Ethical Hacking and Countermeasures

Version 6

Module LVII

Computer Forensics and Incident Handling

Scenario

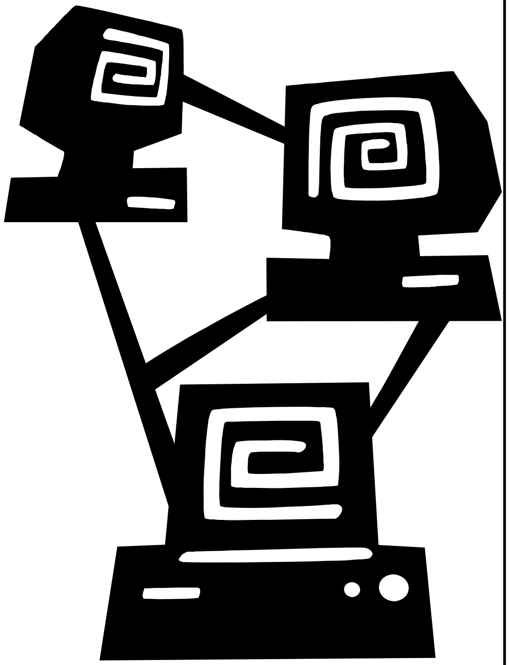
OrientRecruitmentInc is an online human resource recruitment firm. The web server of the firm is a critical link.

Neo, the network administrator sees some unusual activity that is targeted towards the web server. The web server is overloaded with connection requests from huge number of different sources.

Before he could realize the potential of the attack, the website of OrientRecruitmentInc falls prey to the much famous Denial of Service Attack.

The company management calls up the local Incident Response Team to look into the matter and solve the DoS issue.

What steps will the incident response team take to investigate the attack?

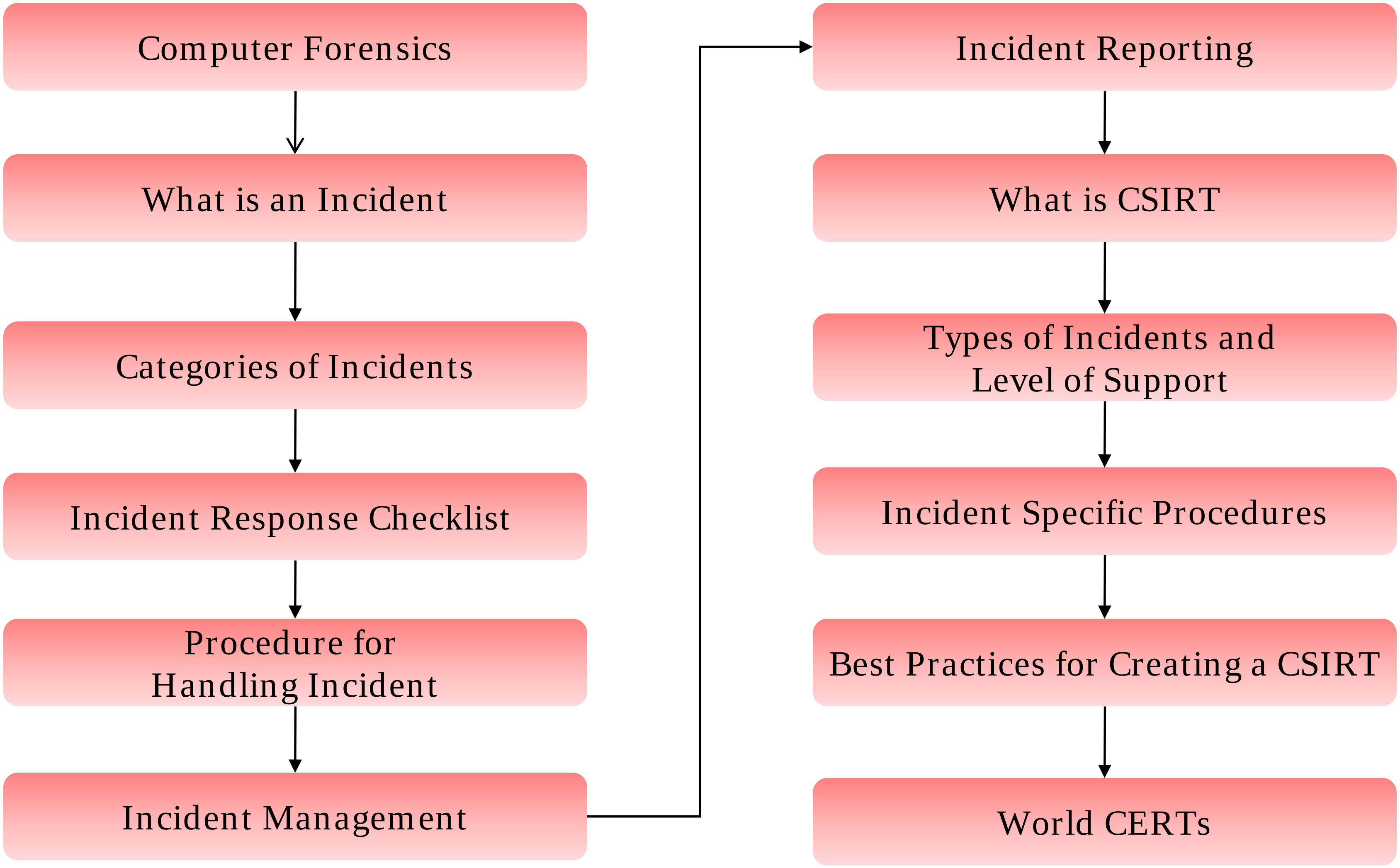


Module Objective

This module will familiarize you with:

- Computer Forensics
- What is an Incident
- Categories of Incidents
- Incident Response Checklist
- Procedure for Handlig Incident
- Incident Management
- Incident Reporting
- What is CSIRT
- Types of Incidents and Level of Support
- Incident Specific Procedures
- Best Practices for Creating a CSIRT
- World CERTs

Module Flow



Computer Forensics

What is an Incident

Categories of Incidents

Incident Response Checklist

Procedure for Handling Incident

Incident Management

Incident Reporting

What is CSIRT

Types of Incidents and Level of Support

Incident Specific Procedures

Best Practices for Creating a CSIRT

World CERTs

To Know More About Computer Forensics, Attend EC-Council's CHFI Program

Computer Forensics

What is Computer Forensics

“The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.”

"Forensic Computing is the science of capturing, processing and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.”

CEH™ Certified Ethical Hacker

Need for Computer Forensics

“Computer forensics is equivalent of surveying a crime scene or performing an autopsy on a victim”

{Source: James Borek 2001}

Presence of a majority of electronic documents

Search and identify data in a computer

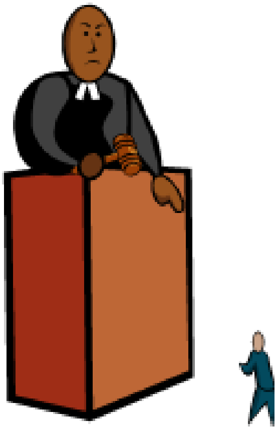
Digital Evidence can be easily destroyed, if not handled properly

