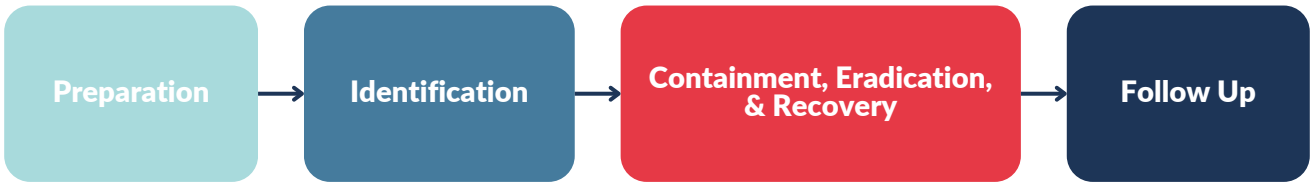
POWERED BY EDGE NETWORKS

CYBERSECURITY INCIDENT RESPONSE PLAN

Introduction

A company needs to effectively respond to and manage security incidents that may compromise the confidentiality, integrity, or availability of the company's information systems, data, or network resources. This document presents a security incident response plan that is based on security incident response best practices. It creates objectives for actionable procedures that can be measured, evaluated, scaled, and revised as necessary per each specific incident.



Phases

Preparation Phase: Staff is appropriately trained, and procedures are developed and tested.

Identification Phase: Responsibility for managing the response to a security incident is assigned, the scope of the incident is determined, and if appropriate, the security incident response team is notified.

Containment Phase: The risk of continued operations is assessed, and further loss or damage is prevented.

Eradication Phase: The cause of the security incident is determined, and vulnerabilities are mitigated.

Recovery Phase: All data and services impacted by a security incident are returned to full operational status.

Follow-up Phase: Lessons are identified that will enable an even more effective response to and management of the next security incident.

Plan Maintenance

This plan will be reviewed and tested at least annually, and the Record of Changes above is updated accordingly.

Preparation Phase

This phase is intended to be completed before the company is impacted by a security incident.

Security Incident Response Team (SIRT)

The company will organize and maintain a security incident response team (SIRT) that will respond to and manage security incidents.

Team	Responsibilities	Employees
Management	• Activates plan • Makes financial and staffing decisions • Communicates with upper • management • Provides staff support	
Coordination	• Notifies response team • Maintains incident status • Informs affected management, users, and third-party organizations • Conducts follow-up	
Response	• Determines the extent of damage to information systems, network resources, and/or data • Recommends course of action • Carries out containment, eradication, and recovery processes	

Identification Phase

The identification phase is focused on determining whether a security incident has occurred and, if one has occurred, determining the type and severity of the incident.

Immediate Action

- [ ] **Assign an Incident Coordinator**
  Once a possible security incident is detected by or reported to the company's information technology department, a SIRT member will be assigned to coordinate the response to the incident. This person will be the incident coordinator.

- [ ] **Incident Documentation**
  Using the Security Incident Identification Form (see below), the incident coordinator will document the facts of the possible security incident. As appropriate, such documentation should include alerts from intrusion detection, intrusion prevention, and/or file-integrity monitoring systems, as well as the detection of unauthorized wireless access points.

- [ ] **Incident Determination**
  The incident coordinator will examine the facts of the possible security incident. The coordinator will then determine if a security incident has occurred. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services. If the coordinator determines that a security incident has NOT occurred, STOP. If the coordinator determines that a security incident has occurred, continue to the next step.

- [ ] **Incident Documentation**
  Using the Security Incident Identification Form (see below), the incident coordinator will document the facts of the possible security incident. As appropriate, such documentation should include alerts from intrusion detection, intrusion prevention, and/or file-integrity monitoring systems, as well as the detection of unauthorized wireless access points.

- [ ] **Incident Classification**
  The incident coordinator will assign a severity level to the security incident.

Security Incident Identification Form

Name & Job Title of Person Completing the Form	
Incident Date & Time	
Discovery Date & Time	
Brief Description of Security Incident *Examples: Denial of service, malicious software, unauthorized access of data/services, lost data, etc.*	
Brief Description of the Impact(s) of the Incident *Type of data and amount breached.*	
Number of Information Systems and/or Services Impacted by Incident	
Outside Organizations Impacted by the Security Incident *If none, state N/A*	
How was the security incident detected?	
Security Level *See table below*	

Severity Level

The following table should be used to assign the severity level to the security incident.

