@usdoj.gov

Stephen Reynolds

serves as the Deputy Chief for Cyber Law and Policy in the Justice Department's National Security Division. In that role, he provides legal and policy advice relating to cyber security and efforts to deter, mitigate and prosecute malicious cyber activity by nation state actors or their proxies, or that otherwise involves national security. Prior to joining NSD, he served as a Deputy Chief and the National Security Coordinator for the US Attorney's Office in Connecticut, where he was a federal prosecutor for 15 years. In that capacity, he developed experience in investigative processes including the use of federal grand juries, subpoenas, search warrants, court orders and court-authorised electronic surveillance. He tried many criminal cases to verdict, including a six-week RICO/VCAR murder trial, a domestic terrorism trial and an espionage trial. He also

supervised Connecticut's National Security Cyber Specialists, its Cyber Working Group, and its investigations and prosecutions of matters involving economic espionage, the theft of trade secrets, cyber intrusions and cybercrime. In 2012, he received an Assistant Attorney General's Exceptional Service Award, and in 2011, he received the Attorney General's Distinguished Service Award. Prior to joining the US Attorney's Office, he worked in private practice at Day, Berry and Howard in Hartford, Connecticut. He also served as a law clerk to United States District Judges Stefan R. Underhill and Alan H. Nevas of the US District Court for the District of Connecticut. He received his JD from Cornell and his BA from Hamilton College.

Deputy Chief for Cyber Law and Policy, Office of Law and Policy, National Security Division, US Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, USA
Tel: +1 202-233-0986; E-mail: nsd.public@usdoj.gov

Mike Buchwald

is a career attorney in the Office of Law and Policy in the National Security Division at the US Department of Justice, focusing on technology issues, including cyber security. He is also a member of the department's Threat Analysis Team on the cyber security risk from the Internet of Things. He represents DOJ in a variety of inter-agency and external meetings. Previously, he served as Counsel and Deputy Staff Director for Oversight and Policy on the Senate Intelligence Committee. He also served as the designated committee staffer to brief Senator Dianne Feinstein on daily national security issues when she served as chairman and vice-chairman of the committee. Before joining the senate committee, he was an attorney at the international law firm of O'Melveny and Myers LLP where he specialised in criminal, congressional and internal investigations of corporations and non-profit entities as a member of the White-Collar Defense and Strategic Counseling groups. After law school, he clerked for a federal judge in California, where he was born and raised. Before law school he worked as a legislative assistant to Senator Feinstein for three years. He earned his JD from UVA Law School and his BA Cum Laude with Distinction in history from Yale University. He is a member of Phi Beta Kappa and a term member of the Council on Foreign Relations. He is admitted to practise law in both Washington, DC and California.

Attorney, Office of Law and Policy, National Security Division, US Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, USA
Tel: +1 202-233-0986; E-mail: nsd.public@usdoj.gov

Abstract Cyber intrusions now affect businesses and organisations of all sizes and in all sectors and industries. The United States Department of Justice employs a whole-of-government approach to investigate, disrupt and deter malicious cyber activity. We work with other law enforcement agencies; the intelligence community; civil, administrative and regulatory agencies; and the military to draw upon each partner's unique expertise and resources, and to use whichever combination of tools will be most effective in responding to and countering a particular threat. Meeting the cyberthreat requires the help and cooperation of the private sector as well. When deciding whether to notify law enforcement of a cyber incident, organisations weigh the anticipated benefits of a pro-active approach against legal, business, reputational and other practical concerns. This paper explains why working with law enforcement is the smart choice before, during and after a cyber intrusion or attack. We can help victims understand what happened; we can share context and information about related incidents; we can ensure a proper investigation and preservation of evidence; we can assist victims in dealing with regulators; and we are uniquely situated to work with other parts of the federal government to respond with possible criminal prosecution, economic sanctions, diplomatic pressure, intelligence operations and military action. Although primarily directed towards victim organisations, we hope this paper helps answer questions that all organisations' leadership and counsel may have as they decide how their response may affect their business or mission, whether they are witnesses (eg internet service providers) or victims.

KEYWORDS: cyber security, cyber incident response, government cyber response, law enforcement cyber response, cyber information sharing, cyber intrusion, cyberattack

INTRODUCTION

Every day, news headlines feature stories of malicious cyber activity — from data breaches and computer intrusions, to compromises of business e-mail, as well as denial-of-service and ransomware attacks. Organisations are being relentlessly targeted by those who seek to steal their intellectual property or the personal or financial information of their customers or employees, extort them, or otherwise disrupt their business or mission. And these threats are happening on multiple fronts — whether the work of an individual hacker, organised crime, terrorist organisations, or nation states and their proxies. These evolving cyberthreats affect organisations of all sizes and in all sectors and industries, causing them to work tirelessly — not only to detect, mitigate and deter cyberthreats, but also, when an incident happens, to contain the damage to their organisation, to their customers and to their reputations.

