Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents[1]

Version 2.0 (September 2018)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to a cyber incident can be critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* a data breach incident, ransomware attack, or other cyber incident occurs.

The Cybersecurity Unit originally published this "best practices" document to help organizations prepare a cyber incident response plan and, more generally, to better equip themselves to respond effectively and lawfully to a cyber incident. This updated version includes additional incident response considerations, including ransomware, information sharing pursuant to the Cybersecurity Information Sharing Act of 2015, cloud computing, and working with cyber incident response firms. It distills lessons learned by federal investigators and prosecutors and input from private sector companies that have managed cyber incidents. It includes advice on preventing cyber incidents, as well as advice on working effectively with law enforcement. Like its predecessor, it was drafted primarily for smaller organizations and their legal counsel; however, it may be useful for larger organizations with more experience in handling cyber incidents as well.

I. Steps to Take *Before* a Cyber Intrusion or Attack Occurs

Having well-established plans and procedures in place for managing and responding to cyber intrusions and attacks is a critical first step toward being prepared to weather a cyber incident. Such pre-planning can help organizations limit damage to their computer networks, minimize work stoppages, expedite mitigation efforts, and enhance the ability of law enforcement to identify and apprehend perpetrators. Organizations should take the steps outlined below before

[1] The guidance contained in this document is intended to help organizations and investigators prevent, mitigate, and respond to cyber incidents; however, it may not apply to all organizations or in every situation. Therefore, failure to take all of the proposed steps or implement all of the measures discussed herein should not be interpreted *per se* as unreasonable or negligent conduct. In addition, this document confers no rights or remedies and does not have the force of law. *See United States v. Caceres*, 440 U.S. 741 (1979). It is also not intended to have any regulatory effect.

a cyber incident occurs.

A. Educate Senior Management about the Threat

Organizations are increasingly aware of the threat posed by cyber incidents such as data breaches and ransomware attacks and the potential cost of inadequately preparing for them. But ensuring that an organization is prepared to manage the risk posed by cyber threats requires a common understanding throughout the organization of the nature, scope, and severity of the threat. In particular, an organization's senior management, board of trustees, and any other governing body responsible for making resource decisions and setting priorities should be aware of how cyber threats can disrupt an organization, compromise its products, impair customer confidence and relations, and otherwise cause costly damage.

Regular briefings about existing and emerging cyber threats and appropriate risk management strategies are one way of keeping senior management informed. Cyber incident preparedness exercises (which are discussed further below) can be another valuable educational tool.

B. Identify Your "Crown Jewels"

The cost and difficulty of protecting an entire enterprise from all manner of cyber threats can be overwhelming. Accordingly, an organization should prioritize its cybersecurity efforts. Different organizations have different mission-critical needs. For some organizations, even a short-term disruption in email service will have a devastating impact on operations. Other organizations may not be so dependent on email to conduct their business, but they may suffer significant harm if certain intellectual property is stolen. For others, the ability to guarantee the integrity and security of the data they store and process is the essential service that must be protected. Before formulating a cyber incident response plan, an organization should first determine which of its data, assets, and services warrants the greatest protection.

Prioritizing the protection of an organization's "crown jewels" and assessing how to manage the risk associated with protecting them are important first steps toward preventing the type of catastrophic harm that can result from a cyber incident. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) provides excellent, free guidance on risk-management planning and policies that provide a prioritized, flexible, and cost-effective approach to protecting critical networks. The NIST Cybersecurity Framework has been widely adopted and can be easily integrated into risk management and incident response planning.[2]

[2] NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://www.nist.gov/cyberframework.

Properly assessing risk is important. It is the key to setting effective cybersecurity priorities. When assessing risk, an organization should evaluate threats that stem from the use of contractors, service providers, and other outside agents that host an organization's data and/or have access to its network, data, or resources (e.g., third-party vendors, law firms, and clearinghouses). An organization's data is only as secure as its greatest point of vulnerability, and that vulnerability might belong to a third party.

C. Have an Actionable Plan in Place … Now!

Organizations should have a plan in place for handling computer intrusions, data breaches, and other cyber incidents before they occur; yet many still lack a formal cyber incident response plan.[3] During a cyber incident, an organization's management and other personnel should be focused on containing the incident, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the incident and the potential source of the threat. An organization should not be creating emergency procedures or considering response options for the first time while in the midst of a cyber incident. Any decisions regarding incident response that can be made beforehand should be captured in the plan to save valuable time during an incident.

The plan should be "actionable," meaning it should: provide specific, concrete procedures to follow in the event of a cyber incident; be up-to-date; include timelines for the completion of critical tasks; and identify key decision makers. At a minimum, the plan should address, or at least provide a process for addressing, the following considerations:

- Who has decision-making responsibility for different elements of an organization's cyber incident response, including public communications, implementing security and mitigation measures, engaging with law enforcement, and resolving legal questions;
- How to contact critical personnel at any time, day or night, and how to proceed if critical personnel are unreachable or unavailable;
- What mission-critical data, networks, assets, or services should receive prioritized attention during an incident;
- How to contact and interact with other parties who host the organization's affected data and services (e.g., cloud storage service providers or commercial data centers);
- How to contact the organization's retained incident response firm or otherwise obtain incident response assistance, if needed;

[3] PONEMON INSTITUTE, THIRD ANNUAL STUDY ON THE CYBER RESILIENT ORGANIZATION (2018), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55015655USEN&. (finding that 77% of respondents lacked a formal incident response plan).

- When and how to restore backed-up data, including measures for insuring the integrity of backed-up data before restoration;
- What criteria will be used to determine whether data owners, customers, or partner organizations need to be notified if their data or networks may have been illegally accessed; and
- When and how to notify law enforcement and/or other government entities.

Once an incident response plan is prepared, all personnel with incident response roles, particularly anyone with a role in making technical, operational, or managerial decisions during an incident, should keep it close at hand. While under normal circumstances it may be most efficient to make the plan available in electronic form on the organization's network, have hard copies readily available in case a cyber incident—for instance, a ransomware attack[4]—renders an organization's online resources inaccessible.

