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

Version 1.0 (April 2015)

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

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may benefit from it.

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

Having well-established plans and procedures in place for managing and responding to a cyber intrusion or attack is a critical first step toward preparing an organization to weather a cyber incident. Such pre-planning can help victim organizations limit damage to their computer networks, minimize work stoppages, and maximize the ability of law enforcement to locate and apprehend perpetrators. Organizations should take the precautions outlined below before learning of a cyber incident affecting their networks.

A. Identify Your "Crown Jewels"

Different organizations have different mission critical needs. For some organizations, even a short-term disruption in their ability to send or receive email will have a devastating impact on their operations; others are able to rely on other means of communication to transact

business, but they may suffer significant harm if certain intellectual property is stolen. For others still, the ability to guarantee the integrity and security of the data they store and process, such as customer information, is vital to their continued operation.

The expense and resources required to protect a whole enterprise may force an organization to prioritize its efforts and may shape its incident response planning. Before formulating a cyber incident response plan, an organization should first determine which of their data, assets, and services warrants the most protection. Ensuring that protection of an organization's "crown jewels" is appropriately prioritized is an important first step to preventing a cyber intrusion or attack from causing catastrophic harm. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) provides excellent guidance on risk management planning and policies and merits consideration.[1]

B. Have an Actionable Plan in Place Before an Intrusion Occurs

Organizations should have a plan in place for handling computer intrusions before an intrusion occurs. During an intrusion, an organization's management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the damage and the potential source of the threat. A cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond.

The plan should be "actionable." It should provide specific, concrete procedures to follow in the event of a cyber incident. At a minimum, the procedures should address:

- Who has lead responsibility for different elements of an organization's cyber incident response, from decisions about public communications, to information technology access, to implementation of security measures, to resolving legal questions;
- How to contact critical personnel at any time, day or night;
- How to proceed if critical personnel is unreachable and who will serve as back-up;
- What mission critical data, networks, or services should be prioritized for the greatest protection;
- How to preserve data related to the intrusion in a forensically sound manner;
- What criteria will be used to ascertain whether data owners, customers, or partner companies should be notified if their data or data affecting their networks is stolen; and
- Procedures for notifying law enforcement and/or computer incident-reporting organization.

[1] The NIST Cybersecurity Framework is available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

All personnel who have computer security responsibilities should have access to and familiarity with the plan, particularly anyone who will play a role in making technical, operational, or managerial decisions during an incident. It is important for an organization to institute rules that will ensure its personnel have and maintain familiarity with its incident response plan. For instance, the procedures for responding to a cyber incident under an incident response plan can be integrated into regular personnel training. The plan may also be ingrained through regularly conducted exercises to ensure that it is up-to-date. Such exercises should be designed to verify that necessary lines of communication exist, that decision-making roles and responsibilities are well understood, and that any technology that may be needed during an actual incident is available and likely to be effective. Deficiencies and gaps identified during an exercise should be noted for speedy resolution.

Incident response plans may differ depending upon an organization's size, structure, and nature of its business. Similarly, decision-making under a particular incident response plan may differ depending upon the nature of a cyber incident. In any event, institutionalized familiarity with the organization's framework for addressing a cyber incident will expedite response time and save critical minutes during an incident.

C. Have Appropriate Technology and Services in Place Before An Intrusion Occurs

Organizations should already have in place or have ready access to the technology and services that they will need to respond to a cyber incident. Such equipment may include off-site data back-up, intrusion detection capabilities, data loss prevention technologies, and devices for traffic filtering or scrubbing. An organization's computer servers should also be configured to conduct the logging necessary to identify a network security incident and to perform routine back-ups of important information. The requisite technology should already be installed, tested, and ready to deploy. Any required supporting services should either be acquired beforehand or be identified and ready for acquisition.

D. Have Appropriate Authorization in Place to Permit Network Monitoring

Real-time monitoring of an organization's *own* network is typically lawful if prior consent for such monitoring is obtained from network users. For this reason, before an incident takes place, an organization should adopt the mechanisms necessary for obtaining user consent to monitoring users' communications so it can detect and respond to a cyber incident. One means of accomplishing this is through network warnings or "banners" that greet users who log onto a network and inform them of how the organization will collect, store, and use their communications. A banner can also be installed on the ports through which an intruder is likely to access the organization's system.