We now know that cyber intrusions are a matter of 'when', not 'if'. As Robert Mueller, then director of the FBI, said in 2012, 'there are only two types of companies: those that have been hacked and those that will be'.[1] That same year, Keith Alexander, then director of the National Security Agency, said the loss of valuable business information and intellectual property from the US through cybertheft constitutes the 'greatest transfer of wealth in history'.[2] Unfortunately, the volume and severity of cyberattacks have only increased in the past five years.[3]

Although the threat from malicious cyber actors is now relentless, so is the effort of the Department of Justice (DOJ) to counter it. DOJ partners with federal law enforcement and other federal departments and agencies to investigate, disrupt and deter malicious cyber activity regardless of who is behind the keyboards. In carrying out this mission, we have proven that law enforcement has a long memory and a long reach.

As set forth below, DOJ is, and has been, committed to using all of the tools at our disposal — whether criminal investigations and prosecutions, civil tools and injunctions, or FBI-led cyber operations — to raise the costs for malicious cyber activity. DOJ is equally committed to enabling, through information gathered in its investigations, the tools of our federal inter-agency partners, including economic sanctions, diplomatic pressure, intelligence operations and military action.

Successfully countering the ever-persistent cyberthreat, however, requires the help and cooperation of organisations of all sizes, sectors and industries. This is true whether the organisation is a victim or a witness (eg an internet service provider).[4] Simply put, if and when you become aware of a cyber incident, it is to your benefit to notify us, and we urge you to do so.

When deciding whether to notify law enforcement of a cyber incident or whether to cooperate fully in an investigation, organisations weigh the anticipated benefits of a proactive approach against legal, business, reputational and other practical concerns. Given the increasing frequency and magnitude of cyber incidents, it is essential that we address the questions and concerns of an organisation's leadership and counsel as they decide how their response is likely to affect their business or mission. This paper explains why working with law enforcement is the smart choice before, during and after a cyber intrusion or attack, and should serve as a guide for what to expect from federal law enforcement.[5]

WHAT TO DO BEFORE A CYBER INCIDENT OCCURS

A quick, effective response is critical to minimising the damage from a cyber incident, recovering, and helping ensure that your organisation and the government take appropriate steps to prevent similar incidents on your and others' networks in the future. The best time to plan such a response is before an incident occurs. In April 2015, DOJ's Criminal Division produced a publicly

available document titled 'Best Practices for Victim Response and Reporting of Cyber Incidents'.[6] It reflects lessons learned from federal prosecutors who have studied the tactics and tradecraft of cybercriminals as part of cyber investigations and prosecutions. It also incorporates input from private sector organisations that have managed cyber incidents.

Having a well-established cyber incident response plan in place is a critical first step toward preparing an organisation to weather a cyber incident. Such a plan should contain specific procedures to follow in the event of a cyber incident, making clear who has critical roles and responsibilities in containing the intrusion, mitigating the harm, collecting and preserving vital information for damage assessment, recovery and future defence measures. At a minimum, a cyber response plan should encompass the following:

- The identification of your mission-critical data and assets (ie the 'crown jewels') and establishment of appropriate network security measures to protect those assets.
- A review and adoption of risk management practices found in expert guidance, such as the 'Cybersecurity Framework' developed by the National Institute of Standards and Technology (NIST), that are appropriate for your organisation's size, budget, sector and risk.
- The adoption or identification of easily obtainable technology that will be used to address an incident, including adequate logging, off-site data back-up, intrusion detection capabilities, data loss prevention technologies, and traffic filtering or scrubbing capabilities, as well as the identification of cyber security firms that can provide these and further mitigation services.
- The alignment of organisational policies, such as those regarding personnel and information technology (eg access controls and system administrator employment termination procedures), with your incident response plan.
- The participation in cyber security sharing across your industry and other industries when possible (eg 'Information Sharing and Analysis Centers' [ISACs] or 'Information Sharing and Analysis Organizations' [ISAOs]). ISACs are non-profit organisations that act as centralised collection points and clearing houses for cyberthreat intelligence between federal, state and local governments and specific industries, such as critical infrastructure.[7] ISAOs are more broadly defined than ISACs, because they can be private or non-profit entities and they range from so-called 'communities of interest' to fee-for-service companies.[8]
- An implementation of appropriate authorisations to permit lawful network monitoring, including through consent mechanisms and 'banners' that greet users upon log-in, and compliance with the procedures of the Cybersecurity Information Sharing Act of 2015 (CISA) permitting network monitoring for 'cybersecurity purposes'.[9]
- Obtaining legal counsel that is sufficiently familiar with technology, laws on electronic surveillance and communications privacy, and cyber incident management to minimise response time during an incident.
- Practising the cyber incident response plan through scenario exercises involving all parties critical to the plan's implementation.

