UNIT III

➨Introduction to Traditional Computer Crime

3.1.1. Introduction

- The first recorded cyber crime took place in the year 1820
- The first spam email took place in 1978 when it was sent over the Arpanet
- The first VIRUS was installed on an Apple computer in 1982

Computer forensics involves the activity of obtaining and analyzing digital information in addition to preserving and documenting it for use as evidence in civil, criminal, or administrative cases.

- The goal of computer forensics is to
  - Do a structured investigation
  - Find out exactly what happened on a digital system
  - Who was responsible for it

3.1.2. Computer Crime:

Computer crime is any criminal offense, activity or issue that involves computers. In computer crime the identification of actual location is difficult. The lack of physical location has created a variety of issues. The absence of international guidelines for cyber-activity adds further more hurdles. International cooperation is necessary to proceed with the criminal investigation. Some examples of computer crime are Child pornography, threatening letters, e-mail spam or harassment, extortion, fraud and theft of intellectual property, embezzlement etc. All computer crimes leave digital tracks.

- Three general categories of computer crime
  - Target- Computer itself is a target of a crime (victim)
  - Mean - Computer is used to commit a crime
  - Incidental - Computer as part of crime
- Computer crime can be launched
  - Against Person
    - Harassment via emails, cyber stalking, email spoofing, carding,
  - Against Property
    - Trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information
  - Against Government
    - Cyber Terrorism, Damaging critical information infrastructures

- Investigation into these types of crimes include
  - Searching computers that are suspected of being involved in illegal activities
    - Discovering data on computer system

    - Recovering deleted, encrypted, or damaged file information
    - Monitoring live activity
    - Detecting violations of corporate policy
- Analysis of gigabytes of data looking for specific keywords
- Examining log files to see what happened at certain times

3.1.3 Traditional computer crime

- Phreakers
- Hacking
- Computer as commodities
- Theft of Intellectual Property

1. Phreakers

Phreakers are yesterday's hacker. Phreakers are the forefather of today's computer hackers. They are attracted by the economical benefits or by the challenges. Preaking- telecommunication fraud - involves the manipulation of telecommunication carriers to gain knowledge of telecommunications. In addition to this Preaking also involves the theft of application services. It is an action of hacking through phone calls, manipulating the access code, access tones, switches etc. An approach to select access code is war-dialing where random numbers are generated and test unitill one is successful. Phreakers would build "Bridges", illegal conference calls which involving numerous individuals around the world. The conference call is billed to someone else who was not the part of the call. Another way to gain illegal access is to use blue boxes. Blue boxes are device that is used to trick and gain access to long distance line. The use of phreaking is illegal.

2. Hacking

Hacking is an illegal intrusion or unauthorized access to or control over a computer system and/or network. Hackers use computer to gain access to unauthorized data or information. Computers are intended target of a criminal or computer may represent cybercrime in a form. The range of hacking activity involves snooping neighbour computer to search top secret government database with the intension of causing destruction.

- Contemporary Motivation

  There are six primary motivations

    - *BORDEM - Informational Voyeurism*
    - *INTELLECTUAL CHALLENGE - Mining of Knowledge (Pure Hackers)*
    - *REVENGE- Insider, Employees*
    - *SEXUAL GRATIFICATION - Stalking, Harassment*
    - *ECONOMIC – Criminal*
    - *POLITICAL - Spies, Terrorist*

- Hierarchy of Contemporary Cyber-Criminals

  Four general categories of cyber criminals

  1. Script Kiddies

  Script kiddies are also known as Skidiots, Skiddie, Victor Skill Deficiency (VSD). Script Kiddies are those who uses existing computer scripts or codes to hack into computers or exploit security vulnerabilities. They lack the expertise to write their own programs or even they do not fully understand the program that they are executing. They range from simple pranks to criminal profiting by capturing bank account.

  2. Cyber Punks

  These are individual's intent on wreaking havoc via internet. It includes vandalism, running destructive programs and general mischief for no economical gain.

  3. Hacker/Crackers

  Sophisticated computer criminals capable of writing code and breaching complex systems are known as Hackers or Crackers. A hacker identifies and exploits the system vulnerabilities but has no economical motivation. Crackers employ their knowledge for personal gain. They are criminal hackers.

  4. Cyber Criminal organization

  Group of criminal minded individual. They use internet to communicate, collaborate and facilitate cyber crime. Their activities are associated with political extreme or economical gain.

3. Computer as commodities

The theft of computer hardware is increasing as the components are becoming smaller and valuable. Similarly software copyright violation is neglected.

Hardware components are more worthy. Computers that are publicly available are vulnerable to theft and difficult to trace. Illegal hardware trade is felicitated by Black Market, Gray market, Internet based auction. Black market dealers are the most organized group involved in trafficking stolen computer components. They select their target to steel only after receiving the order. Gray market dealers are legitimate business with illegal practice of buying from thieves. The internet auctions from its part have increased the possibility of marketing the stolen hardware's as legitimate.

4. Theft of Intellectual Property

Software Piracy is the unauthorized copying of software. Data piracy is the illegal reproduction, distribution and use of software without permission or authorization of the copyright owner of the data. Most retail programs are licensed for use just at one computer or by one user who becomes the licensed user of the program and not the owner. The licensed user are given permission to make copy for backup purpose. Many individuals make multiple copies for personal use or to distribute to their friends against law. They don't even recognize the illegality of their actions. This is due to lack of knowledge regarding software licensing. It is impossible to stop piracy. One solution trying to stop software piracy is Shareware – pay on monthly basis and use.

- ➨ Piracy Identification
    - ➨ Counterfeit hologram
    - ➨ Absence of reserve label and polygraphic packing
    - ➨ Absence of Copyright and adjacent Rights protection sign
    - ➨ Anomalies in packaging material
    - ➨ Absence of high quality image on the CD

3.2. Traditional problems associated with Computer Crime

Earliest computer crime were non technological like theft of computer component, software piracy. Hacking and communication technology complicated computer crime. Criminals have the ability to adapt to changing technologies, environments and life styles which makes law enforcement difficult. Law enforcement community failed to recognize the criminal potentiality of emerging technologies and innovations. Investigators lack technological knowledge and are ill-equipped. Due to this they experiences uncertainty and ineffectiveness in most investigations.

3.2.1. Physicality and Jurisdictional Concerns

Increase in Computer crime is due to

- Intangible nature of computer interaction and criminal activities
- Lack of Physical boundaries
- Multinational crime – able to commit crime in one country while sitting in other
- There is no need of extensive tools, vehicular transportation, storage to commit crime
- Crime moved from real to virtual environment – It insulate the criminal from law enforcement
- Lack of cooperation, funding, politic

3.2.2. Perceived Insignificance, Stereotypes and Incompetence

- Investigators and administrators show great reluctance to pursue computer criminals
- Investigators are more focused on traditional crime
- They lack knowledge and interest in computer crime investigation
- Insiders are long time employee and have good knowledge of their companies' security procedures. They have the ability to mask their intrusion and make it very difficult to identify their activities, causing huge loss to business.
- Identity theft is increasing and it has become a growing concern among investigators

3.2.3. Prosecutorial Reluctance

- Law enforcement prosecutor lack knowledge and experience
- Lack interest, corporation, training and resources
- Focus towards headline catching case
- Giving low priority to electronic crime

3.2.4. Lack of Reporting

- Only 17% of victimizations were reported to law enforcement authorities
- Number of Incidents reported to CERT has increased six fold from 2000 to 2003
- Reason that business fail to report is to assure consumer of data security
- Business do their investigation internally and if prosecution is required then they share their investigation report
- Lack of reporting is due to the perception that reporting will not result in capture of suspect
- Many intrusions are detected long after violation occurred – making investigation difficult

3.2.5. Lack of Resources

- Law enforcement and corporate entity should cooperate with each other
- Corporate has resources to combat computer crime
    - They have administrators to monitor communication and system activity
    - They can establish policies with oversight
    - They have the ability to gather evidence with their resources (CADS- Computer Anomaly Detection Systems)
    - They have fund for investigation
- These resources are not available with law enforcement
    - They need economical support
    - They need training (Upgrading technologies) support
    - Need support for
        - Personnel –to give salary, and recruiting technical skilled person as needed
        - Hardware – to make the forensic lab advanced - remain consistent with technology
        - Software – Upgrade –OS: tools for data capture, analysis, recovery, preservation; password cracking
        - Housing – need to set lab

3.2.6. Jurisprudential Inconsistency

- Need to establish a legality standard
- Very difficult to do it
- Need global cooperation

3.3. Introduction to Identity Theft & Identity Fraud

Identity theft is stealing of personal information and identity fraud is committing illegal activity using that information. Identity theft may happen due to computer theft, loss of backups or compromised information systems. Millions of people get affected every year. This fraud is usually undertaken for economical gain, gaining access to secure or privilege area, to globalize crime by terrorist group or illegal immigration. Personal identification information has become a marketable commodity. Identity fraud is committed when **a credible identity is created** by accessing others credit cards, financial or employment record, computer system.

- Created credible identity is used for criminal activity
  - Small time criminals– use the credentials for placing some order for personal use
  - More Sophisticated criminals –use it for creating additional line of credit, separate bank account – to maximize the profitability of theft
- Credentials are used for identity fraud
  - Names
  - Address
  - Date of birth
  - Social security number
  - Taxpayer Identification number
  - Registration number
  - Passport number
  - City of birth
  - Mother maiden name
  - Biometric information
    - Fingerprints
    - Voice prints
    - Retinal image
- Credentials are collected from
  - Private citizen
  - Company employee
  - Corporate executives
  - Government workers
- Theft – Perpetrated by
  - Individual
  - Social or business network
  - Terrorist group
  - Criminal organizations

3.3.1. Typology of Internet fraud/theft

Identity theft divided into two main categories: financial and nonfinancial. In financial identity theft, the thief uses personal information to access bank accounts, obtain credit cards, or purchases goods.

Nonfinancial identity theft, the thief uses personal information to obtain telephone services, rent apartments, avoid prosecution, or secure a job.

There are five types of identity theft/fraud

- Assumption of Identity
    - Rarest and difficult form of threat
    - Simply assume the identity of victim
- Theft for employment and/or Border entry
    - This is to make illegal immigration or alien smuggling or to obtain employment
- Criminal record identity theft/fraud
    - It is a nonfinancial identity theft. The thief commits a separate crime and provides the victim's name and address to avoid prosecution and a criminal record on him. A victim becomes aware of this crime only when arrest warrant was issued against him.
    - Reverse criminal record identity theft, in this crime the thief hides his true identity and provides the victim's identity to gain employment.
    - Mostly such crimes are committed by friends or relatives
    - Victim faces legal obstacles to rehabilitate his identity. Victim must prove that he did not commit the crime and must receive a judge order to clear the falsely recorded crime on him. In addition to this legal burden, has to face financial burden.
- Virtual identity theft/fraud
    - It involves the creation of personal, professional and other identity to develop a fraudulent virtual personality
    - Virtual personal information is often used for online dating, protecting from prosecution, extramarital affairs, role play and accessing deviant site
- Credit identity theft/fraud
    - Use stolen personal information to create fraudulent account, gaining credit card or lending loan

3.3.2. Physical method of identity theft

Two broad categories of identity theft are physical or virtual. This section discuss on the physical method of identity theft.

