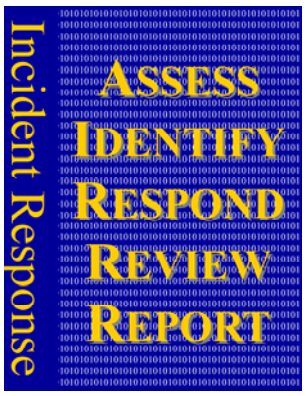
Cyber Security:

Cyber Incident Response Guide

A Non-Technical Guide

Essential for
Business Managers
Office Managers
Operations Managers



Multi-State Information Sharing and Analysis Center

NYS Office of Cyber Security

This appendix is a supplement to the *Cyber Security: Getting Started Guide,* a non-technical reference essential for business managers, office managers, and operations managers. This appendix is one of many which is being produced in conjunction with the *Guide* to help those in small business and agencies to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.dhses.ny.gov/ocs/.

INTRODUCTION

Has your system been *compromised*? How did it happen? What do you do?

Not knowing can be dangerous. This is a true story of how one local government organization learned this lesson. A town began experiencing repeated issues with printers and computers dropping off the network (the computers were used to connect to the statewide criminal justice and motor vehicle systems). A service provider was called in several times to re-connect the network hardware. After discovering illegal software on the computer, the local police were contacted.

The Federal Bureau of Investigation was also contacted and by the next week, the town's computers were confiscated for investigation. The service provider was able to track the intruder's footprint from the town to a nearby city in that state, to Canada to Netherlands, ending in Belgium. The intruder was a 14-year-old boy. The town's Internet service and network were being used for illegal Internet games. Local businesses' financial information was also accessible on the network.

Investigators determined the town lacked a firewall for the Internet and network connection. In the end, the total expense of repair, upgrades, and training totaled $74,000, in addition to business partners' data being compromised.

At some point in time, you will experience an information security incident. The incident may jeopardize your computer security. Someone with malicious intent may seek to gain access to your organization's confidential documents, or they may attempt to alter, delete, or prevent your organization from using your data.

As business manager, you must be aware of incidents that occur. It is imperative for an organization to be able to recognize a security incident. Fast and efficient responses can lead to quick recoveries, minimize the level of damage, and help prevent future incidents. All end users should be familiar with symptoms that may indicate an incident and should know what to do.

PURPOSE

The purpose of this guide is to help you identify information security incidents and establish best practices for handling these incidents. This guide will provide you with a recommended step-by-step process for responding to incidents and developing an incident response team. The guide is intended to complement the existing incident response policy of your organization or serve as a template if you don't yet have one.

This guide describes how to recover from an incident in a timely and secure manner, and to minimize impact on your organization or your business partners.

It is important for an organization to establish an incident response policy, specifying necessary courses of action for dealing with an incident. The policy is a tool used to provide insight, guidance, and handling procedures. It specifies how to identify, respond to, and report an incident. A model policy is included in this guide. As previously mentioned in the **Cyber Security: Getting Started Guide** *(available at* http://www.dhses.ny.gov/ocs/), a single contact person should be designated as responsible for cyber security, ensuring proper policies and procedures are in place and followed.

Establishing a Response Team

A critical step in effective incident response is establishing an Incident Response Team. The goal of the team is to quickly and appropriately handle an incident. The team members should have the authority to make decisions and execute the response plan. The team consists of members described in the roles on the following pages, which may include individuals in your organization and contractors. Smaller teams may consist of only a few people assuming multiple roles. Similar to fire districts employing mutual aid, this may be an opportunity for smaller organizations to enter into trusted partnerships with neighboring organizations to share the roles and responsibilities. Each team member's role and responsibility for responding to incidents should be specifically defined.

Roles and Responsibilities

An incident response team usually consists of at least an executive (or designee), an incident response manager, technical support staff, and a legal contact. These positions may be supplemented by other staff and contractors as warranted.