An additional, integral part of any responsible organisation's incident response plan is the procedure for determining when and how to notify law enforcement and relevant regulatory agencies. With regard to law enforcement specifically, the midst of an ongoing cyber incident is *not* the time to search for the appropriate points of contact. The former general counsel and executive vice president of Sony has publicly stated

that contact information she had obtained from an FBI official during a previous non-cyber security incident proved vital in the immediate aftermath of the cyberattack from North Korea when she urgently needed government assistance.[10] If you don't know the name and contact information of whom you will call in the event of a cyber incident, then you don't yet have a fully developed incident response plan.

Accordingly, *before* a cyber incident occurs, organisations should establish relationships with relevant law enforcement agencies, such as with cyber agents in the local field offices of federal law enforcement agencies or in sector-specific agencies. Key federal points of contact can be found in Appendix H of the National Association of Corporate Directors Cyber-Risk Oversight Handbook,[11] and in Annex D of the National Cyber Incident Response Plan.[12] In addition, through participation in the FBI's InfraGard programme, individuals in the private sector and academia can meet with law enforcement and other government representatives and confer on how best to protect our critical infrastructure.[13]

Within DOJ, contacts include the National Security Cyber Specialists (NSCS) Network, which consists of at least one Assistant United States Attorney (AUSA) in each of the 94 US Attorneys' Offices around the country. Those prosecutors are trained at the intersection of computer crime and national security in order to improve investigation, prosecution and other disruption of computer intrusions and attacks affecting, involving or relating to national security, such as those perpetrated by terrorists, foreign nation states and their proxies, or which target classified or export-controlled information. For purely criminal cyberthreats, each US Attorney's Office also has at least one dedicated Computer Hacking and Intellectual Property (CHIP) prosecutor, who is responsible for prosecuting computer crime offences, serving as the office's legal counsel on matters related to those offences and the collection of electronic and digital evidence, training prosecutors and law enforcement personnel in their region, and conducting public and industry outreach and awareness activities. In sum, there is no shortage of individuals within federal law enforcement and DOJ with which the necessary relationships can be built in advance of a cyber incident.

WHAT TO EXPECT FROM LAW ENFORCEMENT AFTER A CYBER INCIDENT

Despite taking reasonable defensive measures, any organisation can fall victim to a cyber incident. With a well-developed incident response plan in place, your organisation's personnel should be capable of responding in an effective and appropriate manner by assessing the extent of the intrusion, containing the intrusion to prevent continuing damage, recovering, and conducting a damage assessment using logs, server images and other artefacts preserved during the initial stages of the incident response.

If an organisation suspects at any point during its assessment or response that the incident constitutes criminal activity (as opposed to, for example, an incident involving inadvertent exposure of customer data), it should contact law enforcement immediately. Historically, some organisations have been reticent to contact law enforcement following a cyber incident, fearing a loss of control and a perceived 'parade of horribles', such as a swarm of black SUVs and agents in raid jackets seizing and boxing up servers and electronic media, surprise press conferences or criminal charges, stock price hits, calls from law enforcement to regulators, the US government making victim information public in response to Freedom of Information Act (FOIA) requests, and litigation, all of which would result in disruption of its business and/or reputational

harm. Mindful of these concerns, organisations often prefer to conduct private internal investigations in an attempt to resolve the problem on their own before, or in lieu of, involving law enforcement. As a result, some matters are never reported, while others involve delayed reporting, to the potential detriment of an effective law enforcement or other response.

None of these concerns, however, withstand scrutiny when compared against DOJ's and our partner law enforcement agencies' policies and historical practice. The FBI and US Secret Service are victim-centric organisations that prioritise minimising the intrusions into anyone's privacy and the duration and scope of any disruption while conducting a cyber investigation. One of DOJ's core principles is that we do not want to re-victimise the victim.[14] Accordingly, we recognise the need to work cooperatively and discreetly with victim organisations and their incident response personnel. We will use investigative measures that avoid computer downtime or displacement of an organisation's employees. For example, initial incident responses often simply require access to log files and, in some instances, mirror images of affected machines — items that victim organisations and their outside incident response providers have often already collected pursuant to incident response procedures. Witness interviews are planned well in advance, so that the interviewers and interviewees can come prepared to move quickly and efficiently through the necessary lines of inquiry and everyone can get back to their duties. Further, investigators are interested in technical details about an intrusion, and possibly the surrounding business context, rather than sensitive internal communications interpreting or discussing technical details or evaluating an organisation's network security. The privacy of an organisation's customers is also respected during the law enforcement response. In some cases, when information essential to an investigation is intertwined with customer data, law enforcement agents have worked closely with an organisation's personnel to locate artefacts of the intrusion without unduly sifting through sensitive third-party information.