- Mail theft
    - Physical mail boxes in the roadside of the houses contain valuable information like bank statement, insurance detail etc. in it and are often taken by non intended person
- Dumpster Diving

    - It is the process of searching valuable information from commercial or residential trash. The trash information include account number, social security number, tax payer identification number, password. It may be in paper form or in discarded computer media. To avoid paper shredders or disk wiper can be used.
- Theft of computers
    - Physical theft of computer is common technique of identity theft. People store personal information in their computer and for thief it is easy to search for information in computer then in paper. Computer is considered as warehouse of information and it has value in black market. Private residential building, hotel rooms, rest rooms, public transport, airport, government office are areas which is vulnerable to computer theft.
- Bag operations
    - It is a covert entry into hotel rooms to steal photocopy, photos, magnetic media and copy data from laptop. It is mostly done by host government security with the cooperation of hotel staff.
- Child identity theft
    - Identity of children who is less than 18 years are used by criminals to get credit cards. It is very difficult to find this fault as it can be detected only when the child first apply for their credit at the age after 18.
- Insider
    - In corporate and government sectors the insider are the greater risk.
- Fraudulent companies
    - Thieves create fake companies and try to collect personal financial information.
- Card Skimming and ATM Manipulation and Fraudulent Machines
    - Creating dummy card by card skimming – copying the personal information from the magnetic strip of the original credit card. Even thieves have developed fraudulent ATMs.

3.3.3. Virtual or Internet Facilitated Methods

Identity theft is increasing due to the increase in outsourcing of information, online shopping, online banking and increase in commercial globalization. Hacking of personal computers or the financial organizations database provides huge volume of identity related information.

- Phishing
    - This is a form of collecting information through email. The victim is asked to do some update service of their account or asking to fill some form, leading to fake website.
    - Broad categories of phishing
        - Spoofing – sending email hiding under others email
        - Pharming – Redirect the connection between an IP address and its target server
        - Redirectors – redirect network traffic to undesired site by modifying DNS
        - Advance fee fraud – victim give their personal information believing they will receive great financial gain
        - Trojan or spyware – malicious program attached as executable files in email
        - Floating windows –fake site to steel personal information.
- Spyware

    - Spyware aims to gather information without the victim's knowledge. Spyware get installed while the victim download attachment, free software, screensavers, song, image, video, adult website.
- Trojans
    - It is a malware housed within the commercial utility and used to commit criminal acts. Key-logger, backdoors, password stealer are some of the examples of torjan.
- Keyloggers and Password stealers
    - Keyloggers are devices or software programme to record the key stroke and send the information to the perpetrator. Helps in capturing password and other informations. It can even take screenshots. It may be a hardware, software or even a USB.

3.3.4. Crimes facilitated by identity theft/fraud

Identity theft is used by criminals to steal identity related information and use them to facilitate criminal activity. It is a four phase process.

- Procurement of stolen identifier
- Breed document is created or obtained
- Breed document is used to create additional fraudulent documents
- The fraudulent identity is employed in commission of criminal act

Criminal activity done using the fraud identity are student loan fraud, immigration fraud, social security fraud, insurance fraud, credit card fraud, tax fraud, internet scam, weapons trafficking and organized crime. Fraud identity helps to protect from law enforcement.

- Insurance / Loan fraud
    - Distance education and online courses increases the loan fraud as students need not be physically present in the campus. Insurance fraud are done to gain free medical care.
- Immigration fraud / Border crossing
    - Immigration fraud is conducted by individual or organization to gain secure border crossing or used for terrorist activity.

3.4. Types of CF techniques

3.5. Incident and incident response methodology

3.5.1. **Incident**

- *An incident is any unlawful, unauthorized or unacceptable* action that involves a computer system or a computer network. The incident is an event that violates the public law. An incident may cause a great impact on the reputation of an organization and business. Responding to incident consumes much time and resources.

- The following are events that are considered as an incident

- Theft of trade secrets
- Email spam or harassment
- Unauthorized or unlawful intrusions into computing systems
- Embezzlement
- Possession or dissemination of child pornography
- Denial-of-service (DoS) attacks
- Tortious interference of business relations
- Extortion
- Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes

3.5.2. **Incident Response Methodology**

- Seven major components of incident response:
    1. **Pre-incident preparation**
    2. **Detection of incidents**
    3. **Initial response**
    4. **Formulate response strategy**
    5. **Investigate the incident**
    6. **Reporting**
    7. **Resolution**

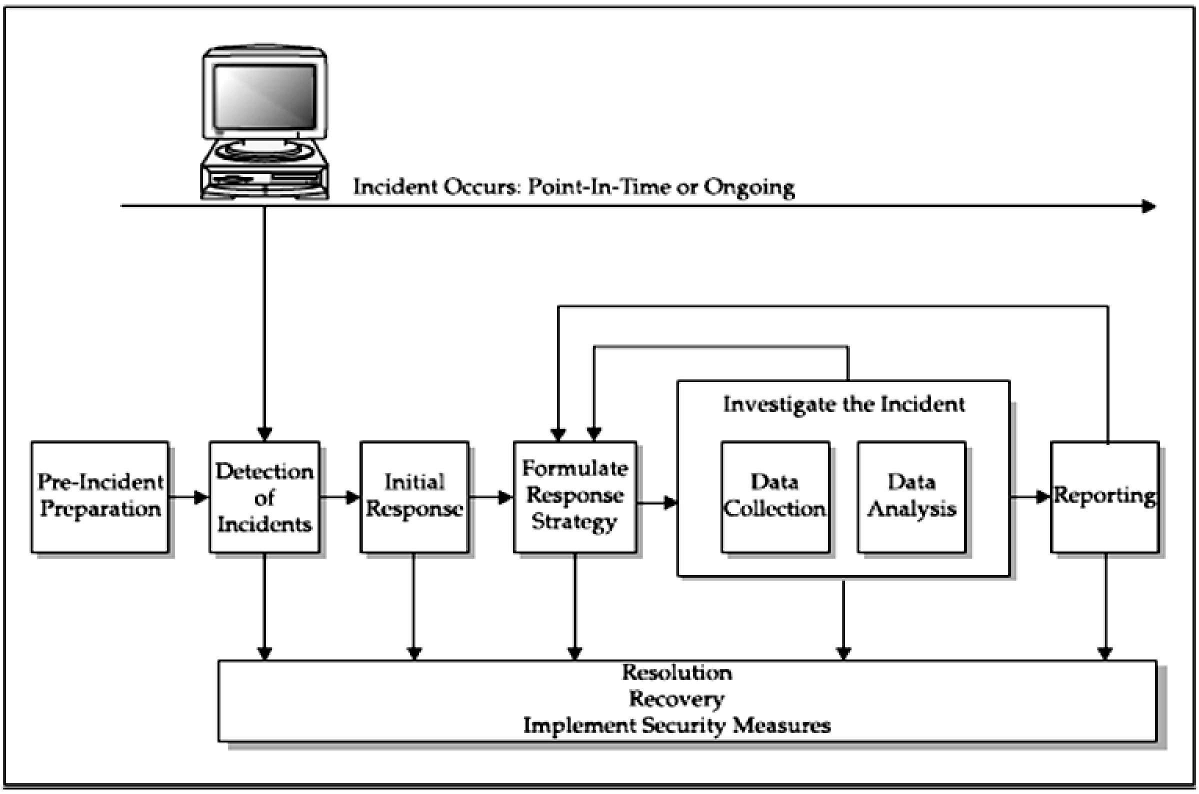


Fig3.1. Components of incident response

1. Pre-incident preparation

Preparation is necessary for successful incident response. Necessary actions need to be taken to prepare an organization and CSIRT before an incident occurs. Computer Security Incident Response Team (CSIRT) is a team of individuals who respond to any computer security incident. Computer security incidents are beyond our control as we cannot predict when the next incident will occur. Incident response is reactive in nature. Pre-incident preparation is only a proactive measure the CSIRT can initiate to ensure that an organization's assets and information are protected. Preparation will involve obtaining the necessary tools, developing techniques to respond to incident and taking actions on the systems and networks that will take part during an incident.

- **Preparing the Organization**
    - It involves developing strategies that will be employed by organization for incident response
        - Host-based security measures implementation
        - Network-based security measures implementation
        - End users training
        - Employing an intrusion detection system (IDS)
        - Strong access control
        - Timely vulnerability assessments
        - Taking backups on a regular basis
- **Preparing the CSIRT**
    - The hardware/ software/ documentation needed to investigate computer security incidents must be collected

- Policies and operating procedures to implement response strategies must be framed
- Employees need to be trained for incident response

2. Detection of incidents

Detection is very important for successful response. It is most important aspects of IR. It is one of the most decentralized phases where IR expertise has least control. Computer security incidents may be reported by an end user or detected by a system administrator or identified by IDS alerts or discovered by many other means. It is identified when someone suspects that an **unauthorized, unacceptable, or unlawful event** has occurred in an organization. Incident occurred may involve an organization's computer networks or data-processing equipment**.** Incident may be reported through one of three avenues- their immediate supervisor, the corporate help desk, incident hotline managed by the Information Security entity. It is necessary to prepare initial response **checklist** to make sure to record facts.

