1.1 Introduction to cyber crime

CrimesinIndia,usingcomputersasthetool,havebeenontherise.Withtheincreasingtrendofcrimesusingcomputers,toolsarebeingbuilttopreventsuchcrimesfromhappening.Intoday'sworld,Internethasbecameanintegralpartofoureverydaylife.Every day,hackersorcriminalsattackour computerstosniffintoourpersonaldataorotherconfidentialdata.

Theterm*cybercrime*referstocrimescommittedusingcomputer(Figure1.1).Traditionally,cybercrimereferstothecrimeinvolvingcomputerandcomputernetwork.

Accordingtothelawenforcementagency,internet-relatedcrimescanbecategorizedas:

1. **Advancedcybercrime/high-techcrime:**Attacksagainstcomputerhardwareandsoftware;
2. **Cyber-enabledcrime:** Numerous'traditional'crimeshavetakenanewturnwiththearrivalofinternet,

*such*ascrimesagainstyoungsters,monetarycri1hes,andevenactsofterrorism.

Cybercrimeshaveanadverseeffectongovernments,businesses,andevenordinarypeople.Forexample,

Barnetisanetworkofinternet-connectedcomputersthatareinfectedbyvirusesandcontrolledasagroup.

Figure 1.1 Cybercrime.

If an individual wants to prevent a cybercrime, he/she has to adopt digital forensic toolstore reduce vulnerability score.

To protect our confidential data or any kind of personal data, the hard drive shouldcleansedusing a solution. As the crimes related to computer are increasing day by day, tools required to) against the same are being developed faster.

1.2 Categories of Cybercrimes.

Cybercrimes can be broadly divided into three major categories (Figure 1.2).

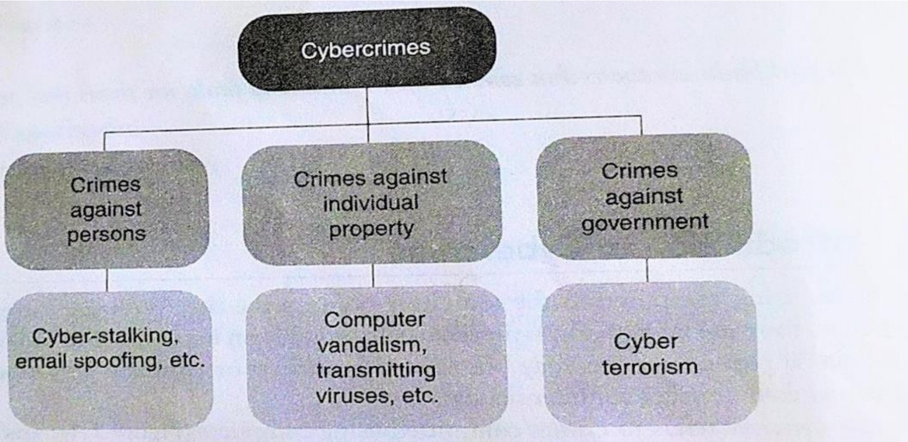

Cybercrimes
Crimes against persons
Crimes against individual property
Crimes against government
Cyber-stalking, email spoofing, etc.
Computer vandalism, transmitting viruses, etc.
Cyber terrorism

Figure 1.2 Categories of cybercrime.

1.2.1 Cybercrimes Against People

Cybercrimes committed against people includecrimessuch as cyber porn,transmission ofchild pornography, harassment of an individual through email, false legal agreement scams, etc. The trafficking, distribution, posting, and dissemination of obscene material, together with pornography and misdemeanour. constitute important Cybercrimes committed against people. The potential impact of such a criminal offense to humanity can hardly be explained. Cyber harassment could be a distinct cybercrime. Various harassments can and do occur in internet, or through the use of internet. This includes sexual, racial, religious, other harassments. People perpetuating such harassments arc guilty of cybercrimes.

1.2.2 CybercrimesAgainstProperty

Cybercrimeagainstallformsofpropertyisthesecondcategoryofcybercrime.Crimesin thiscategory include computerdevilry,meaningdesructionofothersproperty andtransmissionofharmfulviruses,wormorprograms.AnIndian-basedupstartengineerngcompanyloseicsmoneyandreputewhenhe rival company,anassociatedegreebusinessmajor,scarfedthetechnical cataloguefromtheircomputerswiththe assistanceofacompanycyberspysoftware.

1.2.3CybercrimesAgainst Government

CybercrimesagainstGovernmentisthethirdtypeofcyber crime.Cyberterrorismisadistinctcrimeinthiscategory.Thespreadofinternethasshownthatthis mediumisusedbypeopleandteamscothreatentheinternationalgovernmentsconjointlytoterrorizethe votersofarustic.Thiscrimemanifestsitselfinto anactofterrorismonceaprivate'cracks'intoagovernmentormilitarymaintainedwebsite.

1.3Types of Cyber Crimes

Cybercrimescanbebroadlydividedas:

1. Violentor potentiallyviolentcybercrimes:Violentorpotentiallyviolentcybercrimesarethosethatposeaphysical risktosomecharacterorpeople.Theycan befurthercategorizedas:

(a) Cyberterrorism
(b) Cybertalking
(c) Assaultsbythreat
(d) Childpornography

2. Non-violentcybercrimes:Non-violentcybercrimesarethosethat do notdirectlyposeaphysicalrisk

tosome characterorpersons,butindirectlytheydo posearisk.They canbecategorized furtheras:

(a) Cybertheft
(b) Cybertrespass
(c) Cyberfraud
(d) Destructivecybercrimes

Inthissection,wewilldiscusshacking,Dosattack,Trojanattack,creditcardfrauds,cyberpornography.onlinebetting,softwarepiracy,emailspoofing,forgery,phishing,cyberterrorism,Salamiattacks, defama-tion,andcyberstalking.

1.3.1 Hacking

Do not hack, but when you do, it should be ethical!

Eric Raymond, compiler of The New Hacker's Dictionary, defines a hacker as an artless coder. A 'good hack may be a clever answer to a programming difficulty and 'hacking' (Figure 1.3) is the ace of doing it.

According to Raymond, the following five likely characteristics qualify one as a hacker:

1. An individual who enjoys learning details of a programming language or system.
2. An individual who enjoys truly doing the programming instead of simply theorizing it.

.

3. An individual capable of appreciating somebody else's hacking
4. An individual who picks up programming quickly.
5. An individual who is a professional in a specific programming language or system.

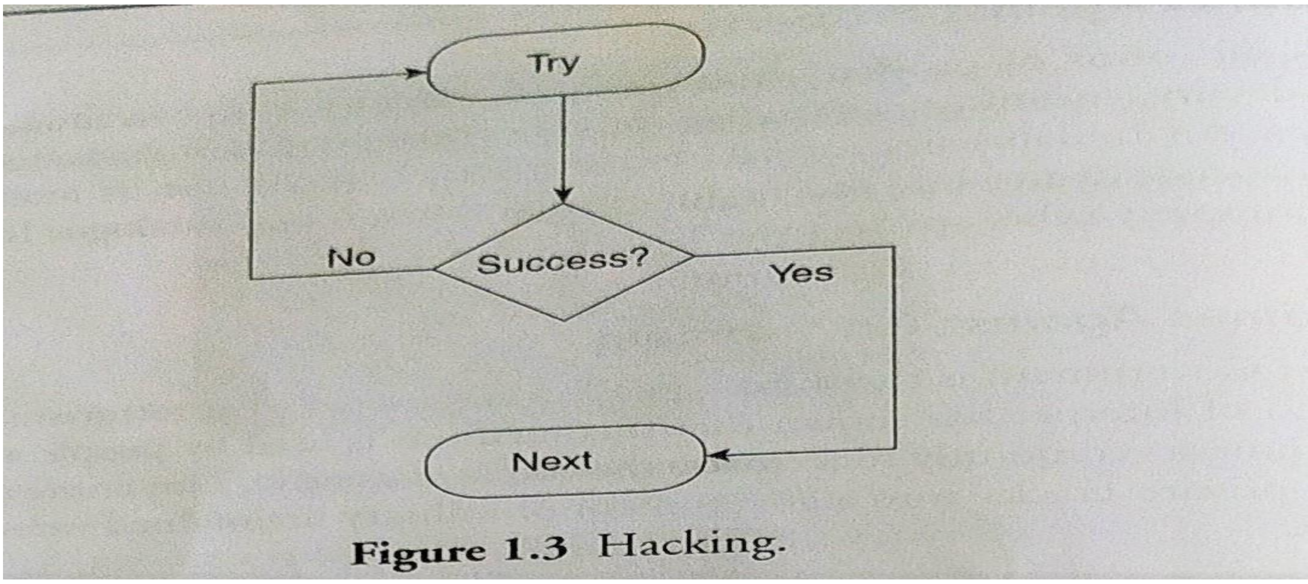


Figure 1.3 Hacking.

1.3.2 Denial-of-ServiceAttacks(DoSAttacks)

ADenial-of-Servic e(DoS)attackisatrialtomakeanonlineserviceunavailablebyoverloadingthenetwork trafficfrommultiplesources.DoStargetsalargevarietyofresources(Figure1.4).