The FBI and US Secret Service also conduct their investigations with discretion and work with a victim organisation to avoid unwarranted and surprise disclosures of information. We take a victim's wishes into account in deciding when and how to pursue a case or other outcome designed to disrupt the cyberthreat. When the investigation reaches a point where decisions will be made that affect what may eventually become known to the public (eg criminal charging decisions), we consult with the victim to hear their questions and concerns. This includes the advance coordination of the contents of our allegations and other public statements concerning the incident with a victim organisation to the best of our abilities. Prosecutors have discretion in deciding whether and when to bring criminal charges, and in exercising that discretion, we generally do not name a victim in a charging document without its consent. Keep in mind that we can take steps to protect a victim's identity in court documents, charges often remain sealed until a defendant is apprehended, and in discovery and at trial, we routinely protect sensitive information from disclosure to the public through protective orders and similar remedies. Accordingly, although a victim organisation will not be allowed to veto law enforcement's decisions, there is ample opportunity for an organisation to raise red flags and otherwise appropriately influence law enforcement's eventual course of action.

As part of our commitment to exercise discretion, DOJ does not, as a general rule, notify regulators of cyber incidents or provide to regulators information DOJ obtains as part of its criminal investigations. If (and only if) you ask us to do so, we will bring your cooperation with law enforcement to the attention of regulators,

such as the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC) and, if applicable, the Department of Defense (DoD),[15] to ensure that when a regulator becomes aware of an intrusion through other means, it is also aware of an organisation's cooperation with law enforcement in investigating the intrusion and mitigating its harm. These US government entities have publicly stated that cooperating with law enforcement is relevant to their decision making and evidence of an organisation behaving reasonably. For example, the FTC has said that 'a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach' and as a result, 'it's likely [the FTC] would view that company more favorably than a company that hasn't cooperated'.[16] And the SEC has signalled that it 'will give substantial credit' to companies that proactively self-report cyber intrusions.[17] In this sense, DOJ can become a victim advocate within the government to ensure that a victim's rights and interests are respected in the broader government response to a cyber incident. If a regulator were to request information obtained from a victim organisation as part of our investigation, our practice is to refer the regulator to the victim's counsel.

On the other hand, turning a blind eye to, or failing to report cyber breaches may invite scrutiny from regulators as well as lawsuits. Law enforcement may be able to provide your organisation with a fuller picture of the facts needed for you to determine how best to meet your disclosure obligations while minimising any impact to an ongoing investigation. Since publicly traded companies are required to report material cyber security risks and incidents,[18] DOJ also has direct lines of communication with SEC attorneys who can help us work through issues that may arise when you cooperate with law enforcement. Also, at least 48 states (as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands) currently have data breach notification laws requiring organisations to notify customers whose data is compromised.[19] Those laws typically allow delays in notification when law enforcement formally requests them in the interests of an investigation (which means that working with law enforcement to understand the scope and scale of the intrusion can, when justified, also give you breathing space to evaluate your various legal obligations).

Moreover, if you are worried about sharing information with the US government because of FOIA, you should know that FOIA provides for exemptions from disclosure for certain categories of information including 'a trade secret', privileged or confidential 'commercial or financial information obtained from a person', and information 'compiled for law enforcement purposes', the release of which could compromise the investigation or privacy.[20] The government will strive to protect confidential information provided by your organisation to the full extent permissible under FOIA and similar open records laws.

The bottom line is that federal law enforcement agencies view victims of intrusions as just that — crime victims that deserve protection and advocacy within the criminal justice system.

THE BENEFITS OF WORKING WITH DOJ AFTER A CYBER INCIDENT

Even after a cyber incident appears to be under control, we must remain vigilant and seek to raise the costs on the responsible actors. Many intruders return to attempt to regain access to networks they previously compromised, often using lessons learned from a victim's prior remediation efforts and returning with more sophisticated methods. Additionally, left unchecked, they will undoubtedly continue to target other victims. So, although network defence and

effective incident response plans are integral parts of the cyber security equation, they must be combined with efforts to disrupt and deter the responsible actors.

To meet this goal, the answer should not be for an organisation to take it upon itself, or to direct others, to access, or damage, without authorisation, another system that may appear to be involved in the intrusion or attack. Regardless of motive, doing so is likely illegal under US and some foreign laws and could result in civil or criminal liability and worse (in national security matters, miscalculation, for example). Furthermore, many intrusions and attacks are launched from compromised systems. Consequently, 'hacking back' can damage or impair another innocent victim's system rather than the intruder's.

Instead, outside of an organisation's own network, the goals of raising the costs of actors should be the responsibility of the US government, utilising its broad array of authorities. Law enforcement can try to seize (or otherwise disrupt the exfiltration of) data stolen by cyber means if it is quickly identified. DOJ, whether through its own authorities, or by supporting the authorities of other departments and agencies, can also take other appropriate actions that will ultimately benefit victims and prospective victims, which are described in more detail below.