Green (Not Severe)	Yellow (Mildly Severe)	Red (Severe)
Incident impacts only noncritical information systems, network resources, or data	Incident impacts up to two critical information systems, network resources, or sources of data	There is imminent danger that sensitive data can be read, modified, or destroyed by an unauthorized person, or the disclosure or access has already occurred
It is prevented by existing security controls	It cannot be prevented by existing security controls	Three or more critical information systems, network resources, or sources of data are impacted
Can be quickly prevented by updating existing security controls	It cannot be prevented by quickly updating existing security controls	Organizations outside of could or are being impacted by the security incident
Does not pose a significant risk to information systems, network resources, or data		The security incident could impact any person's physical safety
		Significant services are being degraded or stopped by the security incident
		It cannot be prevented by existing security controls
		It cannot be prevented by quickly updating existing security controls

Response to Incident Severity

Green Security Incident Response	Yellow Security Incident Response	Red Security Incident Response
The security incident response plan is NOT activated.	The incident coordinator will quickly gather the SIRT-management team and report on the security incident and its severity level.	The incident coordinator will quickly gather the SIRT-management team together and report on the security incident and its severity level.
The incident coordinator will assign appropriate technical staff to remediate and/or monitor the security incident.	The management team will then activate the security incident response plan.	The management team will then activate the security incident response plan.
Assigned technical staff will provide regular status reports to the incident coordinator.	As determined necessary or appropriate, the SIRT-management team will notify management about the security incident.	The SIRT-management team must promptly notify management about the security incident.
Management does not need to be notified.	The SIRT-management team should provide details about the incident and the steps they will be taking to respond to the incident.	The SIRT-management team must provide details about the incident and the steps they will be taking to respond to the incident.

Containment Phase

The containment phase is focused on limiting the scope and magnitude of a security incident.

Immediate Action

- [ ] **Formation of a SIRT**

  SIRT members will gather at the security incident command center. The SIRT will receive a security incident briefing from the incident coordinator.

- [ ] **Maintain a Low Profile**

  While responding to a security incident, SIRT members will be careful not to take actions that might alert an attacker that they have been discovered.

- [ ] **Secure Area**
  As appropriate, SIRT response team members will physically secure the area where a security incident has occurred.

- [ ] **Back-Up Impacted Information Systems**
  As appropriate and possible, the SIRT response team will perform full backups of new media of all information systems impacted by a security incident. The media will then be placed in a sealed plastic bag; the person(s) performing the backup will sign across the seal. The sealed media will then be locked in an access-controlled location.

- [ ] **Determine Risk of Continuing Operations**
  The SIRT management team will determine whether or not information systems, data, and/or network resources impacted by a security incident should continue to be made available to employees and/or customers.

- [ ] **Disable Access to Data or Services**
  As determined necessary, the SIRT response team will disable access to data or services impacted by a security incident.

- [ ] **Estimate Damage**
  The SIRT response team will assess damage to impacted information systems, data, and/or network resources. The team will then create and communicate to the incident coordinator a brief plan of action and time estimate to rebuild or repair the impacted information systems, data, and/or network resources.

- [ ] **Impact Notification**
  The incident coordinator and SIRT management team will notify all appropriate organizations and persons (e.g., information system owners and administrators, management, third-party organizations who use the company's services or data) about the likely impacts of the security incident (e.g., a certain service will be unavailable to customers for 4 hours, etc.). *Note: All interactions with the media concerning security incidents should be via the public relations office.*

- [ ] **Password Changes**
  The SIRT response team will change all authentication credentials (e.g., passwords, physical access codes, etc.) that may have been compromised by the security incident.

- [ ] **Complete Security Incident Containment Form**

  A member of the SIRT response team will complete the Security Incident Containment Form below to keep a record of the incident.

Security Incident Containment Form

Name & Job Title of Person Completing the Form	
Date	
Time	

Disabled Access to Data or Services

Brief description of all information systems, data, and/or network resources whose access was disabled due to the security incident.	
For each information system, data, and/or network resource, list the time when access to it was disabled.	

Information System Backup

Were all information systems impacted by the security incident backed up successfully If not, what was the reason?	
Name and title of person(s) who did the backup(s).	
Time backup(s) started.	
Time backup(s) completed.	
Is the backup media sealed? If not, what was the reason?	
Location where backup media is stored.	

Eradication Phase

The goal of the eradication phase is to eliminate all adverse impacts caused by a security incident and mitigate the vulnerability(s) that led to the incident.

Immediate Action

- [ ] **Determine How the Security Incident Occurred**
  The SIRT response team will examine logs, audit records, and other appropriate sources (e.g., camera data, etc.) to determine how the security incident occurred.

- [ ] **Perform Vulnerability Analysis**
  The SIRT response team will check all information systems impacted by a security incident, plus related systems, for vulnerabilities. For example, if a web server was compromised, all web servers will be checked for vulnerabilities.

- [ ] **Improve and/or Implement Defenses**
  The SIRT response team will mitigate the vulnerability(s) that led to the security incident
  (i.e., turn off an unnecessary service, provide additional training to employees, encrypt data, etc.).