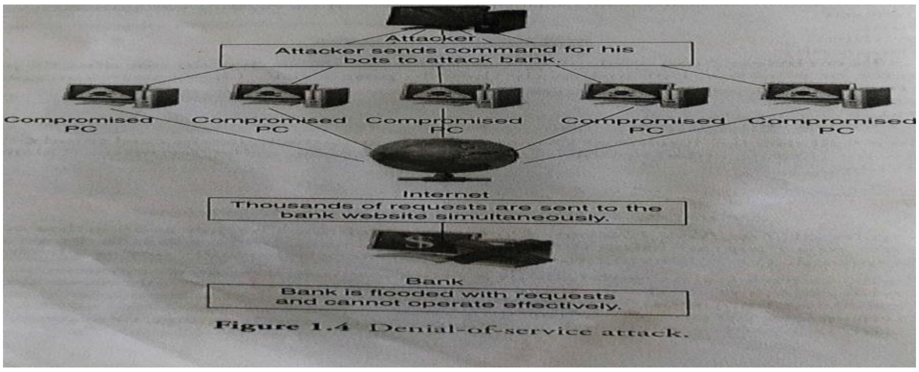

Attacker
Attacker sends command for his bots to attack bank.
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Internet
Thousands of requests are sent to the bank website simultaneously.
Bank
Bank is flooded with requests and cannot operate effectively.

Figure 1.4 Denial-of-service attack.

1.3.3 TrojanAttacks

Trojansaremallparticlesofmalwarethatallowthehackertoeithergainorobtainremoteaccesstoanycomputer.Trojanscanneitherself-replicatenorautomateastheyinteractwiththehackertomeetan<lfulfillhis/herpurpose(Figure1.5).

Trojansneedtobeinstalledfromanexecutablefile(.exe)oracompiler.Sometimes, Trojansexploitthebugsinthebrowser,mediaplayer,etc.OncetheTrojanisinstalled,thehackercan

usethemtoaccessallthe sensitiveorconfidentialandpersonalinformation ordata.

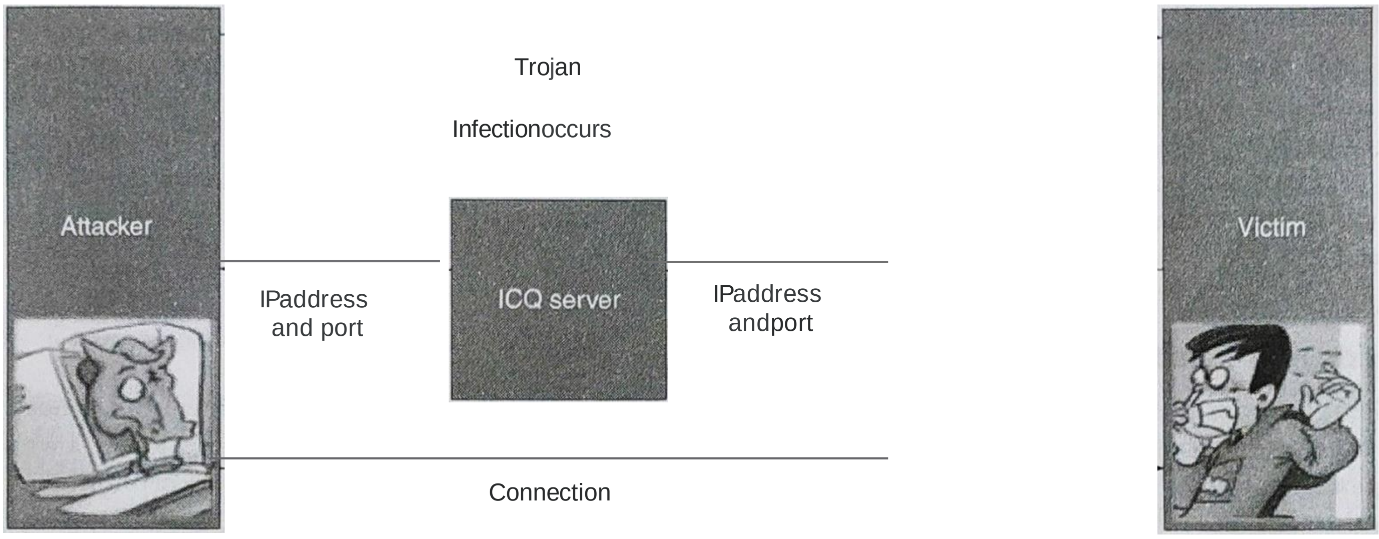


Figure1.5 Trojan.

1.3.4 CreditCardFrauds

Creditcardfraudsusuallyoccurwhenanindividualdiscloseshis/herconfidentialdatasuchascreditcardnumber ,CWnumber,secretcodefortransaction,expirydate,etc.,toanunknownperson,whocouldbea potentialhacker.Thisisoftenthecasewhena cardisstolenorlostorwhenmailsaredivertedfromtheactualrecipienttothehacker.

Thiskindoffraudisanidentityfraudinwhichahackerrakesthenecessaryinformationaboutthecreditcardforhis /herpersonalpurpose.

1.3.5 CyberPornography

Cyberpornographyreferstodistributingpornographyovertheinternet.Peoplecreateanddistributepornorobscenematerialsovertheinternet.Itincludeschildreninvolvedinsexualacts withadults.Itisacriminaloffenseandisclassifiedascausingharmtohumans.ItreferstoSection67of ITAct,whichisthemostseriousIndianLaw. TheotherlawsthatdealwithpornographyareIndecentRepresentationofWomenActandtheIndianPenalCode.Itisaseriouscrime inIndia,butnotconsideredsoinmanyothercountriessuchasUnitedStatesofAmerica(USA).

1.3.6*OnlineBetting*

Onlinebettingisalsocalledonlinegamblingorinternetgamblingandtakesplaceovertheinternet.Onlinegamblingisthebasictermusedforgamblingovertheinternet.Manywebsitesavailableovertheinternetareusedfor gambling.

1.3.7 Software Piracy

Software piracy refers to the act of distributing licensed or paid or copyrighted software for free or at a minimal the internet. It is considered to be the most profitable business. According to the Business software approximately of the total software that are currently being used across the globe Olen or What it means is the unauthorized copying of software and retailing it over the internet for free or at lower cost. The percentage of software piracy grew to 39% in the recent survey carried out in May.

1.3.8. Email Spoofing

Email spoofing refers to sending emails from an unknown or false source. Spoofing means that the hacker an email from your email address. The hacker tries to send spam emails or emails that include attractive offers, which the individual accepts and fills certain details. The hacker simultaneously receives all the necessary email ids and passwords. In recent times, even viruses are transmitted over emails. These viruses reside in our device or emails, and are constantly monitored by the hacker. This will be discussed in detail in Chapter 12.

1.3.9 Forgery/Falsification

Forgery refers to the action of forging a copy or imitation of a document, signature, or banknote. It is done to earn a huge profit by selling the forged resource. Forgery is nothing but the creation of a wrong written document or alteration of an original document with the intention of defraud or deception. Forgery comes under criminal law, with the penal code as Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC). Forgery is a serious crime that harms any human for his/her personal benefit.

1.3.10 Phishing

Phishing is a fraud type wherein the hacker tries to get personal information, including login credentials or any bank account information, by pretending to be a genuine entity in email, messages, or other communication channels. In this type of crime, the victim receives a fake email from a company or organization or a genuine source. These emails generally include an attachment or an outbound link that installs harmful malware or virus on the victim's device or may redirect the victim to a harmful or malicious website, developed to cheat the victim and get the personal and other financial details or 'information such as username, email-ids, passwords, credit card or debit card details, etc. Phishing is an attempt .to obtain sensitive information from the user or victim•

1.3.11 Cyber Terrorism

Cyber terrorism is a planned activity in the cyber space via computer networks. It includes the use Of email as a communication medium. The term 'cyber terrorism? 'is a controversial term that includes actions Of deliberateness, disruption of networks over a large-scale, especially personal desktops or devices which are attached to the internet by using tools such as viruses or malware. Examples of cyber terrorism include hacking of medical database, which involves changing or deleting the facts, leading to a wrong treatment'

1.3.12 Salami Attacks

Salami attack is a combination of many small attacks that can go undetected due to the nature of cybercrime It is also known as salami slicing or penny shaving, where the attacker uses an online database to seize the customer information such as bank/credit card details, deducts minuscule amounts from every account over a period of time•

These amounts, unnoticeably taken from collective accounts, add up to a large amount of money. Most people fail to report such deductions, often letting it go because of the amount involved, which could be a fraction of a cent, so as to avoid

suspicion from the unsuspecting customer. A salami attack is a small attack that can be repeated many times efficiently. Thus, the overall impact of the attack is huge. For example, stealing the round-off amounts from the interest in bank accounts. Even though it is less than I cent per account, when multiplied by millions of accounts over many months, the adversary can retrieve quite a large amount. It is also less likely to be noticeable since your average customer would assume that the amount was rounded down to the nearest cent.

1.3.13 Defamation

Internet is an integral part of our life. It acts as a medium for interacting with people across the globe.

Defamation implies causing harm to a reputed individual in front of others. Harm can be inflicted by oral words, visuals, or any other means. Cyber defamation is a new concept, and it involves defamation of a person or individual by a new or virtual medium. Cyber defamation is considered to be a cybercrime. Cyberdefamation not only affects the welfare of the community, but also the victim.