Familiarity with the incident response plan should be ingrained through regularly conducted exercises. Staging regular exercises has the auxiliary benefit of ensuring the plan is kept up-to-date as inevitable personnel changes occur within an organization.

Exercises can take a variety of forms—from full-blown real-time enactments of incidents to discussions of scenarios explored in a "tabletop" setting. They need not require major time investments. Regardless of the format, it is valuable to perform exercises regularly to make sure communications channels and emergency processes remain up-to-date and familiar. Such exercises should be designed to verify that necessary lines of communication exist, decision-making roles and responsibilities are well understood, technology that may be needed during an actual incident is available and likely to be effective, and personnel have a common understanding of how the organization will handle an emergency. Deficiencies and gaps identified during an exercise should be noted for speedy resolution.

D. Engage with Law Enforcement Before an Incident

Organizations should establish a relationship with their local offices of federal law enforcement agencies long before they suffer a cyber incident. Having a point-of-contact and a pre-existing relationship with law enforcement will ease any subsequent contact if an organization later needs law enforcement assistance. It will also help establish a relationship that fosters bi-

[4] "Ransomware" is malware designed to make data or a device inaccessible, often by encrypting data stored on the device or locking a device's keyboard, until a ransom is paid. Federal departments and agencies have published guidance for Chief Information and Chief Information Security Officers with advice regarding how to avoid and mitigate ransomware attacks. *See, e.g.*, FEDERAL BUREAU OF INVESTIGATION, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

directional information sharing that is beneficial both to potential victim organizations and law enforcement.

As discussed in detail in the next section on responding to a cyber incident, federal law enforcement has focused on improving its outreach to and support of organizations facing cyber threats. At headquarters and in the local field offices throughout the country, law enforcement has dedicated agents and resources to building better lines of communications and instituting policies and practices that better serve victims of cyber attacks and intrusions.

The principal federal law enforcement agencies responsible for investigating criminal violations of the federal Computer Fraud and Abuse Act are the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service). Both agencies conduct regular outreach to private sector companies and other organizations likely to be targeted for intrusions and attacks. Such outreach occurs mostly through the FBI's InfraGard chapters and the Cyber Task Forces in each of the FBI's 56 field offices, and through the Secret Service's nationwide network of Electronic Crimes Task Forces. Organizations will find responsive federal law enforcement nearby, regardless of where they are located.

Federal law enforcement is also a valuable source of cyber threat information that can help prevent a cyber incident. The FBI and Secret Service often develop and share cyber threat information through collaboration with information sharing and analysis organizations, other government agencies, non-governmental organizations, and private sector organizations. In partnership with DHS, the FBI publishes 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. Similarly, in partnership with DHS, federal law enforcement publishes joint products, such as Joint Analysis Reports (JARs) and Joint Technical Advisories (JTAs) that furnish additional cyber threat intelligence. Such products are available to members of InfraGard and Secret Service's Electronic Crimes Task Forces.

E. Have Appropriate Workplace Policies in Place

Because institutionalized familiarity with the organization's plan for addressing a cyber incident can expedite response time and save critical minutes, hours, or even days of recovery time, an organization should adopt internal policies and rules that will help ensure that its personnel are familiar with the incident response plan. For instance, the procedures for responding to a cyber incident can be integrated into routine personnel training.

Some personnel policies can also prevent cyber threats and mitigate potential damage. For

example, promptly revoking the computer credentials of terminated employees—particularly system administrators and information technology staff—can prevent a spiteful ex-employee from damaging a former employer's network or data. An organization that has already adopted such policies should also ensure that they are enforced.

F. Institute Basic Cybersecurity Procedures

Of course, every organization should adopt and maintain commonsense cybersecurity practices. Such practices can be found in guidance and white papers that are readily available from government and private sector sources. However, in law enforcement's experience, certain cybersecurity measures have outsized security benefits.

For instance, the majority of intrusions are conducted using known software vulnerabilities. Therefore, a reasonable patch management program will help prevent many attempted intrusions. Likewise, access controls and network segmentation that appropriately limit the availability of data—particularly information considered to be an organization's "crown jewels"—can minimize the consequences of a breach, regardless of whether the breach is attributable to an insider threat or remote computer intrusions. While not infallible, reasonable password management programs and use of multi-factor authentication can thwart rudimentary password-cracking efforts. In addition, some type of perimeter defense, such as a firewall, can help detect common cyber threats. These are basic cybersecurity measures that may not thwart more sophisticated criminals; however, they are effective against an array of commonly used exploits.

Regardless of the nature of the cyber threat, server logs are typically critical to ascertaining the cause and origin of a cyber incident. A criminal investigation, as well as an internal investigation or audit, will likely rely on log data. Consequently, an organization should enable logging on all its servers and configure them to maintain copies of logs for as long as practicable.[5]

G. Procure Appropriate Cybersecurity Technology and Services Before an Incident Occurs

Ideally, organizations will acquire or have ready access to the technology and services they will need to respond to and recover from cyber incidents. Depending on an organization's resources, the types of assets it wants to protect, and the nature of the cyber threats it needs to counter, this may mean procuring cybersecurity services such as intrusion detection capabilities, data loss prevention technologies (e.g., backups), and/or traffic filtering or scrubbing services.

[5] Ideally, an organization should conduct "informational level logging" (i.e., logging of "normal" events, such as traffic passing through a firewall instead of just traffic that generates alerts and/or is blocked). Such logging can help determine the scope of an intrusion or a breach after it has been detected.

An organization should align the services it procures with the cyber threats that would cause it the greatest harm. Some services do not provide adequate protection against certain threats. For instance, off-site data back-up capabilities may provide only marginal protection against the unlawful exfiltration of data but can be critical when faced with a ransomware attack. Similarly, traffic filtering services can fend off a denial-of-service attack,[6] but they provide no defense against a business email compromise.[7] Technological solutions should be tested regularly by the organization or by contracted third parties to ensure they perform as expected.