Critical details to be recorded in check list are

- Current time and date
- Who/what reported the incident
- Nature of the incident
- When the incident occurred
- Hardware/software involved
- Points of contact for involved personnel

After preparing the initial response checklist, the CSIRT should be activated. Appropriate people in CSIRT must be contacted. They use this check list and begin the initial response phase**.**

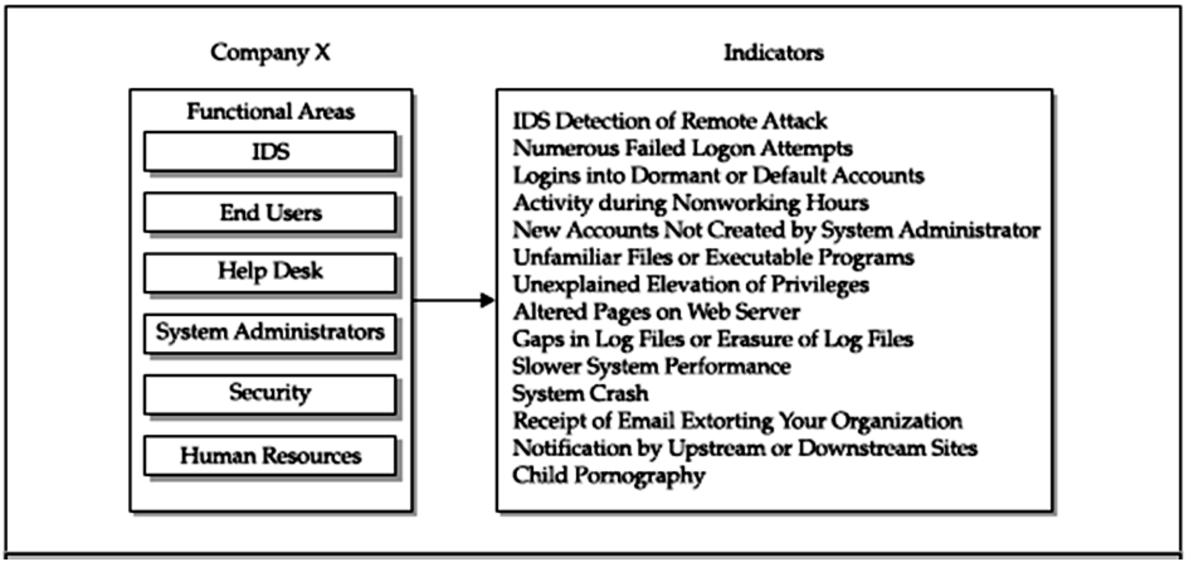

Company X
Indicators
Functional Areas
IDS
End Users
Help Desk
System Administrators
Security
Human Resources
IDS Detection of Remote Attack
Numerous Failed Logon Attempts
Logins into Dormant or Default Accounts
Activity during Nonworking Hours
New Accounts Not Created by System Administrator
Unfamiliar Files or Executable Programs
Unexplained Elevation of Privileges
Altered Pages on Web Server
Gaps in Log Files or Erasure of Log Files
Slower System Performance
System Crash
Receipt of Email Extorting Your Organization
Notification by Upstream or Downstream Sites
Child Pornography

Figure 3.2. Detection of Incidents

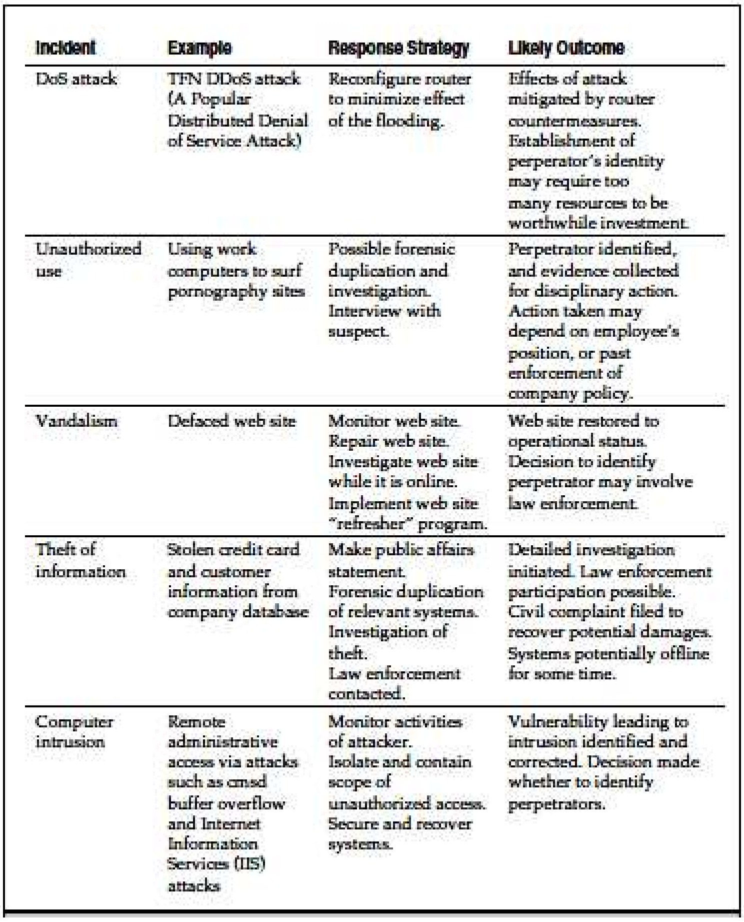
3. Initial Response

Initial investigation starts at this phase. It involves assembling the CSIRT, collecting data, determining the type of incident and assessing the impact. It documents the steps that must be taken to prevent reactions and panic when an incident is detected. It helps to implement a methodical approach. Data is collected without touching the system. Task to be performed for data collection are Interviewing system administrators/business unit personnel, reviewing intrusion detection reports and network-based logs to identify an incident has occurred and reviewing the network topology and access control lists. IR team must verify that an incident has actually occurred or not, which systems are directly or indirectly affected which users are involved, potential business impact and initiate network monitoring. Information collected in this phase is used to begin the next phase, developing a response strategy.

4. Formulate a Response Strategy

The main goal of this phase is to *determine the best response* strategy *for an incident. I*t should consider the political, technical, legal, and business factors that surround the incident. Appropriate response strategy *must be selected and management approval needs to be obtained.*

- **Considering the Totality of the Circumstances**
  - The following factors need to be considered when determining the amount of resources needed, determining of duplication, pursuing civil or criminal investigation.
    - How critical are the affected systems?
    - How sensitive is the compromised or stolen information?
    - Who are the potential perpetrators?
    - Is the incident known to the public?
    - What is the level of unauthorized access attained by the attacker?
    - What is the apparent skill of the attacker?
    - How much system and user downtime is involved?
    - What is the overall dollar loss?
- **Considering Appropriate Responses**
  - Figure 3.3. shows some common situations and their response strategies.



Incident	Example	Response Strategy	Likely Outcome
DoS attack	TFN DDoS attack (A Popular Distributed Denial of Service Attack)	Reconfigure router to minimize effect of the flooding.	Effects of attack mitigated by router countermeasures. Establishment of perperator's identity may require too many resources to be worthwhile investment.
Unauthorized use	Using work computers to surf pornography sites	Possible forensic duplication and investigation. Interview with suspect.	Perpetrator identified, and evidence collected for disciplinary action. Action taken may depend on employee's position, or past enforcement of company policy.
Vandalism	Defaced web site	Monitor web site. Repair web site. Investigate web site while it is online. Implement web site "refresher" program.	Web site restored to operational status. Decision to identify perpetrator may involve law enforcement.
Theft of information	Stolen credit card and customer information from company database	Make public affairs statement. Forensic duplication of relevant systems. Investigation of theft. Law enforcement contacted.	Detailed investigation initiated. Law enforcement participation possible. Civil complaint filed to recover potential damages. Systems potentially offline for some time.
Computer intrusion	Remote administrative access via attacks such as cmsd buffer overflow and Internet Information Services (IIS) attacks	Monitor activities of attacker. Isolate and contain scope of unauthorized access. Secure and recover systems.	Vulnerability leading to intrusion identified and corrected. Decision made whether to identify perpetrators.

Figure 3.3. Possible responses

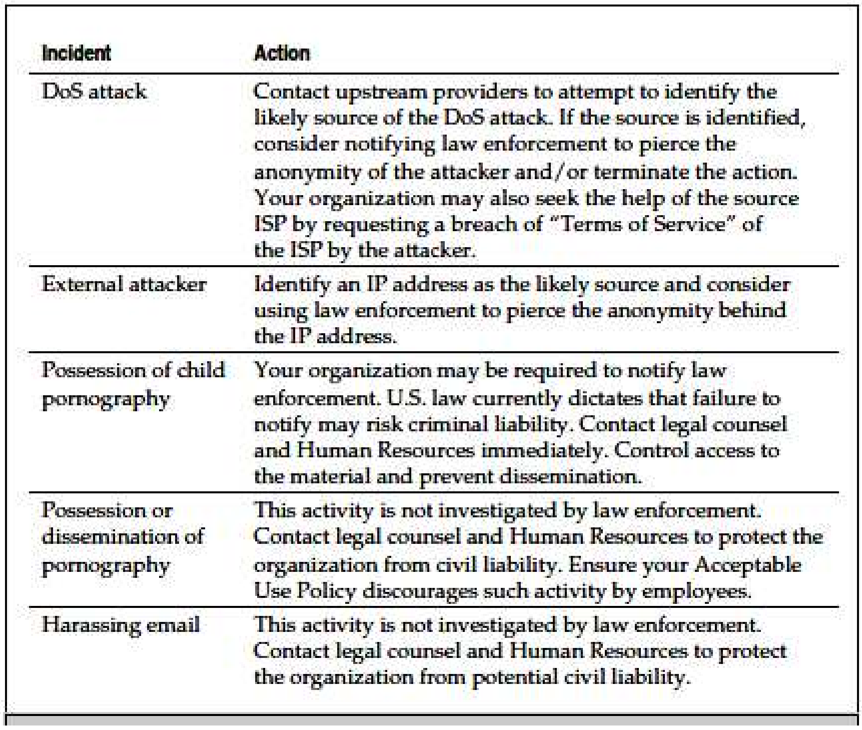
The response strategy must take organization's business objectives into consideration , the response strategy should be approved by upper-level management.
The response strategy option should consider the pros and cons related to the following:

- Estimated loss
- Network and User downtime and its impact to operations
- Is it necessary to take legal actions
- Public disclosure of the incident and its impact to the organization's reputation/business
- Theft of intellectual property and its potential economic impact

– Taking Action

- Organization need to take disciplinary action against an employee or respond to a malicious act by an outsider. Action can be filing civil or criminal complaint, or taking some administrative action or privilege revocation.
- Legal Action
  - File a civil complaint
  - Notify law enforcement
- Administrative Action
  - Disciplining or terminating employees by any actions like letter of reprimand, immediate dismissal, mandatory leave, reassignment of job duties, temporary reduction in pay or withdrawal of certain privileges.

Figure 3.4. shows common scenarios and some potential actions



Incident	Action
DoS attack	Contact upstream providers to attempt to identify the likely source of the DoS attack. If the source is identified, consider notifying law enforcement to pierce the anonymity of the attacker and/or terminate the action. Your organization may also seek the help of the source ISP by requesting a breach of "Terms of Service" of the ISP by the attacker.
External attacker	Identify an IP address as the likely source and consider using law enforcement to pierce the anonymity behind the IP address.
Possession of child pornography	Your organization may be required to notify law enforcement. U.S. law currently dictates that failure to notify may risk criminal liability. Contact legal counsel and Human Resources immediately. Control access to the material and prevent dissemination.
Possession or dissemination of pornography	This activity is not investigated by law enforcement. Contact legal counsel and Human Resources to protect the organization from civil liability. Ensure your Acceptable Use Policy discourages such activity by employees.
Harassing email	This activity is not investigated by law enforcement. Contact legal counsel and Human Resources to protect the organization from potential civil liability.

Figure 3.4. Possible Actions

5. **Investigate the incident**

Investigator performs a thorough collection of data. Then review the data collected to determine what / when / where the incident happened, who did it, how it can be prevented in the future. Investigation is conducted by reviewing host-based evidence, network-based evidence and evidence gathered via traditional, nontechnical investigative steps

People cause incidents using things to destroy, steal, access, hide, attack, and hurt other things. Key task of the investigator is to determine which things were harmed by which people. This is difficult more difficult in computer crime as people are using encryption, steganography, anonymous email accounts, fakemail, spoofed source IP addresses, spoofed MAC addresses, masquerading as other individuals, and other means to mask their true identity. This makes identifying the attacker a time consuming task.