1.3.14 Cyber Stalking

Cyber stalking refers to the use of an electronic medium to threaten someone or an individual or a group of people or certain organization. This may include wrong allegations, threatening calls or messages or emails, wrong accusations, any kind of defamation, wrong identity theft, and many more. Cyber stalking is a criminal offense under various harassment laws. It is a kind of online stalking. Cyber stalkers could be strangers, people who you may know, people who know you, ex-business partners, enemies, and many more.

1.4The Internet Spawns Crime

The internet is a network of communication and content services that is globally accessible. As internet provides a lot of options for buying and selling, crimes are on the rise in this environment. A computer represents a tool of crime as in murder or fraud, the object of crime as in stealing of processor chips, or the theme of crime as in hacking and spreading viruses. The involvement of computers on criminal rule has been much ampler than the narrow field of activities such as hacking and spreading viruses, both not easy for traditional criminal concepts, and facilitating particular types of crimes such as child pornography.Criminal commandment is not just about whether a particular work should be considered criminal or not. It is a law enforcement that investigates those that carry out criminal acts and prosecutes them; it is a procedure more significantly difficult in a computer environment. The implementation of internet technologies is not uniform, particularly between developed and developing nations. Wireless communication technologies have quickly eclipsed wire systems in many developing countries, where the inheritance communication was greatly underdeveloped. Differential technological use may mean dissimilar patterns of threats and vulnerabilities In terms of cybercrimes

1.5Worms Versus Viruses

Worms and viruses are malicious programs that can cause harm to our system. However, both these termsare very different.

1.5.1 Viruses

A virus (vital information resources under siege) is a software that is designed to duplicate itself. This is done by replicating itself into various programs that are stored in the computer. Computer viruses attach themselves to a. program or a file, spreading from one workstation to another, leaving infections as it travels can damage software, or files. Almost all viruses are fond of an executable file, which means acomputer virus can range in harshness, some may cause slightly irritating effects while others cannot affect our computerunless and until we run or release the malicious program. It is significant to make a note that a virus cannot spread without human action, such as running the infected program (Figure 1.6).

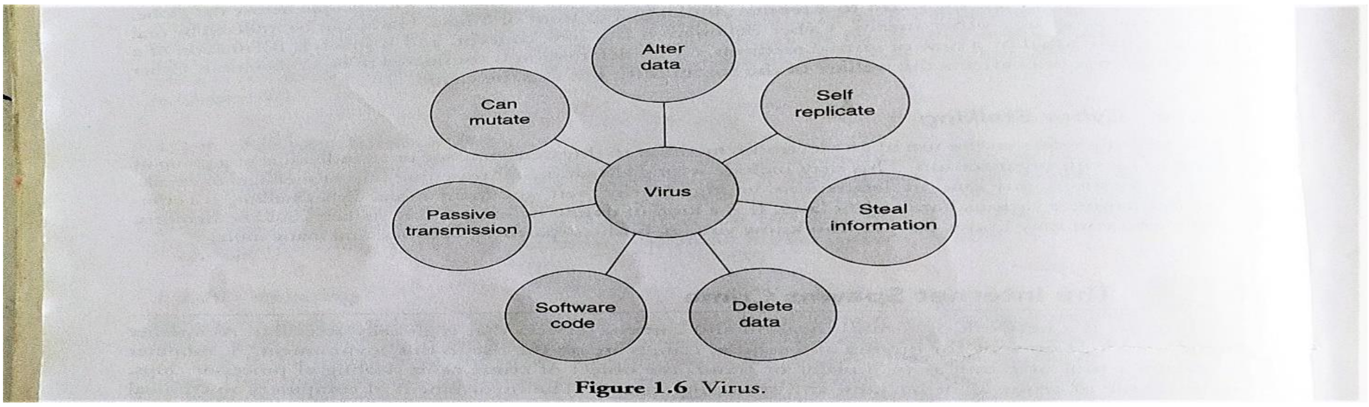


Figure 1.6 Virus.

1.5.2 Worms

A worm (write once read many) is similar to a computer virus by design. It is considered to be a secondary category of virus. A worm spreads from computer to computer, but unlike virus it has the capability to travel without any human action. The main threat with a worm is the capability to replicate itself on our system• So rather than our computer sending a single worm, it could send hundreds or thousands of copies of itself and cause a huge devastating effect. For example, a worm sending out a

copy of itself to everyone listed in the address book, then the worm replicates itself to each of the receiver's address book and it manifests itself• Since the worm copies itself and also travels across networks, it consumes more system memory and network bandwidth, causing web servers and individual computers to stop responding (Figure 1.7).

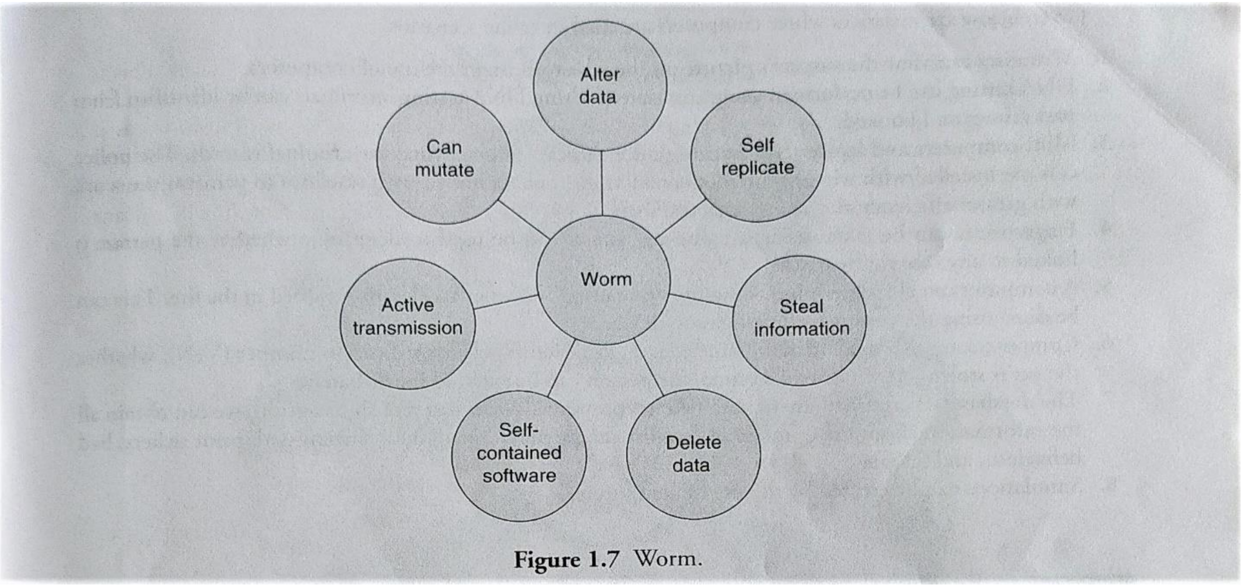
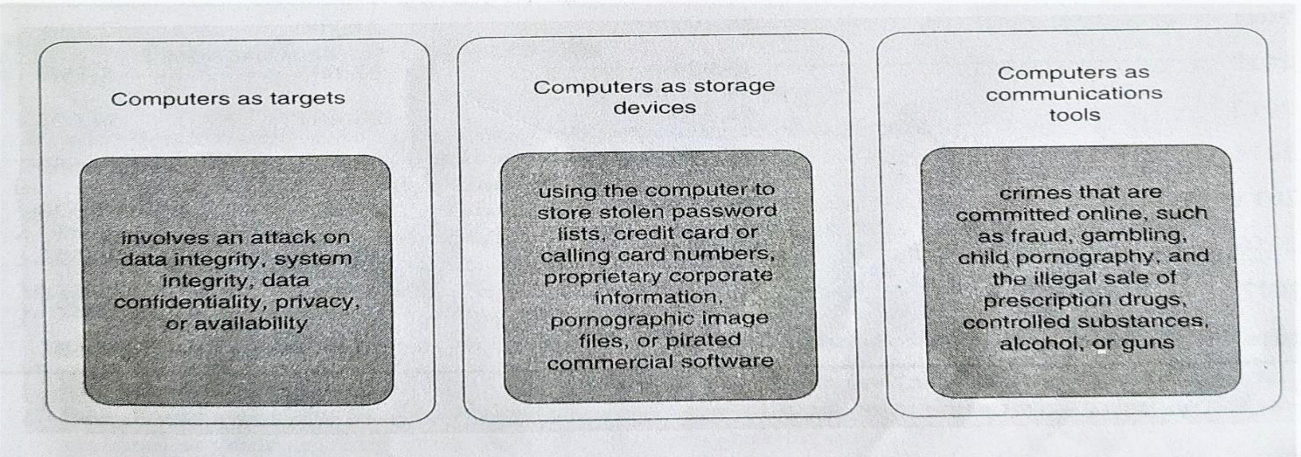


Figure 1.7 Worm.

1.6 Computer Role in Crimes

Computers can play a vital role in crimes as shown in Figure 1.8. They can extract evidences, instrumentality, illegal imports, or the fruit of a crime.

1. They can act as a communication tool.
2. They can be the target of the attacker for criminal activity.
3. They can also be tangential to crime.



Computers as targets

involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Computers as storage devices

using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

Computers as communications tools

crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Figure 1.8 Roles of computer in crimes.

Given below are instances where computers are used in crime scenarios.

1.Witnesses can view the suspect's picture on the screen through the use of computers.