Some organizations choose to retain the services of an incident response firm in preparation for a cyber incident. Incident response firms have technical knowledge, equipment, and experience that many organizations are unable to maintain in-house. Therefore, an incident response firm can increase the speed and effectiveness of an organization's response to a cyber incident. Many incident response professionals are also accustomed to working alongside law enforcement, which may expedite coordination when an organization contacts law enforcement following an incident. Government services associated with mitigating and recovering from a cyber incident may also be available. Organizations may check with the Department of Homeland Security (DHS) or their sector-specific agency regarding the availability of such services.[8]

Some organizations use cloud storage[9] services for the convenience and security such services can provide. There are numerous benefits to using cloud storage; however, it is not a remedy to all cyber threats. Organizations should still assess the sufficiency of the security services they receive in connection with their cloud storage services to ensure they provide adequate protection. Also, contracts and agreements with cloud service providers should anticipate the need to furnish third parties, such as law enforcement and incident response firms, with access to the organization's information and resources during a cyber incident. Organizations should consider including provisions in their contracts and agreements requiring cloud providers to assist third parties with access to an organization's data at the organization's request.

---

[6] A distributed denial-of-service (DDOS) attack uses multiple computers or devices to (1) transmit a torrent of communications traffic at another computer or network to block communications to and from the targeted system (a volumetric attack), (2) consume the processing capability of the target computer (a protocol attack), or (3) establish a connection with the target computer that exhausts its resources by monopolizing processes (an application attack). The attacking computers or devices are typically infected by malware that allows them to be centrally controlled by the perpetrator of the attack.

[7] A "business email compromise" is a sophisticated scam targeting businesses working with foreign suppliers and businesses that regularly perform wire transfer payments. The FBI has provided more information about such schemes at https://www.ic3.gov/media/2015/150122.aspx

[8] Organizations can contact DHS for such assistance at https://www.us-cert.gov or by calling (888) 282-0870.

[9] Cloud storage involves storing data on remote servers rather than locally. For instance, an organization may choose to store its data on a cloud storage provider's network rather than on its own system. Cost, accessibility, and security are often cited as advantages of using cloud storage.

H. Have Appropriate Authorization in Place to Permit Network Monitoring

The ability to monitor network traffic is critical to detecting and preventing cyber incidents. Monitoring can also be instrumental to analyzing an ongoing intrusion or other security breach. But monitoring network communications can implicate federal civil and criminal statutes. Accordingly, in addition to procuring the technical ability to monitor their systems and devices for cybersecurity threats, organizations should also establish the legal authority to conduct such monitoring before it begins.

In general, the monitoring of wire and electronic communications is regulated by federal electronic surveillance statutes. The Wiretap Act prohibits the interception of wire and electronic communications, except with a court order or consistent with one of the statute's exceptions.[10] Similarly, the Pen Register/Trap and Trace (PRTT) Act prohibits the use or installation of a device or process that captures, records, or decodes non-content information (i.e., dialing, routing, addressing, or signaling information), except with a court order or consistent with the statute's exceptions.[11] As discussed below, both statues include exceptions that may apply to cybersecurity monitoring, including an exception for providers of wire or electronic communication services who conduct monitoring to protect their "rights or property."[12] Many states have comparable laws with similar exceptions. Congress simplified matters in 2015 when it enacted the Cybersecurity Information Sharing Act of 2015 (CISA), which explicitly authorized organizations to conduct many cybersecurity activities.

CISA provides private entities with broad authority to conduct cybersecurity monitoring of their own networks, or a third party's networks with appropriate consent.[13] CISA expressly preempts contrary state law and authorizes cybersecurity monitoring "notwithstanding any other provision of law," meaning it overrides any conflicting laws, including the Wiretap Act and the PRTT Act.[14] CISA also provides private entities with liability protection against any legal action brought in any court—state or federal—for cybersecurity monitoring conducted in accordance with CISA.[15]

It is important, however, to recognize the limits of CISA's monitoring authority. CISA only authorizes private entities to monitor information or an information system for a "cybersecurity purpose." A "cybersecurity purpose" means for the "purpose of protecting an

[10] 18 U.S.C. § 2510 et seq.
[11] 18 U.S.C. § 3121 et seq.
[12] 18 U.S.C. § 2511(2)(a), 3121(b)
[13] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), N., 129 Stat. 2242, 2936 – 2956 (2015).
[14] 6 U.S.C. §§ 1503(a), 1507(k).
[15] 6 U.S.C. § 1505(a).

information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[16] Thus, CISA authorizes monitoring to prevent a cyber incident and to inform response efforts to avoid further damage. However, CISA does not authorize monitoring conducted for purposes unrelated to cybersecurity, such as in support of administrative investigations for employee misconduct having nothing to do with a cybersecurity threat.

Because CISA only allows monitoring for cybersecurity purposes, organizations that intend to monitor their networks for other reasons must have another legal basis for doing so that satisfies the Wiretap Act and PRTT statute. The most common means of complying with those statutes is by obtaining prior consent to monitor using network log-on warnings or "banners."[17] For example, an organization may use log-in banners with click-through buttons to obtain consent or to inform users that their use of the network constitutes consent to the organization's interception of their communications.

In the absence of a log-on banner, organizations may look to computer user agreements, workplace policies, and personnel training to establish that users of their network consented to monitoring. It is advisable, though, for organizations to obtain written acknowledgement from their personnel that they were notified that their communications were monitored and that use of the organization's network constituted consent to such monitoring. Doing so will provide an organization with ready proof that its monitoring was lawfully conducted with users' consent.

An organization might also lawfully intercept communications using other statutory exceptions. For instance, the Wiretap Act and PRTT Act each have an exception that allows a provider of an electronic communication service—such as e-mail—to intercept communications to protect its rights or property.[18] The Department's Computer Crime and Intellectual Property Section, which manages the Cybersecurity Unit, has published an online manual on monitoring electronic communications that includes guidance on the rights or property exception, as well as other exceptions to the Wiretap Act and PRTT Act.[19]

---

[16] 6 U.S.C. § 1501(4).

[17] 18 U.S.C. §§ 2511(2)(c)-(d), 3121(b)(3). More guidance on banners, including a model banner, can be found in our manual on searching and seizing electronic evidence and in a 2009 legal opinion prepared by the Department of Justice's Office of Legal Counsel. *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (3d ed. 2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; Stephen G. Bradbury, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, 33 OP. O.L.C. 1 (2009), http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf

[18] 18 U.S.C. §§ 2511(2)(a) (ii), 3121(b)(2).