First, we can often determine where your organisation's intrusion falls within a wider range of malicious cyber activities — (eg if it is part of a campaign targeting a certain class of victims or technologies) — and share related information to help your organisation understand what happened, so that you can conduct a damage assessment and identify what else may still be at risk. Experienced law enforcement agents, such as the FBI's Cyber Division, are often familiar with patterns of malicious cyber activity they are seeing across the country and around the world, in some instances over the course of several years. The Department of Homeland Security (DHS) also has components dedicated to cyber security that not only collect and report on cyber incidents, phishing, malware and other vulnerabilities, but also provide certain incident response services. DHS's National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24x7 centralised location for cyber security information sharing, incident response and incident coordination. These components of the federal government can work with your security and technical teams to help you quickly identify and stop the activity and better understand the incident, whether it be the theft of proprietary technology, valuable customer information, or some other kind of loss. They can also tell you if other organisations in your sector have been affected or engage in two-way information sharing with other similarly situated victims (should your organisation not wish to reveal to others that it has be victimised). The more complete your understanding of what happened, the better able you will be to mitigate any damage, recover, and identify and defend against similar activity in the future.

We can also provide context. For example, in 2015, an online retailer learned that it had been hacked and that personally identifiable information (PII) related to approximately 100,000 customers had been stolen. The hacker threatened to expose the company's customer information unless the victim company paid him off. Although this initially sounded like a typical act of extortion, the hacker, Ardit Ferizi, supported the Islamic State of Iraq and Syria (ISIS) and intended to inspire physical attacks against US service members, using that PII to publish an online 'kill list'. Fortunately, the company was working with law enforcement and avoided making a payment that would have supported a terrorist organisation.

Second, reporting the cyber intrusion to law enforcement creates a culture of

information sharing that will not only benefit your organisation, but others across the US and around the world. Disclosing information about the intrusion with the US government can enable us to connect it to related incidents and to share valuable insights and information with you from other investigations by law enforcement and the US intelligence community. Often, the government requires only technical details — such as logs and malware samples — to advance its investigation, not privileged or proprietary information. And usually this technical information can be anonymised so that the government can share it with others in the private sector, so they can take steps to protect themselves against the same intrusions, and possibly provide further technical information back to the government, thereby creating a virtuous cycle of cyberthreat information sharing. For example, the Cybersecurity Information Sharing Act of 2015 (CISA) encourages public–private collaboration related to the sharing of certain types of cyber information, and provides organisations with certain liability protection when they share — with each other or the government — information defined by statute that comprises indicators of cyberthreats, or techniques to defend against cyberthreats.[21] Rest assured that anonymised information shared by law enforcement and other US government partners never identifies, or provides information allowing for the identification of, a cooperating victim.

Furthermore, US law enforcement agencies store information about investigations on secure networks, and access to case information at those agencies is limited to those with a legitimate need to know. In sum, a victim's disclosure of information about an intrusion often enables the government to connect it to, and reciprocally share, information about related incidents and malware, enabling the victim and other organisations to better protect their networks.

Third, quick action by the US government to investigate and preserve evidence maximises your options and gives you a chance of a successful action to disrupt the perpetrators of a cyber incident. Quick reporting — and in turn, quick responsive action and information sharing — allows for proper investigation and preservation of evidence that will maximise the chances of successful action to identify and disrupt the perpetrators. In fact, after looking at the statistics on 'time-to-discovery' of a cyber incident and comparing it to the 'time-to-exfiltration' of important information, Verizon determined that by increasing time-to-exfiltration and lowering time-to-discovery, organisations can stop cyber intrusions from becoming exfiltration.[22] Additionally, speed is essential in any investigation, but especially in a cyber investigation, because the electronic evidence can dissipate quickly.

Fourth, DOJ is uniquely situated to work with other parts of the federal government so that the United States can pursue any number of options in response to a cyber intrusion — including criminal investigation and prosecution, economic sanctions, diplomatic pressure, intelligence operations and even military action. US law enforcement agents have a history of arresting so-called 'hard targets', be they terrorists or hackers (or both), who may have seemed beyond the reach of the US government because they are living in foreign countries. The combination of persistence and cooperation with foreign partners has brought many to justice over the years. For example, Ferizi, the ISIS hacker, was extradited to the US from Malaysia, pleaded guilty and in September 2016 was sentenced to 20 years' imprisonment.[23]

Even when an investigation has yet to result in an arrest, criminal conviction and prison sentence, public charges have contributed to the overall DOJ deterrence and disruption mission and demonstrated to nation states and cybercriminals alike that we can identify them and are committed to

bringing hackers to justice. For example, in April 2017 DOJ charged two officers of the Russian Federal Security Service (FSB) and two criminal conspirators with computer hacking, economic espionage and other criminal offences in connection with a conspiracy to access Yahoo's network and the contents of webmail accounts. Those charges revealed that officers from the FSB unit that serves as the FBI's point of contact in Moscow on cybercrime matters were instead using criminal hackers — one of whom had already been publicly charged in two separate investigations in the United States — to target American webmail providers, technology companies and others. The public revelation of FSB officers working with a wanted cybercriminal, and allowing him to further victimise his targets on the side (eg by searching compromised accounts for credit card and other information that could be monetised), laid bare for the public and international community the nexus between the Russian state apparatus and the Russian criminal underworld and demonstrated that the Russian government is not acting as a responsible stakeholder in combatting international cybercrime. Furthermore, one of the hackers charged by DOJ was arrested in Canada and the US is seeking his extradition.