Responsible Executive (or designee): The person who is accountable for the organization's operations, and has the following responsibilities:

- overseeing the entire response process
- managing the overall response activities for all security incidents
- decision-making regarding which courses of action will be taken
- determining when it is appropriate to share information outside the organization

Incident Response Manager (IRM): The person who has the overall responsibility to ensure the implementation, enhancement, monitoring and enforcement of security policies and procedures. This person may be the organization's designated Information Security Officer. This person should understand incident handling, be familiar with the organization's network and systems, and is responsible for the following:

- serving as the initial point of contact
- notifying and briefing management and the Responsible Executive as appropriate
- accessing the situation and assisting in fixing the problem
- providing options and recommendations to management on how to respond
- coordinating activities and communicating within the incident response team
- developing and maintaining all documentation relating to the incident

Technical Support Staff: Usually consists of IT staff and other members of the organization with the following responsibilities:

- assessing the situation and providing recommendations to the IRM
- assisting the IRM in gathering information
- helping the IRM in response and remediation
- providing any other support to the IRM as needed

Legal Contact: The organization's attorney/general counsel/equivalent, whose responsibilities are focused on the following:

- provides advice as appropriate

Training and Exercise

The IRM is responsible for implementing the incident response policy and procedures. This individual should work with management to ensure all users are trained in their response role. Continuous

awareness training and monitoring are important for strong computer security. Response drills are good tools to test the plan.

Overview: Incident Handling

Below are five elements for successful incident handling and the individuals responsible for taking the action. Depending on the structure of your organization, multiple individuals may be involved in performing the following:

- **Identify** the problem (All end users)
- **Assess** if this a security incident (IRM)
- **Respond** to the incident (Technical Support Staff)
- **Report** in accordance with the incident response plan (Technical Support Staff and IRM)
- **Review** the overall effectiveness of the response procedures (Responsible Executive, IRM, and Technical Support Staff)

IDENTIFY

The first step is to identify whether or not you have a problem. Any user who notices signs of anomalous activity should contact the IRM who will work with the organization's technical support staff. A cyber security incident is considered to be any adverse event that threatens the *confidentiality*, *integrity* or *availability* of your organization's information resources.

Possible causes of cyber incidents include the following:

- attempts to gain *unauthorized access* to a system or its data
- unwanted disruption or *denial of service* (*DoS*)
- *unauthorized access* to critical computers, servers, *routers*, *firewalls*, etc.
- changes to system hardware or software without approval
- *virus* or *worm* infection, spyware, malware
- loss or inconsistent electrical power

Symptoms

Signs a computer has been *compromised* may include the following:

- abnormal response time or non-responsiveness
- unexplained account lockouts
- passwords not working
- website homepage won't open or has unexplained changes/content
- programs not running properly
- running unexpected programs
- lack of disk space or memory
- bounced-back emails
- inability to connect to the network
- constant or increasing crashes
- abnormal hard drive activity
- connecting to unfamiliar sites
- browser settings changed
- extra toolbars that cannot be deleted

This list is not comprehensive, but is intended to raise your awareness level of potential signs. If you are unsure about a possible incident, treat signs as a security incident and notify the IRM who will

work with the organization's technical support staff.

ASSESS

The next step is to determine if the anomalous activity is an actual security incident. The IRM will assess the situation. Members of the Technical Support Staff may be called to assist in the initial assessment.

Questions the response team needs to address include: What are the symptoms? What may be the cause? What is being impacted? How wide spread is it? What part of the system or network is impacted? Could this impact your business partners?

Gather Information

The IRM should document all relevant information into a logbook. The following types of information should be documented:

- organization's name
- characteristics of incident
- date and time incident was detected
- list of symptoms noticed
- scope of impact
  - How widespread
  - Number of users impacted
  - Number of machines affected
- nature of incident
  - *Denial of Service*
  - Malicious code
  - Scans
  - *Unauthorized access*
  - Other

It is recommended that forms be readily available to document this information. The information can be used for future references, information sharing, and incident reporting, and should be kept in one location (such as in a logbook).

RESPOND

Once it is determined that your organization has a cyber security incident, the process for responding has several steps and may involve several people, as the Technical Support Staff responds under the direction of the IRM. It is important to be familiar with these procedures.

Briefing of Executives

Management should be notified immediately when a significant incident is detected. Briefing is a critical step in response, providing management with an assessment of the situation to help determine the necessary courses of action. As more information becomes available throughout the response process, additional briefings should take place which will help management determine if it is necessary to take additional steps, such as bringing in more resources, sharing information or involving law enforcement.

Initial Response

It is important to determine the origin of the incident, where possible, identify what systems have been *compromised* and what data may have been accessed. This information will help determine the necessary course of action.