2. DNA testing and can booked.be performed using computers. Using DNA testing, criminals can be identified from past crimes

3. Mini computers and laptops are used in police vehicles to determine the criminal records. The police cars are installed with wireless internet connections that are linked with satellites to perform the work with greater efficiency and in an easier manner.

4. Fingerprints can be taken using a computer and it can be used to determine whether the person is linked to any case in the past.

5. A computer can also determine how a fire was caused and what accelerant was used in the fire. This can be done using the computer investigation device.

6. Computers are also used at traffic junctions to find the vehicle identification number (VIN), whether the car is stolen, etc. In case of a crime, the person can be arrested immediately.

7. The databases of criminals are maintained in computers. With just a push of button, we can obtain all the information about the criminal. Also a list can be maintained of all citizens with prior tickets, bad behaviour, and felonies.

Simulations can be created by the use of computers.

1.7Cybercrime Statistics in India

Total cybercrimes, including fishing malicious code, website intrusion, denial of service, scanning, etc., that occurred in the last eight years are given in Table 1.

Table 1.1 Year-wise cybercrimes in India (Statistics presented in the Lok Sabha 2018)

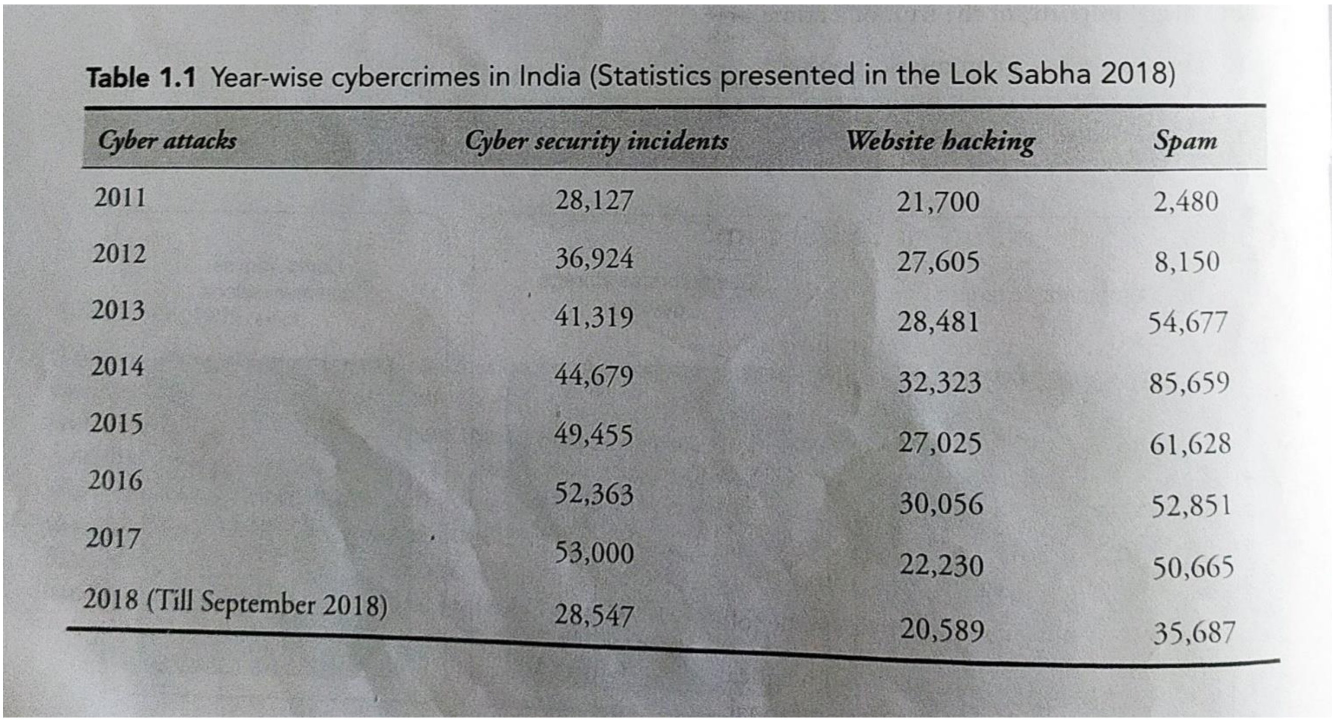


Table 1.1 Year-wise cybercrimes in India (Statistics presented in the Lok Sabha 2018)

Cyber attacks	*Cyber security incidents*	*Website hacking*	*Spam*
2011	28,127	21,700	2,480
2012	36,924	27,605	8,150
2013	41,319	28,481	54,677
2014	44,679	32,323	85,659
2015	49,455	27,025	61,628
2016	52,363	30,056	52,851
2017	53,000	22,230	50,665
2018 (Till September 2018)	28,547	20,589	35,687

2.1Introduction to Digital Forensic

Forensic science is a well-established science that plays a critical role in criminal justice systems. The origin of the word "forensic" can be traced back to the Latin word "forensis", which means open court. Forensic science is often referred to as forensics. Forensic science is applied in both criminal and civil actions. Therefore, effectively forensics means legal or related to courts.

Digital forensics is also referred to as digital forensic science, a branch of computer forensic science that includes the restoration and inspection of material detected in digital devices, often in relation to a cybercrime. Information and Communications Technology (ICT) working environments face the challenge of prolonged computer use for activities that are not work-related. User activity portrayals

may consist of browsing the Internet for one's own purpose and utilizing online search engines for work-related information. However, browsing sessions are not specific to only the above-mentioned activities.

With the emergence of ICT, there have been simultaneous advancements in social networking, mobile technology, cloud computing, and storage solutions that have increased the information flow within organizations. This has weakened the security of organizational data. The increasing activity in ICT-focused environments has also led to an increase in the misuse of computer and network. A common employee can use simple password cracking tools to gain access to managerial account information, for fraud and theft of company resources as many open source tools are available to perform illegal activities.

Increased computer and network misuse have led to an increase in computer-related investigations. Investigation includes certain hypothesis or observable phenomenon that is verified by These developments in investigation have led to auditing being the key in answering questions user activity and cybercrime,

The field of digital forensics has made some rapid developments over the past few years due in tools and systems that allow ordinary computer users to be more proficient in performing difflicult audit tasks. Many literature and internet searches are available that guide a trivial and easy user on how to perform simple tasks aimed at gaining access to any computer. This has enabled the computer user to access ail types of information, such as copied music. pornography, confidential documents, illegal software and so on. Thus, there is an increased demand in computer security mechanisms in an effort to control such activities and a growing need for forensic tools to gather accurate digital evidence, According to Beebe, the lack of digital forensic standardization and process results in limited prosecution that is not acceptable in the court of law.

Numerous forensic tools are freely available, creating a misconception among the common man that anyone can conduct a computer forensic investigation. The forensic tools used have various features that facilitate digital forensic investigations (DFIs). In a court of law, the process followed in gathering the digital evidence and the digital evidence itself is important. Unfortunately, the court proceedings focus on scrutinizing the validity of the process followed in evidence handling before considering its value.

Numerous procedures have been proposed for the collection of digital forensic evidence. Committees such as the Digital Forensic Research Workshop Group (DFRWS) and the American Society of Digital Forensics and e Discovery (ASDFED) have proposed processes to be followed in the collection of digital evidence. From this, it follows that there -is no standard forensic process in place that can be followed by digital forensic investigators. It would be a serious mistake for a forensic investigator to ignore the procedure of evidence collection in cases where the evidence aids in proving the case and leaves no doubt in the minds of those having to decide on the matter. Where evidence is presented without proof of thorough procedure, the defence may question the forensic procedure followed to collect the digital evidence. The famous American court case of Simpson is an example where the forensic process was scrutinized by the defence. In this case, the crime scene evidence was collected. However, a robust evidence collection process was not followed, hence, the evidence was invalidated by the defence. Tools' Such as Encase have been accepted as a reliable solution in computer crime investigations.' Both the Process followed when using Encase and the resulting digital evidence have been accepted as reliable. Other tools have also been used successfully, such as FrK and Sleuth Kit. Some are commercially available while others are open source. Many of these tools have been validated and accepted as reliable by the American •However, the evidence collection process and the digital evidence presentation are vital' in •any successful prosecution. Digital forensics can be defined as follows:

Digital Forensic is a series of steps to uncover and analyze electronic data through scientific method, The major goal of the process is to duplicate original data and preserve original evidence then performing the series of the investigation by collecting/identifying and validating the digital information for the purpose of reconstructing past events.

2.2 Need of Digital Forensics

Computer forensics is the process of using of science and technology with sciences to collect, analyze, and present proofs •the criminals or civil courts. Network administrator and security staff administer and manage networks and information systems should have complete knowledge computer forensics. The meaning of the word 'forensics" is% bring to the court".

It is necessary for network administrator and security staff of networked organizations to practice computer forensics and should have knowledge of laws, because rate of cybercrimes is increasing greatly.If your network is attacked and intruder is caught, then good knowledge about computer forensics will help to provide evidence and prosecute the case in the court.There are many risks if you practice computer forensics badly. If you do not take it in account, then vital evidence might be destroyed. New laws are being developed to protect customers' data; but, if certain kind of data is not properly protected, then many liabilities can be assigned to the organization. As organizations are increasing in number and the risk of hackers and contractors is also increasing, so they have developed their own security systems. Organizations have developed security devices for their network like intrusions detection systems (IDS), proxies, firewalls which report on the security status of network of an organization. So, technically, the major goal of computer forensics is to recognize, gather, protect and examine data in such a way that protects the integrity of the collected evidence to use it efficiently and effectively in a case.