A banner, however, is not the only means of obtaining legally valid consent. Computer user agreements, workplace policies, and personnel training may also be used to obtain legally sufficient user consent to monitoring. Organizations should obtain written acknowledgement from their personnel of having signed such agreements or received such training. Doing so will provide an organization with ready proof that they have met legal requirements for conducting network monitoring.

Any means of obtaining legally sufficient consent should notify users that their use of the system constitutes consent to the interception of their communications and that the results of such monitoring may be disclosed to others, including law enforcement.[2] If an organization is a government entity (*e.g.*, a federal, state, or local agency or a state university) or a private entity acting as an instrument or agent of the government, its actions may implicate the Fourth Amendment. Consequently, any notice on the system of such an entity or organization should also inform users of their diminished expectation of privacy for communications on the network.

E. Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident

Cyber incidents can raise unique legal questions. An organization faced with decisions about how it interacts with government agents, the types of preventative technologies it can lawfully use, its obligation to report the loss of customer information, and its potential liability for taking specific remedial measures (or failing to do so) will benefit from obtaining legal guidance from attorneys who are conversant with technology and knowledgeable about relevant laws (*e.g.*, the Computer Fraud and Abuse Act (18 U.S.C. § 1030), electronic surveillance, and communications privacy laws). Legal counsel that is accustomed to addressing these types of issues that are often associated with cyber incidents will be better prepared to provide a victim organization with timely, accurate advice.

Many private organizations retain outside counsel who specialize in legal questions associated with data breaches while others find such cyber issues are common enough that they have their own cyber-savvy attorneys on staff in their General Counsel's offices. Having ready access to advice from lawyers well acquainted with cyber incident response can speed an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing.

---

[2] More guidance on banners, including a model banners, 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 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed. 2009), available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; and 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. Off. Legal Counsel 1 (2009), available at http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf.

F. Ensure Organization Policies Align with Your Cyber Incident Response Plan

Some preventative and preparatory measures related to incident planning may need to be implemented outside the context of preparing a cyber incident response plan. For instance, an organization should review its personnel and human resource policies to ensure they will reasonably minimize the risk of cyber incidents, including from "insider threats." Proper personnel and information technology (IT) policies may help prevent a cyber incident in the first place. For instance, a practice of promptly revoking the network credentials of terminated employees—particularly system administrators and information technology staff—may prevent a subsequent cyber incident from occurring. Furthermore, reasonable access controls on networks may reduce the risk of harmful computer misuse.

G. Engage with Law Enforcement Before an Incident

Organizations should attempt to establish a relationship with their local federal law enforcement offices long before they suffer a cyber incident. Having a point-of-contact and a pre-existing relationship with law enforcement will facilitate any subsequent interaction that may occur if an organization needs to enlist law enforcement's assistance. It will also help establish the trusted relationship that cultivates bi-directional information sharing that is beneficial both to potential victim organizations and to law enforcement. 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. Both agencies conduct regular outreach to private companies and other organizations likely to be targeted for intrusions and attacks. Such outreach occurs mostly through the FBI's Infragard chapters and Cyber Task Forces in each of the FBI's 56 field offices, and through the U.S. Secret Service's Electronic Crimes Task Forces.

H. Establish Relationships with Cyber Information Sharing Organizations

Defending a network at all times from every cyber threat is a daunting task. Access to information about new or commonly exploited vulnerabilities can assist an organization prioritize its security measures. Information sharing organizations for every sector of the critical infrastructure exist to provide such information. Information Sharing and Analysis Centers (ISACs) have been created in each sector of the critical infrastructure and for key resources. They produce analysis of cyber threat information that is shared within the relevant sector, with other sectors, and with the government. Depending upon the sector, they may also provide other cybersecurity services. The government has also encouraged the creation of new information sharing entities called Information Sharing and Analysis Organizations (ISAOs) to accommodate organizations that do not fit within an established sector of the critical infrastructure or that have

unique needs.[3] ISAOs are intended to provide such organizations with the same benefits of obtaining cyber threat information and other supporting services that are provided by an ISAC.