Investigation can be divided into two phases:

- **Data collection**
- **Forensic analysis**

Figure 3.5. illustrates the possible steps taken during the two phases of investigation

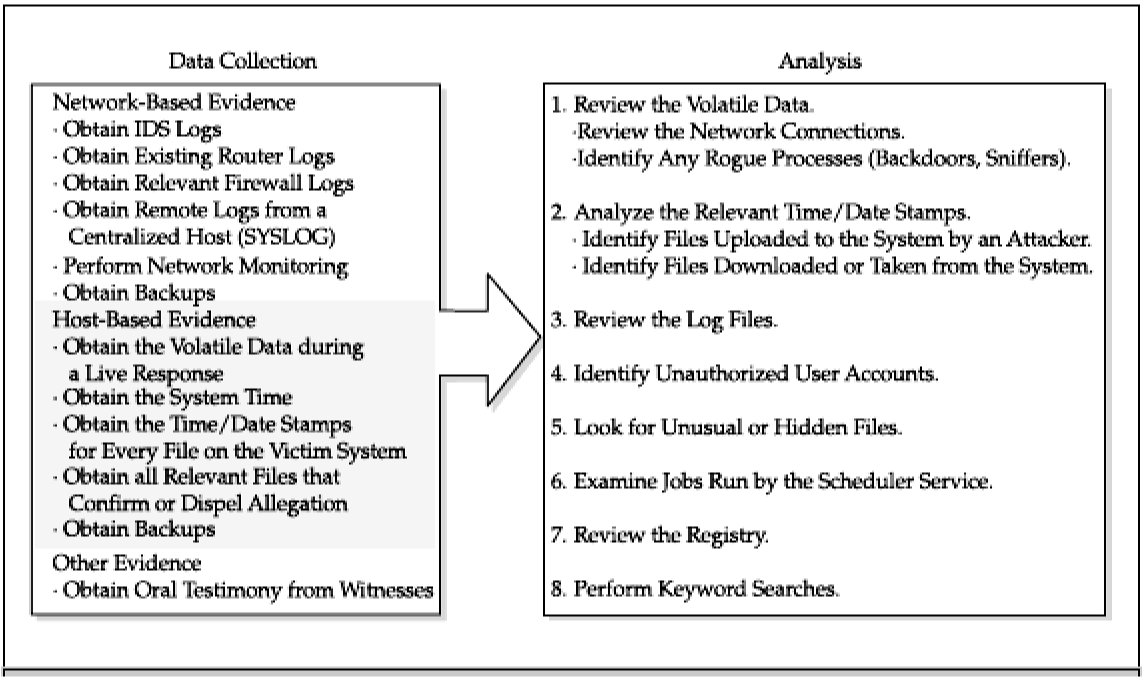

Data Collection
Network-Based Evidence
· Obtain IDS Logs
· Obtain Existing Router Logs
· Obtain Relevant Firewall Logs
· Obtain Remote Logs from a Centralized Host (SYSLOG)
· Perform Network Monitoring
· Obtain Backups
Host-Based Evidence
· Obtain the Volatile Data during a Live Response
· Obtain the System Time
· Obtain the Time/Date Stamps for Every File on the Victim System
· Obtain all Relevant Files that Confirm or Dispel Allegation
· Obtain Backups
Other Evidence
· Obtain Oral Testimony from Witnesses
Analysis
1. Review the Volatile Data.
·Review the Network Connections.
·Identify Any Rogue Processes (Backdoors, Sniffers).
2. Analyze the Relevant Time/Date Stamps.
· Identify Files Uploaded to the System by an Attacker.
· Identify Files Downloaded or Taken from the System.
3. Review the Log Files.
4. Identify Unauthorized User Accounts.
5. Look for Unusual or Hidden Files.
6. Examine Jobs Run by the Scheduler Service.
7. Review the Registry.
8. Perform Keyword Searches.

Figure3.5. Possible investigation phase steps

– Data Collection

Data collection is the process of collecting the facts and clues that should be considered during forensic analysis. If necessary data is not collected then investigation will be difficult. It is necessary to collect data before performing any investigation. Data collection phase can be divided into three fundamental areas: host-based information, network-based information, and other information.

- **Host-based Information** includes logs, records, documents, and any other information that is found on a system and not obtained from network-based nodes. It include gathering information in two different manners: *live data collection* and *forensic duplication*.

- *Live data collection :* first step of data collection, any volatile information from a host is collected before it is lost. Listed below are few volatile information
  - The system date and time
  - The applications currently running on the system
  - The currently established network connections
  - The currently open sockets
  - The applications listening on the open sockets
  - The state of the network interface

Live response must be performed to collect this information.Itis conducted when a computer system is still powered on and running. Three variations of live response:

Initial live response : Obtaining only the volatile data

In-depth response: In addition to volatile data it also collect nonvolatile information such as log files

Full live response All data for the investigation is collected

Forensic duplication: Provides the “mirror image” o working copy of the target system. Investigator can work on this copy without altering or destroying potential evidence.

- **Network-based Evidence** : Includes information obtained from the following sources:
  - IDS logs
  - Consensual monitoring logs
  - Nonconsensual wiretaps
  - Pen-register/trap and traces
  - Router logs

- Firewall logs
- Authentication servers

- **Other Evidence**: Involves testimony and other information obtained from people. Nontechnical way of collection like collecting personnel files, interviewing employees, interviewing witnesses and document the information gathered

– Forensic Analysis

It includes reviewing all the data collected like - log files, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files. Also it includes software analysis, review time/date stamps, perform keyword searches, and take any other necessary investigative steps. It include looking through information that has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation. Figure3.6. shows the major steps taken during forensic analysis.

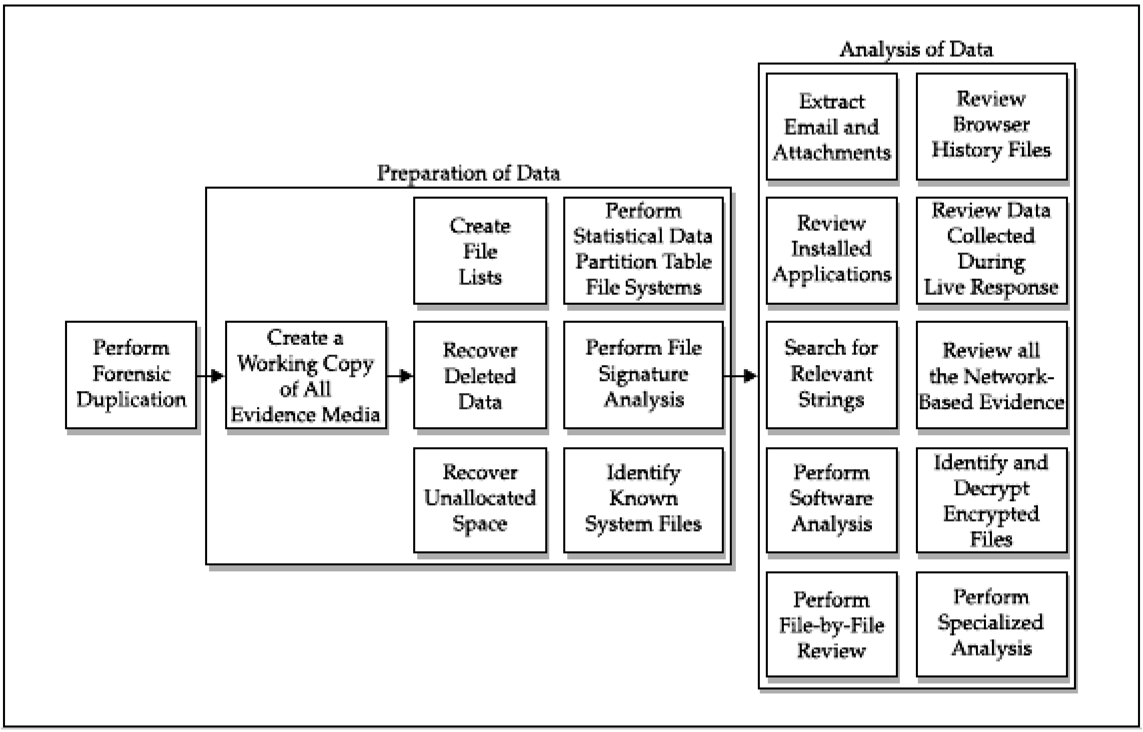

Analysis of Data
Preparation of Data
Perform Forensic Duplication
Create a Working Copy of All Evidence Media
Create File Lists
Perform Statistical Data Partition Table File Systems
Recover Deleted Data
Perform File Signature Analysis
Recover Unallocated Space
Identify Known System Files
Extract Email and Attachments
Review Browser History Files
Review Installed Applications
Review Data Collected During Live Response
Search for Relevant Strings
Review all the Network-Based Evidence
Perform Software Analysis
Identify and Decrypt Encrypted Files
Perform File-by-File Review
Perform Specialized Analysis

Figure3.6. Performing forensic analysis

6. Reporting

Create reports that accurately describe the details of an incident. Report should be understandable to decision makers, must withstand legal scrutiny, produced in a timely manner.
Guidelines to for reporting phase:

- Document immediately
- Write concisely and clearly
- Use a standard format
- Use editors

7. Resolution

The goal is to implement host-based, network-based, and procedural countermeasures. To prevent an incident from causing further damage and to return organization to a secure, healthy operational status.

3.6. Forensic duplication and investigation

3.6.1. Forensic duplicates as admissible evidence

Set of legal standards are defined to provide an item or writing or to be admitted into evidence. The process of collection must also follow standard. Best evidence rule is U.S. Federal Rules of Evidence (FRE) §1002 states that the item or information presented in court must be the original. Some exceptions to this rule is situation where the originals themselves cannot be obtained due to business needs. The exceptions are defined in two rules:

- FRE §1001-3, Definitions and Duplicates:
    - *"If data are stored by computer or* similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."
- FRE §1003, Admissibility of Duplicates:
    - "A duplicate is admissible to the same extent as an original unless
        - a genuine question is raised as to the authenticity of the original or
        - in the circumstances it would be unfair to admit the duplicate in lieu of the original."