In March 2016, DOJ charged seven hackers who were employed by two Iran-based computer companies that performed work on behalf of the Iranian government, including the Islamic Revolutionary Guard Corps, for their role in widespread distributed denial-of-service (DDoS) attacks on the public-facing websites of nearly 50 US banks over 176 days in 2011 and 2013. At their peak, those attacks disrupted hundreds of thousands of customers' ability to access their accounts online and conduct transactions, and the affected banks' remediation costs were in the tens of millions of dollars. One of the hackers also repeatedly gained access to the Supervisory Control and Data Acquisition (SCADA) system of a dam in New York, allowing him to obtain information regarding the dam's status and operation. Again, these charges exposed a group of actors who may have previously thought that they could operate behind a veil of cyber anonymity to disrupt the US's critical infrastructure without consequence. Now they must live the rest of their lives in fear of extradition to the US, with limited professional, educational or foreign travel opportunities.

In 2014, DOJ charged five Chinese military officers with computer hacking, economic espionage and other offences directed at six American victim companies in the US nuclear power, metals and solar products industries. These charges sent a clear signal to China that the status quo of its persistent targeting of American entities for the benefit of its own commercial sector was unacceptable and considered by the US government to be a criminal act. It further drove home the message that, despite the Chinese ambassador's earlier public statements to the contrary,[24] the US government could and was prepared to publicly attribute the Chinese government's hacking activities down to the name and face of the person behind the keyboard.

But criminal prosecution alone is not enough and may not always be the most appropriate US government tool to deploy against the cyberthreat. Fortunately, it's not our only tool.

Working with law enforcement, DOJ can also take aggressive action to disrupt hackers by seizing or disabling their infrastructure. For example, the Criminal Division and US Attorneys' Offices have a demonstrated track record of dismantling botnets[25] that have hijacked millions of innocent computers worldwide. In April 2017, for instance, DOJ made public an extensive effort to disrupt and dismantle the Kelihos botnet — a global network of tens of thousands of infected computers under the alleged control of a cybercriminal that was allegedly used to facilitate malicious activities including

harvesting log-in credentials, distributing hundreds of millions of spam e-mails and installing ransomware and other malicious software. According to court documents, the Kelihos botnet distributed enormous volumes of unsolicited spam e-mails advertising counterfeit drugs, deceptively promoting stocks in order to fraudulently increase their price (so-called 'pump-and-dump' stock fraud schemes), work-at-home scams and other frauds. In order to liberate the victim computers from the botnet, DOJ obtained civil and criminal court orders to: 1) establish substitute servers so that infected computers could no longer communicate with the criminal operator, and 2) block any commands sent from the criminal operator attempting to regain control of the infected computers.[26] The Kelihos botnet takedown was only the latest in a long line of DOJ's criminal botnet disruptions, which have also included notable takedowns of the Coreflood and Gameover ZeuS botnets.

The DOJ's investigations, which can often attribute who is behind the cyberattack, also enable a variety of responses by other parts of the US government. Even if we do not arrest the hacker, the federal government may be able to take other action to punish those responsible for, or unjustly enriched by, the victim's loss. For example, under Executive Order 13694, the Treasury Department can issue sanctions against a foreigner that has, through cyber-enabled activities, benefited from stolen information.[27] Other Executive Orders can also provide the necessary authority to sanction malicious cyber actors. As another example, consider the worldwide criticism of North Korea for their hack into Sony's systems — as well as the additional economic sanctions imposed on the country in 2015 — which could not have occurred without the FBI's actions, in partnership with Sony, to uncover who was responsible for the intrusion.

If there is reasonable cause to believe that a company 'has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States', the Commerce Department can add the company to its 'Entity List', which is a way to impose additional licence requirements on organisations seeking to do business with a listed company.[28] For example, in one recent cyber prosecution, a company and its affiliates were added to the Entity List on the basis of their involvement in activities contrary to the national security and foreign policy interests of the United States.[29]

Additionally, the Office of the United States Trade Representative (USTR) can bring a trade action under various trade agreements if a foreign country benefits from trade secret theft.[30] 'The United States uses all trade tools available to ensure that its trading partners provide robust protection for trade secrets and enforce trade secrets laws', according to a USTR report made public in April.[31]

Finally, drawing in part on information developed through DOJ investigations, the US State Department may be able to engage in diplomacy on the victim's behalf. In fact, the State Department and other parts of the US government have engaged diplomatically over the years to try to establish basic international norms in cyberspace. The most tangible result has been the agreement reached in September 2015 between former US President Obama and Chinese President Xi Jinping affirming that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[32] Although we are still monitoring the extent to which China will honour this commitment, the fact that the commitment was made is itself significant, as is the fact that at the November 2015 G20 Summit in Turkey, leaders representing the 20 largest economies in the world agreed to similar

norms related to acceptable behaviour in cyberspace.[33]

In short, the federal government is uniquely situated to pursue many options that will benefit the victim of a cyber intrusion and the country as a whole.