The first step the Technical Support Staff should take is to isolate the problem, which may mean disconnecting the equipment from the network or if no network exists, the Internet. Additionally, the Incident Response Team should examine the equipment and check the appropriate logs, such as the firewall and system logs for signs of unauthorized access. Performing a *vulnerability scan* is helpful to identify vulnerabilities that may have led to the incident. It may be necessary to bring in an outside expert to provide assistance.

If it is determined that the incident warrants potential legal action, it is essential to preserve the evidence in the original form as much as possible. It is important to keep thorough and detailed logs of all actions to accurately document information for an investigation. The Legal Contact may provide advice on the proper procedures for collecting evidence and assist with contacting law enforcement, if necessary.

Recovery

Once the cause is determined, the Technical Support Staff is responsible for appropriate remediation and restoration. Management should be informed of the progress. Basic recovery steps may include the following:

- Remove vulnerabilities and install or update *routers* or *firewalls* to prevent future *unauthorized access*.
- Reinstall clean versions of the operating system.
- Install vendor security patches.
- Change all passwords.
- Conduct a *vulnerability scan* of the *compromised* machine/system before reconnecting to the network.
- Reconnect to the network.
- Monitor the system closely.
- Document recovery procedures to submit to the IRM for logging.

The necessary courses of action will depend on the cause of the incident. For example:

Cause	Course of Action
Unauthorized Employee Access	Review access rights and modify
Denial of Service Attack	Have your *ISP* block the activity
Virus or Worm	Update antivirus and virus scan the machine

REPORT

The IRM now compiles the logs of actions taken. The report should include the following:

- dates and times when incident was detected
- list of symptoms
- scope of impact
- step-by-step actions

The logbook can be a useful resource to refer to if future incidents occur. A sample log template is included with this guide.

For significant events, a report should be provided to the Responsible Executive (or designee).

REVIEW

Once the incident has been handled, a debriefing will help management examine the effectiveness of the response procedures and determine any necessary procedure or policy changes. Review helps to identify strengths and weaknesses in the response plan. The team should analyze the incident for lessons learned. Discussion should include: Was the problem discovered in proper fashion? Was the response appropriate? Was enough information obtained? Did the steps go well? How was the organization affected? Is the organization still vulnerable?

The team recommends the next steps, which may include information sharing or amending policies as appropriate. Management will determine what information will be shared and with whom.

GLOSSARY

The following defined terms are used in this guide:

Availability The extent to which information is operational, accessible, functional and usable upon demand by the authorized entity (e.g., a system or user).

Compromised The disclosure of sensitive information to persons not authorized access or having a need-to-know.

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Denial of Service (DoS) An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.

Firewalls A security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization's internal computer network.

Integrity The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

ISP Internet Service Provider (ISP) is an organization that provides Internet access.

Routers A device that forwards data packets along networks.

Unauthorized Access Gaining access into any computer system or network without expressed permission of the owner.

Virus A self-replicating program that spreads by inserting copies of itself into other programs.

Vulnerability Scan The process where a computer or network is checked for security issues, missing patches or misconfigurations. The scan results are typically compiled into a report, identifying the vulnerability along with remediation steps to correct the issue.

Worm A worm is a special type of virus that can spread automatically via e-mail, Internet relay chat or other network transport mechanisms.

INCIDENT LOG

Reported by: ▪ **Name:** ▪ **Phone:** ▪ **E-mail:**
Date & Time of incident detection:
Nature of Incident: ☐ **Denial of Service** ☐ **Unauthorized Access** ☐ **Malicious Code (worm, virus)** ☐ **Website Defacement** ☐ **Scans and Probes** ☐ **Other (describe)**
Incident description (What were the signs?):
Details: (e.g. virus name, events, etc)
Business impact (e.g. what information or services are impacted?)
Course of Action:
Additional Notes:

Appendix
Model Cyber Incident Response Policy
[Organization Name]

Purpose
This policy is established to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operation of a business and a swift and complete response to any incidents is necessary in order to maintain that availability and protect public and private information.

