United States
Secret Service
Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

AN INTRODUCTORY GUIDE

Cyber incidents and data breaches continue to proliferate globally, targeting organizations across all industries and sectors. The worldwide monetary loss to cybercrime is measured in the hundreds of billions. The global cyber threat is a challenge due to the nature of transnational commerce, its interconnected networks and supply chains, and the use of electronic payment systems. This is compounded by the proliferation of increasingly sophisticated tools available to cybercriminals, jurisdictional uncertainty in transnational cases, and lenient attitudes towards cybercrime in some countries. Cybercrime has no borders and no border protection. In 2018, transnational cybercrime investigation cases led by the U.S. Secret Service accounted for $1.9 billion in actual financial losses and $6.8 billion in potential losses averted due to law enforcement action.

A comprehensive and integrated approach to cybersecurity with organized cyber incident response policies is the only sustainable path to achieving continuity in uncertain times. An organization cannot anticipate every disruption or prevent every cyber incident. Even the most advanced tools and methods do not guarantee perfect cybersecurity implementation. Organizations must anticipate an evolving risk environment and be prepared to respond at a moment's notice when a disruption to their business occurs. Accomplishing continuity of operations requires a resilient approach to cybersecurity - an integrated, holistic way to manage security risks, business continuity, disaster recovery, and information technology (IT) operations. To achieve this, a comprehensive plan for incident management and incident response (IR), with regular testing and updating, is crucial.

Criminals maneuver in the anonymity of cyberspace using tradecraft to limit risk from law enforcement. To build on the principle of deterrence, the role of law enforcement in an organization's IR plan is critical to our nation's cybersecurity strategy. It is essential for an organization to develop a trusted relationship with law enforcement and integrate them into the development of a cyber IR plan. This early preparation can facilitate a mutually created framework for restoring business operations to a victim organization while assisting in evidence collection for law enforcement. Preplanning and rehearsing a cyber IR plan helps target the relevant sources of evidence for a criminal investigation, while facilitating speedy restoration of business operations. Engagement with law enforcement before, during, and after a cyber incident will increase opportunities to arrest and prosecute cybercriminals. This collective effort will result in the enhancement of our strategic focus to dissuade criminals from continuing to target your organization. A growth in partnerships between the private sector and law enforcement built on trust and communication will continue to shape cyber resiliency, layer by layer.

The U.S. Secret Service has extensive experience in cyber IR and the subsequent criminal investigations, and we offer this guide outlining basic steps an organization can take before, during, and after a cyber incident. This guide is built upon an in-depth analysis of the methods and tools used to identify, locate and arrest significant cybercriminals, the industry technical framework of the National Institute of Standards and Technology (NIST), and the legal framework of the Department of Justice.

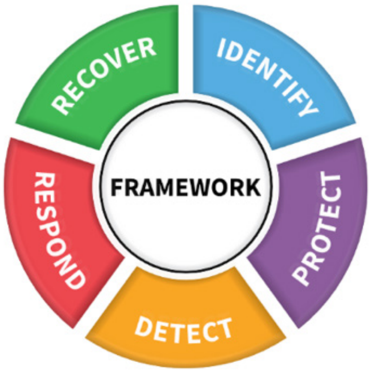
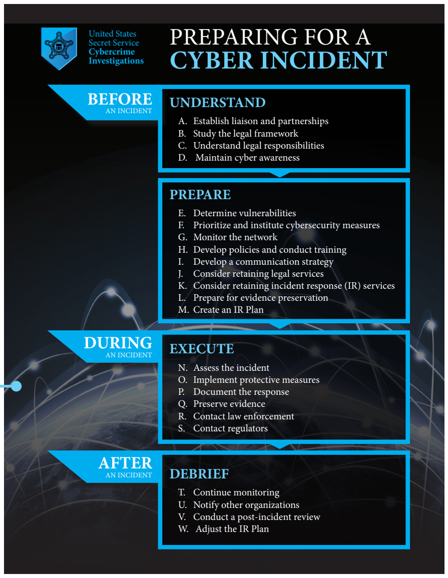


Figure 1: NIST Framework

In 2014, NIST published a Framework for Improving Critical Infrastructure Cybersecurity (Figure 1), with revisions in 2017 and 2018.

In 2015, the Department of Justice published Best Practices for Victim Response and Reporting of Cyber Incidents, with a revision in 2018.