There are two types of duplicate:

- Forensic Duplicate:
    - File that contains every bit of information from the source in a raw bit stream format. Produce identical byte stream from duplicate as from the original. A 5GB hard drive would result in a 5GB forensic duplicate. A forensic duplicate may be compressed after the duplication process
    - Two tools that create a forensic duplicate
        - Unix dd command and dfcldd command
        - Open-source Open Data Duplicator

- Qualified Duplicate:
    - Same as forensic duplicate, but allows embedded metadata or certain types of compression. This file contains every bit of information from the source.
    - Stored in an altered forms
        - In-band hashes
        - Empty sector compression
    - Sector(in-band hashes)
        - Tools read some number of sectors from the source, generate a hash and store the sectors followed by hash to output file
        - Even if sector group fails restoration can continue which is not possible when storing a file
    - Empty sector compression
        - Minimizing the size of the output file
        - If the tool comes across 500 sectors, all filled with zeros, it will make a special entry in the output file that the restoration program will recognize
    - Tools that create qualified forensic duplicate output files are SafeBack and EnCase

- **Restored Image:**
    - A forensic duplicate or qualified forensic duplicate restored a storage medium to another storage medium. Duplication is difficult to do if second hard drive does not have the same geometry as the original one. SafeBack, EnCase, and dd will create a restored image from the qualified forensic duplicate.

- **Mirror Image**

- Created from hardware that does a bit-to-bit copy from one hard drive to another (copy even the OS)

3.6.2.FORENSIC DUPLICATION TOOL REQUIREMENTS

- The tool must have the ability to image every bit of data on the storage medium
  - The tool must create a forensic duplicate or mirror image
  - The tool must handle read errors
  - The tool must not make any changes to the source medium
  - The tool must have the ability to be held up to scientific and peer review

3.6.3. Creating a Forensics Duplicate of a Hard Drive

True forensic duplicate are created in Unix operating environment. One tool to create duplicate is dd command. It is part of GNU software suite. It runs on Unix/Linux/Mac OS X. It can recognize almost any hardware. The dd command was improved by DoD Computer Forensics Lab and re-released as dcfldd command. It is the forensic version of dd command. Another tool is the Open Data Duplicator from openforensics.org. This Unix tool allows an investigator to perform multiple functions as the image is being created.
Software tools: Encase is very expensive full suite of forensic tool based on windows. It has a great market penetration. Its popularity is based primarily on the easy-to-navigate GUI interface. A flexible scripting language is included which allows the examiner to customize the types of searches performed by the tool.Safeback is a specialized imaging tool. It is a small application that is designed to run from a DOS boot floppy. It offers four modes of operation:

- The Backup function produces a forensically sound image file of the source media.
- The Restore function restores forensically sound image files.
- The Verify function verifies the checksum values within an image file.
- The Copy function performs the Backup and Restore operations in one action.

3.7. Preparation for IR:

Preparation is necessary for any well-executed incident response. Incident preparation provides rapid answers to the questions that will be asked *after an incident occurs:*

- What exactly happened?
- What system(s) was affected by the incident?
- What information was compromised?
- What files were created, modified, copied, or deleted?
- Who may have caused the incident?
- Who should you notify?
- What steps can you take to rapidly recover to normal business procedures?

3.7.1. Overview of pre-incident preparation

It involves organization steps as well as computer security incident response team (CSIRT) preparation steps. The following preparation is recommanded:

- Identify corporate risk.
- Prepare hosts for incident response and recovery.
- Prepare network by implementing network security measures.
- Establish policies and procedures that allow to meet incident response objectives.
- Create a response toolkit for use by the CSIRT.
- Create a CSIRT that can assemble to handle incidents.

3.7.2. Identifying Risk

Critical assets are the ones that produce the greatest liability, or potential loss, to organization. The following are some examples of critical assets: **Corporate reputation, Confidential business information, Nonpublic personally identifiable information.** Critical assets are critical to the continued success of the organization. The initial step of pre-incident preparation is identifying and prioritizing the risk by answering the following

- **What are your critical assets?**
  - Produce the greatest liability, or potential loss
  - Organizations assets
    - Corporate reputation
    - Confidential business information
- **What is their exposure?**
  - people, processes, or technology result in or contribute to loss
  - unpatched web servers, Internet-facing systems, untrained employees, and lack of logging
- **What is the threat?**
  - Anyone connected to the Internet?
  - Anyone with physical access to a corporate building?
  - Only individuals physically within a secure area?

This ensures that available resources are spend efficiently. It is used for preparing for the incidents that is most likely to affect business.

3.7.3.Preparing individual hosts

Steps that one can take to help any investigator respond effectively are:

- **Record cryptographic checksums of critical files**
  - Use MD5 , use scripting language to automate this process (Tripwire package)
- **Increase or enable secure audit logging**
  - Operating system and applications need significant logging
- **Build up your host's defenses**
  - If host is completely secure, many security incidents would be avoided
  - Three cornerstones of secure hosts:
    - Make sure that all operating system and application software is the most recent. Use the latest release and make sure that all patches, hot fixes, and updates are installed
    - Disable unnecessary services. If you are not using an application or network service, it should not be running. Unnecessary services introduce unnecessary risk
    - When faced with configuration choices, choose wisely. Many security exposures are introduced through sloppy system administration
- **Back up critical data and store media securely**
  - Take regular, complete system backups
  - Backups allows to figure out what was modified, deleted, added,
  - Some backups save time/date information, which may be useful for checking the times files and directories were last accessed, modified, or created
  - Disadvantages:
    - Difficult to find a system to restore
    - Backup may be taken after compromise,
    - May not have accurate time-of-last-access
- **Educate users about host-based security**
  - Users play a critical role in overall security
  - Users should know what types of actions they should and should not take
  - Should know the danger inherent in networking software installed by users
  - Users should be educated about the proper response to suspected incidents
    - Immediately notify a designated contact
    - To take *no investigative actions, because these actions can often destroy evidence*
    - Make timely response

These steps are not a one-time function. Since hosts change over time with new users, software, and network configuration, these host preparation steps are best incorporated into organizational policies and procedures.

3.7.4. Preparing a Network

- Network-based security measures are to be consider for incident response
- Network administrators play a critical role during incident response
- Network-based logging is absolutely essential - only hope to accumulate evidence.
- Network administrators are responsible for
  - the network architecture and topology
  - Devices like firewalls, routers, and intrusion detection systems
  - Reconfiguring these devices to block certain traffic during incident response
- Network security actions include the following:
  - **Install firewalls and intrusion detection systems**
    - Configure - simply to protect network, as well as to log activities
    - May decide to deny certain attacks and not log, or permit attacks and log in detail to learn more about the attacker
  - **Use access control lists on routers**
    - Access control lists (ACLs) allow certain types of traffic while prohibiting potentially dangerous traffic
  - **Create a network topology conducive to monitoring**
    - In the event of an incident, you must know the network topology in order to determine the best response strategy
  - **Encrypt network traffic**
    - enhances the security of any network - SSL,VPN, SSH
    - When attackers use encrypted protocols to access your systems, network monitoring and IDS systems are useless.
  - **Require authentication**
    - Authentication is both a host-based and network-based security measure
    - Usernames and passwords are often guessed easily
    - Using additional authentication—Kerberos, IP Security Protocol

3.7.5. E**stablishing appropriate policies and procedures**

- Absent a proper policy make it difficult to legally monitor
- Without any policies employees have an expectation of privacy
  - Cannot monitor their daily activities, peruse their email, observe their web-browsing habits, access their voice-mail systems, or review the contents of their computer system whenever you feel like it
  - Insiders may be emailing vital trade secrets to competitors, and hackers may be holding an electronic cocktail party on organizations networks
- With some preparation, planning, proper policies, and in-place procedures, one can determine when to respond to an incident. Organization can also take the rights to monitor the activities of employees or unauthorized intruders.
- **Determining Your Response Stance**
  - Need to determine organizations stance on responding to incidents
  - When an organization is the victim of a computer intrusion, denial-of-service (DoS) attack, insider theft of intellectual property, or other network-based computer crime, the organization can respond in several different ways:
    - Ignore the incident altogether.
    - Defend against further attacks.
    - Defend against further attacks by identifying and disabling the initiators (bycriminal arrest or civil action).
    - Perform surveillance and counterintelligence data gathering.
- Five factors that will influence how you respond to computer security incidents:
  - The effect the incident has on your business
  - Legal issues and constraints
  - Political influence or corporate politics
  - Technical capabilities of the response team
  - Funding and available resources
- **Considering Business Issues**

Companies consider business-based decisions before any other .When an e-commerce web site gets hacked and defaced, fixes the site first then secure the system by patching any security hole. Damages to the victim are unable to accept customers for a period of time and organization lose reputation.

- **Considering Legal Issues**

It is necessary to consult legal counsel whenever administrative or judicial proceedings may be the outcome of the actions you take. Any constraints or guidelines legal advisors provide are certainly to be followed to the letter.

- **Considering Political Issues**

Corporate politics dictate the overall security philosophy. If the corporate atmosphere is to trust everyone, allowing each user maximum freedom and flexibility, then obviously incident may be conducted in an unbiased fashion with the intent to enforce its policies.

- **Considering Technical Capabilities**

Effective incident response requires good, hard-working people who are technically savvy, aware of the corporate politics, knowledgeable about the business, and capable of reporting accurate, useful information to upper-level management.

mediocre fixes and recommendations.

- **Benefits of Sound Policies**

Four pieces of information that corporate responders can obtain without the legal documentation and headaches that may be necessary for law enforcement personnel to endure are

    - **Subscriber information**
    - **Transactional information**
    - **Electronic communications**
    - **Full-content monitoring**

  –

- **Developing Acceptable Use Policies (AUP)**
  - Decide whom to trust on network.
    - Monitor on-site employees as well as individuals using remote-access services.
    - Determine whether you will monitor all activities or just a few select ones. Or monitor only after suspect
    - Control and regulate employee behavior.
  - Orient employees to the AUPs.
    - Advertised throughout the corporation and incorporated into new employee orientation.
    - Employees will need to positively acknowledge - written signature
    - Provide refresher overview course on policies when major changes are made to policies.
  - Be consistent and clear in AUPs.
  - **Before developing policies first** decide who is responsible for writing and updating the policies, as well as who should enforce those policies.
  - AUPs affect everyone in an organization: the users, managers, internal auditors, legal staff, system administrators, and technical staff. Therefore, each group affected by the policy should be part of its approval process
- **Designing AUP**

Follow a consistent and clear procedure in designing AUPs. Start at the top looking down. Create several separate AUPs, rather than a single big one. **Design from the Top Down. Create structured list.**

  - Technical
    - Who can add and delete users?
    - Who can access machines remotely?
    - Who can scan your machines?
    - Who can possess password files and crack them?
    - Who gets root-level access to what?
    - Is posting to newsgroups allowed?

        - Is Internet Relay Chat (IRC) or instant messenger permitted?
        - Will you condone use of pirated software?
    - Behavioral
        - What web use is appropriate?
        - How you will respond to sexual harassment, threats, and other
        - inappropriate email messages?
        - Who can monitor and when?
        - Who can possess and use “hacker tools”?
- **Creating Separate Policies**
    - Create a few smaller policy documents rather than to produce one enormous AUP
    - **Acceptable Use Policy**
        - Governs what behaviour is expected by each user
    - **User Account Policy**
        - Dictates how accounts are added to systems, who has root-level access, and even establish controls of where and when users can access prized resources
    - **Remote Access Policy**
        - Establishes who can access your systems remotely and how they can access those systems.
    - **Internet Usage Policy**
        - Covers how and when users can use the Internet, which is often a frequent source of misunderstanding between employers and employees.
- **Developing Incident Response Procedures**

Procedures are the implementation of the policies of your organization

3.8. Creating response tool kit.

Regardless of the status of network, host, and policy preparation, the CSIRT will need to be prepared to respond to incidents. The response toolkit is a critical component of pre-incident preparation, and it is one of the few components in your control. The response toolkit includes the hardware, software, and documentation used during response.