2.3 Rules of Computer/DigitalForensic

While performing a DFI, the investigator should go by the following rules:

Rule 1. An examination should never be performed on the original media.
Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.
Rule 3. The copy of the evidence must be an exact, bit-by-bit copy (Sometimes referred to as a bit-stream copy).
Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified (Use a write blocking device when possible).
Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.
Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

2.4 Types of Digital Forensics

Digital forensics is a constantly evolving scientific field with many subdisciplines. Some of these subdisciplines are as follows:

1. Computer Forensics — the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops, and storage media in support of investigations and legal proceedings. The purpose of computer forensics is to obtain evidence from various computer systems, storage mediums, or electronic documents. Throughout the course of our investigations, we can obtain a wide range of information, including system and file transfer logs; internet browsing history; email and text communication logs; hidden, deleted, temporary, and password-protected files; sensitive documents and spreadsheets; and many more.
2. Network Forensics — the monitoring, capture, storing, and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, that is, worms, virus, or malware attacks, abnormal network traffic and security breaches. The purpose of network forensics is to monitor and analyze computer network

traffic, including LAN/WAN and internet traffic, with the aim of gathering information, collecting evidence, or detecting and determining the extent of intrusions and the amount of compromised data.

1.Should contribute to the society and human being.
2.Should avoid harm to others.
3.Should be honest and trustworthy.
4.Should be fair and take action not to discriminate.
5.Should honor property rights, including copyrights and patents.

6. Should give proper credit to intellectual property.
7. Should respect privacy of others.

8. Should honor confidentiality.

2.5.1 Unethical Norms for Digital Forensic Investigation

The investigator should not:

1. Uphold any relevant evidence.
2. Declare any confidential matters or knowledge learned in an investigation without an order from a court of competent jurisdiction or without the client's consent.
3. Express an opinion on the guilt or innocence belonging to any party.
4. Engage or involve in any kind of unethical or illegal conduct.
5. Deliberately or knowingly undertake an assignment beyond his or her capability.
6. Distort or falsify education, training or credentials.
7. Display bias or prejudice in findings or observations.
8. Exceed or outpace authorization in conducting examinations.

2.6 Digital Forensic Investigations

Digital investigations, DFIs, forensic examination, and forensic investigations have been used to describe an investigation where a digital device forms part of the incident. For the purposes of this study, the term "digital forensic investigation" (DFI) is used. The terms will, however, be used interchangeably in this section to reflect the opinions of other authors. The successful outcome of a DFI is the presentation of digital evidence. A DFI is conducted by an appropriately certified investigator.

A DFI is thus a special type of investigation wherever scientific procedures and techniques used can permit the results, that is, the digital proof, to be allowable in a court of law. The results of a DFI should have a legal basis. Proof cannot be directly read, and a few tools are employed to look at the state of the information. One in every tool to watch the state of digital knowledge is indirect knowledge observation. This is similar to being told concerning one thing rather than seeing it for you, formally referred to as rumour within the rules of proof. The burden you attribute to the evidentiary worth relies on the extent to which the tool is trustworthy.

Digital forensic investigation or DFI is a special type of investigation where the scientific procedures and techniques used will be allowed to view the results — digital evidence — to be admissible in a court of law.

2.7Introduction to Digital Evidences

The field of computer security includes events that provide a successful courtroom experience, which are both worthwhile and satisfactory. Investigation of a computer security incident leads to a legal proceeding, such as court proceeding, where the digital evidence and documents obtained are likely used as exhibits in the trial.

To meet the requirements of the judging body and to withstand or face any challenges, it is essential to follow thc evidence-handling procedures. Also, it is necessary to ensure that the evidence-handling procedures chosen are not difficult to implement at your organization as this can sometimes become an overhead for an organization. In this chapter, we will discuss; the collection, handling, and storage of information in an appropriate manner. We will also explain the effective and efficient evidence-handling procedures along with the guidelines for implementing these procedures in your organizations.

While investigating a computer security -incident, we are sometimes unsure and indecisive whether anitem (viz., a chip, floppy disk, etc.) should be considered as an evidence or an attachment.

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.

Evidence can be stated as any information that can be confident or trusted and can prove something related to a case in trial, that is, indicating that a certain substance or conditionis present. It is safe to use such information as evidence during an investigation. Many materials or objects can help us prove our case, such as document, electronic media, electronic files, printouts, or other objects obtained during an investigated as evidence or proof and handled according to your organ 170 F,

Figure 2.1 Examples of digital devices.

2.7.1 The Best Evidence Rule

The best evidence rule is that the original or true writing or recording must be confessed in court to prove its contents without any expectations. In the best evidence rule, an original copy of the document is considered as superior evidence. One of the rules states that if an evidence is readable by sight or reflects the data.

accurately, such as any printout or data stored in a computer or similar devices or any other output, it is considered as "original". It states that multiple copies of electronic files may bc a part of the "original" or equivalent to the "original". The collected electronic evidence is mostly transferred to different media.

Hence, many computer security professionals are dependent on this rule.We define best evidence as the most complete copy or a copy which includes all necessary parts of evidence, which is closely related to the original evidence. One of the best evidences is having the original evidence media. Let us say a client has a copy of the original evidence media. Then, it is considered as the best evidence. We treat forensic duplication by considering it as the best evidence. Therefore, when we say "best evidence", it refers to the evidence we have in our power.

2.7.2 Original Evidence

Sometimes the procedure adopted to deal with a situation or case takes it outside the control of the client/ victim. We also assume that a case with proper diligence or a case with persistent work will end up in a judicial proceeding, and we will handle the evidences accordingly. If criminal or civil proceedings (proceedings other than criminal proceeding in a court) are a possibility, then we often persistently push the client/victim to allow us to handover all the original evidences, since we have evidence-handling procedures in place.

For our purpose, we define original evidence as the truth or real(original) copy of the evidence media which is given by a client/victim. We define best incidence as the most complete copy, which includes all the necessary parts of the evidence that are closely related to the original evidence. It is also called as duplication of evidence media. There should be an evidence protector which will store either the best evidence or original evidence for every investigation in the evidence safe.

2.8Rules of Digital Evidence

Rule of evidence is also called as law ofevidence. It surrounds the rules and legal principles that govern all the proof of facts.

This rule helps us to determine what evidence must or must not be considered by a trier off act. The rule of evidence is also concerned with the amount, quality, and type of proof which helps us to prove in a litigation. The rules may vary according to the criminal court, civil court, etc. The rules must be:

1. Admissible: The evidence must be usable in the court.
2. Authentic: The evidence should act positively to an incident.
3. Complete: A proof that covers all perspectives.
4. Reliable: There ought to be no doubt about the reality of the specialist's decision.
5. Believable: The evidence should be understandable and believable to the jury.

Rule 103: Rule of evidence

1. Maintaining a claim of error.
2. No renewal of objection or proof.
3. Aim an offer of proof. 4. Plain error taken as notice.

Evidence collection should always be performed to ensure that it will withstand legal proceedings. Key criteria for handling such evidence are outlined as follows:

1• The proper protocol should be followed for acquisition of the evidence irrespective of whether it physical or digital. Gentle handling should be exercised for those situations where the device may be damaged (e.g., dropped or wet).

2. in handling through may disk be formatting, required for it may need situations. to be shut For example, down immediately when the device to preserve is actively theother hand, in some situations, it would not be appropriate to shut down the device so that digital forensics expert can examine the device's temporary memory.

3.All physical and/or digital should be collected, retained, and transferred using a preserved change of a custody

4.All materials should be date and time stamped, identifying who collected the evidence and the it is being transported to after initial collection.

5. When Proper storing logs should evidence, be maintained suitable access when controls transferring should possession.be implemented and tracked to the evidence has only been accessed by authorized individual.

2.9Characteristics of Digital Evidence

This section provides a few hints of the essence and characteristics of digital evidence. These can help and challenge investigators during an investigation.

2.9.1 Locard's Exchange Principle

According to Edmond Locard's principle, when two items make contact, there will be an interchange. The Locard principle is often cited in forensic sciences and is relevant in digital forensics investigations.When an incident takes place, a criminal will leave a Locard hint evidence exchange at principle. the scene Many and remove methodsa hint evidence from the scene. This alteration is known as the been suggested in conventional forensic sciences to strongly prosecute criminals. Techniques used consist of blood analysis, DNA matching, and fingerprint verification. These techniques are used to certicance of a suspected person at a physical scene. Based on this principle, Culley suggests that where Ty there the exit is communication with a computer system, clues will be left.

2.92 Digital Stream of Bits

Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays to display information. The information in continuous bits will rarely make sense, and tools are needed to show (hest structures logically so that it is readable.Thecircumstances in which digital evidence are found also helps the investigator during the inspection• Metadata is used to portray data more specifically and is helpful in determining the background of evidence.

2.10Types of Evidence.

There are many types of evidence, each with their own specific or unique characteristics. Some of the types of evidence are as follows:

1. Illustrative evidence
2, Electronic evidence
3.Documented evidence
4.Explainable evidence
5.Substantial evidence
6.Testimonial

2.10.1 Illustrative Evidence

Illustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is a common form of proof. For example, photographs, videos, sound recordings, X-rays, maps, drawing, graphs, charts, simulations, sculptures, and models.