For recovering Deleted, Encrypted, or Corrupted files from a system

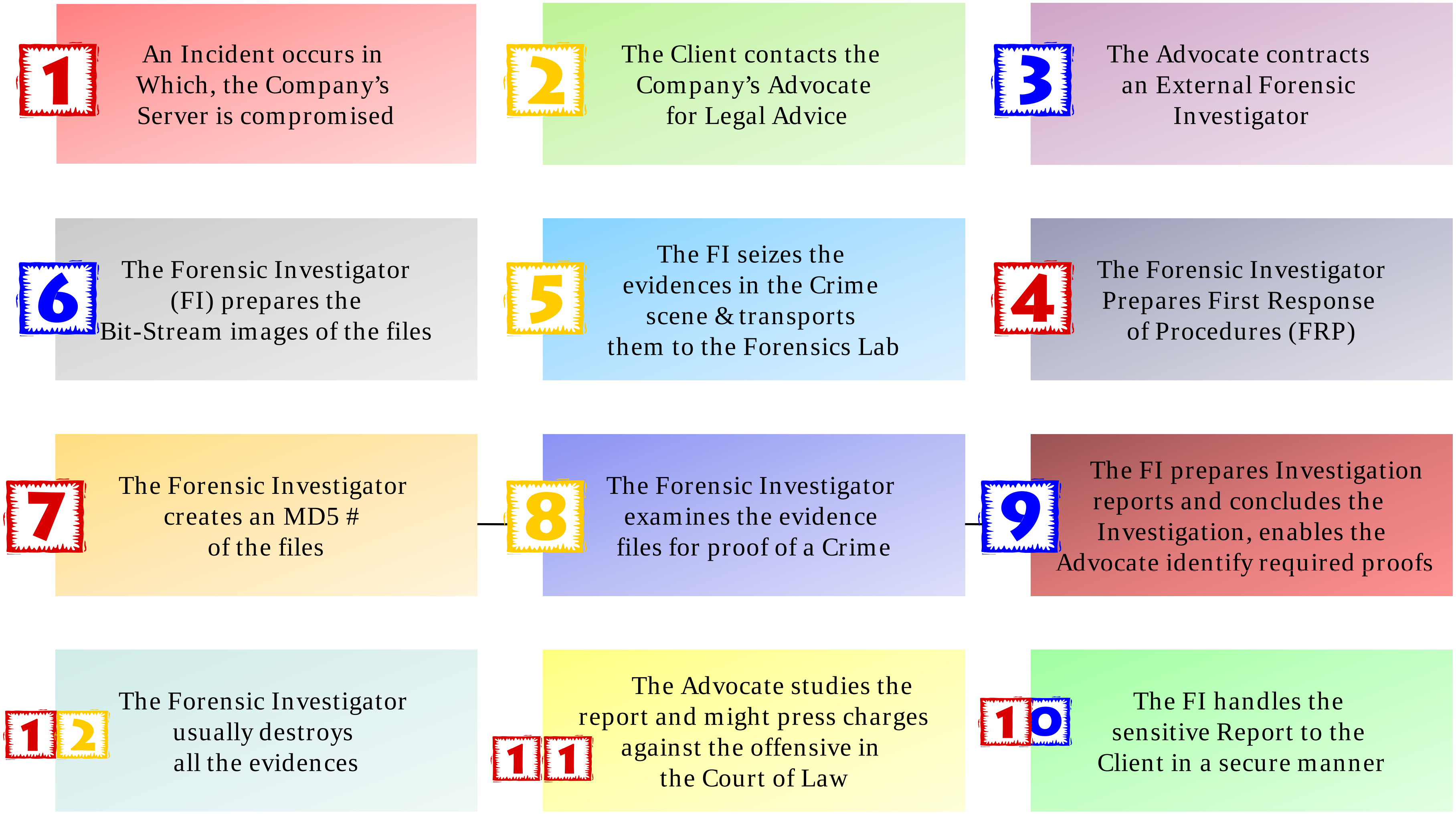
Objectives of Computer Forensics

To recover, analyze and present computer-based material in such a way that it can be **presented as evidence in a court of law**

To identify the evidence in short time, estimate potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator

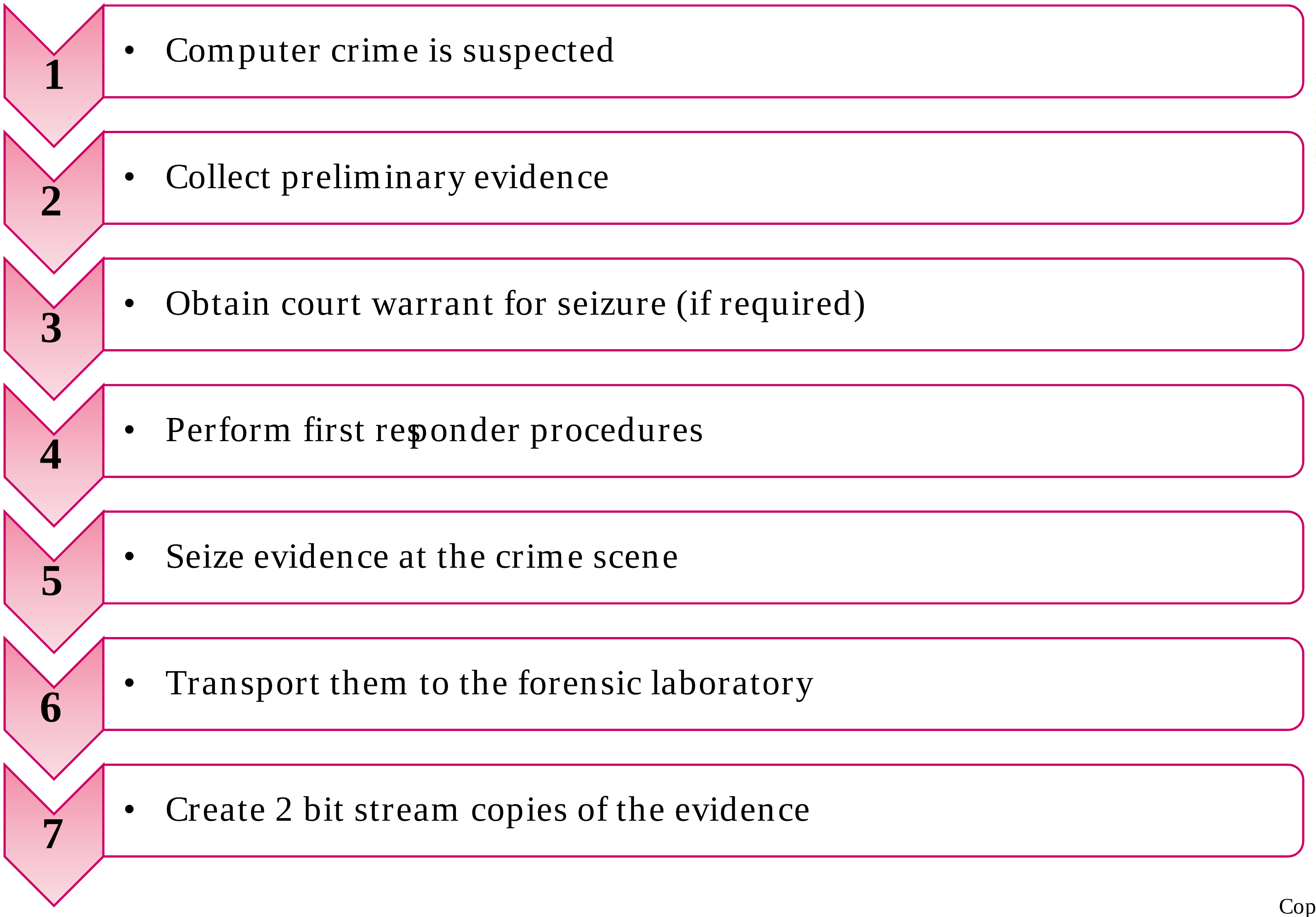


Stages of Forensic Investigation in Tracking Cyber Criminals



1. An Incident occurs in Which, the Company's Server is compromised
2. The Client contacts the Company's Advocate for Legal Advice
3. The Advocate contracts an External Forensic Investigator
4. The Forensic Investigator Prepares First Response of Procedures (FRP)
5. The FI seizes the evidences in the Crime scene & transports them to the Forensics Lab
6. The Forensic Investigator (FI) prepares the Bit-Stream images of the files
7. The Forensic Investigator creates an MD5 # of the files
8. The Forensic Investigator examines the evidence files for proof of a Crime
9. The FI prepares Investigation reports and concludes the Investigation, enables the Advocate identify required proofs
10. The FI handles the sensitive Report to the Client in a secure manner
11. The Advocate studies the report and might press charges against the offensive in the Court of Law
12. The Forensic Investigator usually destroys all the evidences

Key Steps in Forensic Investigations



1. Computer crime is suspected
2. Collect preliminary evidence
3. Obtain court warrant for seizure (if required)
4. Perform first responder procedures
5. Seize evidence at the crime scene
6. Transport them to the forensic laboratory
7. Create 2 bit stream copies of the evidence

Key Steps in Forensic Investigations (cont'd)

8
- Generate MD5 checksum on the images

9
- Prepare chain of custody

10
- Store the original evidence in a secure location

11
- Analyze the image copy for evidence

12
- Prepare a forensic report

13
- Submit the report to the client

14
- If required, attend the court and testify as expert witness

List of Computer Forensics Tools

- Helix
- Pslist
- Fport
- Psloggedon
- RegScanner
- X-Ways Forensics
- Traces Viewer
- Sleuth Kit
- SMART
- Penguin Sleuth Kit
- Process Explorer
- Autoruns
- Irfan View
- Adapterwatch
- Necrosoft Dig
- Visual TimeAnalyzer
- Evidor
- Ontrack
- Forensic Sorter
- Directory Snoop

Incident Handling

Present Networking Scenario

Increase in the number of companies venturing into e-business coupled with high Internet usage

Decrease in vendor product development cycle and product testing cycle

Increase in the complexity of Internet as a network

Alarming increase in intruder activities and tools, expertise of hackers, and sophistication of hacks

Lack of thoroughly trained professionals as compared to the number and intensity of security breaches

What is an Incident

Computer security incident is defined as “Any real or suspected adverse event in relation to the security of computer systems or computer networks”

- Source:www.cert.org

It also includes external threats such as gaining access to systems, disrupting their services through malicious spamming, execution of malicious codes that destroy or corrupt systems

Category of Incidents: Low Level

Low level incidents are the least severe kind of incidents

They should be handled within one working day after the event occurs

They can be identified when there is:

