

# [ Incident Response

**Incident response is the process of responding in an organized manner to a compromise or attempted compromise of organizational information technology assets**

# [ Basic Definitions

Event

Adverse  
events

Computer  
Security  
Incident

# [Preparation

---

**Incident response policy**

---

**Incident response plan**

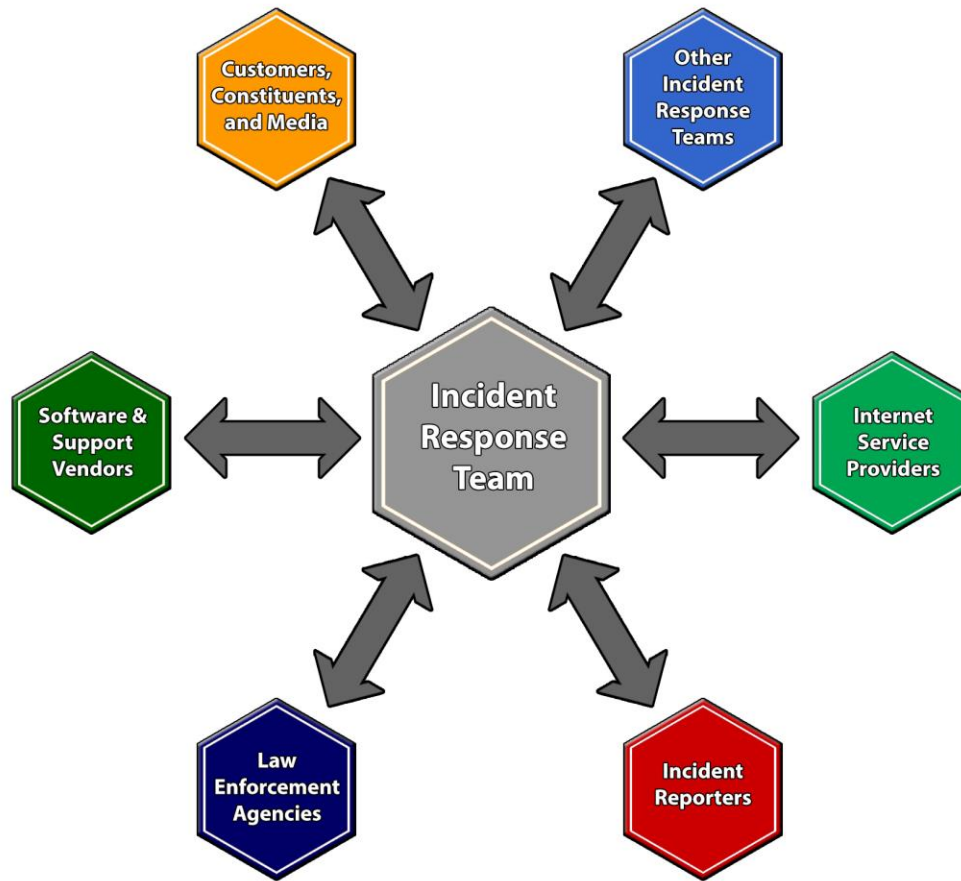
---

**Related incident response procedures**

# [ Incident Response Tools

**Specific software may be needed for incident-handling activities such as forensics analysis**

# [ Communication Planning



# Communication with Law Enforcement

- Law enforcement reporting will vary by country, state, economy, and jurisdiction
- Forensics policy, standards, and procedures should contain requirements as noted by the law enforcement partner

# [ Media

All members of the incident response process should be aware of how to interact with the media

Provide accurate and timely updates to the media

# [ The Incident Response Team

- **Virtual teams:** All members have other regular duties
- **Some organizations have permanent team members**
- **Hybrid:** Certain permanent core members and others called up as necessary
- **Centralized vs. Decentralized**



# [ Other Considerations

- Contact information
- On-call information for other teams
- Issue tracking system
- Smartphones
- Encryption software
- War room
- Secure storage facilities
- Incident analysis

# [ Detection and Analysis

- **Events may have a negative impact, they will not necessarily be classified as security incidents**
- **Indicator**
  - An event that means an incident is actually occurring or has occurred
- **Precursor**
  - An event that may signal an incident in the future

# [ Common Sources of Precursors and Indicators

**NIST SP 800-62 Rev2  
provides “Common Sources  
of Precursors and Indicators”**

# [Types of Intrusion Systems

**Network-based  
intrusion  
systems**

**Host-based  
intrusion  
systems**

# [ Intrusion Detection Techniques

**Signature- or  
pattern-matching  
systems**

**Protocol-  
anomaly-based  
systems**

**Statistical-  
anomaly-based  
systems**

# [ False Positives and False Negatives

---

**False positives occur when the IDS or IPS identifies something as an attack, but it is in fact normal traffic**

---

**False negatives occur when it failed to interpret something as an attack when it should have**

---

# [Anti-Malware Systems

**To remain effective, anti-malware solutions:**

- Require continual updates
- Must be monitored to ensure they are still active and effective

# [ Security Information Event Management (SIEM)

- Provide a common platform for log collection, collation, and analysis in real time
- Historical reporting capability



# [ Incident Analysis

Incident analysis focuses on understanding what constitutes an incident in the organization instead of drive-by scans, abnormal behavior, or new system configurations