[19] *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, *supra* note 16, at 172-177.

I. Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management

Preventing and responding to cyber incidents can raise a host of unique legal questions. Furthermore, decisions made during a cyber incident may later have legal consequences. During a cyber incident, many organizations have found it beneficial to obtain legal advice from attorneys who are conversant with technology and knowledgeable about relevant laws, including the Computer Fraud and Abuse Act[20] and laws governing electronic surveillance, communications, data privacy, and information-sharing. Legal questions may also arise concerning how to interact with investigators, whether the thresholds for mandatory breach reporting have been met, and how to weigh liability for taking specific remedial measures or failing to do so. Even before an incident, organizations may face questions regarding the workplace policies required to institute threat detection and data loss prevention programs and the suitability of different types of cyber insurance.

Many private sector organizations retain or consult outside counsel who specialize in legal questions associated with data breaches, while others manage cyber issues so frequently that they have their own cyber-savvy attorneys on staff. Regardless of how an organization chooses to structure its legal representation, having ready access to advice from lawyers who are well acquainted with cyber incident response can speed up an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing. Regardless of whether an organization uses outside or in-house counsel, its lawyers should be included in incident response planning and exercises to acquaint them with legal issues likely to arise during a cyber incident and to give them the opportunity to prepare to address them in advance.

J. Establish Relationships with Private and Public Cyber Information-Sharing and Analysis Organizations

Staying up-to-date on new and emerging cyber threats can be a daunting task, but having access to cyber threat intelligence and information about commonly exploited vulnerabilities can help an organization set its security priorities. Information Sharing and Analysis Centers (ISACs) exist for every sector of the "critical infrastructure" and provide actionable cyber threat information.[21] The "critical infrastructure" of the United States consists of 16 sectors,[22] and most

[20] 18 U.S.C. § 1030.

[21] Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21), 2013 WL 503845 (Feb. 12, 2013).

[22] As set forth in PPD-21, the critical infrastructure consists of the following sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy;

sectors have a dedicated ISAC. ISACs share analysis of cyber threat information within their respective sectors, with other sectors, and with the government. Depending upon the sector, they may provide other cybersecurity services as well.

The federal government has also encouraged the creation of information-sharing entities called Information Sharing and Analysis Organizations (ISAOs) to accommodate organizations that do not fall within an established sector of the critical infrastructure or that have unique needs.[23] ISAOs are intended to provide such organizations with the same benefits of obtaining cyber threat information and other supporting services from ISACs.

As discussed above, CISA authorizes monitoring for a cybersecurity purpose; however, it was enacted principally to facilitate cyber threat information sharing. CISA authorizes non-federal entities to share cyber threat indicators with and to receive cyber threat indicators from the federal government and other non-federal entities, such as ISACs and ISAOs. When a non-federal entity engages in indicator sharing in accordance with CISA, it receives liability protection for the act of sharing that information and other statutory protections as well, including exemptions from federal and state disclosure laws and protection from having shared information used for certain state and federal regulatory purposes.[24]

The federal government is also a valuable source of cybersecurity information. As discussed further below, the FBI and Secret Service regularly share cyber threat information with the private sector through established programs. Furthermore, the DHS National Cybersecurity and Communications Integration Center (NCCIC), while not a law enforcement organization, routinely provides alerts, vulnerability information, and analysis reports that can help organizations detect, prevent, and mitigate incidents. It also provides automated feeds of indicators of compromise that organizations can access for free.[25]

Historically, some private sector organizations have expressed concern that the Federal

---

financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater systems. *Id.*

[23] *See* Exec. Order No. 13,691, 80 Fed. Reg. 9347 (Feb. 20, 2015), available at http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[24] For instruction on how to share and receive information consistent with CISA, please review DEP'T OF JUSTICE & DEP'T OF HOMELAND SEC., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf, and DEP'T OF HOMELAND SEC., CYBERSECURITY INFORMATION SHARING ACT – FREQUENTLY ASKED QUESTIONS, https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf.

[25] See the US-CERT web site for additional information, available at https://www.us-cert.gov; https://www.us-cert.gov/ais.

Trade Commission (FTC) or Department of Justice might consider sharing cybersecurity threat information with other private sector organizations to be a violation of federal antitrust laws. Those concerns, however, have been addressed in policy and by statute. The FTC and the Department's Antitrust Division issued a joint statement in 2014 reaffirming their views that antitrust laws are not—and should not be—an impediment to legitimate cyber threat information sharing. Furthermore, CISA included a statutory exception to liability under antitrust laws for sharing cyber threat indicators and defensive measures in accordance with that statute.[26]

II. Responding to a Cyber Incident: Executing Your Incident Response Plan

An organization can fall victim to a cyber intrusion or attack even after taking reasonable precautions. Consequently, being prepared to execute a vetted, actionable cyber incident response plan is critical. A robust incident response plan does more than merely provide procedures for handling an incident; it also provides direction on how a victim organization can continue operating while managing an incident and explains how to work with law enforcement and/or incident response firms as an investigation is being conducted. An organization's incident response plan should give serious consideration to all of the steps outlined below.

Step 1: Make an Initial Assessment

a. Data Collection

During a cyber incident, a victim organization should immediately assess the nature and scope of the incident. It is important at the outset to ascertain whether the incident was caused by a malicious act, human error, or a technological glitch—or possibly a combination of those factors. The nature of the incident will determine the type of assistance an organization will need, the type of damage it will need to mitigate, and the remedial efforts that may be required.

Having appropriate logging capabilities enabled can be critical to identifying the origin of a cyber incident. A system administrator should use all available logs to attempt to identify:

- the affected computer systems;
- the apparent origin of the incident, intrusion, or attack;
- any malware used in connection with the incident;
- any remote servers to which data was sent (if information was exfiltrated); and
- the identity of any other victim organizations, if such data is apparent in logged data.

[26] See 6 U.S.C. § 1503(e)(1).