- Loss of personal password
- Suspected sharing of organization’s accounts
- Unsuccessful scans and probes
- Presence of any computer virus or worms

C|EH™ Certified Ethical Hacker

Category of Incidents: Mid Level

The incidents at this level are comparatively more serious and thus, should be handled the same day the event occurs

They can be identified by observing:

- Violation of special access to a computer or computing facility
- Unfriendly employee termination
- Unauthorized storing and processing data
- Destruction ofproperty related to a computer incident (less than $100,000)
- Personal theft of datarelated to computer incident($100,000)
- Computer virus or worms of comparatively larger intensity Illegal access to buildings

Category of Incidents: High Level

These are the most serious incidents and are considered as "Major" in nature

High level incidents should be handled immediately after the incident occurs

These include:

- Denial of Service attacks
- Suspected computer break-in
- Computer virus or worms of highest intensity; e.g.Trojan back door
- Changes to system hardware,firmware, or software without authentication
- Destruction of property exceeding $100,000
- Personal theft exceeding $100,000 and illegal electronic fund transfer or download/sale
- Any kind of pornography, gambling, or violation ofany law

How to Identify an Incident

A system alarm from an intrusion detection tool indicating security breach

Suspicious entries in a network

Accounting gaps of several minutes with no accounting log

Other events like unsuccessful login attempts, unexplained new user or files, attempts to write system files, modification, or deleting of data

Unusual usage patterns, such as programs being compiled in the account of users who are non-programmers

How to Prevent an Incident

A key to preventing security incidents is to eliminate as many vulnerabilities as possible

Intrusions can be prevented by:

- Scanning the network/ system for security loopholes
- Auditing the network/ system
- Deploying Intrusion Detection/ Prevention Systems on the network/ system
- Establishing Defense-in-Depth
- Securing Clients for Remote Users

Defining the Relationship between Incident Response, Incident Handling, and Incident Management

Figure 2 illustrates the relationship between the terms incident response, incident handling, and incident management. Incident response is one of the functions performed in incident handling; incident handling is one of the services provided as part of incident management.

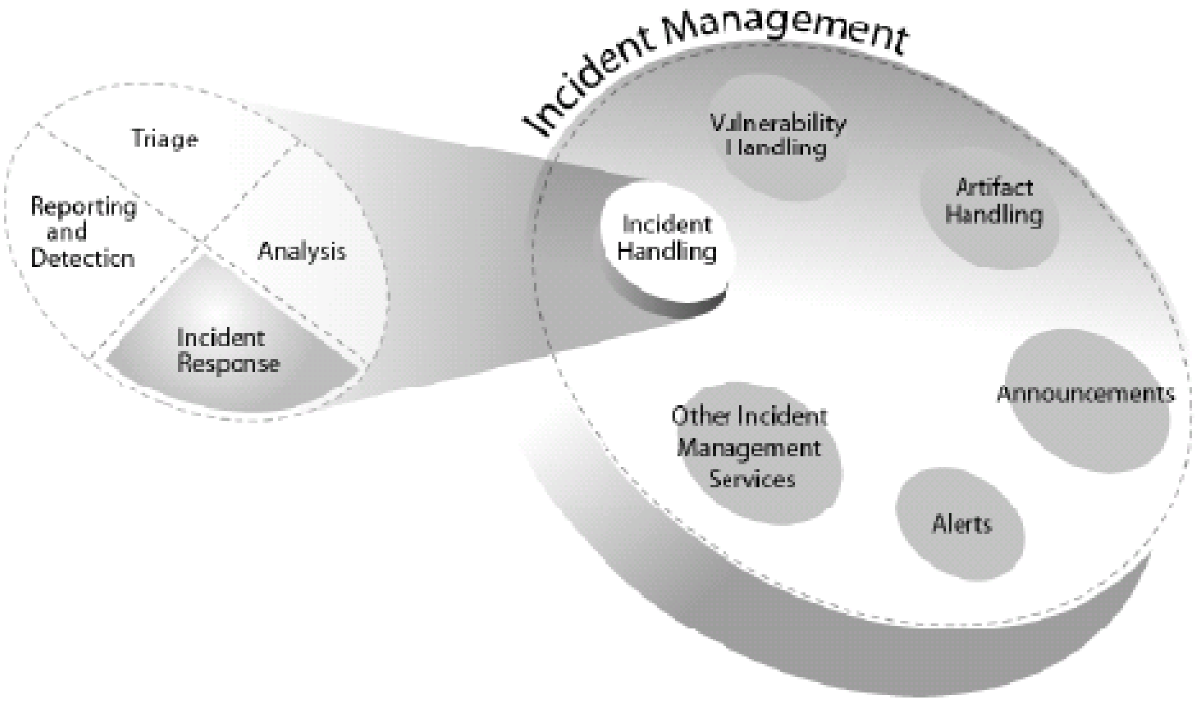


Figure 2: Defining the Relationship between Incident Response, Incident Handling, and Incident Management

Incident Response Checklist

Potential Incident Verified

Contact department/ agency security staff

- I.T. Manager -
- [designee/ others by department procedure] -

Security designee will contact CSIRT member

- Call 802-250-0525 (GOVnet Beeper)
  - GOVnetwill then contact CSIRT members (csirt@.state.vt.us)
  - If no response within ten minutes call the Office of the CIO

Isolate system(s) from GOVnet [unless CSIRT decision is to leave the system connected to monitor active hacker]

Begin a log book - who/ what / when / where

Identify the type of Incident - Virus, worm, and hacker

Preliminary estimation of extent of problem, number of systems

Incident Response Checklist (cont’d)

Contact local police authority with jurisdiction at location of incident (This MUST BE coordinated with CSIRT)

Follow server/ operating system specific procedures to snapshot the system

Inoculate/ restore the system

Close the vulnerability and ensure that all patches have been installed

Return to normal operations

Prepare report and conduct follow-up analysis

Revise prevention and screening procedures

Remember to log all actions!

Handling Incidents

Incident handling helps to find out trends and patterns regarding intruder activity by analyzing it

It involves three basic functions:

- Incident reporting,
- Incident analysis, and
- Incident response

It recommends network administrators for recovery, containment, and prevention to constituents

It allows incident reports to be gathered in one location so that exact trends and pattern can be recognized and recommended strategies can be employed

It helps the corresponding staffs to understand the process of responding and to tackle unexpected threats and security breaches

Procedure for Handling Incident

The incident handling process is divided into six stages

These stages are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up

Stage 1: Preparation

Preparation enables easy coordination among staff

Create a policy

Develop preventive measures to deal with threats

Obtain resources required to deal with incidents effectively

Develop infrastructure to respond and support activities related to incident response

Select team members and provide training

EC-Council

Stage 2: Identification

Identification involves validating, identifying, and reporting the incident

Determining the symptoms given in ‘how to identify an incident’

Identifying the nature of the incident

Identifying events

Protecting evidence

Reporting events

Stage 3: Containment

Containment limits the extent and intensity of an incident

It avoids logging as root on the compromised system

Avoid conventional methods to trace back as this may alert the attackers

Perform the backup on the system to maintain the current state of the system for facilitating the post-mortem and forensic investigation later

Change the system passwords to prevent the possibility of Spywares being installed

Stage 4: Eradication

Investigate further to uncover the cause of the incident by analyzing system logs of various devices such as firewall, router, and host logs

Improve defenses on target host such as:

- Reloading of a new operating system
- Enabling firewalls
- Assigning new IP address

Install all the latest patches

Disable any unnecessary services

Install anti-virus software

Apply the Company’s security policy to the system

Stage 5: Recovery

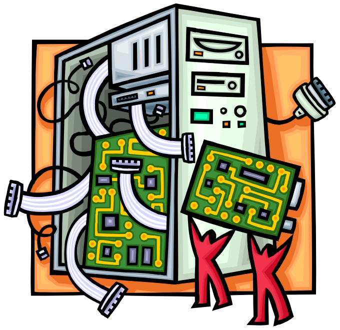
Determine the course of actions

Monitor and validate systems

Determine integrity of the backup itself by making an attempt to read its data

Verify success of operation and normal condition of system

Monitor the system by network loggers, system log files, and potential back doors



Stage 6: Follow-up

Post-mortem analysis:

- Perform a detailed investigationof the incident to identify the extent of the incident and potential impact prevention mechanisms

Revise policies and procedures from the lessons learned from the past

Determine the staff time required and perform the following cost analysis:

- Extent to which the incidents disrupted the organization
- Data lost and its value
- Damaged hardware and its cost

Stage 6: Follow-up (cont'd)