3.8.1.The Response Hardware

Hardware specifications suggested for IR team is given below

High-end processor, A minimum of 256MB of RAM, Large-capacity IDE drives, Large-capacity SCSI drives, SCSI card and controller, A fast CD-RW drive, Extra power extenders for peripherals, Extra power-extension cords, Numerous SCSI cables and active terminators, Parallel-to-SCSI adapters, Ribbon cables with more than three plugs, Power strips, An uninterruptible power supply (UPS), CD-Rs, 100 or more, Labels for the CDs, A permanent marker for labeling CDs, Jaz or Zip media, Folders and folder labels for evidence, Operating manuals, A digital camera, Lockable storage containers for evidence, Printer and printer paper, Burn bags

3.8.2. The Response Software

Many specific software tools are used during incident response to investigate various operating systems and applications. The following is a list of the more generic software that forms the basis of any software toolkit:

- Two to three native operating systems on the machine, such as Windows 98, Windows NT, Windows 2000, and Linux,
- Safeback, EnCase, DiskPro, or another forensics software package, used to re-create exact images of computer media for forensic-processing purposes
- All the drivers for all of the hardware on your forensic
- Selection of boot disks (DOS, EnCase, Maxtor, and so on)
- Quick View Plus or some other software that allows you to view nearly all types of files
- Disk-write blocking utilities
- An image of the complete setup on backup media such as DVD

3.8.3. The Networking Monitoring Platform
It need a machine that can handle the amount of traffic the network has. The system running the network monitor should be a Pentium-class machine, 500MHz or higher, with at least 512MB of RAM, 30GB hard drive.Network monitor system must have a NIC.

3.8.4. Documentation
The CSIRT must document all actions and findings. Documentation is necessary for further disciplinary, civil, or criminal action, as well as for a thorough response. Key areas for documentation include how the evidence is obtained, all actions taken, and where and how the evidence is stored.

3.9. Establishing an Incident Response Team

IR team must have hard workers who show attention to detail, remain in control, do not rush the important things, and document what they are doing.

- **Deciding on the Team's Mission**
  - Establish a 24-hour, 7-day-a-week hotline for clients during the duration of the investigation.
  - Control and contain the incident.
  - Collect and document all evidence related to an incident.
  - Maintain a chain of custody (protect the evidence after collection).
  - Select additional support when needed.
  - Protect privacy rights established by law and/or corporate policy.
  - Provide liaison to proper law enforcement and legal authorities.
  - Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure.
  - Provide expert testimony.
  - Provide management
- **Training the Team**
  - The mission of your CIRT may be to achieve all or most of the following:
    - Respond to all security incidents or suspected incidents using an organized, formal investigative process.
    - Conduct a complete investigation free from bias (well, as much as possible).
    - Quickly confirm or dispel whether an intrusion or security incident actually occurred.
    - Assess the damage and scope of an incident.

3.10. Types of Computer Forensics Technology

Cyber forensics technology and systems support discovery, analysis, and reconstruction of evidence. CF focuses on **real-time, online** evidence gathering rather than the traditional offline computer disk forensic technology. Evidence are extracted from the following:

- computer systems
- computer networks
- computer media
- computer peripherals

Opportunity for cyber crime is increasing and it is crucial to make advances in law enforcement and forensic computing techniques.

Two components of cyber forensics technology

1. Computer forensics
   - Deals with gathering evidence from computer media seized at the crime scene. Gathering evidence include the following activities imaging storage media, recovering deleted files, searching slack and free space. The evidence collected is preserved to take legal action. Several computer forensic tools are available to investigators

2. Network forensics
   - Deals primarily with in-depth analysis of computer network intrusion evidence. It is more technically challenging as it involves gathering digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not

preserved within permanent storage media. Current commercial intrusion analysis tools are inadequate to deal with today's networked, distributed environments

Today's computer forensics is generally performed **postmortem** (after the crime or event occurred). In a networked, distributed environment, it is essential to perform forensic-like examinations of victim information systems on an almost **continuous basis and support of various objectives. It** is essential to **continued functioning** of critical information systems and infrastructures. Only very **few forensic tools** are available to assist in preempting the attacks or locating the perpetrators

- Objectives
    - Timely cyber attack containment
    - Perpetrator location and identification
    - Damage mitigation
    - Recovery initiation in the case of a crippled, yet still functioning, network
- Sources of data evidence
    - Intrusion detection system logs
    - Firewall logs
    - Audit trails
    - Network management information
- Also inspect
    - Contents or state of memory
    - Registers
    - Basic input/output system
    - Buffers
    - Cache
- Types of computer forensics technology used by
    1. Military
    2. Law enforcement
    3. Business computer specialists

3.10.1. Types of Military Computer Forensic Technology

It Includes **evaluation and indepth examination** of data related to both the **trans- and post-cyberattack. The k**ey objectives include r**apid discovery** of evidence, estimation of **potential impact** of the malicious activity on the victim, assessment of the **intent and identity** of the perpetrator. **Real-time tracking** of potentially malicious activity is especially **difficult** when the pertinent information has been intentionally hidden, destroyed, or modified in order to elude discovery.

Cyber forensic concepts are new and untested. National Institute of Justice (NIJ) and National Law Enforcement and Corrections Technology Center (NLECTC) together test new ideas and prototype tools for CF. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership CF technology moved from military research and development (R&D) laboratories into the hands of law enforcement.

3.10.2. Types of Law Enforcement: Computer Forensic Technology

CF involves the **preservation, identification, extraction, processing and documentation** of computer evidence. Special forensic software tools and techniques are required.

- Tools and techniques
    - Help to hide evidence
    - They are valuable resource for law enforcement
    - Have become important resources for use in internal investigations, civil lawsuits, and computer security risk management
    - Used to create computer evidence without the knowledge of the computer operator
    - Used to identify passwords, logons, and other information
    - Used to identify backdated files
-

3.10.2.1. Computer Evidence Processing Procedures

Computer Evidence processing procedures and methodologies should conform to **federal computer evidence processing standards.** Training and certification programs have also been developed for the International Association of Computer Investigation Specialists (IACIS).

1. Preservation of Evidence

- Computer evidence is fragile and susceptible to alteration or erasure. Computer forensic instructors should expose their trainees to bit stream backup theories that ensure the preservation of all storage levels that may contain evidence.

2. Disk Structure
   - Need a good understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk.

3. Data Encryption
   - Should become familiar with different forms of encryption, password recovery software

4. Matching a Diskette to a Computer
   - Specialized techniques and tools that conclusively tie a diskette to a computer must be familiarized

5. Data Compression
   - Should know how compression works and how compression programs can be used to hide and disguise sensitive data, how password-protected compressed files can be broken.

6. Erased Files
   - Should know how to recover the erased files using DOS programs or data-recovery tools.

7. Internet Abuse Identification and Detection
   - Should know how to use specialized software to identify how a targeted computer has been used on the Internet.

8. The Boot Process and Memory Resident Programs
   - Should know how the operating system can be modified to change data and destroy data.

3.10.3. Types of business computer forensic technology

1. Remote monitoring of target computers

Data Interception by Remote Transmission (DIRT) from Codex Data Systems (CDS) is a powerful remote control monitoring tool. Monitor from a remote command centre without physical access. Also remotely seize and secure digital evidence prior to physically entering suspect premises.

2. Creating trackable electronic documents

IDS tools identify unauthorized intruders who access, download, and view these tagged documents.

3. Theft recovery software for laptops and PCs

PC PhoneHome is a software application that will track and locate a lost or stolen PC or laptop anywhere in the world. It is easy to install. It is also completely transparent to the user.

4. Basic forensic tools and techniques

Many are available likely for digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking online activity, finding and recovering hidden and deleted data, locating stolen computers, creating trackable files, identifying software pirates, and so on.

5. Forensic services available

Services include but are not limited to

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring available
- Tracking and location of stolen electronic files
- Honeypot sting operations

- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses

3.11. Types of Computer Forensics Systems

Any product that can remotely be tied to network or computer becomes a “forensics” system.

3.11.1. Internet security systems

Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.

Establishing a corporate Internet security policy involves the following:

- High-level management policy statement
- Systematic analysis of organizations assets
- Examination of risks
- Develop implementation strategy

- A powerful technique for securely sending information is public key encryption or public key infrastructure.
- Firewalls are a basic means for providing network security.
- Payment gateway secure the payment information provided by the customer to the merchant..
- Variety of security products are available to implement an access control system.
- Secure virtual private networks (SVPN) provide significant reduction in internal corporate networking costs to achieved secure, encrypted, Internet protocol (IP)-level network communications over less expensive public networks.
- Smart card is equivalent to an electronic safe deposit box. A smart card contains a semiconductor chip with logic and nonvolatile memory. The software within the card detects intrusion and tampering and monitors abnormal usage.

3.11.2. Intrusion detection systems

Intrusion detection systems help computer systems prepare for and deal with attacks. They collect information from a variety of vantage points within computer systems and networks and analyze this information for symptoms of security problems.

Intrusion detection systems perform a variety of functions:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis of abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations

Some systems provide additional features, including

- Automatic installation of vendor-provided software patches
- Installation and operation of decoy servers to record information about intruders

Vulnerability assessment products (*scanners*) perform rigorous examinations of systems. It provides both passive and active examination to determine weaknesses that might allow security violations.

Network security management is a process that establishes and maintains policies, procedures and practices required for protecting networked information system assets.

3.11.3 Firewall security systems

Firewall technology is a first line of defense. It form a barrier against outside attacks. These firewall gateways provide a choke point at which security and auditing can be imposed. They allow access to resources on the Internet from within the organization while providing controlled access from the Internet to hosts inside the virtual private network.

The following are the primary benefits of using a firewall:

- Protection from vulnerable services
- Controlled access to site systems
- Concentrated security
- Enhanced privacy
- Logging and statistics on network use and misuse
- Policy enforcement

3.11.4. Storage area network security systems

Disaster recovery services use storage area networks (SANs). It is used to restore thousands of terabytes of business data and get hundreds of companies running. SANs are a new methodology for attaching storage using a separate network to connects all storage and servers.

3.11.5. Network disaster recovery systems

Network disaster recovery (NDR) is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization’s critical business functions.

3.11.6. Public key infrastructure systems

PKI is an environment that provides trust and confidentiality in data transmission and storage. PKI accomplishes these goals for an enterprise through policy and technology components. Technology component determine and identify the roles, responsibilities, constraints, range of use, and services available.