In addition, the initial assessment of the incident should document:

- which users are logged onto the network;
- which processes are running;
- current external connections to the computer systems; and
- all open ports and their associated services and applications.

Any communications received by the organization that might relate to the incident (in particular, threats, claims of credit, or extortionate demands) should be documented and preserved. Suspicious calls, emails, or other requests for information about the incident should also be treated as part of the incident.

Evidence that an intrusion or other criminal act has occurred will typically include network logs and file creation data indicating that someone improperly accessed, created, modified, deleted, or copied files, logs, or other data; changed system settings; or added or altered user accounts or permissions on the network. In addition, an intruder may have left behind indicators of compromise, such as "hacker tools" or data from another intrusion.

An intruder with "root level access" has the highest privileges given to a user working with an operating system or other program and has as much authority on the network as a system administrator, including the authority to access files, alter permissions and privileges, and add or remove accounts. In the case of a root-level intrusion, victims should be vigilant for signs that the intruder has gained access to multiple areas of the network.

The victim organization should ensure that its actions do not unintentionally or unnecessarily modify stored data. *Such modification could hinder incident response and internal or criminal investigations. In particular, potentially relevant files should not be deleted and, at the very least, any modifications should be recorded.*

b. Working with Incident Response Firms

Increasingly, victim organizations enlist private sector cybersecurity or incident response firms to assess and respond to cyber incidents on their behalf. Incident response firms are often on scene collecting evidence before federal investigators are even initially contacted. Therefore, in choosing such a firm, an organization should ensure it selects one that is well acquainted with forensically sound methods of evidence collection that do not taint or destroy evidence. An incident response firm should also be capable of preserving data in a manner that will allow it to

be used later as evidence.

A victim organization may direct its incident response firm to prepare a forensic report about the causes and consequences of a cyber incident. The organization may later seek to protect that report from disclosure in connection with any civil litigation or regulatory action that results from the incident. When a forensic report is prepared at the direction of an organization's attorneys, the organization may seek to withhold it from anyone outside the organization under a claim of attorney-client communications or attorney work product privileges. Setting aside the legal viability of such claims of privilege, withholding of such information from law enforcement—or even delaying the sharing—can make criminal investigation more difficult.

It is important to emphasize that law enforcement's need for a crime victim's information differs from that of parties interested in assessing whether the victim organization is liable for the incident. Law enforcement is responsible for investigating a criminal violation with the objective of identifying, apprehending, and prosecuting the perpetrator, as appropriate. Accordingly, law enforcement is focused on collecting information *about the perpetrator's criminal conduct* that can be used to identify and prosecute her or him. Therefore, the information that law enforcement needs is frequently limited to technical data that can be used to track activities and events on a victim company's network.

Such technical information is distinct from, but sometimes commingled with, an incident response firm's assessment of the strengths or weaknesses of an organization's cybersecurity practices prior to an incident or its performance during the incident. Law enforcement is flexible and willing to work with a victim organization to find a suitable means of obtaining technical information about a cyber incident consistent with the victim organization's concerns and the needs of law enforcement, which may sometimes mean obtaining something other than the full forensic report. Alternative means of producing sought after technical data may include producing a summary of an incident response firm's report, creating an excerpted version of a forensic report, or interviewing personnel who can provide the required technical data.

Federal investigators may need to coordinate with a victim organization's incident response firm to procure the technical data the firm has already collected. A victim company can assist law enforcement by facilitating such coordination. Good channels of communication between federal investigators and an incident response firm will avoid duplication of effort, minimize disruption of the victim organization's operations, and expedite the investigation.

Step 2: Implement Measures to Minimize Continuing Damage

Understandably, an organization that has suffered a cyber incident typically will

immediately institute measures to prevent any further damage. Such steps may include rerouting network traffic, filtering or blocking a distributed denial-of-service attack, or isolating all or parts of the compromised network. In the case of an intrusion, a system administrator may elect either to block further unauthorized access to the system or to allow it to continue to help identify the source of the attack and/or the scope of the compromise.

An organization that has prepared for a cyber incident by backing up its data may elect to abandon data stored on a compromised network and restore the network to a prior state using saved data. However, before doing so, it should confirm that the backed-up data is not also compromised. Failure to confirm the integrity of the backed-up data may result in re-infection.

If a victim organization obtains information regarding the location of exfiltrated data or the apparent origin of a cyber attack, it has several options. First and foremost, we strongly recommend that it share this information with law enforcement *immediately*. Federal investigators may be able to secure the stolen data using its legal authority. However, the organization may also choose to contact the system administrator of the network on which its stolen data resides or from which the attack originates. Doing so may stop the attack, assist in regaining control of stolen data, or help determine the true origin of the malicious activity. A victim organization may also choose to blunt the damage of an ongoing intrusion or attack by "null routing"[27] malicious traffic, closing the ports being used by the intruder to gain access to the network, or otherwise altering the configuration of a network to thwart the malicious activity. Wherever possible, the organization should coordinate its actions with law enforcement to avoid taking measures that unnecessarily taint evidence or limit investigative options.

The victim organization should keep detailed records of whatever steps it takes to mitigate the damage and keep track of any incurred costs. Such information may be used later to establish criminal violations, recover remediation costs from the perpetrator, or determine the perpetrator's sentence if he or she is later prosecuted and convicted.

Step 3: Record and Collect Information

1. *Keep Logs, Notes, Records, and Data*

A victim organization should take immediate steps to preserve existing log files. *If a victim organization has not enabled logging on an affected system, it should do so immediately*. It should also consider increasing the default size of log files on its servers to prevent vital information from

[27] A null route directs the system to drop network communications that are destined for a specified IP address on the network, so a system will no longer send any response to the originating IP address. This means the system will continue to receive data from the attackers but will no longer respond to them.

being overwritten. Computer file logs that may assist in analyzing or investigating an incident come in a variety of forms, including event logs, active directory logs, and browser history logs. Forensic examinations are based on artifacts found in various repositories (e.g., registry hives, prefetch data, and scheduled tasks). Preventing as much of that data as possible from being erased or overwritten can be crucial to performing a post-incident analysis or investigation.