Responsible Executive
If the incident affects multiple departments, the Chief Executive shall be the Responsible Executive. If only one department is impacted, the executive responsible for that department shall fill this role. The responsibilities of the executive include, but are not limited to:

- receiving initial notification and status reports from the Incident Response Manager
- consulting with other executives on public notification, involvement of the organization's attorney and notification of law enforcement
- preparing and delivering press releases
- consulting with other executives and appropriate staff on priorities for response and recovery
- advising the Incident Response Manager on priorities

Incident Response Manager
The [organization name] designates that [The person filling the role of Incident Response Manager]/[actual name] has responsibility for preparing for and coordinating the response to a cyber incident. Responsibilities include, but are not limited to:

- training users to recognize and report suspected incidents
- developing and testing response plans
- being the point of contact should any employee believe an incident has occurred
- involving the identified technical support to address the incident
- notifying the appropriate executives that an incident has occurred if significant
- advising executive regarding notification of law enforcement and the [organization name] attorney if appropriate
- providing information to executive responsible for notifying the press and public
- coordinating the logging and documentation of the incident and response to it
- making recommendations to reduce exposure to the same or similar incidents

Technical Support Staff
The [business providing Information Technology services] shall provide technical support to the Incident Response Manager. Responsibilities include, but are not limited to:

- assessing the situation and providing corrective recommendations to the Incident Response Manager
- helping the Incident Response Manager make initial response to incidents
- responding to the incident to contain and correct problems
- reporting to the Incident Response Manager on actions taken and progress
- participating in review of the incident and development of recommendations to reduce future exposure
- consulting with other executives on public notification, involvement of the organization's attorney, and notification of law enforcement
- assisting with preparation of press releases
- consulting with other elected officials and appropriate staff on priorities for response and recovery
- advising the Incident Response Manager on priorities

Legal Counsel
The [organization's] attorney shall provide advice as called upon.

Some Resources

Key Organizations

- Department of Homeland Security, National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov
- Multi-State Information and Analysis Center http://msisac.cisecurity.org/
- Carnegie Mellon University/CERT Coordination Center http://www.cert.org/csirts/
- Information Security and Privacy Advisory Board http://www.nist.gov/itl/csd/sma/ispab.cfm
- National Institute of Standards and Technology, Computer Security Division http://csrc.nist.gov/
- Forum of International Response Security Teams http://www.first.org

Incident Response

- Defining Incident Management Processes: A Work in Progress (www.cert.org/archive/pdf/04tr015.pdf)
- CERT/CC, Avoiding the Trial-by-Fire Approach to Security Incidents (http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymattersmar99.cfm)
- NIST SP-800-86 "Guide to Integrating Forensic Techniques into Incident Response" (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf)
- National Information Assurance (IA) Approach to Incident Management (IM) (http://www.cnss.gov/Assets/pdf/CNSS-048-07.pdf)

Incident Reporting/Documentation

- NIST, Special Publication 800-12: "An Introduction to Computer Security - The NIST Handbook, Chapter 12 Computer Security Incident Handling" (http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter12-printable.html)
- NIST Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations Information Security" (http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf)
- Incident Management articles (in particular CNDSP accreditation): (https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/incident/223.html)
- CERT/CC, CSIRT Services (http://www.cert.org/csirts/services.html)

Incident Detection

- MS-ISAC/US-CERT, Current Malware Threats and Mitigation Strategies (http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf)
- NCSD, Cyber Security Responses to Physical Security Breaches (http://www.us-cert.gov/reading_room/cssp_cyberresponse0712.pdf)

Incident Response Team

- CERT/CC, Action List for Developing a Computer Security Incident Response Team (http://www.cert.org/csirts/action_list.html)
- CERT/CC, Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed? (http://www.cert.org/csirts/csirt-staffing.html)
- CERT/CC, Creating a Computer Security Incident Response Team: A Process for Getting Started (http://www.cert.org/csirts/Creating-A-CSIRT.html)
- Handbook for Computer Security Incident Response Teams (CSIRTs), CMU/SEI-2003-HB-002 (http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html)

User Awareness

- US-CERT, Protect Your Workplace Campaign http://www.us-cert.gov/reading_room/distributable.html)
- OnGuardOnline – a consortium of the Department of Justice, Federal Trade Commission, Department of Homeland Security, US Postal Service, and Securities and Exchange Commission www.onguardonline.gov
- StaySafeOnline http://www.staysafeonline.info/

Incident Recovery

- US-CERT, Recovering from a Trojan Horse or Virus (http://www.us-cert.gov/reading_room/trojan-recovery.pdf)
- US-CERT, Computer Forensics (http://www.us-cert.gov/reading_room/)