II. Responding to a Computer Intrusion: Executing Your Incident Response Plan

An organization can fall victim to a cyber intrusion or attack even after taking reasonable precautions. Consequently, having a vetted, actionable cyber incident response plan is critical. A robust incident response plan does more than provide procedures for handling an incident; it also provides guidance on how a victim organization can continue to operate while managing an incident and how to work with law enforcement and/or incident response firms as an investigation is conducted.[4] An organization's incident response plan should, at a minimum, give serious consideration to all of the steps outlined below.

A. Step 1: Make an Initial Assessment

During a cyber incident, a victim organization should immediately make an assessment of the nature and scope of the incident. In particular, it is important at the outset to determine whether the incident is a malicious act or a technological glitch. The nature of the incident will determine the type of assistance an organization will need to address the incident and the type of damage and remedial efforts that may be required.

Having appropriate network logging capabilities enabled can be critical to identifying the cause of a cyber incident. Using log information, a system administrator should 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 were sent (if information was exfiltrated); and
- The identity of any other victim organizations, if such data is apparent in logged data.

[3] *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.

[4] Often in the case of data breaches, organizations may learn that they have been the victim of an intrusion from a third party. For instance, law enforcement may discover evidence; while conducting a data breach investigation that other organizations have also been breached, or a cybersecurity company's forensic analysis of a customer's network following a breach may uncover evidence of other victims. Organizations should be prepared to respond to such receiving such notice.

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

- Which users are currently logged on;
- What the current connections to the computer systems are;
- Which processes are running; and
- All open ports and their associated services and applications.

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

Evidence that an intrusion or other criminal incident has occurred will typically include logging or file creation data indicating that someone improperly accessed, created, modified, deleted, or copied files or logs; changed system settings; or added or altered user accounts or permissions. In addition, an intruder may have stored "hacker tools" or data from another intrusion on your network. In the case of a root-level intrusion,[5] victims should be alert for signs that the intruder gained access to multiple areas of the network. The victim organization should take care to ensure that its actions do not unintentionally or unnecessarily modify stored data in a way that could hinder incident response or subsequent criminal investigation. In particular, potentially relevant files should not be deleted; if at all possible, avoid modifying data or at least keep track of how and when information was modified.

B. Step 2: Implement Measures to Minimize Continuing Damage

After an organization has assessed the nature and scope of the incident and determined it to be an intentional cyber intrusion or attack rather than a technical glitch, it may need to take steps to stop ongoing damage caused by the perpetrator. Such steps may include rerouting network traffic, filtering or blocking a distributed denial-of-service attack,[6] or isolating all or parts of the compromised network. In the case of an intrusion, a system administrator may decide either to block further illegal access or to watch the illegal activity to identify the source of the attack and/or learn the scope of the compromise.

If proper preparations were made, an organization will have an existing back-up copy of critical data and may elect to abandon the network in its current state and to restore it to a prior

[5] 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.

state. If an organization elects to restore a back-up version of its data, it should first make sure that the back-up is not compromised as well.

Where a victim organization obtains information regarding the location of exfiltrated data or the apparent origin of a cyber attack, it may choose to contact the system administrator of that network. Doing so may stop the attack, assist in regaining possession 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"[7] 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.

The victim organization should keep detailed records of whatever steps are taken to mitigate the damage and should keep stock of any associated costs incurred. Such information may be important for recovering damages from responsible parties and for any subsequent criminal investigation.

C. Step 3: Record and Collect Information

1. *Image the Affected Computer(s)*

Ideally, a victim organization will immediately make a "forensic image" of the affected computers, which will preserve a record of the system at the time of the incident for later analysis and potentially for use as evidence at trial.[8] This may require the assistance of law enforcement or professional incident response experts. In addition, the victim organization should locate any previously generated backups, which may assist in identifying any changes an intruder made to the network. New or sanitized media should be used to store copies of any data that is retrieved and stored. Once the victim organization makes such copies, it should write-protect the media to safeguard it from alteration. The victim organization should also restrict access to this media to maintain the integrity of the copy's authenticity, safeguard it from unidentified malicious insiders, and establish a chain of custody. These steps will enhance the value of any backups as evidence in any later criminal investigations and prosecutions, internal

---

[6] A Distributed Denial of Service (DDOS) attack involves the orchestrated transmission of communications engineered to overwhelm another network's connection to the Internet to impair or disrupt that network's ability to send or receive communications. DDOS attacks are usually launched by a large number of computers infected by malware that permits their actions to be centrally controlled.