A victim organization should document or record any ongoing suspicious network activity. A victim organization may use a "sniffer" or other network-monitoring tool to record communications between the intruder and any of its targeted servers during an attack. Such monitoring implicates federal surveillance statutes such as the Wiretap Act but is typically lawful when conducted in accordance with CISA's cybersecurity monitoring provision[28] or a statutory exception, such as consent[29] or the rights or property exception.[30] Many organizations consult with their legal counsel beforehand to make sure such monitoring is conducted lawfully and consistent with the organization's employment agreements and privacy policies.

In addition, a victim organization should direct its personnel and personnel from incident response firms to keep a contemporaneous written record of all steps undertaken. Documenting actions while responding to the incident or shortly thereafter will minimize the need to rely solely on the recollections of personnel to reconstruct the order of events. As the investigation progresses, information that was collected by the organization during incident response may have unanticipated significance.

The types of information that a victim organization should record and retain include:

- a description of all incident-related events, including dates and times;
- information about incident-related phone calls, emails, and other contacts;
- the identity of persons working on tasks related to the intrusion, including a description of their role or responsibilities, the amount of time spent, and the approximate hourly rate for those persons' work;
- the identity of the systems, accounts, services, data, and networks affected by the incident and a description of how these network components were affected;
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the organization and in criminal prosecutions;

[28] 6 U.S.C. § 1503(a).
[29] 18 U.S.C. §§ 2511(2)(c)-(d).
[30] 18 U.S.C. § 2511(2)(a)(ii).

- information regarding network topology;
- the type and version of software being run on all affected systems; and
- any peculiarities in the organization's network architecture, such as proprietary hardware or software.

Ideally, as few employees as practicable should be assigned the responsibility of retaining custody of such information. This will help to ensure that records are properly preserved, can be produced later, and are available as evidence. Proper handling of this information can be useful in rebutting claims in subsequent legal proceedings (whether criminal or civil) that electronic evidence has been tampered with or altered.

2. *Image the Affected Computers and Check Backups*

A victim organization, or the incident response firm it hires, may make a "forensic image" of the affected computers to preserve a record of a server at the time of the incident for later analysis and potentially for use as evidence at trial. A "forensic image" is an exact, bit-for-bit copy of data on an electronic device. An image provides a perfect "snapshot" of the system at the time the image was created, including deleted files, slack (apparently empty) storage space, system files, and executable files. It is important to create an image using forensically sound procedures; otherwise, there is a risk of altering the system in a manner that compromises its analytic or evidentiary value.

Once a victim organization makes copies, it should write-protect the media to help ensure that it is not altered. A victim organization should also restrict access to the preserved media. Doing so and documenting who has maintained possession of the media (i.e., recording the "chain of custody") will help later establish the authenticity of the copy. It may also protect it from malicious insiders. Properly trained personnel will know the generally accepted methods of generating and preserving copies of data.

The victim organization should also locate any regularly generated backups, which may assist in identifying any changes an intruder made to the systems. Such backups should be isolated from the affected systems to prevent them from being overwritten or altered. If they are later used to restore the system, they should first be checked on isolated computers in case they also turn out to be compromised or infected.

Computer intrusions are commonly only discovered long after the initial intrusion occurred. Consequently, an organization should be prepared to retrieve backups that are quite old to find one that pre-dates the intrusion.

Step 4: Notify

1. *People Within the Organization*

The incident response plan should identify the appropriate points of contact (POCs) within the organization who must be notified of the cyber incident. POCs will typically include senior management, incident response firms, information technology and physical security coordinators, communications or public affairs personnel, and inside and outside legal counsel. POCs should be promptly alerted *in the manner described in the incident response plan*. Adhering to the agreed upon means of contacting POCs will help prevent social engineering attacks designed to extract sensitive information from unsuspecting personnel. Once contacted, POCs should be apprised of any information needed to inform immediate incident management decisions.

In addition to identifying POCs, the incident response plan should describe the circumstances under which POCs should be contacted. Minor cyber incidents may be handled without immediately notifying all POCs; if so, the plan should describe those incidents and the subset of POCs who should be contacted. An incident response plan that sets triggers or thresholds for notification can help avoid over-notification, which can undermine the effectiveness of the plan.

2. *Federal Responders*

A victim of a cyber incident can receive assistance from federal agencies that are poised to investigate the incident, help mitigate its consequences, and help prevent future incidents. Federal law enforcement has highly trained investigators who specialize in responding to cyber incidents to identify, apprehend, and disrupt the activities of criminals who cause cyber incidents and to prevent harm to other potential victims. In addition to law enforcement, other federal responders like DHS provide technical assistance to protect assets, mitigate vulnerabilities, and can offer on-scene response personnel to aid in incident recovery.[31]

a. Contacting Law Enforcement

If an organization suspects a cyber incident was the result of criminal activity, it should contact law enforcement as soon as practicable. Historically, some companies have been reluctant to contact law enforcement following a cyber incident fearing that a criminal investigation could disrupt their business or cause unwarranted reputational harm. Such fears are misplaced. Federal

[31] Annex D of the NATIONAL CYBER INCIDENT RESPONSE PLAN (2016), available at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf, provides detailed instructions for reporting a cyber incident to the federal government.

investigators are committed to minimizing the harm and inconvenience that might result from reporting a cyber incident. Recognizing that a data breach or cyber attack can be a harrowing event, investigators take care not to further victimize an organization that has suffered a breach or attack.

The FBI and Secret Service strive to conduct cyber investigations that cause as little disruption as possible to a victim organization's normal operations. They also recognize the need to work cooperatively and discreetly with victims. Whenever possible, they will use investigative techniques that avoid computer downtime or displacement of an organization's employees. When it is necessary to use a disruptive investigative technique, the FBI and Secret Service will do so with the goal of minimizing the duration and scope of any disturbance and will work alongside the victim organization to ensure that any concerns are fully addressed.