- [ ] **Decide Whether to Rebuild or Repair**
  As necessary, the SIRT management team will determine whether information systems impacted by a security incident should be rebuilt or repaired. Criteria used by the management team to make this decision will include the type of access and privileges gained by an attacker, the length of the incident, and the time and effort required to rebuild or repair the information systems.

- [ ] **Locate Most Recent "Trusted" Backup**
  If a decision has been made to rebuild an information system, the incident coordinator will locate and acquire a backup(s) that is known to be good (i.e., not compromised, etc).

Security Incident Eradication Form

Name & Job Title of Person Completing the Form	
Date	
Time	
Information System Name	
Names and titles of all persons performing forensics on the impacted information system	
Was the vulnerability (or vulnerabilities) that caused the security incident identified? If yes, provide a detailed description.	
Describe the validation procedure(s) used to ensure the vulnerability (or vulnerabilities) has been mitigated	
Information System Name	
Names and titles of all persons performing forensics on the impacted information system	
Was the vulnerability (or vulnerabilities) that caused the security incident identified? If yes, provide a detailed description.	
Describe the validation procedure(s) used to ensure the vulnerability (or vulnerabilities) has been mitigated	

Recovery Phase

The goal of the recovery phase is to return all data and/or services impacted by a security incident to full operational status.

Immediate Action

- [ ] **Repair or Rebuild Information Systems**

  Depending on the decision(s) made in the rebuild/repair step, the SIRT response team will take one of two actions for each compromised information system:

  - Action 1: Repair the compromised information system. Any configuration changes, files, applications, or malicious code must be completely removed from the system(s). All repairs must be documented.
  - Action 2: Completely rebuild the compromised information system. As possible, rebuild the system from the original vendor media and trusted data backup.

- [ ] **Validate Information Systems**

  The SIRT response team will verify that the information systems that were rebuilt or repaired are functioning as expected.

- [ ] **Decide When to Restore Operations**

  If data or services have been made unavailable to employees, customers, or business partners because of the security incident, the SIRT management team will determine when the data or services can be made available again.

- [ ] **Notification**

  The SIRT management team will notify appropriate management when impacted data and/or services are fully available and functional. The incident coordinator will notify appropriate organizations (e.g., information system owners and administrators, third-party organizations who use the company's services or data, etc.) when impacted data and/or services are fully available and functional.

- [ ] **Data Breach Reporting**

  If the security incident has resulted in suspected or confirmed loss, theft, or unauthorized access of sensitive data, notify all external parties (e.g., individuals affected, the media, state and federal agencies, etc.).

Note: All interactions with the media concerning a security incident should be via the public relations office.

- [ ] **Monitor Data and Services**

  Information technology (IT) staff will carefully watch logs and traffic to and from all company data and services that were impacted by the security incident. If possible, logging and auditing will be increased on information systems impacted by the security incident.

Follow-Up Phase

The focus of the follow-up phase is to identify lessons that will enable the company to respond more effectively to and manage the next security incident.

Immediate Action

- [ ] **Conduct a Lessons-Learned Meeting**

  Using the questions listed below – Security Incident Follow-up Form, the Manager of Technical Services will conduct a lesson-learned meeting. Each employee who participated will provide feedback on the security incident response.

- [ ] **Produce a Follow-Up Report** >

  The incident coordinator will compile a follow-up report that describes the security incident, lessons learned by employees, and recommendations for better responding to and managing the next security incident. *[Click here for an Incident Report template]*

- [ ] **Create an Executive Summary**

  The incident coordinator will produce an executive summary of the follow-up report for management.

- [ ] **Distribute Executive Summary**

  The SIRT management team will send the executive summary to the appropriate management.

- [ ] **Implement Approved Recommendations**

  All recommendations approved by management will be submitted to the company's change control process and implemented.

Security Incident Follow-Up Form

Name & Job Title of Person Completing the Form	
Date	
Time	
Briefly describe the security incident and what actions were taken	
How much time was spent responding to the incident?	
What were the costs (direct and indirect) of the incident?	
What did the company do well in responding to and managing the incident?	
What difficulties were encountered in responding to and managing the incident?	
Was there sufficient preparation for the incident?	

What preparation was not done that could have been?	
Did detection of the incident occur promptly? If not, why not?	
What additional tools could have helped the company better respond to and manage the security incident?	
Was the incident quickly and sufficiently contained? If not, what additional tools or processes could have helped contain the incident?	
Was communication among SIRT members adequate? If not, what could be improved?	
Was communication with outside organizations adequate? If not, what could be improved?	
Was communication with customers adequate? If not, what could be improved?	
Were remediation procedures adequate to prevent future occurrences?	
Additional Information	