Fifth, if your cyber intrusion does become public, reporting it to law enforcement will help answer the many questions you will be asked by your board of directors, shareholders, customers, the news media and the public at large, who will want to know that the organisation did everything in its power to protect itself and those stakeholders. Cooperating with law enforcement can be the first step to show that an organisation is taking a cyber incident seriously and doing everything in its power to mitigate the intrusion so that it can get back to business as usual. The tremendous value of cooperating with law enforcement, including drawing on the collective holdings of the law enforcement and intelligence communities to investigate, mitigate and remediate intrusions and attacks, almost always outweighs any potential disruption from the investigation.

CONCLUSION

The DOJ follows a whole-of-government approach to investigate, disrupt and deter malicious cyber activity. We work with law enforcement agencies; the intelligence community; diplomatic, civil, administrative and regulatory agencies — as well as victims and the private sector — to draw upon each partner's unique expertise and resources, and to use whichever tool or combination of tools will be most effective in responding to a particular threat. In sum, DOJ's investigations, by attributing malicious cyber activity, can enable a variety of responses by the other parts of the US government to disrupt and deter malicious cyber actors.

Our approach also provides many benefits to victims of cyber intrusions and attacks: we can help you understand what happened; we can share context and information about related incidents or malware; we can ensure proper investigation and preservation of evidence; we can assist you in dealing with regulators; and we are uniquely situated to work with other parts of the federal government so that the US can pursue the perpetrators through criminal investigation and prosecution, economic sanctions, diplomatic pressure, intelligence operations and even military action.

The victims with whom we partner are increasingly satisfied with our help. Polling by Accenture released in April 2017 revealed that when individuals work with the government, they are significantly more likely to express confidence in the ability of law enforcement to prosecute cybercrime. Specifically, respondents who interact with government regularly (daily or multiple times per day) were more than twice as likely as those who don't to express confidence in government's ability to protect their data (64 per cent versus 27 per cent) and significantly more confident in the ability of law enforcement to prosecute cybercrime (67 per cent versus 36 per cent).[34] In short, we are here to help, and we look forward to working with you and demonstrating our abilities before, during and after a cyber incident.

Notes and References

1. Mueller, R. S. (March 2012), Speech, RSA Cyber Security Conference San Francisco, CA FBI, available at https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (accessed 31st May, 2017).
2. Rogin, J. (July 2012), 'NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"', foreignpolicy.com, at http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/ (accessed 31st May, 2017).
3. See eg 'Symantec Internet Security Threat Report', Vol. 22, April 2017, available at https://www.symantec.com/security-center/threat-report (accessed 31st May, 2017); 'Verizon 2017 Data

Breach Investigations Report', 10th edn, April 2017, available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (accessed 31st May, 2017).