The four sections of this guide (Understand, Prepare, Execute, and Debrief) describe what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations. This guide does not constitute legal advice and is only for reference purposes. The corresponding flowchart (Figure 2) reflects these sections and provides an at-a-glance view of the basic steps described below. The sequence of these steps is not fixed, and will depend on your organization's specific needs.



United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

BEFORE AN INCIDENT

UNDERSTAND

A. Establish liaison and partnerships
B. Study the legal framework
C. Understand legal responsibilities
D. Maintain cyber awareness

PREPARE

E. Determine vulnerabilities
F. Prioritize and institute cybersecurity measures
G. Monitor the network
H. Develop policies and conduct training
I. Develop a communication strategy
J. Consider retaining legal services
K. Consider retaining incident response (IR) services
L. Prepare for evidence preservation
M. Create an IR Plan

DURING AN INCIDENT

EXECUTE

N. Assess the incident
O. Implement protective measures
P. Document the response
Q. Preserve evidence
R. Contact law enforcement
S. Contact regulators

AFTER AN INCIDENT

DEBRIEF

T. Continue monitoring
U. Notify other organizations
V. Conduct a post-incident review
W. Adjust the IR Plan

Figure 2: U.S. Secret Service Cyber Preparedness Chart

UNDERSTAND

A. Establish liaison and partnerships:

Begin by identifying law enforcement agencies responsible for combating cybercrime within your geographic area. Determine what cybersecurity information and resources they have available publically or through partnership initiatives.

The Secret Service operates **Cyber Fraud Task Forces (CFTFs)**. This is a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia. The goals and priorities of the CFTFs are to combat cybercrime through prevention, detection, mitigation, and investigation of cyber incidents. The 40 strategically located CFTFs boast a strong alliance of over 4,000 private sector partners, 2,500 international, federal, state and local law enforcement partners, and 350 academic partners. State and local law enforcement CFTF partners are trained by the Secret Service National Computer Forensics Institute (NCFI). The CFTFs host partner meetings to discuss the latest in prevention, detection, mitigation, and cooperation among law enforcement and private sector organizations. CFTF partners receive quarterly bulletins, which include current trends in cybercrime and detection, policy, legal topics, and other CFTF developments. This partnership model facilitates incident response and allows the Secret Service to be a trusted resource to an organization for guidance during an initial stage of a cyber-incident.

The U.S. Secret Service shares the law enforcement responsibility for protecting the United States from cybercriminals with the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) Homeland Security Investigations (HSI) and Cybersecurity and Infrastructure Security Agency (CISA). Although there is overlapping jurisdiction in some authorities, the FBI has sole jurisdiction on cybercrime related to counter terrorism, foreign intelligence and nation state adversaries. Additionally, local and state police departments may have resources dedicated to investigate cybercrime or maintain a relationship with a federal task force.

When and where possible, you are encouraged to establish liaison with public and private cybersecurity organizations. The cyber domain evolves continually and information sharing is crucial to remain current on cybercrime trends, tactics, and methods.

B. Study the legal framework:

Consult with external and internal legal experts who are familiar with technology, data breaches, and cyber incident management. Learn the laws and regulations governing communications, data privacy, information-sharing, and monitoring. Learn where your organization is storing the data and where the individuals/entities, whose data your organization is storing, reside, to determine jurisdiction over the data. In 1986, the United States Congress enacted the Computer Fraud and Abuse Act (CFAA), as an amendment to 18 U.S.C. 1030. The CFAA has since been amended multiple times to address advancements in technology and cybercrime. The CFAA criminalizes knowingly accessing a computer without authorization, obtaining protected information, with the intent to defraud, intentionally causing unauthorized damage to a protected computer, knowingly and with intent to defraud trafficking in passwords or access information, and extortion involving computers.

Multinational organizations, particularly those transmitting and storing data transnationally, must make additional considerations when working towards greater cyber resilience. These considerations will vary based on the specific country where an organization operates, transmits and stores data. Consider the citizenship of those whose data your organization handles. Learn if and how your organization is protected by laws and regulations as a potential victim of a data breach. For example, the European Union (EU) has enacted a single EU-wide data protection reform, the General Data Protection Regulation (GDPR), allowing EU citizens to better control their personal data, while allowing businesses to reduce red tape and to benefit from greater consumer trust.