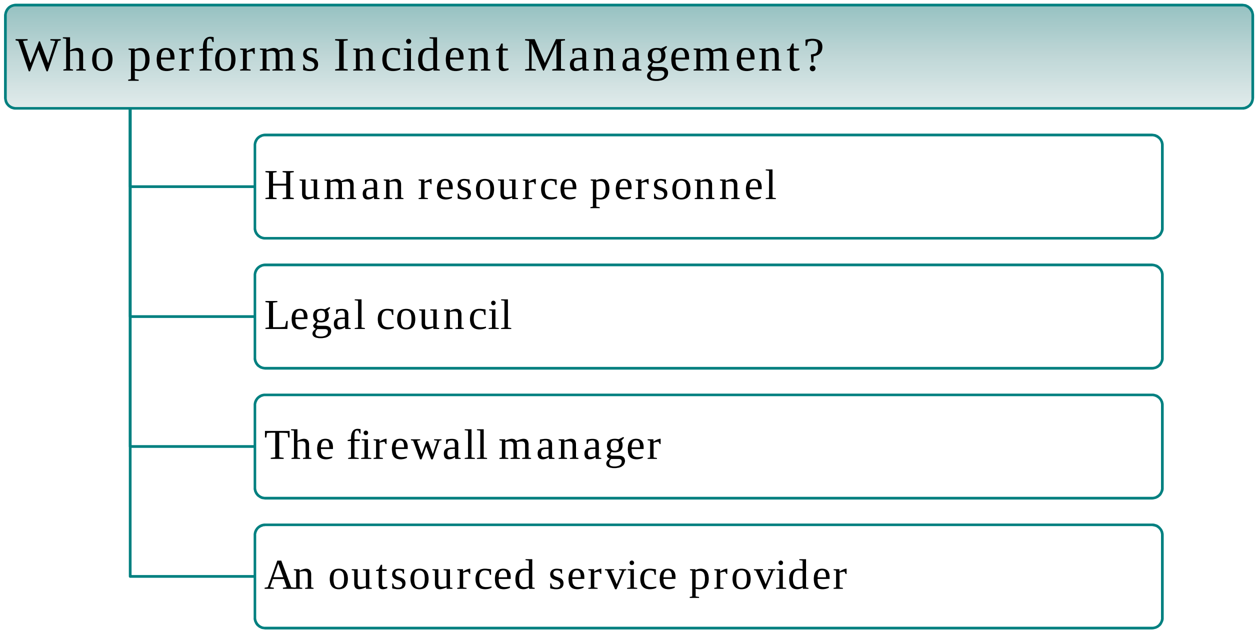
Document the response to incident by finding answers to the following:

- Was the preparation for the incident sufficient?
- Whether the detection occurred promptly or not, and why?
- Using additional tools could have helped or not?
- Was the incident contained?
- What practical difficulties were encountered?
- Was it communicated properly?

Incident Management

Incident management is not just responding to an incident when it happens but includes proactive activities that help prevent incidents by providing guidance against potential risks and threats

Includes the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency

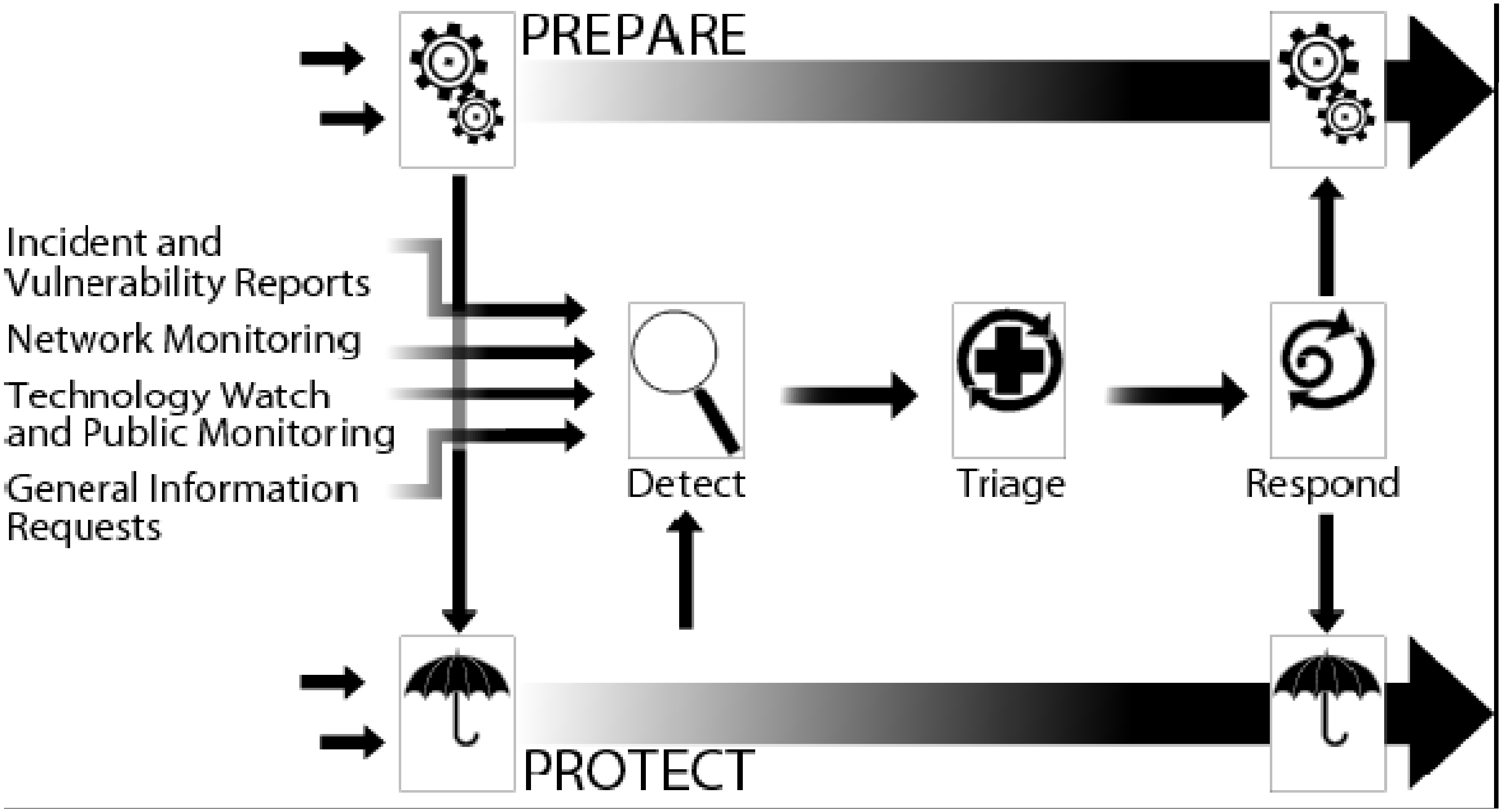


Who performs Incident Management?

- Human resource personnel
- Legal council
- The firewall manager
- An outsourced service provider

Incident Management (cont'd)

Figure : Five High-Level Incident Management Processes


PREPARE
Incident and Vulnerability Reports
Network Monitoring
Technology Watch and Public Monitoring
General Information Requests
Detect
Triage
Respond
PROTECT

Source: *www.cert.org/archive/pdf/04tr015.pdf*

Why don't Organizations Report Computer Crimes

Misunderstanding the scope of the problem

- This does not happen to other organizations

Proactive reporting and handling of the incident will allow many organizations to put their spin on the media reports

Potential loss of customers

Desire to handle things internally

Lack of awareness of the attack

Estimating Cost of an Incident

Tangible: Can be quantified

- Lost productivity hours
- Investigation and recovery efforts
- Loss of business
- Loss or theft of resources

Intangible: More difficult to identify and quantify

- Damage to corporate reputation
- Loss of goodwill
- Psychological damage
  - Those directly impacted may feel victimized
  - May impact morale or initiate fear
- Legal liability
- Effect on shareholder value

EC-Council

Whom to Report an Incident

Incident reporting is the process of reporting the information regarding the encountered security breach in a proper format

The incident should be reported to the CERT Coordination center, site security manager, or other sites

It can also be reported to law enforcement agencies such as FBI,USSS Electronic crimes branch, or Department of Defense Contractors

It should be reported to receive technical assistance and to raise security awareness to minimize the losses

Incident Reporting

When a user encounters any breach, report the following:

- Intensity the security breach
- Circumstances, which revealed the vulnerability
- Shortcomings in the design and impact or level of weakness
- Entry logs related to intruder’s activity
- Specific help needed should be clearly defined
- Correct time-zone of the region and synchronization information of the system with a National time server via NTP

Vulnerability Resources

US-CERT Vulnerability Notes Database:

- Descriptions of these vulnerabilitiesare available from this web page in a searchable database format, and are published as "US-CERT Vulnerability Notes".