A PKI consists of

- A certificate authority that issues and verifies digital certificates
- A registration authority that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

3.11.7. Wireless network security systems

Protecting wireless network from viruses is complicated process. Business is working hardly to provide security in wireless network.

3.11.8. Satellite encryption security systems

Satellite communications is becoming a security nightmare. Providing security is essential to provide protection of intellectual property distribution, electronic commerce, electronic battlefields and national security. Multi layer Encryption on top of compressed data is to be transmitted to a satellite (uplink) from Earth and then transmitted down to Earth (downlink). Then it is decrypted. This compression, multilayer encryption provides confidentiality and authentication.

3.11.12. Biometric security systems

Biometric system is the computer hardware and software used to recognize or verify an individual.

3.11.13. Homeland security systems

Homeland security is defined as the deterrence, prevention, and preemption of and defense against aggression targeted at a countries territory, sovereignty, population, and infrastructure.

3.12. Understanding Computer Investigations

3.12.1.Preparing a Computer Investigation

Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy. Collect evidence that can be offered in court or at a corporate inquiry. This is a two step process of investigating the suspect's computer and preserving the evidence on a different computer. Follow an accepted procedure to prepare a case. Approach each case methodically to evaluate the evidence thoroughly and to document the chain of evidence. Documentation is called Chain of custody which route the evidence from the time it is found to until the case is closed or goes to court.

Cases may be categorised as

- Involving a computer to execute crime
    - Eg: Drug dealer using computer to sell drug
    - Computers can contain information that helps law enforcement determine chain of events leading to a crime and contain evidence that can lead to a conviction.
    - Law enforcement officers should follow proper procedure when acquiring the evidence as digital evidence can be easily altered by an overeager investigator.
    - Hard disk and storage media include intact files, such as e-mail messages, deleted files, and hidden files. Files on the disks are probably password protected. Special software tools and experts are needed to make the investigation.

- Involving company policy violation
    - Eg: Running personal company using another companies resources
    - Personal tasks during work hours can waste company time. Employees misusing resources can cost companies millions of dollars. Misuse includes surfing the Internet, sending personal e-mails, using companies computers for personal tasks.
    - Company need to have a well defined policies and procedures. It is necessary to take a systematic approach against the employee.

The typical steps of a forensics investigation are:

- gathering evidence

- preparing a case
- preserving the evidence
-

3.12.2. Taking a Systematic Approach

- Investigator should apply the following standard system analysis steps While preparing for the case.
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence disk drive
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

The amount of time and effort needed for each step varies and it depends on the nature of the case. A systematic approach helps to gather as much information as possible. Investigator need to prepared for the unexpected and always have a contingency plan for the investigation**.**

3.12.2.1. Assessing the Case

Systematically outline the case details and begin assessing the case as follow:

- Situation—Employee abuse case
- Nature of the case —Side business conducted on the employer’s computer
- Specifics of the case —involves registering domain names for clients and setting up their Web sites at local ISPs
- Type of evidence —Small-capacity USB drive.
- Operating system —Microsoft Windows XP.
- Known disk format —FAT16.
- Location of evidence —One USB drive recovered from the employee’s assigned computer

Based on case details case requirements can be determined.

- Type of evidence
- Computer forensics tools needed
- Requirement of special operating systems

3.12.2.2. Planning Your Investigation

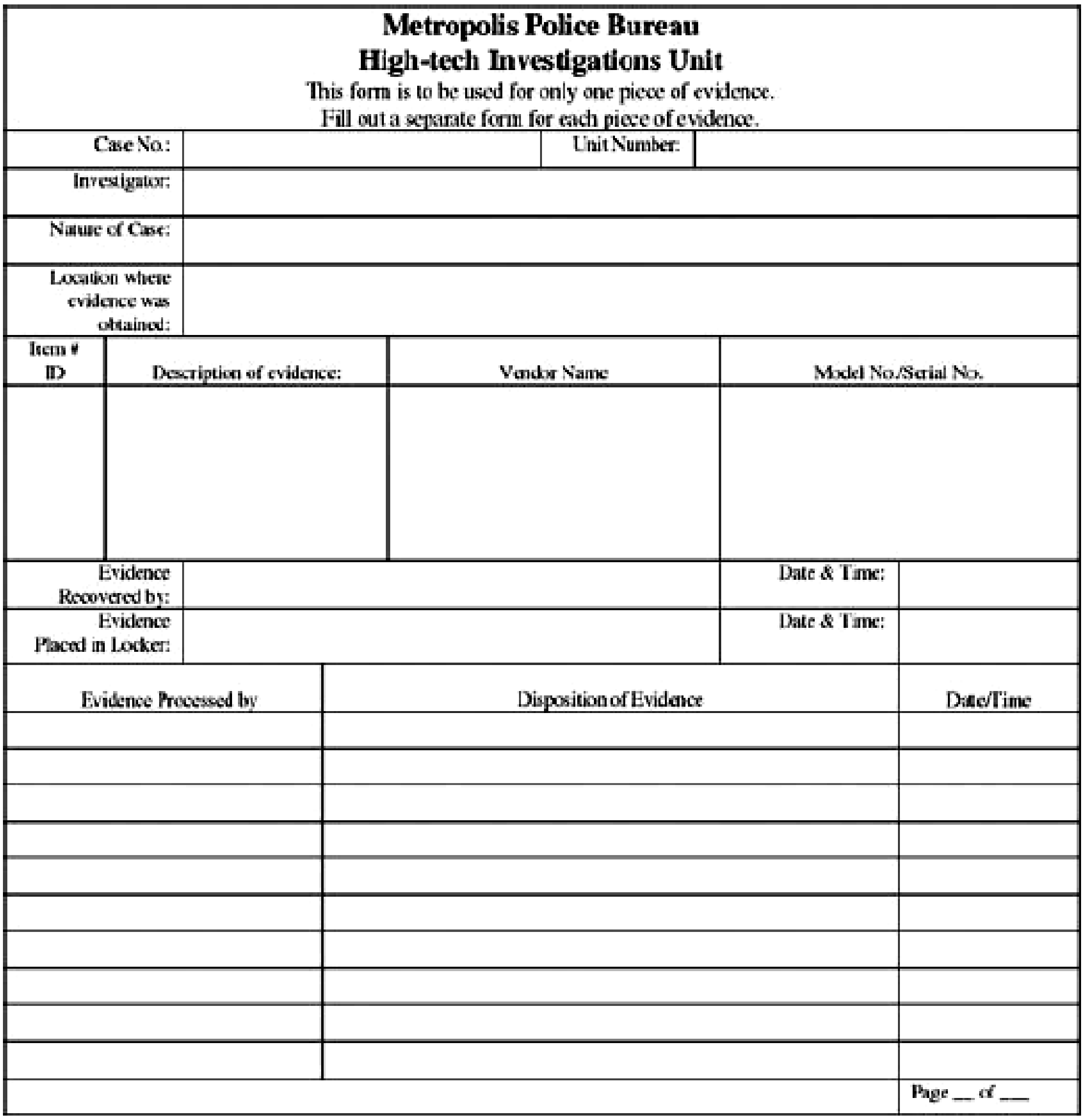
Once the requirement is identified the investigator need to plan investigation. Identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis. These steps become the basic plan for investigation. It indicates what and when to do. A basic investigation steps include the following activities:

- Acquire the evidence
- Complete an evidence form and establish a chain of custody
- Transport the evidence to a computer forensics lab
- Secure evidence in an approved secure container
- Prepare a forensics workstation
- Obtain the evidence from the secure container
- Make a forensic copy of the evidence
- Return the evidence to the secure container
- Process the copied evidence with computer forensics tools

An evidence custody form helps to document what has been done with the original evidence and its forensics copies

The first rule for all investigations is to preserve the evidence. Evidence should not be tampered or contaminated. IT Department manager confirms that the storage media is locked in a secure cabinet. The evidence has to be documented. The document include the detail about the media, who recovered it, when and who possessed it. This is done with the help of an evidence custody form, called a chain-of-evidence form. This identifies what has and has not been done with the original evidence and forensic copies of the evidence.

- Two types of form are available
  - Single-evidence form (Figure 3 12.1)
    - Lists each piece of evidence on a separate page
  - Multi-evidence form (Figure 3 12.2)

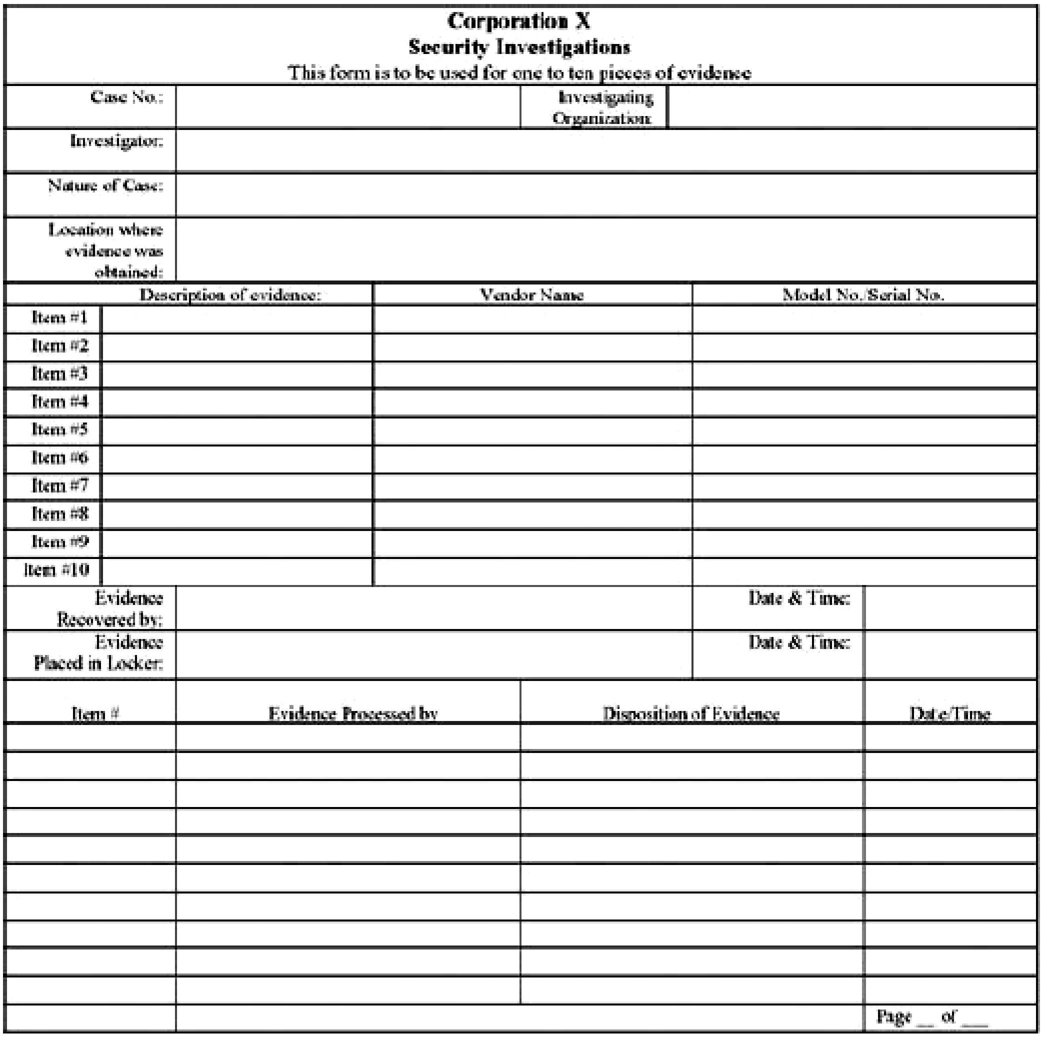


Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.
Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of ___