C. Understand legal responsibilities:

Understand your organization's responsibility regarding data protection and data breach reporting under federal, state, local, and international law. Determine the threshold for mandatory breach reporting and which entities require notification as there is no comprehensive law in the United States that addresses data privacy and protection, but there are sector-specific laws. The U.S. Federal Trade Commission (FTC) is responsible for protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices, whereas the U.S. Securities and Exchange Commission (SEC) was established to protect investors, maintain fair, orderly, and efficient markets. The U.S. Department of Health and Human Services (HHS) oversees the compliance with the Health Insurance Portability and Accountability Act (HIPAA). Additionally, each state may have its own legislation concerning data privacy.

Determine if your organization is required to implement threat detection and data loss prevention programs for compliance under federal, state, local, and international law. Identify the legal consequences of decisions your organization will make, during a potential incident, and how to prepare for potential interaction with law enforcement and/or regulatory agencies. If using contracted third-party services for storing or transmitting your organization's data, determine how responsibility is shared between your organization and contracted third-party service providers. Determine what provisions to include in contracts and agreements with these providers, to include including cooperation during a cyber incident, and furnishing information to IR firms and law enforcement agencies. Consider cyber insurance, if available and suitable for your organization.

D. Maintain cyber awareness:

Continually learn about existing and emerging cyber threats and risk management strategies by participating in cybersecurity events and educational programs. Such events are often sponsored by private firms as well as law enforcement agencies. Develop a further understanding of the threat environment and the protective measures available to your organization. Subscribe to receive timely information about cyber security issues, vulnerabilities, and exploits from reputable cybersecurity organizations. For example, DHS created the National Cyber Awareness System which provides subscribers access to timely information about security topics and threats. For a more customized approach to preparedness for your organization, consider seeking industry-specific guidance and consult with cybersecurity services organizations.

E. Determine vulnerabilities:

Identify network and device vulnerabilities specific to your organization's operations. It is important to consider all devices, stationary and mobile, with network and data access. Such devices include desktop and laptop computers, printers, copiers, internet of things (IoT) devices, cellphones (organization and employee-owned), and any other devices that are connected to a network or other devices, wirelessly or through Ethernet cables. Assess how and where your organization backs up data. Evaluate vulnerabilities associated with using contracted third-party service providers and other outside entities that host and/or have access to your organization's network and data. These include cloud and backup storage, software services, or any other contractors and vendors that have some level of access to your network and data. Learn how your organization's data is being protected by these contracted third-parties, and understand your responsibilities and liabilities when it comes to using contracted third-parties. When entering into a contract with a third-party vendor, ensure your contract includes a stipulation on them notifying your organization when they are subject of a data breach, and on what effect the breach has on your network and data.

The Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. If your organization's line of work can potentially affect critical infrastructure and public safety, the directive delivers policy statements defining the roles various federal, state, and local agencies will play in carrying out in the protection of critical infrastructure. In 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 established DHS CISA, a federal risk advisor, collaborating with partners to defend against threats and build a more secure and resilient infrastructure.

F. Prioritize and institute cybersecurity measures:

Ensure that basic cybersecurity best practices, such as robust passwords, multi-factor authentication, disabling USB storage devices, and perimeter defense (firewalls) are instituted. As an additional layer of security, consider using data encryption that resides on networks and devices (at rest), as well as for data that is transmitted (point-to-point). Subsequently determine which data, assets, and services warrant the greatest protection and prioritize cybersecurity efforts based on mission-critical needs. Specific measures may include, instituting access controls and network segmentation that appropriately limit the availability of data, particularly mission-critical data, and maintaining server logs (firewall, event and active directory), which could be critical to establishing the cause and origin of a cyber incident. Consider procuring cybersecurity technology and services that align with threats that would cause most harm to your organization, and may include intrusion detection capabilities, data loss prevention, and traffic filtering or scrubbing. Test technological solutions regularly, to include involving contracted third-party service providers, to ensure they perform as expected. Routinely review access privileges and discontinue access when employees leave your organization. Routinely back up data, ensure the backups are not connected to the network, and are stored securely offsite.

G. Monitor the network:

Consider monitoring your organization's network traffic (internal and external, inbound and outbound), which can be critical to detecting, analyzing, preventing, and addressing cyber incidents. However, prior to procuring technology to monitor systems and devices for cybersecurity threats, understand your organization's responsibilities under federal, state, local, and international law and ensure compliance when conducting such monitoring. Consider using log-in banners, user agreements, workplace policies, training, and written acknowledgement from employees and contractors to inform that their use of the network constitutes consent to your organization monitoring the communications, in accordance with applicable laws and regulations. The Cybersecurity Information Sharing Act of 2015 (CISA), explicitly authorized organizations to monitor their own information systems, and, upon written consent, the systems of other organizations, for cybersecurity purposes. The Department of Homeland Security (DHS) created the Automated Indicator Sharing (AIS) to enable the exchange of cyber threat indicators between the Federal Government and the private sector. Note that the laws in some countries and regions may restrict your ability to monitor the content of employees' communications and may not allow employees to consent to such monitoring. Consider additional steps to preventing employee error, such as implementing email filtering and web restrictions.