NVD (National Vulnerability Database):

- Integrates all publicly available U.S.Government vulnerability resources and provides references to industry resources

CVE (Common Vulnerabilities and Exposures List):

- List or dictionary of publicly known information security vulnerabilities and exposures international in scope and free for public use

OVAL (Open Vulnerability Assessment Language):

- A three-leveled vulnerability handling method consisting of a characteristics schema for collecting configuration data from systems for testing

What is CSIRT

Computer Security Incident Response Team (CSIRT): Incident Response Services 24x7

- CSIRT provides 24x7 Computer Security Incident Response Services to any user, company, government agency or organization
- CSIRT provides a reliable and trusted single point of contact for reporting computer security incidents worldwide
- CSIRT provides the means for reporting incidents and for disseminating important incident-related information

EC-Council

CSIRT: Goals and Strategy

CSIRT's goals:

- To organize the management of security problems by taking a proactive approach to our customers' security vulnerabilities and by responding effectively to potential information security incidents
- To minimize and control the damage
- To provide or assist with effective response and recovery
- To help prevent future events

Strategy of CSIRT:

- It provides a single point of contact for reporting local problems
- It identifies and analyzes what has happened including the impact and threat
- It researches solutions and mitigation strategies
- It shares response options, information, and lessons learned

Why an Organization needs an Incident Response Team

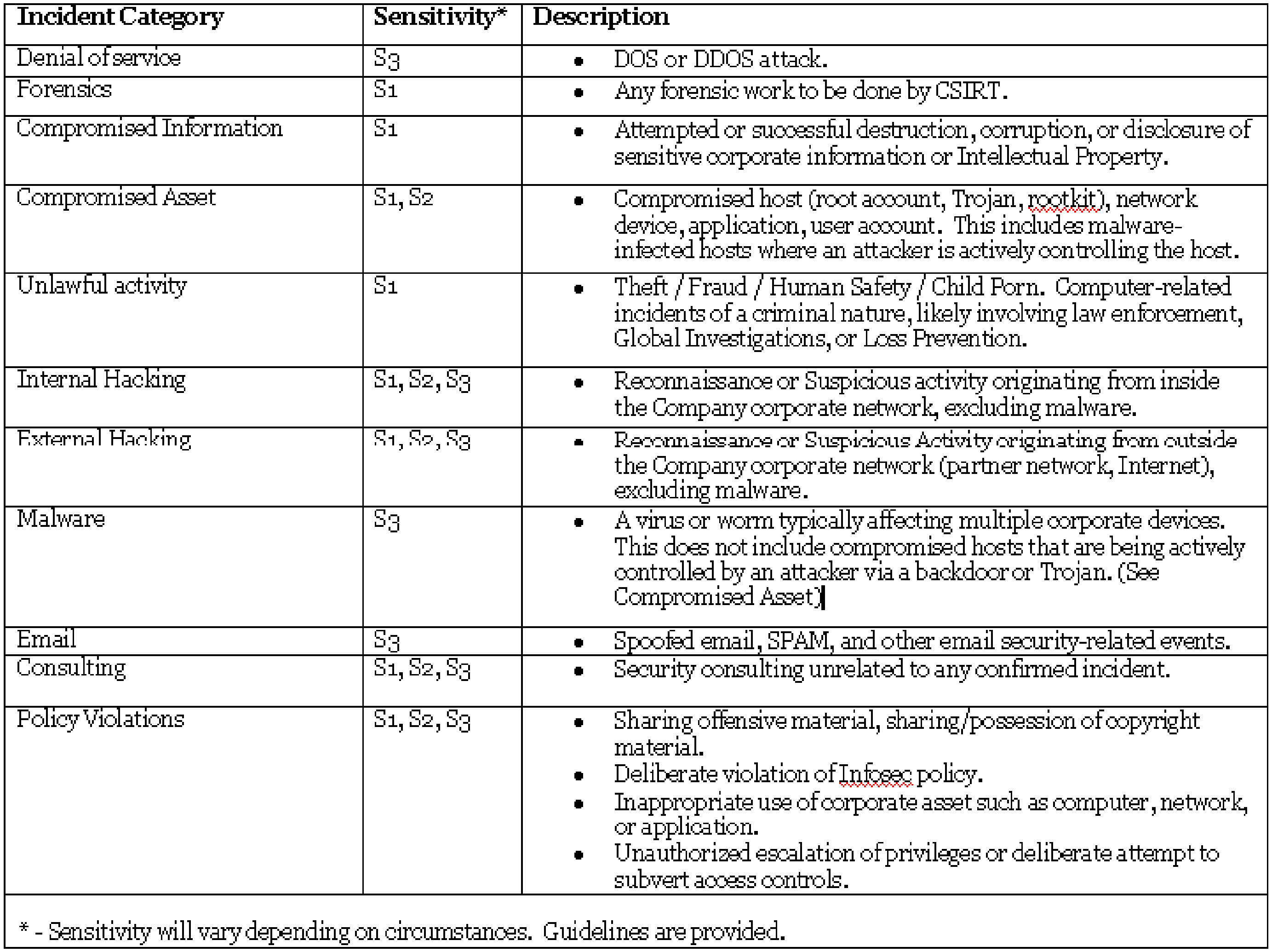
Incident Response Team helps organizations to recover from computer security breaches and threats

It is a formalized team that performs incident response work as its major job function

As an ad-hoc team, it is responsible for ongoing computer security incident

CSIRT Case Classification

Incident Categories: All incidents managed by the CSIRT should be classified into one of the categories listed in the table below



Incident Category	Sensitivity*	Description
Denial of service	S3	- DOS or DDOS attack.
Forensics	S1	- Any forensic work to be done by CSIRT.
Compromised Information	S1	- Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	- Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	- Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	- Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	- Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	- A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	- Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	- Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	- Sharing offensive material, sharing/possession of copyright material. - Deliberate violation of Infosec policy. - Inappropriate use of corporate asset such as computer, network, or application. - Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

* - Sensitivity will vary depending on circumstances. Guidelines are provided.

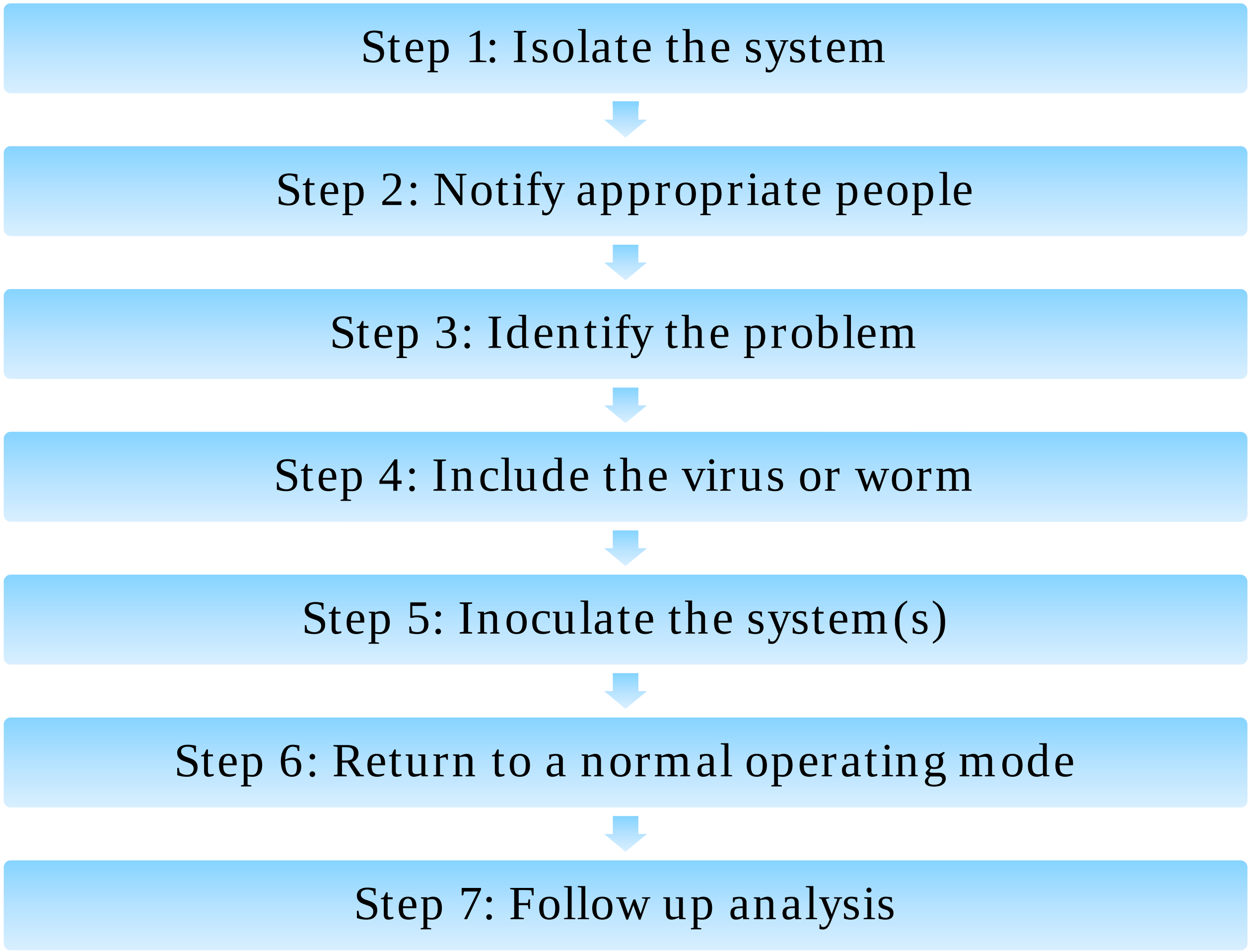
Source: *http://www.first.org/resources/guides/csirt_case_classification.html*