2.10.2 Electronic Evidence

Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased. The evidences or proof that can be obtained from an electronic source is called as digital evidence (viz., emails, hard drives, word-processing documents, instant message logs, ATM transactions, cell phone logs, etc.)

2.10.3 Documented Evidence

Documented evidence is similar to demonstrative evidence. However, in documentary evidence, the proof is presented in writing (viz., contracts, wills, invoices, etc.). It can include any number of medias. Such documentation can be recorded and stored (viz., photographs, recordings, films, printed emails, etc.).

2.10.4 Explainable Evidence (Exculpatory)

This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case. It is also referred to as exculpatory evidence.

2.10.5 Substantial Evidence

A proof that is introduced in the form of a physical object, whether whole or in part, is referred to as substanrial evidence. It is also called as physical evidence. Such evidence might consist of dried blood, fingerprints, and DNA samples, casts of footprints, or tires at the scene of crime.

2.10.6 Testimonial

It is a kind of evidence spoken by a spectator under oath, or written evidence given under oath by an official declaration, that is, affidavit. This is one of the common forms of evidence in the system.

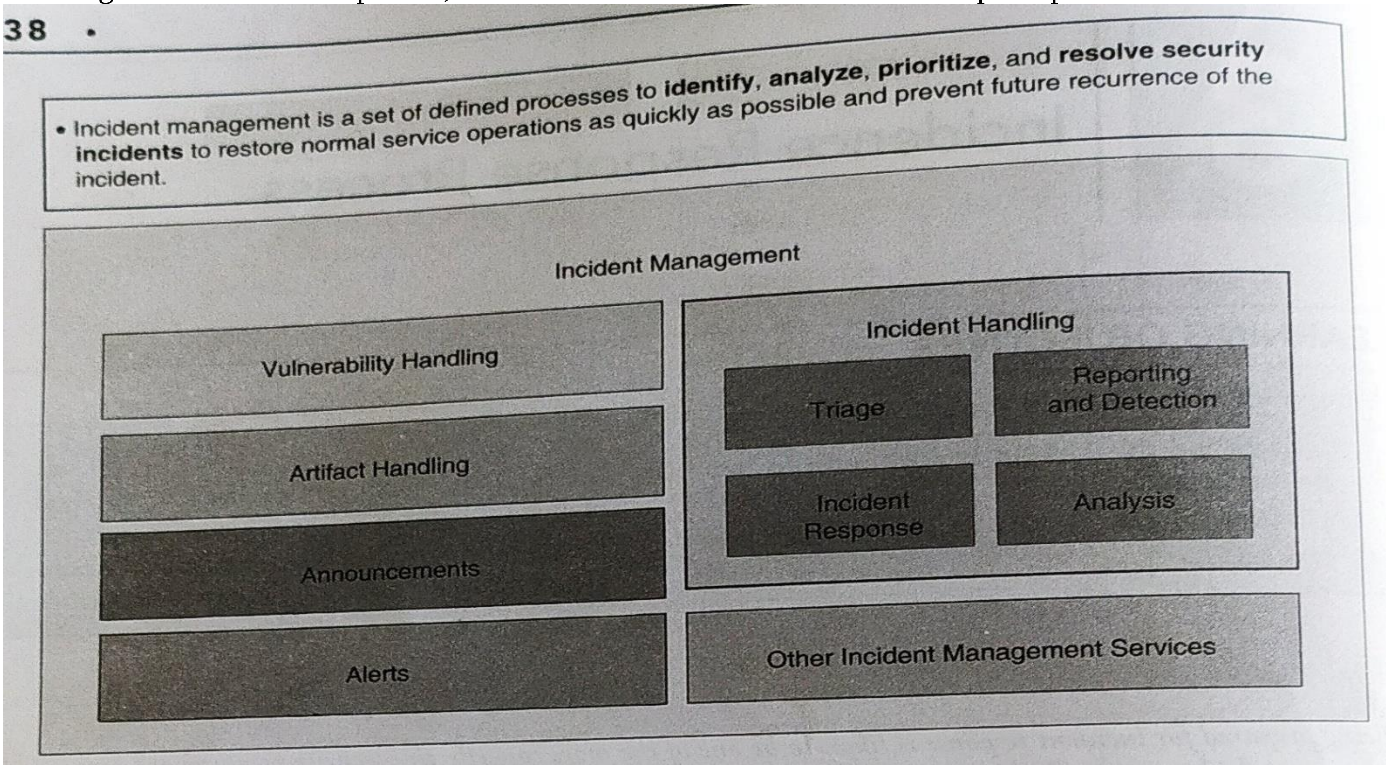
2.11Challenges in Evidence Handling

While responding to a computer security incident, a failure to adequately document is one of the most common mistakes made by computer security professionals. Analytical data might never be collected. critical data may be lost, or data's origin and meaning may become unknown. As there are many evidences collected, the evidence collected based on technical complexity is the fact that the properly retrieved evidence requires a paper trial. Such documentations give an impression of having a certain quality against the natural instincts Of the technical practical knowledge of individuals, who often investigate computer security incidents.

3.1 Introduction

According to incidence response (IR) investigator team, they have responded to a gamut of incidents: criminal incidents, incidents that involved civil litigation, and incidents that disrupted business but were not actionable (cases where criminal or civil action was improbable). They also have developed incident response plans for numerous organizations, ranging from financial services institutions to companies that produce mainstream products. During their various responses and program development engagements, they sought to design an incident response process that will work with each type of incident you may encounter. They believe that the incident response process they introduce in this chapter meets the needs of any organization or individual who must respond to computer security incidents. They also believe that law enforcement or hired investigators should understand all of the phases of this methodology, even if they perform actions during only a portion of the entire process.

Before we delve into the specifics of the incident response methodology, there are some basic questions that need answers about incident response. Some of them are "What are computer security incidents", "What are the goals of incident response", and "Who is involved in the incident responseprocess"?



38 •

- Incident management is a set of defined processes to **identify, analyze, prioritize**, and **resolve security incidents** to restore normal service operations as quickly as possible and prevent future recurrence of the incident.

3.1.1 An Incident

In info technology, an occurrence or an incident (attack) is an event wherever a service or element fails to produce a feature or service that it had been designed to deliver.

3.1.2 An Incident Response

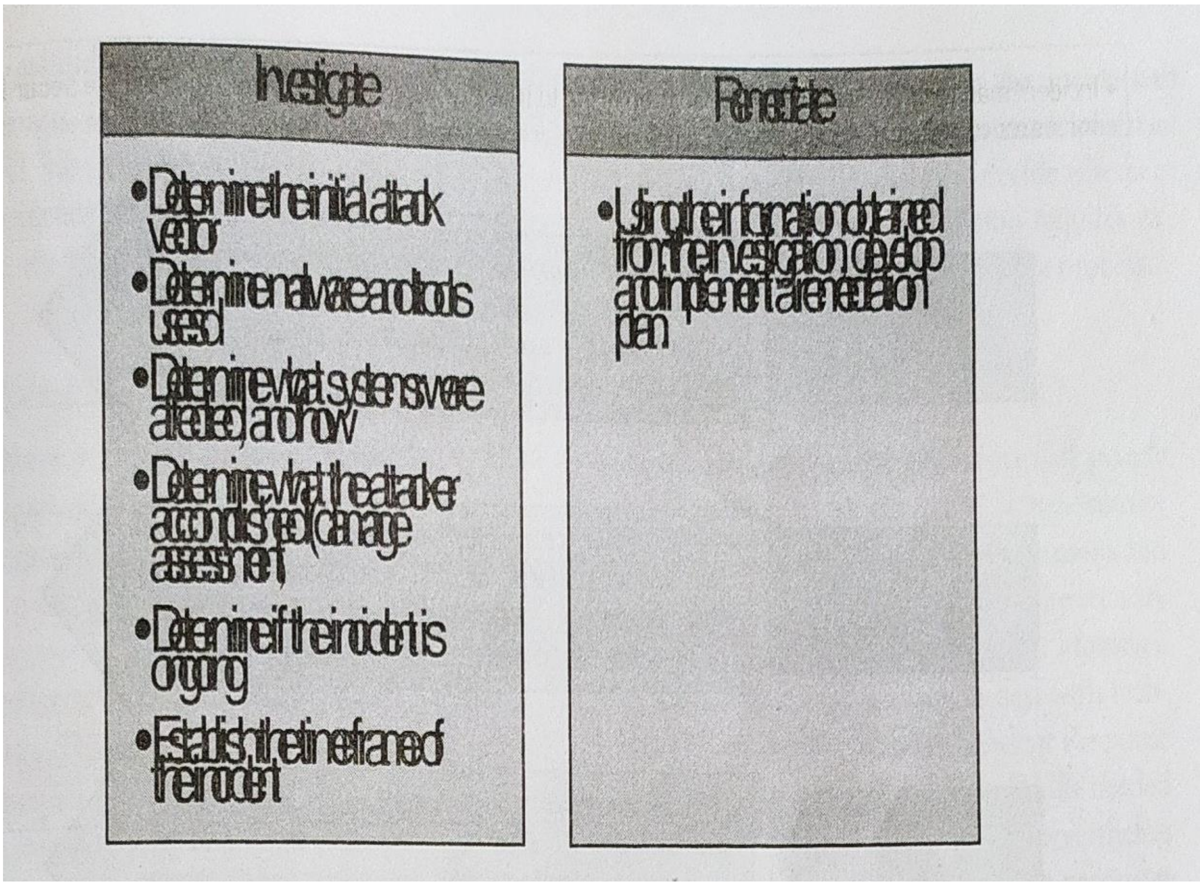
Incident response is an associate degree-organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident) and its goals are to handle the situation in a way that limits damage and reduces recovery time and costs. An occurrence response set-up includes a policy that defines, in specific terms, what constitutes an occurrence and provides a piecemeal method that ought to be followed once an occurrence happens.