[7] A null route directs the system to drop network communications that are destined for 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 no longer respond to them.

[8] A "forensic image" is an exact, sector-by-sector copy of a hard disk. Software capable of creating such copies of hard drives preserve deleted files, slack space, system files, and executable files and can be critical for later analysis of an incident.

investigations, or civil law suits.

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

The victim organization should take immediate steps to preserve relevant existing logs. In addition, the victim organization should direct personnel participating in the incident response to keep an ongoing, written record of all steps undertaken. If this is done while responding to the incident or shortly thereafter, personnel can minimize the need to rely on their memories or the memories of others to reconstruct the order of events. As the investigation progresses, information that was collected by the organization contemporaneous to the intrusion may take on unanticipated significance.

The types of information that the victim organization should 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, the amount of time spent, and the approximate hourly rate for those persons' work;
- 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 cases;
- information regarding network topology;
- the type and version of software being run on the network; and
- any peculiarities in the organization's network architecture, such as proprietary hardware or software.

Ideally, a single, designated employee will retain custody of all such records. This will help to ensure that records are properly preserved and can be produced later on. Proper handling of this information is often useful in rebutting claims in subsequent legal proceedings (whether criminal or civil) that electronic evidence has been tampered with or altered.

3. Records Related to Continuing Attacks

When an incident is ongoing (*e.g.*, during a DDOS attack, as a worm is propagating through the network, or while an intruder is exfiltrating data), the victim organization should record any continuing activity. *If a victim organization has not enabled logging on an affected*

server, it should do so immediately. It should also consider increasing the default size of log files on its servers to prevent losing data. A victim organization may also be able to use a "sniffer" or other network-monitoring device to record communications between the intruder and any of its targeted servers. Such monitoring, which implicates the Wiretap Act (18 U.S.C. §§ 2510 et seq.) is typically lawful, provided it is done to protect the organization's rights or property or system users have actually or impliedly consented to such monitoring. An organization should consult with its legal counsel to make sure such monitoring is conducted lawfully and consistent with the organization's employment agreements and privacy policies.

D. Step 4: Notify[9]

1. *People Within the Organization*

Managers and other personnel within the organization should be notified about the incident as provided for in the incident response plan and should be given the results of any preliminary analysis. Relevant personnel may include senior management, IT and physical security coordinators, communications or public affairs personnel, and legal counsel. The incident response plan should set out individual points-of-contact within the organization and the circumstances in which they should be contacted.

2. Law Enforcement

If an organization suspects at any point during its assessment or response that the incident constitutes criminal activity, it should contact law enforcement immediately. Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harboring such concerns should not hesitate to contact law enforcement.

The FBI and U.S. Secret Service place a priority on conducting cyber investigations that cause as little disruption as possible to a victim organization's normal operations and recognize the need to work cooperatively and discreetly with victim companies. They will use investigative measures that avoid computer downtime or displacement of a company's employees. When using an indispensable investigative measures likely to inconvenience a victim organization, they will do so with the objective of minimizing the duration and scope of any disruption.

The FBI and U.S. Secret Service will also conduct their investigations with discretion and

[9] Some private organizations are regulated by the federal government and may be subject to rules requiring notification if a data breach or other cyber incident occurs. While guidance to such organizations for notifying regulators is beyond the scope of this document, a cyber incident response plan should take into account whether a victim organization may need also to notify regulators and how best to do so.

work with a victim company to avoid unwarranted disclosure of information. They will attempt to coordinate statements to the news media concerning the incident with a victim company to ensure that information harmful to a company's interests is not needlessly disclosed. Victim companies should likewise consider sharing press releases regarding a cyber incident with investigative agents before issuing them to avoid releasing information that might damage the ongoing investigation.

Contacting law enforcement may also prove beneficial to a victim organization. Law enforcement may be able to use legal authorities and tools that are unavailable to non-governmental entities[10] and to enlist the assistance of international law enforcement partners to locate stolen data or identify the perpetrator. These tools and relationships can greatly increase the odds of successfully apprehending an intruder or attacker and securing lost data. In addition, a cyber criminal who is successfully prosecuted will be prevented from causing further damage to the victim company or to others, and other would-be cyber criminals may be deterred by such a conviction.