H. Develop policies and conduct training:

Develop internal policies addressing cybersecurity in general, and, more specifically, for handling cyber incidents. Develop a framework for your organization's employees to be cognizant of and maintain good "cyber hygiene," and encourage employees to recognize and swiftly report suspicious activity. Studies have shown that employees have continually been a weak link in organizations' cyber resilience, intentionally (insider threat) or unintentionally (insider risk). Conduct regular briefings with employees and keep them informed on cybersecurity procedures and responsibilities. If possible, test your employees to enhance cybersecurity awareness.

I. Develop a communication strategy:

After having acquired an understanding of the legal framework and specific reporting requirements, develop a communication strategy for your organization to implement during a cyber incident. Establishing a communication strategy prior to a cyber incident, which requires a swift response, should be an important component of an organization's preparation phase. Consider establishing "out of band" communication methods. Determine how you will communicate with all employees, those that will participate in the IR Plan execution and those who will not. At a minimum, an organization should have preapproved notification templates for law enforcement, regulatory agencies, and, if applicable, media. Communication templates can vary depending on a specific situation and reporting requirements. Continuous proactive liaison with law enforcement will help understand the requirements law enforcement may have during an incident and a subsequent investigation, and should be included in your organization's communication strategy.

J. Consider retaining legal services:

Consider retaining the services of experts to address legal issues and assist with decision making during a potential cyber incident. Include them in IR planning and tabletop exercises for an opportunity to address questions regarding interacting with contracted third-parties, issuing public communications, addressing local reporting requirements, coordinating with law enforcement, and engaging with IR firms.

K. Consider retaining IR services:

Consider retaining an IR firm to expedite your organization's response to a cyber incident. If considering an IR firm, ensure that it has experience with local data protection laws and regulations, is using forensically sound methods of evidence collection and data preservation, and has well established channels of communication with law enforcement. Law enforcement is responsible for investigating criminal violations with the objective of identifying, apprehending, and prosecuting perpetrators. Thus, law enforcement is focused on collecting information about the criminal conduct, and is frequently limited to technical data that can be used to track activities and events on the network. This technical information may be distinct from, but sometimes commingled with information collected by the IR firm, and law enforcement may need to coordinate with the IR firm to obtain technical data the firm has already collected. This coordination can minimize disruption of an organization's operations, avoid duplication of efforts, and expedite an investigation.

L. Prepare for evidence preservation:

While prioritizing and instituting preventative cybersecurity measures is of utmost importance, preparation should include preemptive measures for dealing with an incident when, not if, one occurs. This includes understanding that evidence preservation begins well before having detected a cyber incident. Some evidence preservation will depend on the type of incident and organization-specific vulnerabilities, but there are general rules to ensuring evidence preservation. The average cyber incident remains undetected for months. There are rules your organization should implement to support evidence preservation during an incident, such as maintaining server logs (firewall, event and active directory) for at least a year and maintaining a current network map. Maintaining an up-to-date network map, that includes authorized remote connections, will expedite detection and isolation of an incident, as well as assist with the investigation and prosecution.

M. Create an Incident Response (IR) Plan:

Develop an IR Plan with specific and concrete procedures to follow in the event of a cyber incident. The IR Plan should include the following:

a. **An IR Team consisting of decision makers and critical personnel (senior management, legal counsel, human resources, corporate security, IT security, public relations), and, if needed, a retained IR firm. If retaining the services of an IR firm, collaborate with the IR firm on your organization's IR Plan and review their processes.**

b. **Assignment of specific tasks and timelines for the completion of critical tasks.**

c. **Contact information for the members of the IR Team, day and night, and how to proceed if they are unreachable or unavailable.**

d. **Contact information for senior management, communications personnel, shareholders, and legal counsel, and a description of the circumstances under which each should be contacted.**

e. **Consider "out of band" communication methods to coordinate during an IR event, so that when a cyber incident occurs, you are not using your organization's integrated communications (email, phones, etc.) to prevent intruders from monitoring your organization's IR.**