Types of Incidents and Level of Support

The Computer Security Incident Response Team will assign resources according to the following priorities, listed in the decreasing order:

- Threats to the physical safety of human beings
- Root or system-level attacks on any machine either multi-user or dedicated-purpose
- Compromise restricted confidential service accounts or software installations, in particular those with authorized access to confidential data
- Denial of service attacks on any of the above two items
- Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks, and destructive virus outbursts
- Compromise of individual user accounts, i.e. unauthorized access to a user or service account
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. Netnews and e-mail forgery, unauthorized use of IRC bots
- Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent

Incident Specific Procedures-I (Virus and Worm Incidents)



Step 1: Isolate the system

Step 2: Notify appropriate people

Step 3: Identify the problem

Step 4: Include the virus or worm

Step 5: Inoculate the system(s)

Step 6: Return to a normal operating mode

Step 7: Follow up analysis

Log all actions in every phase*

EC-Council

Incident Specific Procedures-II (Hacker Incidents)

(A) Attempted Probes into a State of Vermont System

- Step 1: Identify the problem
- Step 2: Notify appropriate people
- Step 3: Identify the Hacker
- Step 4: Notify CERT
- Step 5: Follow up analysis

(B) Active Hacker Activity

- Step 1: Notify Appropriate People
- Option 1: Removal ofHacker from the system
  - Step 2: Snap-shot the System
  - Step 3: Lock out the Hacker
  - Step 4: Restore the System
  - Step 5: Notify other Agencies
  - Step 6: Follow up Analysis
- Option 2: Monitoring of Hacker Activity

(C) Evidence of Past Incidents

Log all actions in every phase*

EC-Council

Incident Specific Procedures-III (Social Incidents, Physical Incidents)

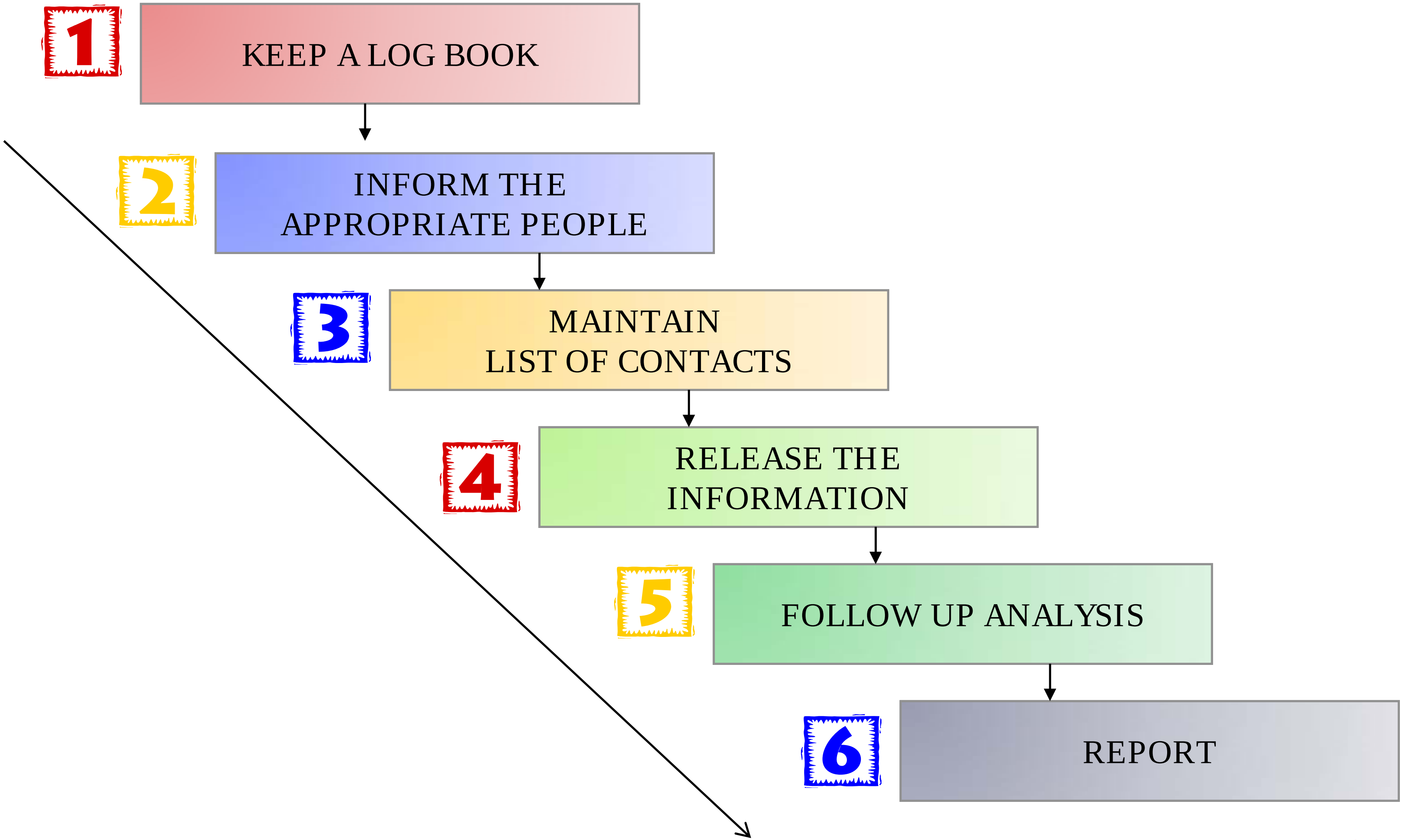
Social Incidents:

- Step 1: Identify Potential Risk
- Log all actions*

Physical Incidents:

- Step 2: Notify Appropriate People
- Log all actions*

How CSIRT Handles Case: Steps



1 KEEP A LOG BOOK

2 INFORM THE APPROPRIATE PEOPLE

3 MAINTAIN LIST OF CONTACTS

4 RELEASE THE INFORMATION

5 FOLLOW UP ANALYSIS

6 REPORT

Example of CSIRT

Internal CSIRT provides services to their parent organization such as bank, manufacturing company, university, or any government agencies

National CSIRT provides services to the entire nation example being Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

Analysis Centers synthesize data, determine trends, and patterns in an incident activity to predict future activity or provide early warnings

Vendor teams identify vulnerabilities in software and hardware products

Incidents Response Providers offer services to paid clients

Best Practices for Creating a CSIRT

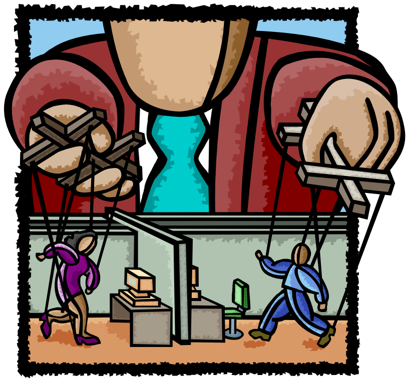
1. Obtain management support and buy-in
2. Determine the CSIRT strategic plan
3. Gather relevant information
4. Design the CSIRT vision
5. Communicate the CSIRT vision and operational plan
6. Begin CSIRT implementation
7. Announce the operational CSIRT

Step 1: Obtain Management Support and Buy-in

Without management approval and support, creating an effective incident response capability can be extremely difficult and problematic

Once the team is established, how is it maintained and expanded with budget, personnel, and equipment resources?

Will the role and authority of the CSIRT continue to be backed by management across the various constituencies or parent organization?



Step 2: Determine the CSIRT Development Strategic Plan

Are there specific timeframes to be met? Are they realistic, and if not, can they be changed?

Is there a project group? Where do the group members come from?

How do you let the organization know about the development of the CSIRT?

If you have a project team, how do you record and communicate the information you are collecting, especially if the team is geographically dispersed?