In addition, as of January 2015, at least forty-seven states have passed database breach notification laws requiring companies to notify customers whose data is compromised by an intrusion; however, many data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice would impede an investigation. State laws also may allow a victim company to forgo providing notice 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 acquired and accessed. Organizations should consult with counsel to determine their obligations under state data breach notification laws. It is also noteworthy that companies from regulated industries that cooperate with law enforcement may be viewed more favorably by regulators looking into a data breach.

3. The Department of Homeland Security

The Department of Homeland Security has components dedicated to cybersecurity that not only collect and report on cyber incidents, phishing, malware, and other vulnerabilities, but also provide certain incident response services. The National Cybersecurity & Communications Integration Center (NCCIC) serves as a 24x7 centralized location for cybersecurity information sharing, incident response, and incident coordination. 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. A victim organization may also

[10] For instance, data that are necessary to trace an intrusion or attack to its source may not be obtainable without use of legal process (e.g., a search warrant, court order, or subpoena) that may be unavailable to a private party. Furthermore, some potentially useful intrusion detection techniques require law enforcement involvement. For instance, under 18 U.S.C. § 2511(2)(i) a network owner may authorize law enforcement to intercept a computer trespasser's communications on the network owner's computers during an investigation.

obtain technical assistance capable of mitigating an ongoing cyber incident.

4. *Other Potential Victims*

If a victim organization or the private incident response firm it hires uncovers evidence of additional victims while assessing a cyber incident—for example, in the form of another company's data stored on the network—the other potential victims should be promptly notified. While the initial victim can conduct such notification directly, notifying victims through law enforcement may be preferable. It insulates the initial victim from potentially unnecessary exposure and allows law enforcement to conduct further investigation, which may uncover additional victims warranting notification. Similarly, if a forensic examination reveals an unreported software or hardware vulnerability, the victim organization should make immediate notification to law enforcement or the relevant vendor.

Such notifications may prevent further damage by prompting the victims or vendors to take remedial action immediately. The victim organization may also reap benefits, because other victims may be able to provide helpful information gleaned from their own experiences managing the same cyber incident (*e.g.*, 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. Do Not Use the Compromised System to Communicate

The victim organization should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about an incident or to discuss its response to the incident. If the victim organization must use the compromised system to communicate, it should encrypt its communications. To avoid becoming the victim of a "social engineering" attack (*i.e.*, attempts by a perpetrator to convince a target to take an action through use of a ruse or guile that will compromise the security of the system or data), employees of the victim organization should not disclose incident-specific information to unknown communicants inquiring about an incident without first verifying their identity.

B. Do Not Hack Into or Damage Another Network

A victimized organization should not attempt to access, damage, or impair another system that may appear to be involved in the intrusion or attack. Regardless of motive, doing so is likely illegal, under U.S. and some foreign laws, and could result in civil and/or criminal liability. 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.

IV. After a Computer Incident

Even after a cyber incident appears to be under control, remain vigilant. Many intruders return to attempt to regain access to networks they previously compromised. It is possible that, despite best efforts, a company that has addressed known security vulnerabilities and taken all reasonable steps to eject an intruder has nevertheless not eliminated all of the means by which the intruder illicitly accessed the network. Continue to monitor your system for anomalous activity.

Once the victim organization has recovered from the attack or intrusion, it should initiate measures to prevent similar attacks. To do so, it should conduct a post-incident review of the organization's response to the incident and assess the strengths and weaknesses of its performance and 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

- Identify mission critical data and assets (*i.e.*, your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.
- Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.
- Create an actionable incident response plan.
    - Test plan with exercises
    - Keep plan up-to-date to reflect changes in personnel and structure
- Have the technology in place (or ensure that it is easily obtainable) that will be used to address an incident.
- Have procedures in place that will permit lawful network monitoring.
- Have legal counsel that is familiar with legal issues associated with cyber incidents
- Align other policies (*e.g.*, human resources and personnel policies) with your incident response plan.
- Develop proactive relationships with relevant law enforcement agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may require in the event of an incident.

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.
    - "Image" the network
    - Keep all logs, notes, and other records
    - Keep records of ongoing attacks
- Consistent with your incident response plan, notify—
    - Appropriate management and personnel within the victim organization should
    - Law enforcement
    - Other possible victims
    - Department of Homeland Security
- 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.