Figure 3 12.1 single-evidence form



Corporation X

Security Investigations

This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Description of evidence:		Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			
Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	
Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 3 12.2 A sample multi-evidence form used in a corporate environment

An evidence custody form usually contains the following information:

- Case number
- Investigating organization
- Investigator.
- Nature of case
- Location evidence was obtained
- Description of evidence
- Vendor name
- Model number or serial number
- Evidence recovered by
- Date and time
- Evidence placed in locker
- Item number/Evidence processed by/Disposition of evidence/Date/Time
- Page

A single-evidence form lists only one piece of evidence per page. This form helps in tracking separate pieces of evidence. One can accurately account what was done to the evidence and what was found. Use evidence forms as a reference for all actions taken during your investigative analysis. Both multi-evidence and single-evidence forms can be used in investigation. Single-evidence form is kept with the evidence and multi-evidence form in report file. Two forms provide redundancy that can be used as a quality control for evidence.

13.12.2.3. Securing Your Evidence

Evidence includes computer system and associated storage media. Evidence may sometime be small enough to fit into an evidence bag. Some items are too large and cannot fit into evidence bag. In such case we can use large evidence bags, tape, tags, labels, and other products. Computer media when contact with static electricity the digital data may get destroyed. To avoid this use computer safe products like Antistatic bags, Antistatic pads. Computer evidence must be placed in a well-padded container to prevent damage. Use evidence tape to seal all openings on the computer cabinet. The investigator must write initials on the tape to prove that it is not tampered. Computer components require specific temperature and humidity ranges. Make sure to provide safe environment for transporting and storing evidence until a secure evidence container is available.

13.12.3. Procedures for Corporate High-Tech Investigations

Develop formal procedures and informal checklists to cover all issues important to high-tech investigations. Procedures ensure that correct techniques are used in an investigation and informal checklists helps to be certain that all evidence is collected and processed properly.

Employee Termination Cases

Employee abuse of corporate assets like viewing pornography in the workplace and sending inappropriate e-mail messages are major reason for termination. Organization must have appropriate policies and investigator must consulting with organization’s general counsel and human resources department for specific directions on how to handle investigations.

Internet abuse investigations

- To conduct an investigation on the internet abuse of an organizations internal private network the investigator needs the following:
  - Organization’s Internet proxy server logs
  - Suspect computer’s IP address
  - Suspect computer’s disk drive
  - Computer forensics analysis tool
- Recommended steps for this investigation are
  - Use standard forensic analysis techniques and procedures
  - Use appropriate tools to extract all Web page URL information
  - Contact the network firewall administrator and request a proxy server log
  - Compare the data recovered from forensic analysis to the proxy server log
  - Continue analyzing the computer’s disk drive data

Investigator must research private law of the country as these laws are different in different countries. Some state or federal laws supersede organization’s employee policies. It is necessary to consult with the organizations attorney.

E-mail abuse investigations

- To conduct an investigation on email abuse like spam, inappropriate message, harassment investigator need to do the following.
    - An electronic copy of the offending e-mail that contains message header data
    - If available, e-mail server log records
    - For e-mail systems that store users' messages on a central server, access to the server
    - Access to the computer so that you can perform a forensic analysis on it
    - Your preferred computer forensics analysis tool
- Recommended steps
    - Use the standard forensic analysis techniques
    - Obtain an electronic copy of the suspect's and victim's e-mail folder or data
    - For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
    - Examine header data of all messages of interest to the investigation

Attorney-Client Privilege Investigations

Attorney-Client Privilege (ACP) rule is to keep all findings confidential. Attorney is the ultimate authority of the evidence. Many attorneys like to extract all data from drive as well as have printouts of the data recovered. Investigator must persuade and educate many attorneys on viewing digital evidence like CAD files. Viewing data in binary files is also a problem.

- Steps for conducting an ACP case
    - Request a memorandum from the attorney directing you to start the investigation
    - Request a list of keywords of interest to the investigation
    - Initiate the investigation and analysis
    - For disk drive examinations, make two bit-stream images using different tools
    - Compare hash signatures on all files on the original and re-created disks
    - Methodically examine every portion of the disk drive and extract all data
    - Run keyword searches on allocated and unallocated disk space
    - For Windows OSs, use specialty tools to analyze and extract data from the Registry
        - AccessData Registry Viewer
    - For binary data files such as CAD drawings, locate the correct software product
    - For unallocated data recovery, use a tool that removes or replaces nonprintable data
    - Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- Other guidelines
    - Minimize written communications with the attorney
    - Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
    - Assist attorney and paralegal in analyzing the data
- If you have difficulty complying with the directions
    - Contact the attorney and explain the problem
- Always keep an open line of verbal communication with attorney. All communication via e-mail must be encrypted.

Media Leak Investigations

In the corporate environment it is difficult to control sensitive data. An employee can send organizations sensitive data to news.

- Consider the following for media leak investigations
    - Examine e-mail
    - Examine Internet message boards
    - Examine proxy server logs
    - Examine known suspects' workstations
    - Examine all company telephone records, looking for calls to the media
- Steps to take for media leaks investigations are
    - Interview management privately
    - To get a list of employees who have direct knowledge of the sensitive data
    - Identify media source that published the information
    - Review company phone records
    - Obtain a list of keywords related to the media leak
    - Perform keyword searches on proxy and e-mail servers
    - Discreetly conduct forensic disk acquisitions and analysis
    - From the forensic disk examinations, analyze all e-mail correspondence
    - And trace any sensitive messages to other people
    - Expand the discreet forensic disk acquisition and analysis
    - Consolidate and review your findings periodically
    - Routinely report findings to management

Industrial Espionage Investigations

All suspected industrial espionage cases should be treated as criminal investigations. Dealing with foreign nationals might be violations of International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR).

- Staff needed for making this investigations are
    - Computing investigator who is responsible for disk forensic examinations
    - Technology specialist who is knowledgeable of the suspected compromised technical data
    - Network specialist who can perform log analysis and set up network sniffers
    - Threat assessment specialist (typically an attorney)

- Guidelines to follow are
    - Determine whether this investigation involves a possible industrial espionage incident
    - Consult with corporate attorneys and upper management
    - Determine what information is needed to substantiate the allegation
    - Generate a list of keywords for disk forensics and sniffer monitoring
    - List and collect resources for the investigation
    - Determine goal and scope of the investigation
    - Initiate investigation after approval from management

- Planning considerations are
    - Examine all e-mail of suspected employees
    - Search Internet newsgroups or message boards
    - Initiate physical surveillance
    - Examine facility physical access logs for sensitive areas
    - Determine suspect location in relation to the vulnerable asset
    - Study the suspect’s work habits
    - Collect all incoming and outgoing phone logs
- Steps to follow are
    - Gather all personnel assigned to the investigation and brief them on the plan
    - Gather resources to conduct the investigation
    - Place surveillance systems
    - Discreetly gather any additional evidence
    - Collect all log data from networks and e-mail servers
    - Report regularly to management and corporate attorneys
    - Review the investigation’s scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

Many years of experience is needed to become a skilled interviewer and interrogator. Corporate investigator is a technical person who acquires the evidence for an investigation. Large organizations may have well trained and experienced full time investigators. Interview is usually conducted to collect information about some facts from a witness or suspect. Interrogation is trying to get a suspect to confess .Role as a computing investigator is to instruct the investigator conducting the interview on what questions to ask and what the answers should be.

- Ingredients for a successful interview or interrogation
    - Being patient throughout the session
    - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
    - Being tenacious

3.12.4 Understanding Data Recovery Workstations and Software

Investigations are conducted on a computer forensics lab (or data-recovery lab). Computer forensics and data-recovery are related but different. Data recovery doesn't need a sterile target drive. It is just a backup of data and knows what data is being retrieved. Computer forensics workstation is specially configured personal computer loaded with additional bays and forensics software. Forensics boot floppy disk and write-blocker devices are used to avoid altering the evidence. Write blocker connects a hard drive in trusted read-only mode. Some Linux boot CDs mount all drives read-only.

Setting Up your Computer for Computer Forensics

- Basic requirements
  - A workstation running Windows XP or Vista
  - A write-blocker device
  - Computer forensics acquisition tool
    - Like FTK Imager
  - Computer forensics analysis tool
    - Like FTK
  - Target drive to receive the source or suspect disk data
  - Spare PATA or SATA ports
  - USB ports
- Additional useful items
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

3.12.5. Conducting an Investigation

- Items needed to gather resources identified in investigation plan are
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool

  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

Gathering the Evidence

Avoid damaging the evidence by using anti static bag. The following steps are to be performed to secure the evidence.

  - Meet the IT manager to interview him
  - Fill out the evidence form, have the IT manager sign
  - Place the evidence in a secure container
  - Complete the evidence custody form
  - Carry the evidence to the computer forensics lab
  - Create forensics copies (if possible)
  - Secure evidence by locking the container

Understanding Bit-Stream Copies

  - Bit-stream copy is a bit-by-bit copy of the original storage medium. It is an exact copy of the original disk.
  - Bit-stream image is a file containing the bit-stream copy of all data on a disk or partition. It is known as forensic copy.

Acquiring an Image of Evidence Media

- First rule of computer forensics is preserve the original evidence and conduct analysis only on a copy of the data.

Analyzing Your Digital Evidence

- Recover data to make an analysis. Recover from deleted area, file fragment. Forensics tools such as ProDiscover Basic can retrieve deleted files for use as evidence.

3.12.6. Completing the Case

After retrieved and analyzed the evidence investigator need to produce a final report stating what he did and what he found. Generate the document. The report generated by the forensic tools is also included in the document. **Repeatable findings:** Repeat the steps and produce the same result, using different tools. If required, use a report template to document the report. Report should show conclusive evidence. It should conclude that suspect did or did not commit a crime or violate a company policy.

Critiquing the Case

- Investigator must answer the following assessment questions to improve the investigation:
  - How could you improve your performance in the case?
  - Did you expect the results you found? Did the case develop in ways you did not expect?
  - Was the documentation as thorough as it could have been?

- What feedback has been received from the requesting source?
- Did you discover any new problems? If so, what are they?
- Did you use new techniques during the case or during research?