Step 3: Gather Relevant Information

Meet with key stakeholders to discuss the expectations, strategic direction, definitions, and responsibilities of the CSIRT

The stakeholders could include:

- Business managers
- Representatives from IT
- Representatives from the legal department
- Representatives from human resources
- Representatives from public relations
- Any existing security groups, including physical security
- Audit and risk management specialists

Step 4: Design your CSIRT Vision

In creating your vision, you should:

- Identify your constituency: Who does the CSIRT support and service?
- Defineyour CSIRT mission, goals, and objectives: What does the CSIRT do for the identified constituency?
- Select the CSIRT services to provideto the constituency (or others): How does the CSIRT support its mission?
- Determine the organizational model: How is the CSIRT structured and organized?
- Identify required resources: What staff, equipment, and infrastructure is needed to operate the CSIRT?
- Determine your CSIRT funding: How is the CSIRT funded for its initial startup and its long-term maintenance and growth?

Step 5: Communicate the CSIRT Vision

Communicate the CSIRT vision and operational plan to management, constituency, and others who need to know and understand its operations

As appropriate, make adjustments to the plan based on their feedback

Step 6: Begin CSIRT Implementation

Hire and train initial CSIRT staff

Buy equipment and build any necessary network infrastructure to support the team

Develop the initial set of CSIRT policies and procedures to support your services

Define the specifications for and build your incident-tracking system

Develop incident-reporting guidelines and forms for your constituency

CEH™ Certified Ethical Hacker

Step 7: Announce the CSIRT

When the CSIRT is operational, announce it to the constituency or parent organization

It is best if this announcement comes from sponsoring management

Include the contact information and hours of operation for the CSIRT in the announcement

This is an excellent time to make the CSIRT incident-reporting guidelines available

World CERTs

http://www.trusted-introducer.nl/teams/country.html

Asia Pacific CERTs

- Australia CERT (AUSCERT)
- Hong Kong CERT (HKCERT/CC)
- Indonesian CSIRT (ID-CERT)
- Japan CERT-CC (JPCERT/CC)
- Korea CERT (CERT-KR)
- Malaysia CERT (MyCERT)
- Pakistan CERT(PakCERT)
- Singapore CERT (SingCERT)
- Taiwan CERT (TWCERT)
- China CERT (CNCERT/CC)

North American CERTs

- CERT-CC
- US-CERT
- Canadian Cert
- Cancert
- Forum of Incident Response and Security Teams
- FIRST

World CERTs (cont'd)

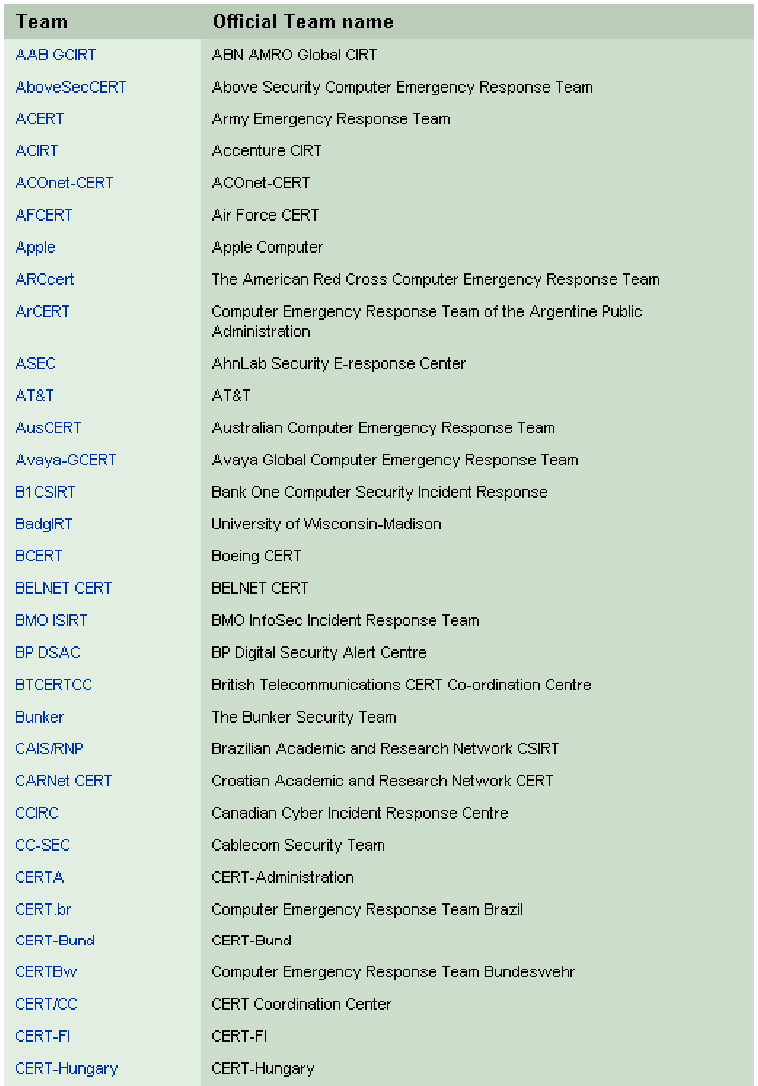
South American CERTs

- CAIS
- CAIS- Brazilian Research Network CSIRT
- NIC BR Security Office Brazilian CERT
- NBS

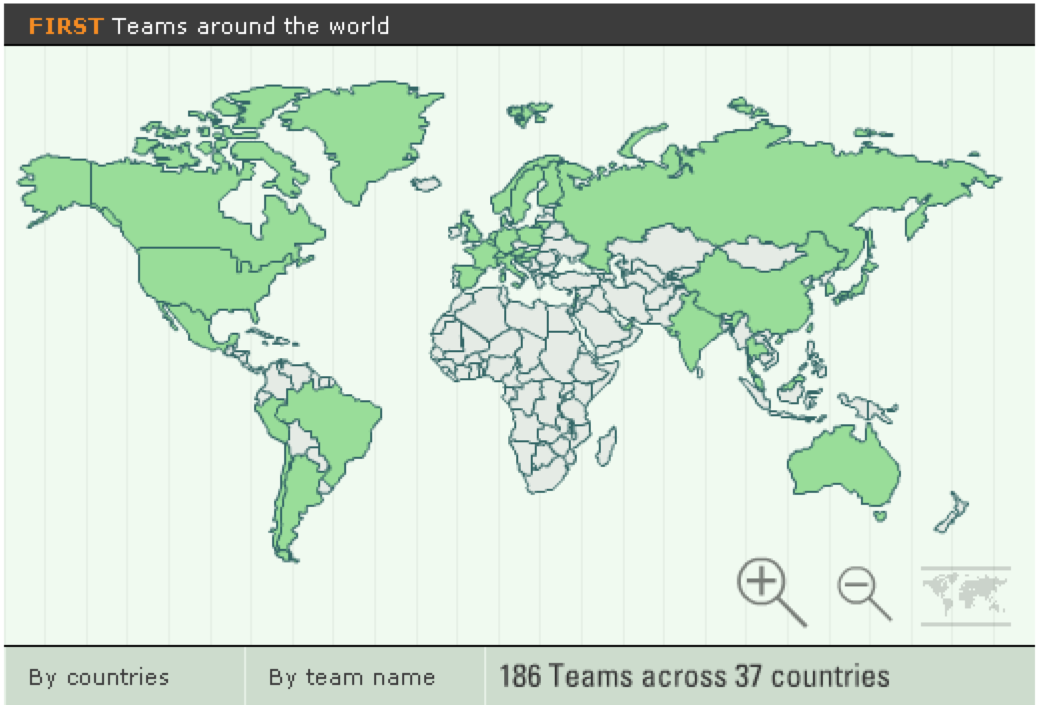
European CERTs

- EuroCERT
- FUNET CERT
- CERTA
- DFN-CERT
- JANET-CERT
- CERT-NL
- UNINETT-CERT
- CERT-NASK
- Swiss Academic and Research Network CERT