f. **Prioritization of what mission-critical data, networks, assets, or services should receive primary attention during an incident and procedures for implementing security measures, such as segmenting the network (isolating the threat).**

g. **Procedures for preserving evidence for potential criminal prosecution. These should include procedures already in action (server logs and network maps), along with predetermined incident-specific procedures that can be quickly implemented as part of the IR Plan.**

h. **Instructions for contacting and engaging with law enforcement, to include providing known, and relevant information about the incident.**

i. **Steps for resolving legal questions, such as compliance with data protection under the law.**

j. **Procedures for notifying regulatory agencies, if and when applicable.**

k. **Instructions for contacting contracted third-party service providers, and other outside entities who host the affected data and services, such as cloud storage service providers and commercial data centers.**

l. **Procedures for restoring backed-up data, including measures for insuring the integrity of backed-up data before restoration.**

m. **Templates for issuing public communications for compliance with under the law.**

n. **Conduct tabletop exercises to ensure that employees become and remain familiar with the IR Plan, and that communication channels and emergency processes remain up-to-date.**

o. **If using contracted third-parties to transmit and store data, inquire about and study their IR Plan.**

p. **Keep the IR Plan up-to-date and maintain hard copies easily accessible by the IR Team. Do not save the digital copy of the IR Plan on your primary systems where it can be accessed by intruders.**

Following the above steps will save valuable time during an incident. Documenting the steps taken will save valuable time during your organization's interaction with law enforcement and will create a solid foundation for investigating and prosecuting the intruders. The sequence of above steps will depend on your organization's specific needs and responsibilities under federal, state, local, and international law.

EXECUTE

N. Assess the incident:

Immediately assess the nature and scope of the incident, to determine whether the incident was caused by a malicious act, human error, a technological glitch, or a combination of those factors. This step will define the type of assistance needed to mitigate the specific damage. Do not switch off power to the affected network or device. If your organization's network has appropriate logging capabilities, a system administrator can attempt to identify the affected computer systems, apparent origin of the incident, any malware used, and/or any remote servers where data was transferred. Additionally, this step will enable documenting which users are logged onto the network, which processes are running, current external connections to computer systems, and all open ports and associated services and applications. Ensure that your organization does not unintentionally or unnecessarily modify stored data, which can hinder IR and the investigation.

O. Implement protective measures:

To prevent further damage, begin implementing the protective measures outlined in the IR Plan, while maintaining detailed records of the steps taken to mitigate the damage. This information may be used later to establish criminal violations and recover remediation costs from the intruders, dependent on federal, state, local, and international law.

P. Document the response:

Direct the IR Team and IR firm personnel to keep a contemporaneous written record of all steps undertaken, to assist the investigation and reconstructing the order of events. Record the descriptions, dates and times of all incident-related events, incident-related phone calls, emails, and other contact, along with the identity, roles, and responsibilities of IR personnel (internal and contracted) performing tasks related to the incident. Include technical information, such as the identity of systems, accounts, services, data, and networks affected by the incident. Other information to include is the amount and type of damage inflicted, information regarding network topology, 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. Document and save communications relating to the incident, in particular threats, claims of credit, extortion demands, suspicious calls, emails, or other requests for information about the incident.

Q. Preserve evidence:

Typically, a cyber incident is a result of a malicious (criminal) action, and therefore a crime scene that needs to be preserved. Some examples of evidence to preserve and document include, previously maintained server logs (firewall, event and active directory), an up-to-date network map that includes authorized remote connections, a list of affected servers, disk images, memory images, communications from intruders, screenshots and copies of malware, ransomware and any other relevant information. A timeline of events is crucial in reconstructing the incident and preparing the preserved evidence for investigation and prosecution.

Consider imaging the affected systems using forensically sound procedures to preserve a record 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 of an electronic device, and provides a snapshot of the system at the time the image was created, including deleted files, slack (apparently empty) storage space, system files, and executable files. Protect the media by restricting access to ensure that it is not altered, and document who has maintained possession of the media to establish a chain-of-custody.

When using regularly generated backups, ensure that they are isolated from the affected systems and check them on isolated computers prior to using them to restore the system. Intrusions are commonly only discovered long after an initial intrusion occurred, and may require the retrieval of old backups to pre-date the intrusion. Isolated backups are particularly critical in mitigating ransomware attacks.