# [ Response

- When an incident is detected, a containment strategy must be decided
- Containment may include:
  - Disconnecting devices from the network
  - Shutting systems down
  - Redirecting traffic

# Containment Strategy Considerations

---

**Need to preserve forensic evidence for possible legal action**

---

**Availability of services the affected component provides**

---

**Potential damage leaving the affected component in place may cause**

---

**Time required for the containment strategy to be effective**

---

**Resources required to contain the affected component**

# [ Delaying Containment

There may be legal implications if the organization knows about the compromised system and then the compromised system is used to attack another system

# [Triage

---

**An analysis of the incident must be performed to determine the overall impact**

---

**The assessed impact level of the incident dictate the actions that should be taken**

# [ Common Containment Activities

---

**Backing up the affected system**

---

**Disconnecting the affected system**

---

**Changing system, application, and user passwords**

---

**Analyzing network traffic**

---

**Modifying firewall rules**

---

**Reviewing system, application, and security logs**

---

# [ Post-Incident Activity

---

**A post-incident report should document the security incident and all recovery activities**

---

**Update incident response policy and procedures based on lessons learned**

# [ Forensics Investigations

---

**Identifying evidence**

---

**Collecting or acquiring evidence**

---

**Examining or analyzing the evidence**

---

**Presentation of findings**



# [ Criminal Behavior

- Behavior is intentional and serves to fulfill some purpose
- Computer criminals have specific MOs and leave behind signature behaviors

# [ General Guidelines

---

**All of the general forensic and procedural principles must be applied**

---

**Actions taken should not change evidence**

---

**Train people who access original digital evidence**

---

**All activity relating to digital evidence must be fully documented, preserved, and available for review**

---

**Individual is responsible for all actions taken with respect to digital evidence while it is in his possession**

# [ Five Rules of Evidence

**Be  
authentic**

**Be  
accurate**

**Be  
complete**

**Be  
convincing**

**Be  
admissible**

# [Types of Analysis

- **Media**
- **Network**
- **Software**
  - Author Identification
  - Content Analysis
  - Context Analysis
- **Hardware/Embedded Device**

# Emergency Response Plans and Procedures

---

**Have plans to recover and restore operations**

---

**Key personnel must receive training**

---

**Plans must be tested to ensure effective execution**

---

**Plans must be constantly reviewed and updated**

---

# [ Maximum Tolerable Downtime (MTD)

**Maximum amount of time that a business function can be unavailable before the organization is harmed to a degree that puts the survivability of the organization at risk**

# [ Recovery Time Objective (RTO)

**The period of time within which a business function or information system must be restored after a disruption**

# [ Recovery Point Objective (RPO)

**The point in time to which data could be restored in the event of a business continuity disruption**



# [ Business Impact Analysis (BIA)

- **Assesses impacts to an organization that would result from a business disruption**
- **Aids in the identification of critical organizational functions**
- **Helps determine recovery time objectives**

# [Stakeholder Input

**Conducting a BIA requires participation from stakeholders in all organizational business units**

- Direct interviews with stakeholders
- BIA questionnaires
- Review of organizational policies and procedures
- Reviews of organizational contractual requirements

# [ BIA Project Stages



# [ Disaster Recovery Planning

- Focuses on the restoration of IT functions after a business disruption event
- Details the steps to restore critical IT systems in the event of a disaster

# [Types of Backups

Backup Type	Data Backed Up	Time to Complete
Full Backup	All data are copied to backup media	The full system backup takes the longest time to complete
Differential Backup	A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup saves the files that are different or new since the last full backup	The differential backup takes less time than the full system backup but more time than an incremental backup
Incremental Backup	An incremental backup provides a backup of files that have changed or are new since the last incremental backup	The incremental backup is the fastest backup type to perform when compared with full and differential backups

# [ Off-Site Storage

- Backup tapes should be stored off-site at a secure location
- Ensure that they are available for restoration should the primary facility become unavailable

# [ Electronic Vaulting

---

Appliance sits at the source location

---

Collects data backups from individual systems

---

Transmits them to the vendor location

---

The backup is encrypted

---

Data backups may be restored from the electronic vault to the source system

# [ Remote Journaling

---

**Journals and database transaction logs are transmitted electronically to an offsite location**

---

**Transaction logs can then be applied against a copy of the database at the offsite location**

---

**The offsite copy can be restored quickly**



# [ Clustering

- Clustering refers to a method of configuring multiple computers so that they effectively operate as a single system
- Can be performed for:
  - High-availability
    - Active / Passive
  - Load balancing
    - Active / Active

# [ RAID Levels

---

**RAID 0 – Striped Set**

---

**RAID 1 – Data Mirroring**

---

**RAID 5 – Striped Set with Parity**

---

**RAID 10 (1+0) – Data is mirrored then striped**

# [ Testing and Drills

**Checklist  
Test**

**Structured  
Walkthrough  
Test**

**Simulation  
Test**

**Parallel Test**

**Full  
Interruption  
Test**

# [ Plan Review and Maintenance

- **Review BCPs and DRPs:**
  - On an annual basis, at a minimum
  - After significant changes
- **Ensure that the plan is continually up to date**