4. This discussion in this paper is primarily focused on the relationship between a victim of a cyber incident and federal law enforcement. Many of the issues and guidance discussed herein, however, are equally applicable and relevant to witnesses of cyber intrusions, including internet service providers that become aware of cyber incidents involving their infrastructure or services being used to victimise another organisation.
5. This paper discusses best practices and explains why notifying and working with law enforcement is the smart choice for an organisation before, during, and after a cyber incident. It does not address mandatory reporting requirements that may arise pursuant to law, regulation, or contract. Such required reporting should continue to occur through designated points of contact using existing procedures.
6. 'Best Practices for Vitim Response and Reporting of Cyber Incidents', (April 2015), US Department of Justice, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf (accessed 31st May, 2017).
7. Presidential Decision Directive-63 (PDD-63), signed on 22nd May, 1998, led to the formation of ISACs when it formally asked each critical infrastructure sector to establish a sector-specific organisation to share information about threats and vulnerabilities with each other and the Federal Government.
8. On 13th February, 2015, Executive Order 13691, entitled 'Promoting Private Sector Cybersecurity Information Sharing', expanded the concept of private sector cyber security information sharing by encouraging the formation of ISAOs. The goal of sharing through ISAOs was to 'protect[] the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States', while protecting 'civil liberties of individuals' and preserving,business confidentiality,, according to the Executive Order.
9. Section 104(a)(1)(A)-(C) and (b)(1)(A)-(C).
10. Grande, A. 'Ex-Sony GC Says FBI's Help Was Vital In Breach Aftermath', available at https://www.law360.com/articles/822133/ex-sony-gc-says-fbi-s-help-was-vital-in-breach-aftermath (accessed 31st May, 2017). In response, former FBI Director Jim Comey said, 'The Sony attack was awful; it could have been a lot worse. We had agents and analysts there within hours. We knew Sony because they had taken the time to talk to us beforehand. We didn't need to know secrets from them'. Id.
11. Clinton, L. 'Cyber Risk Oversight', Directors Handbook Series, available at https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf (accessed 31st May, 2017).
12. 'National Cyber Incident Response Plan' (December 2016), Homeland Security, available at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf (accessed 31st May, 2017).
13. InfraGard, available at https://www.infraguard.org/application/general/moreinfo (accessed 31st May, 2017).
14. See, eg 'Principles of Federal Prosecution, United States Attorney's Manual', Title 9, Chapter 9-27.230 (discussing the interests of any victims), available at https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.230 (accessed 31st May, 2017); 'Intake and Charging Policy for Computer Crime Matters', Attorney General Eric Holder, United States Department of Justice (11th September, 2014), available at https://www.justice.gov/criminal-ccips/file/904941/download (accessed 31st May, 2017).
15. See, eg Cassidy, S., Fein, A. and Sorrenti, J. (October 2016), 'Inside Government Contracts — DoD Finalizes Rule on Policies for Cyber Incident Reporting', available at https://www.insidegovernmentcontracts.com/2016/10/dod-finalizes-rule-policies-cyber-incident-reporting/ (accessed 31st May, 2017) (for reporting requirements for DoD contractors and subcontractors).
16. Eichorn, M. (May 2015), 'If the FTC Comes to Call', FED. TRADE COMM'N BUS. Blog, available at https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (accessed 31st May, 2017).
17. Herzinger, K. Ross, A. and Beaman, G. (February 2016), 'SEC Speaks—What to Expect in 2016', ORRICK, available at http://blogs.orrick.com/securities-litigation/2016/02/23/sec-speaks-what-to-expect-in-2016/ (accessed 31st May, 2017).
18. US Securities and Exchange Commission, 'CF Disclosure Guidance: Topic No. 2', available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed 31st May, 2017).
19. NCSL, 'Security Breach Notification Laws', available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed 31st May, 2017).
20. See 5 U.S.C. §§ 552(b)(4) and (b)(7) (2016).
21. See 6 U.S.C. § 1504(c)(1)(B)(i). CISA does not displace other avenues of information sharing. Instead, it provides congressionally authorised pathways for information sharing that offer unique advantages — including liability protection — to those who use them.
22. Verizon, 'How long since you took a long hard look at your cybersecurity?', available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (accessed 31st May, 2017).
23. US Department of Justice, ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison (September 2016), https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison (accessed 31st May, 2017).
24. See, eg 'Beijing's Brand Ambassador: A Conversation

with Cui Tiankai', Foreign Affairs (July/August 2013), available at https://www.foreignaffairs.com/interviews/2013-05-15/beijings-brand-ambassador (accessed 31st May, 2017). 'I don't think anybody has so far presented any hard evidence, evidence that could stand up in court, to prove that there is really somebody in China, Chinese nationals, that are doing these [cyberattacks]'.

25. A 'botnet' is a network of Internet-connected devices, which may include computers, servers, mobile devices and other connected devices infected with malicious software and controlled as a group without the owners' knowledge, eg to send spam messages.
26. US Department of Justice, 'Justice Department Announces Actions to Dismantle Kelihos Botnet', available at https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0 (accessed 31st May, 2017).
27. 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities', (April 2015), Federal Register, Vol. 80, No. 63, available at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf (accessed 31st May, 2017).
28. See Part 744 of the 'Export Administration Regulations', available at https://www.gpo.gov/fdsys/pkg/CFR-2016-title15-vol2/xml/CFR-2016-title15-vol2-part744.xml (accessed 31st May, 2017).
29. 'Addition of Certain Persons to the Entity List', available at https://www.federalregister.gov/documents/2014/08/01/2014-17960/additions-to-the-entity-list (accessed 31st May, 2017). Listing PRC Lode Technology Corporation, which was a company owned by Su Bin, a Chinese national currently serving a prison term for conspiring with Chinese air force officers to exploit computer systems of US companies and DoD contractors to illicitly obtain and export information, including controlled technology, related to military projects.
30. Similarly, Section 337 the Tariff Act of 1930 (19 U.S.C. § 1337) is an economic tool available to US industries.
31. https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF (accessed 31st May, 2017).
32. See Press Release, White House, FACT SHEET: President Xi Jinping's State Visit to the United States (25th September, 2015), available at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed 31st May, 2017).
33. G20 Leaders' Communiqué, Antalya Summit 6 (2015), available at http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/ (accessed 31st May, 2017).
34. 'Most US Citizens Want Government Agencies to Strengthen Cyber Defense Mechanisms to protect their Digital Data, Accenture Research Finds' (April 2017), Accenture, available at https://newsroom.accenture.com/news/most-us-citizens-experiencing-cyber-insecurity-and-wish-government-agencies-had-stronger-cyber-defense-mechanisms-to-protect-their-digital-data-accenture-research-finds.htm (accessed 31st May, 2017).