R. Contact law enforcement:

If there is suspicion that the cyber incident is a result of criminal activity, contact law enforcement as predetermined in the IR Plan. Once this contact is established, share forthcoming press releases regarding the incident with the investigators before releasing information that might impede the investigation. Having established liaison with law enforcement will streamline this step by clarifying what entities your organization should contact and when. Becoming a member of a Secret Service CFTF and having followed the steps outlined in this guide should have prepared your organization. Some organizations assume that contacting a law enforcement agency, such as the Secret Service, will publicize the incident and make the organization subject to civil lawsuits. When it comes to civil litigation the Secret Service is subject to Federal Court subpoenas, but not state or local court jurisdiction. Additionally, information concerning ongoing criminal investigations is subject to strict internal policies and Department of Justice regulations that govern federal law enforcement.

S. Contact regulators:

Depending on the type of incident, and if required, contact regulatory agencies as predetermined in the IR Plan. This is an important step in your organization's response to a cyber incident. Proper execution of this step of the IR Plan largely depends on your organization understanding its responsibilities regarding data protection and data breach reporting under federal, state, local, and international law.

The Secret Service, similar to other federal law enforcement agencies, is not mandated to notify regulators, and criminal investigators are focused on deterrence and apprehension of criminals. Furthermore, federal government agencies are independent of each other and information sharing among them is subject to the Privacy Act of 1974.

DEBRIEF

T. Continue monitoring:

After a cyber incident appears to be under control, continue monitoring systems for anomalous activity. Remain vigilant for new signs of re-infection and compromise.

U. Notify other organizations:

If there is evidence that the cyber incident has affected another organization, notify the organization. If this incident is being investigated by law enforcement, the notification may need to be issued by them to maintain the integrity of a potential criminal case. Additionally, the Cybersecurity Information Sharing Act of 2015 (CISA) enabled organizations to participate in the exchange of cyber threat indicators with the Federal Government though the DHS Automated Indicator Sharing (AIS).

V. Conduct a post-incident review:

Review the performance of the incident response and note the deficiencies and gaps in executing the IR Plan, to include determining if each step in the plan was followed or why not. Assess the roles and responsibilities of the members of the IR Team, and if applicable, the IR firm and the legal experts.

W. Adjust the IR Plan:

Address shortcomings in security practices according to the findings of the post-incident performance review. Adopt measures to prevent similar attacks in the future, consider acquiring resources to better secure its systems. Adjust the roles and responsibilities of the IR Team and other participants of the incident response.

Further resources:

www.secretservice.gov/investigation U.S. Secret Service Criminal Investigations

www.nist.gov/topics/cybersecurity U.S. National Institute of Standards and Technology

www.dhs.gov/be-cyber-smart U.S. Department of Homeland Security Cyber-Smart Campaign

www.justice.gov/criminal-ccips U.S. Department of Justice Computer Crime and Intellectual Property Section

www.cisa.gov/about U.S. Dept. of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)

www.ice.gov/hsi U.S. Department of Homeland Security Homeland Security Investigations

www.fbi.gov/investigate/cyber U.S. Federal Bureau of Investigation

www.ftc.gov U.S. Federal Trade Commission

www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business
U.S. Federal Trade Commission, Data Breach Response: A Guide for Business

https://enterprise.verizon.com/resources/reports/dbir Verizon Data Breach Investigations Reports

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02016R0679-20160504
European Union General Data Protection Regulation

www.enisa.europa.eu European Union Agency for Cybersecurity

www.pcisecuritystandards.org Payment Card Industry (PCI) Security Standards Council

United States
Secret Service
**Cybercrime
Investigations**

PREPARING FOR A CYBER INCIDENT

BEFORE AN INCIDENT

UNDERSTAND

A. Establish liaison and partnerships
B. Study the legal framework
C. Understand legal responsibilities
D. Maintain cyber awareness

PREPARE

E. Determine vulnerabilities
F. Prioritize and institute cybersecurity measures
G. Monitor the network
H. Develop policies and conduct training
I. Develop a communication strategy
J. Consider retaining legal services
K. Consider retaining incident response (IR) services
L. Prepare for evidence preservation
M. Create an IR Plan

DURING AN INCIDENT

EXECUTE

N. Assess the incident
O. Implement protective measures
P. Document the response
Q. Preserve evidence
R. Contact law enforcement
S. Contact regulators

AFTER AN INCIDENT

DEBRIEF

T. Continue monitoring
U. Notify other organizations
V. Conduct a post-incident review
W. Adjust the IR Plan

◀ BACK