The FBI and Secret Service also will work with victim companies to avoid unwarranted disclosure of information. They will generally coordinate public statements concerning the incident with victim companies to ensure that harmful or sensitive information is not needlessly disclosed. Victim companies should likewise consider sharing press releases regarding a cyber incident with investigators before issuing them to avoid releasing information that might impede the ongoing investigation.

i. The Benefits of Contacting Law Enforcement

Contacting law enforcement may also prove beneficial to a victim organization. Law enforcement can use tools and legal authorities that are unavailable to private entities to identify and apprehend whoever is responsible for a cyber incident. Federal investigators can obtain data to trace an intrusion or attack to its source using search warrants, court orders, and subpoenas. U.S. law enforcement also frequently enlists the assistance of international law enforcement partners to obtain evidence and conduct investigations in other countries. These tools and relationships can greatly increase the odds of successfully apprehending an intruder or attacker and securing exfiltrated data. An arrest can also prevent further damage to the victim organization and deter other would-be cyber criminals.

Law enforcement also has incident response services it can deploy in connection with major cyber incidents. The FBI's Cyber Task Forces located in each of its 56 field offices across the country deliver investigative response services through the FBI's Cyber Action Team (CAT), which consists of a cadre of highly trained and experienced FBI special agents and computer scientists capable of deploying globally in response to particularly sophisticated cyber incidents. The FBI is also equipped to collect and analyze malware and to provide programs and resources that allow companies to receive intelligence on cyber threats affecting their industries.

Reporting a data breach to law enforcement may also affect data breach notification requirements. As of August 2018, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed data breach reporting laws requiring companies to notify customers whose data has been compromised or to report breaches to state agencies. However, many data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice will impede an investigation. Some state laws also allow a victim company to forego notification altogether if the victim company consults with law enforcement and thereafter determines that the breach will not likely result in harm to the individuals whose personal information has been taken or accessed.

Reporting a cyber incident to law enforcement may have additional benefits for organizations in regulated industries. Regulatory agencies will sometimes inquire about the cause of a data breach or other cyber incident. The FTC has affirmed that it views companies that report data breaches and cyber incidents to law enforcement and cooperate with the subsequent investigation more favorably than those that do not.[32] Upon request of the company, the Department of Justice is also willing to inform regulatory agencies of any cooperation that a company facing a regulatory inquiry has furnished to the government.

ii. Law Enforcement and Information Sharing During a Cyber Incident

The enactment of CISA has made cooperating with law enforcement simpler by addressing common concerns about legal impediments to sharing information with the government. While CISA was not enacted to address law enforcement's evidence-gathering needs, its information-sharing provision authorizes private entities to share specific types of cyber threat information with any federal agency, including law enforcement agencies. Specifically, CISA authorizes non-federal entities to voluntarily share "cyber threat indicators"[33] and "defensive measures"[34] with law enforcement for a cybersecurity purpose,[35] notwithstanding any other provision of law.[36] Such authorized sharing can be particularly helpful during a cyber incident.

CISA's authorization to share information with the federal government is bolstered by liability protection that covers cyber threat indicators and defensive measures that a private entity

---

[32] Mark Eichorn, *If the FTC Comes to Call*, FTC: BUS. BLOG (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call.
[33] A "cyber threat indicator" is defined by 6 U.S.C. § 1501(6).
[34] A "defensive measure" is defined by 6 U.S.C. § 1501(7).
[35] A "cybersecurity purpose" is defined by 6 U.S.C. § 1501 (4).
[36] *See* 6 U.S.C. § 1503(c).

shares with other private entities and with DHS, as provided for by CISA.[37] CISA's explicit liability protection also extends to communications between non-federal and federal entities—including law enforcement agencies—about cyber threat indicators and defensive measures that were previously shared with DHS pursuant to CISA and subsequently shared by a non-federal entity with another agency to describe a cybersecurity threat or develop a defensive measure.[38]

Organizations that report incidents or other information to law enforcement receive certain legal protections for doing so. Law enforcement treats information collected during a criminal investigation as sensitive information that is safeguarded from unwarranted or unnecessary disclosure. In addition, the Freedom of Information Act[39] (FOIA) exempts certain records or information gathered for law enforcement purposes from disclosure. CISA also affords protection from state and federal disclosure laws when cyber threat indicators are shared with the FBI, Secret Service, or another federal entity consistent with CISA.[40] It is also noteworthy that law enforcement does not routinely disclose evidence it gathers during its cyber investigations to regulators.

b. The Department of Homeland Security

DHS has components dedicated to cybersecurity that not only collect and report on cyber incidents, phishing, malware, and other vulnerabilities, but also provide certain non-law enforcement incident response services, including technical assistance. The NCCIC serves as an around-the-clock centralized location for cybersecurity information sharing and non-investigative asset response coordination.[41] By contacting the NCCIC, a victim organization can both share and receive information about an ongoing incident that may prove beneficial to both the victim organization and the government.

3. *Regulators*

Some private sector organizations are regulated by state and federal regulatory agencies and may be required to report a data breach or other cyber incident. While guidance to such organizations concerning how to notify regulators is beyond the scope of this document, a cyber

---

[37] *See* 6 U.S.C. §§ 1503(c), 1504(c)(1)(B), 1505(b)(2).
[38] *See* 6 U.S.C. § 1504(c)(1)(B)(i).
[39] 5 U.S.C. § 552, as amended by Pub. L. No. 104-231, 110 Stat. 3048.
[40] Relevant FOIA exemptions include Exemption 4 (which provides for non-disclosure of confidential commercial information) and Exemption 7 (which provides for non-disclosure of certain information compiled for law enforcement purposes). *See* DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT (2009), https://www.justice.gov/oip/doj-guide-freedom-information-act-0. Further, cyber threat indicators and defensive measures shared in accordance with CISA with the federal government or with or by a State, tribal, or local government is exempt from FOIA and similar disclosure laws. *See* 6 U.S.C. §§ 1504(d)(3), 1503(d)(4)(B).
[41] *See* Presidential Policy Directive – United States Cyber Incident Coordination (PPD-41), 2016 WL 3996354 (Jul. 26, 2016).

incident response plan should take into account whether a victim organization may need to notify regulators and how best to do so. Organizations should consult with counsel to ascertain their obligations under state data breach notification laws and similar applicable regulations.