3.1.3 An Incident Response Plan

An incident response plan provides a step-by-step process, which should be followed during an occurrence of incident.

3.1.4 Goals of Incident Response

The primary goal of incident response is to effectively remove a threat from the organization's computing environment, while minimizing damages and restoring normal operations as quickly as possible. This goa^l is accomplished through two main activities:



Investigate

- Determine the initial attack vector
- Determine malware and tools used
- Determine what systems were affected, and how
- Determine what the attacker accomplished (damage assessment)
- Determine if the incident is ongoing
- Establish the time frame of the incident

Remediate

- Using the information obtained from the investigation, develop and implement a remediation plan

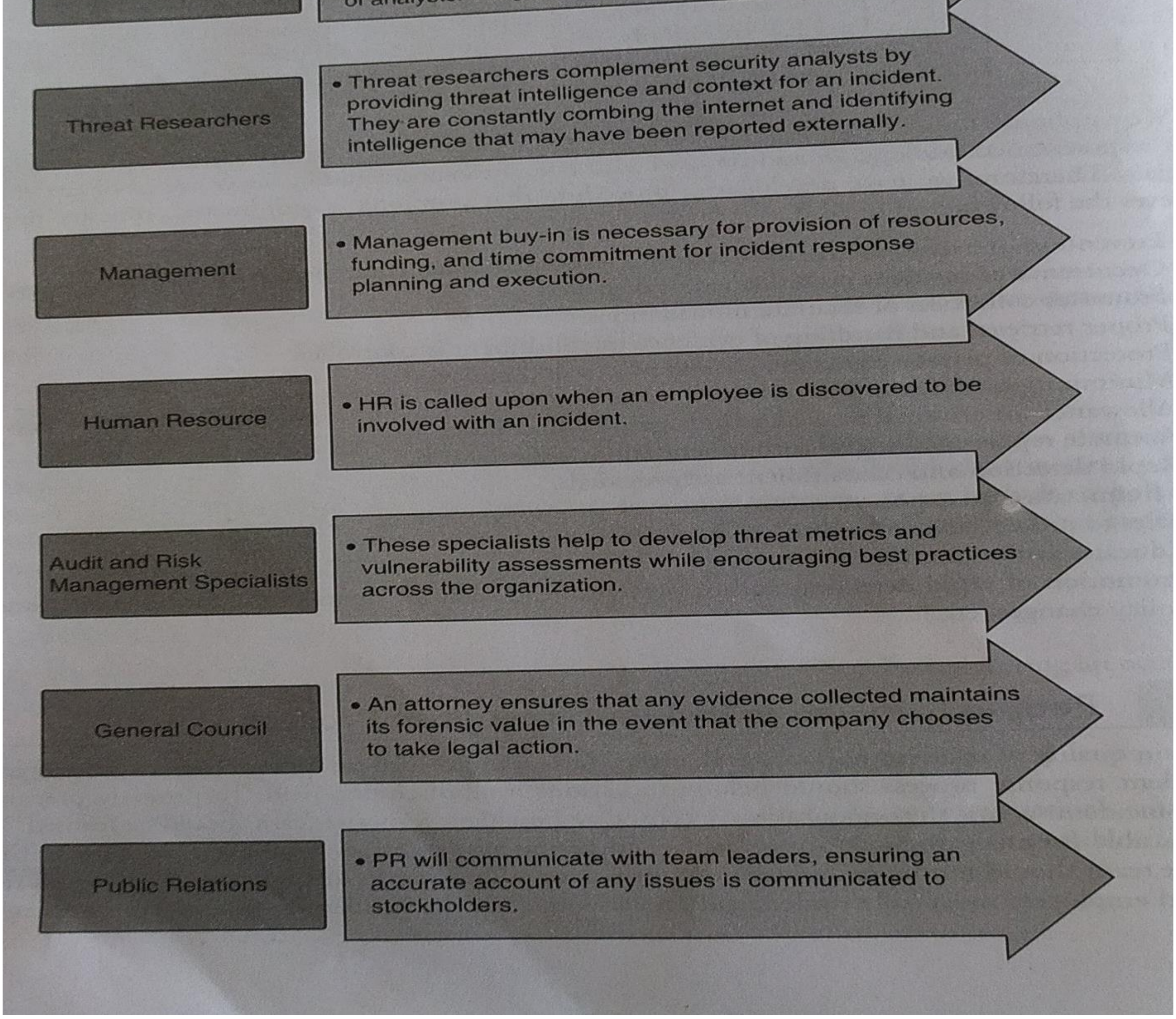
We emphasize the goals of corporate security professionals with legitimate business concerns in our incident response methodology. In addition, we also take into consideration the concerns of law enforcement officials. Therefore, we have developed a procedure that promotes a coordinated, cohesive response and achieves the following:

1. Prevention of a disjoint and non-cohesive response (which could be disastrous).
2. Occurrence of incident is confirmed or dispelled.
3. Promotes collection of accurate information.
4. Proper retrieval and handling of evidence establishment is controlled.
5. Protection of privacy rights established by law and policy.
6. Minimization of disruption to business and network operations.
7. Allowance for criminal or civil action against the culprit.
8. Accurate reports and useful recommendations are provided.
9. Rapid detection and containment are provided.
10. Minimization to exposure and compromise proprietary data.
11. Tries to protect your organization's reputation and assets.
12. Educates senior administration.
13. Promotion of rapid detection and/or prevention of such incidents in the future (via lessons learned, policy changes, etc.).

3.2 People Involved in Incident Response Process

The main quality of incident response is that they have a multisided discipline. Hence, the people involved in incident response process should belong to various multidiscipline field. To properly prepare for and address incidents across the organization, a centralized incident response team should be formed. This team is responsible for analyzing security breaches and taking any necessary responsive measures. The incident response team should not be exclusively responsible for addressing security threats. All business representatives and employees must fully understand and advocate for the incident response plan in order to ensure.

that emergency procedures run smoothly. Each area of the company has unique responsibilities during an incident. At its core. an IR team should consist of:



gency procedures run smoo

At its core, an IR team should consist of:

Incident Response Manager
- The incident response manager oversees and prioritizes actions during the detection, analysis, and containment of an incident and also responsible for conveying the special requirements of high severity incidents.

Security Analysts
- The manager is supported by a team of security analysts that work directly with the affected network to research the time, location, and details of an incident. There are two types of analysts: Triage Analysts and Forensic Analysts.

Threat Researchers
- Threat researchers complement security analysts by providing threat intelligence and context for an incident. They are constantly combing the internet and identifying intelligence that may have been reported externally.

Management
- Management buy-in is necessary for provision of resources, funding, and time commitment for incident response planning and execution.

Human Resource
- HR is called upon when an employee is discovered to be involved with an incident.

Audit and Risk Management Specialists
- These specialists help to develop threat metrics and vulnerability assessments while encouraging best practices across the organization.

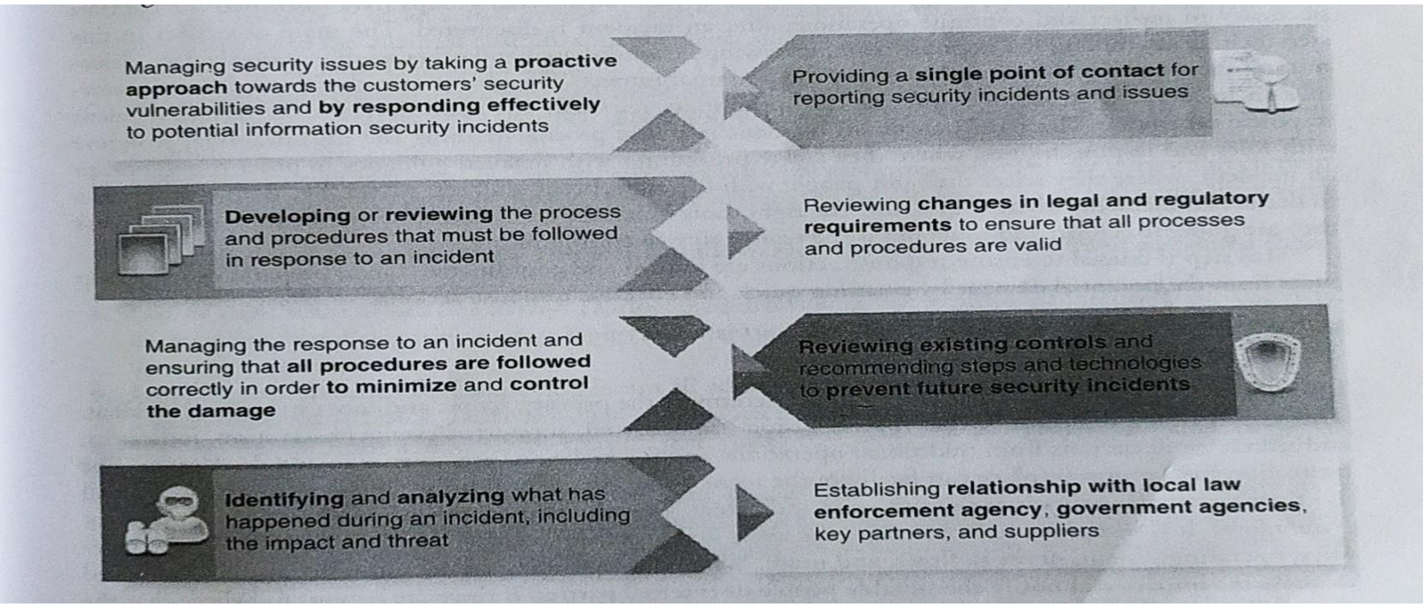
General Council
- An attorney ensures that any evidence collected maintains its forensic value in the event that the company chooses to take legal action.

