Incident Response
Richard Baskerville
Georgia State University

Information Security Incident

A security incident is a change of state in a bounded information system from the desired state to an undesired state, where the state change is caused by the application of a stimulus external to the system.

Common Incident Types
- Virus contamination: 64%
- Insider abuse of internet (porno, pirate, abusive email): 44%
- Laptop/mobile theft: 42%
- Misrepresented by phishing: 33%
- Unauthorized access to info: 29%
- Denial of service attacks: 29%
- Password sniffing: 17.3%
- Website Defacement: 13.5%
- System penetration: 13%
- Wireless network abuse: 7.6%

Impacts of Incidents
- Theft/Loss of customer data: 17%
- Financial fraud: 19.5%
- Theft of proprietary information: 9%
- Telecom fraud: 5%
- Average organizational loss: $234k
- Highest average losses per type of incident:
  - Wireless exploits: $770k
  - Personal data loss: $710k
  - Fraud: $450k
- Losses due to non-malicious insider actions: 60%

Team-Orientation
The Nerd SWAT Response?
- CERT - Computer Emergency Response Team
- CERT/CC - The US CERT at CMU/SEI
- CIRT - Computer Incident Response Team
- CSIRT - Computer Security Incident Response Team
- IRT - Incident Response Team
- IRC - Incident Response Capability
- IHT - Incident Handling Team
- IMT - Incident Managing / Management Team
- CIRC - Computer Incident Response Capability or Center
- SIRT - Security Incident Response Team
- SERT - Security Emergency Response Team
Corporate incident response policy = incident response “capability”.


Security Team: ad hoc, uncoordinated actions. Not a CSIRT, no organized capability.


### Preparation

- Operating systems and boot disks archive
- Security patches archive
- Reinstallation tools
- Backup procedures
- Cryptographic checksums of critical files
- Backup media
- Resource Kit
- Test systems and networks
- Audit trail

### Organizing A CSIRT

- Security Team—Using Existing IT Staff
- Internal Distributed CSIRT
- Internal Centralized CSIRT
- Combined Distributed and Centralized CSIRT
- Coordinating CSIRT

### A Capability

### CSIRT Services
Organizing An Internal CSIRT


- Security Team—Using Existing IT Staff
  - Incident handling tasks and services are conducted by the system and network administrators or other security experts who normally maintain, configure, and protect the organization’s hosts and networks. (Not a CSIRT.)
- Internal Distributed CSIRT
  - A formally recognized entity composed of staff from other divisions or sectors of the enterprise who report to a central CSIRT manager.
- Internal Centralized CSIRT
  - A dedicated, centrally located entity with full responsibility for all incident reporting, analysis, and response.

Organizing An External CSIRT


- Combined Distributed and Centralized CSIRT
  - A dedicated, centralized entity that interacts with team members who are distributed throughout the organization in various geographic sites and divisions. A centralized team provides high-level analysis and recommends recovery and mitigation strategies; providing incident, vulnerability, and artifact response support for the distributed team members and other parts of the enterprise.
- Coordinating CSIRT
  - An entity that coordinates and facilitates incident and vulnerability handling activities across a broad, diverse, and usually external constituency: sharing information, providing mitigation strategies and recommendations for incident response and recovery, researching and analyzing trends and patterns of incident activity within the constituency, providing resources and references for incident management such as vulnerability databases, clearinghouses for security tools, or advisory and alert services.

Identification

From Mitropoulos, et al. (2006)

- Audit log collection, examination and analysis
- Incident reporting and assessment
- System information
- Disk imaging of the affected system
- Other systems analysis

Alert or Escalation levels.

- Green – monitoring.
- Orange – CSIRT Alert: threat identification and categorization
- Red – General Alert: notify administrators, evidence collection and subsystems shutdown

Event Triggers


- Known or suspected intrusion or access by an unauthorized individual.
- Authorized user attempting to circumvent security procedures or elevate access privileges.
- Unexplained modifications of files, software, or programs.
- Unexplained or erratic system responses.
- Presence of suspicious files, shortcuts, or programs.
- Malware infection (for example, virus, worm, Trojan).
- Receipt of suspicious e-mail attachments, files, or links.
- Spillage incidents (for example processing or storage of information classified at a higher level than the system the file resides on, or the transmission or attempted transmission of classified information across the public Internet).
- Violations of published system secure operating procedures.

Malicious Event Indicators

From Walker (2008)

- A system alarm or similar indication from an intrusion detection tool
- Suspicious entries in system or network accounting (e.g. A UNIX user obtains root access without going through the normal sequence)
- Accounting discrepancies
- Unsuccessful login attempts
- Unexplained new user accounts
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial/disruption of service or inability of one or more users to login to an account
- Unexplained system crashes
- Poor system performance
- Operation of a program or sniffer device to capture network traffic
- “Door knob rattling” (e.g. Use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual time of usage (remember, more computer security incidents occur during non-working hours than any other time)
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- Unusual usage patterns (e.g. programs are being compiled in the account of a user who does not know how to program)
Automated Event Detection
From Walker (2008)

Sensors and Trigger Detected Malicious Events
From Walker (2008)

- Network, system, service and information reconnaissance (Profiling)
- Access to assets (Profiling)
- Illicit Data extraction (e.g. printing, write to removable media)
- Installation and control of data loggers or malicious software
- Communications Usage (e.g. P2P, VOIP, encrypted messaging, steganography)
- Changing file permissions
- Altering file content
- Erasing files/data

Baselining: Storage of Event Characteristics
From Walker (2008)

- Malicious insider event characteristics
- Enterprise management system events
- Operating system events
- Entire data stream for critical assets and services
- COTS Application transaction logs
- Event logs
- Detected vulnerabilities
- Forensic evidence
- IDS/IPS signature triggers
- Gateway inspection and filtering logs
- Anti-Malware logs
- Bespoke application logs
- CIS policy violations
- Access control logs

Triage

Triage is the process of sorting, categorizing, and prioritizing incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital where patients who need to be seen immediately are separated from those who can wait for assistance.

Incident Mitigation and Containment
From Mitropoulos (2006) and ISACA (2005)

- Disabling specific system services
- Changing of passwords and account disabling
- Network disconnection of the compromised system
- Temporary shutdown of the compromised system
- Data preservation and Forensics
- The restoration of the compromised system

Investigation
From ISACA (2005)

- Evidence collection
- Technical data
- Human and behavioral data
- Ongoing monitoring
- Legal consultation
- Engaging law enforcement
- Publicity and organizational considerations
- Identifying the perpetrator(s)
- Conducting interviews
**Eradication**

- Changing of all passwords in all compromised systems
- Complete elimination of intruder access and the dedication of possible changes
- Complete reinstallation of the compromised systems
- Systems rebuilding

**Recovery**

- System rebuilding from scratch
- Restoration of user data from trusted backups
- System configuration review and auditing
- Review of the protective and detective mechanisms

**Followup**

- Trace back
  - IP marking trace back
  - ICMP-based trace back
  - IP tunneling trace back
  - Host-based trace back
  - Application based trace back
- Forensic analysis
  - Computer forensics
  - Network forensics
  - Software forensics

**Methodology**

- ISACA (2005) Cybercrime Incident Response and Digital Forensics

**Incident Response**

Richard Baskerville

Georgia State University