It is worth noting that the Department of Justice does not have a regulatory role in regard to data breaches or cyber incidents. Accordingly, reporting a cyber incident to the Department or to federal criminal investigators will not lead to regulatory enforcement action by the Department for the incident.

4. *Other Potential Victims*

If a victim organization or the incident response firm it hires uncovers evidence of additional victims while responding to a cyber incident, it should consider promptly notifying the other presumed victims. A notifying organization may choose to contact other victims directly; however, there are benefits to allowing law enforcement to contact other victims. Doing so may insulate the notifying victim from unwanted exposure and allow law enforcement to conduct further investigation.

Similarly, if a forensic examination reveals an unreported software or hardware vulnerability, the victim organization should notify law enforcement, the relevant vendor, or a public or private entity that receives and disseminates vulnerability disclosures, such as the NCCIC. Such notifications may prevent others from being victimized and afford potential victims the opportunity to protect themselves. The notifying organization may also benefit because other victims may be able to provide helpful information from their own experience managing the same cyber incident, including information regarding the perpetrator's methods, a timeline of events, or effective mitigation techniques that may thwart the intruder.

III. What Not to Do Following a Cyber Incident

A. Use a Compromised System to Communicate

The victim organization should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about mitigation strategies or how it intends to respond to the incident. Otherwise, it risks informing the perpetrator of its plans, which may allow him or her to circumvent or disrupt mitigation efforts.

To avoid becoming the victim of a "social engineering" attack (i.e., use of a ruse or guile to lure a target into taking action that will compromise the security of the system or data), employees of the victim organization should not disclose incident-specific information to anyone

inquiring about an incident without first verifying their identity. A victim should keep track of any odd or suspicious inquiries concerning the incident and share them with law enforcement.

B. Hack into or Damage Another Network

A victim of an intrusion or data breach may conduct an investigation that uncovers information linking a computer that is not controlled by the victim to the incident. For instance, a victim organization's server logs may reveal the Internet Protocol (IP) address of a computer that suspiciously accessed the victim's network or downloaded data.[42] Such information may provide valuable information that government authorities can use to investigate the incident.

However, a victim organization should not unilaterally respond to a cyber incident by accessing, modifying, or damaging a computer it does not own or operate, even if the computer appears to have been involved in an attack or intrusion. Regardless of the victim's motive, doing so may violate federal law[43] and possibly also the laws of many states[44] and foreign countries, if the accessed computer is located abroad.[45] A violation of those laws could result in civil and criminal liability.

Taking retaliatory action may be ill-advised for other reasons too. For instance, it may cause unintended harm. Many intrusions and attacks are launched from systems a perpetrator has compromised and used as an intermediary to relay his or her communications. This tactic is commonly adopted by perpetrators to conceal their identities by interposing systems between them and their victims. But it also means that efforts to access or attack a computer linked to the incident—sometimes called "hacking back"—could wind up targeting an unwitting, innocent victim whose system is being exploited by the perpetrator. Accessing data on an intermediary system may also intrude upon the privacy of third parties whose data is stored there.

A private party who accesses another computer in response to an intrusion may also unknowingly interfering with a law enforcement investigation. A perpetrator targeted by a private party may change tactics or modify operations if he or she detects a hack back attempt; such a deviation in behavior can undermine an ongoing law enforcement investigation that is tracking the perpetrator. Furthermore, a perpetrator who detects a hack back attempt may choose to retaliate, causing further damage to the victim.

---

[42] An Internet Protocol address is a number assigned to every device connected to a network. It is used to route Internet communications between a sender and a recipient.

[43] *See* 18 U.S.C. § 1030.

[44] A summary of state computer crime statutes is available at http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[45] A summary of the computer crime statutes worldwide is available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

Instead of taking unilateral action, a victim should promptly contact and begin collaborating with law enforcement by providing any information that might help trace the perpetrator. Federal investigators possess legal authority that can help identify the perpetrators and secure stolen data, even if either (or both) is located abroad. Law enforcement is prepared to use such authority to assist victims and advance an investigation.

IV. What to do After a Cyber Incident Appears to be Resolved

Even after a cyber incident appears to be under control, a victim organization should remain vigilant. Many intruders attempt to regain access to previously compromised systems. It is possible that, despite its best efforts, a company that has addressed known security vulnerabilities and taken all reasonable steps to expel an intruder has not discovered all of the intruder's means of gaining entry to the network. A victim organization should continue to monitor its system for anomalous activity and be vigilant for new signs of re-infection and compromise.

Once the victim organization has recovered from the attack or intrusion, it should adopt measures to prevent similar attacks in the future, such as addressing shortcomings in its security practices, acquiring resources to better secure its systems, and fortifying relationships with law enforcement and other key response organizations. It should conduct a post-incident review of the organization's performance and assess the strengths and weaknesses of its execution of its incident response plan. Part of the assessment should include ascertaining whether the organization followed each of the steps outlined above and, if not, why not. The organization should note and discuss deficiencies and gaps in its response and take remedial steps as needed.

Cyber Incident Preparedness Checklist		
Before a Cyber Attack or Intrusion		
Educate the organization's senior management about cyber threats and risk management.		
Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.		
Identify mission critical data and assets (*i.e.*, your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.		
Create an actionable incident response plan.	Test the plan by conducting exercises.	
	Keep the plan up-to-date to reflect changes in personnel and structure.	
Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident.		
Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable).		
Institute basic cybersecurity procedures, such as a patch management program.		
Have procedures in place that will permit lawful network monitoring.		
Ensure legal counsel is familiar with legal issues associated with cyber incidents.		
Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan.		
During a Cyber Attack or Intrusion		
Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.		
Minimize continuing damage consistent with your cyber incident response plan.		
Collect and preserve data related to the incident by --	"Imaging" the network.	
	Keeping all logs, notes, and other records.	
	Keeping records of ongoing attacks.	
Consistent with your incident response plan, notify --	Appropriate management and personnel within the victim organization.	
	Law enforcement.	
	Department of Homeland Security.	
	Other possible victims.	
Do not --	Use compromised systems to communicate.	
	"Hack back" or intrude upon another network.	
After Recovering from a Cyber Attack or Intrusion		
Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.		
Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.		