http://www.first.org/about/organization/teams/



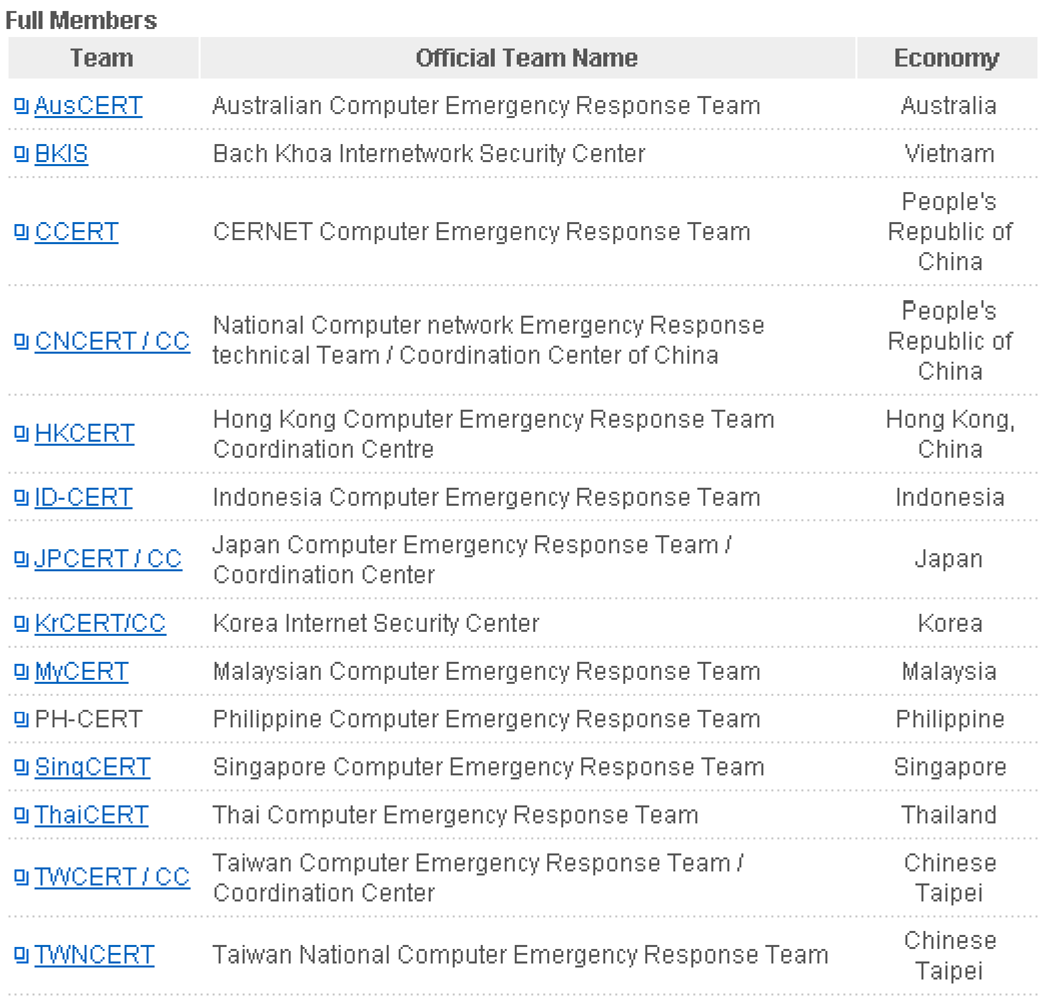
Team	Official Team name
AAB GCIRT	ABN AMRO Global CIRT
AboveSecCERT	Above Security Computer Emergency Response Team
ACERT	Army Emergency Response Team
ACIRT	Accenture CIRT
ACOnet-CERT	ACOnet-CERT
AFCERT	Air Force CERT
Apple	Apple Computer
ARCcert	The American Red Cross Computer Emergency Response Team
ArCERT	Computer Emergency Response Team of the Argentine Public Administration
ASEC	AhnLab Security E-response Center
AT&T	AT&T
AusCERT	Australian Computer Emergency Response Team
Avaya-GCERT	Avaya Global Computer Emergency Response Team
B1CSIRT	Bank One Computer Security Incident Response
BadgIRT	University of Wisconsin-Madison
BCERT	Boeing CERT
BELNET CERT	BELNET CERT
BMO ISIRT	BMO InfoSec Incident Response Team
BP DSAC	BP Digital Security Alert Centre
BTCERTCC	British Telecommunications CERT Co-ordination Centre
Bunker	The Bunker Security Team
CAIS/RNP	Brazilian Academic and Research Network CSIRT
CARNet CERT	Croatian Academic and Research Network CERT
CCIRC	Canadian Cyber Incident Response Centre
CC-SEC	Cablecom Security Team
CERTA	CERT-Administration
CERT.br	Computer Emergency Response Team Brazil
CERT-Bund	CERT-Bund
CERTBw	Computer Emergency Response Team Bundeswehr
CERT/CC	CERT Coordination Center
CERT-FI	CERT-FI
CERT-Hungary	CERT-Hungary



FIRST Teams around the world

186 Teams across 37 countries

http://www.apcert.org/about/structure/members.html



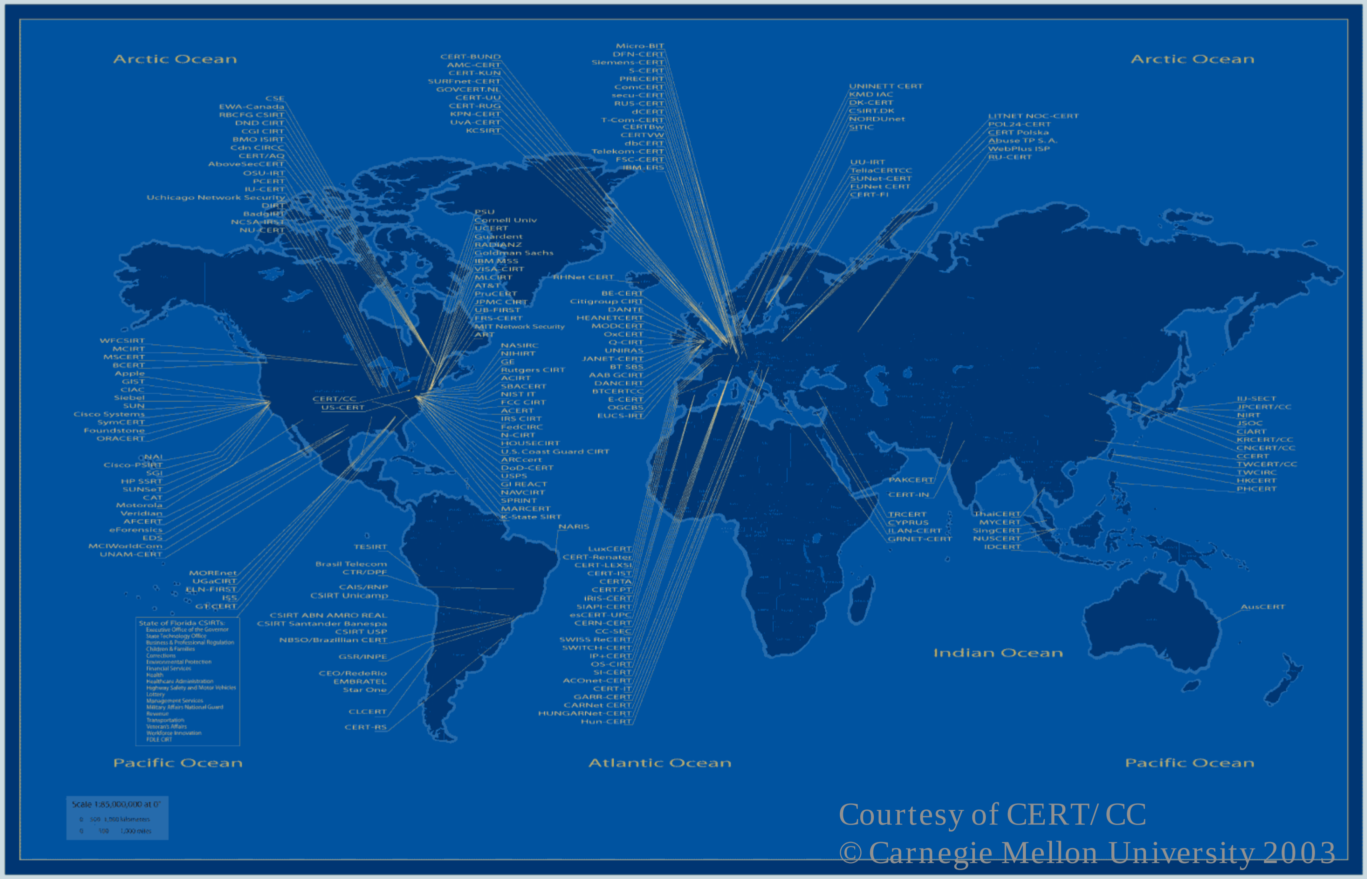
Full Members

Team	Official Team Name	Economy
AusCERT	Australian Computer Emergency Response Team	Australia
BKIS	Bach Khoa Internetwork Security Center	Vietnam
CCERT	CERNET Computer Emergency Response Team	People's Republic of China
CNCERT / CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
JPCERT / CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PH-CERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
ThaiCERT	Thai Computer Emergency Response Team	Thailand
TWCERT / CC	Taiwan Computer Emergency Response Team / Coordination Center	Chinese Taipei
TWNCERT	Taiwan National Computer Emergency Response Team	Chinese Taipei

IRTs Around the World

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



Courtesy of CERT/ CC
© Carnegie Mellon University 2003

Summary

Increase in the number of products and relative increase in the number of hacking tools has put security in the spotlight

Computer security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks

Handling Incidents involves three basic functions: incident reporting, incident analysis, and incident response

Incident reporting is the process of reporting the information regarding the encountered security breach in a proper format

CSIRT provides rapid response to maintain the security and integrity of the systems

Without management approval and support, creating an effective incident response capability can be difficult and problematic

"When did the computer start writing itself a paycheck?"

"Today at work, I received 650 E-mails from feedme@homecat.com! Was that *you?*"