Public Relations
- PR will communicate with team leaders, ensuring an accurate account of any issues is communicated to stockholders.

Computer Security Incident Response team. (CSIRT') is a team whose members worked for incidence response process. In order to resolve an incident/attack, the CSIRT works together as an interdisciplinary team. CSIRT has the appropriate legal, technical, and other expertise necessary. Its members decide whether to apply incidence response or not based on seriousness of the incident. When an organization requires its capabilities, the CSIRT is normally an effectual team accumulation to conduct an initial response process

3.2.1 Role of Computer Security Incident Response Team

There is always a division between human resources who investigate laptop security incidents and people who investigate normal crimes. Separate functions for company security human resources and laptop security human resources area units are characterized by several companies. Network attacks (e.g., laptop intrusions and Denial of Service attacks) are solely responded to by Computer Security Incident Response Team. The security officers or corporate investigators perform the investigation once an additional crime is committed. However, it is very common for the corporate security human resource to be defenseless and unready to deal with technical evidence. This technical proof is commonly insignificant and easy for the PC Security Incident Response Team to interpret. On balance, the members of your Incident Response Team have the technical skills needed to perform investigations that involve technical proof. The members could be employed to do so, nevertheless of the incident that created the technical evidence. In future, we can predict of a partitioned field in corporate investigations. It is necessary that everyone would need to obtain and understand technical evidence.



Managing security issues by taking a **proactive approach** towards the customers' security vulnerabilities and **by responding effectively** to potential information security incidents

Providing a **single point of contact** for reporting security incidents and issues

Developing or **reviewing** the process and procedures that must be followed in response to an incident

Reviewing **changes in legal and regulatory requirements** to ensure that all processes and procedures are valid

Managing the response to an incident and ensuring that **all procedures are followed** correctly in order **to minimize** and **control the damage**

Reviewing existing controls and recommending steps and technologies **to prevent future security incidents**

Identifying and **analyzing** what has happened during an incident, including the impact and threat

Establishing **relationship with local law enforcement agency**, **government agencies**, key partners, and suppliers

3.2 Incident Response process

The basic incident process encompasses six phases: Initial Response, Investigation, Remediation, Tacking Of Significant Investigative Information, and Reporting. The dynamic relationship among those phases ishighlighted in Fig.3.1.

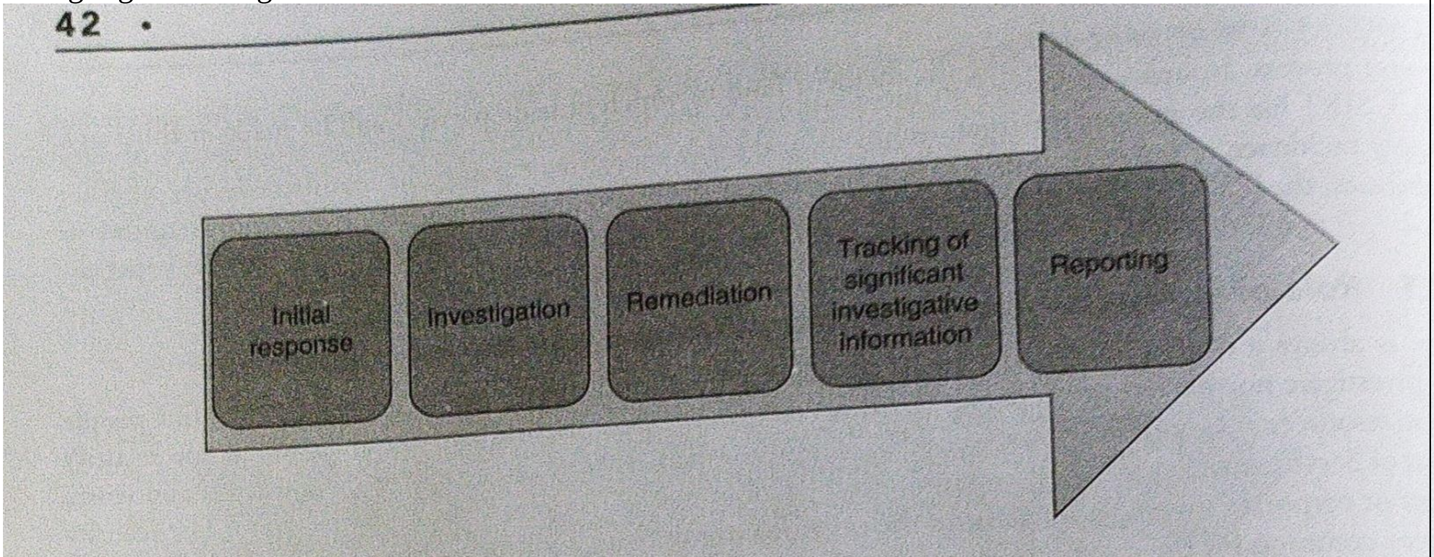


Figure 3.1 Dynamic relationship among six phases.

3.3.1 Initial Response

Initial response includes those activities that respond to an incident: policies, tools, procedures, effective governance and communication plans. It also implies that the affected groups have instituted the necessary to recover and continue operations after an incident is discovered. The main objectives in step include assembling the response team, reviewing network-based and other readily available data, mining the type of incident, and assessing the potential impact. The goal is to gather enough initial information to allow the team to determine the appropriate response. the team develops the formal incidence response capability; where they create an incident response process defining the organizational structure with roles and responsibilities; where they create procedures with detailed guidance in order to respond an incident; where they select the right people with the appropriate skill set; where they define the criteria to declare an incident; where they define the right tools to handle an incident; where the team defines what they are going to report; and to whom is the team going to communicate.

This step is crucial to ensure response actions are known and coordinated. Good preparations will he}: them limit the potential damage by ensuring quick and effective response actions,

3.3.2 Investigation

Investigation is the phase where team personneldetermine the priority, scope, and root cause of the incidence This step is where the team verifies fan occasion has occurred, supported events observation, indicators and search for deviations from traditional operations and for malicious acts or tries to and do damage. The protection mechanism in place can facilitate the team doing the identification. Incident handler team use their experience to look at the signs and indicators. The observation might occur at network, host, or system level. It is where the team leverages the alerts and logs from routers, firewalls, IDS, SIEMs AV gateways, operating system, network flows; and more. When distinguishing an occasion, the team is compelled to assess 'the impact and notify the suitable people or external parties. If there are reasons to believe that team will engage 'law enforcement? it is where the team ensures chain of custody. It is at this stage that the team outlines the next steps.

3.3.3 Remediation

Remediation IS the post-incident repair of affected systems/ communication, and instruction to affected parties, and analysisthat confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) Will be made at this stage in cooperation with OGC. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

3.3.4 Tracking of Significant Investigative Information

We mentioned earlier in this chapter that many of the challenges to effective incident response are nontechnical. Staying organized is one of those challenges and is an especially big one. We hate to use the term "situational awareness,' but that is what we are talking about here, Your investigations must have a mechanism to easily track critical information and share it with the ancillary teams and the organization's leadership. You should also have a way to refer to specific incidents, other than "the thing that started last Tuesday." Establish an incident numbering or naming system and use that to refer to and document any information and evidence related to a specific incident.

What is “significant investigative information'? We have found a handful of data points that are critical to any investigation. These items must be tracked as close to real time as possible, because team members will use them as the "ground truth" when it comes to the current status of the investigation. This data will also be the first thing that team members will reference when queries come in from management.

1.List of evidence collected: This should include the date and time of the collection and the source of

the data, whether it be an actual person or a server.. Ensure that a chain of custody is maintained for

each item. Keep the chain of custody with the item,' and its presence in this list is an indicator to

you
that an item has been handled properly.

2.List of affected systems: Track how and when tile system was identified. Note that “affected" includes
systems that are suspected of a security compromise as well as those simply accessed by a suspicious
account.

3.List of any files of interest: This list usually contains only malicious software, but it may also contain
data files or captured command output. Track the system the file was found on as well as the file system metadata.

4.List of accessed and stolen data: This includes file names, content, and the date of suspected expo-

5.List of significant attacker activity: During examinations of live response or forensic data, you may discover significant activities; such as logins and malware execution. Include the system affected and the date and time of the event.

6.List of netw6.ork-based IOCs: Track relevant IP addresses and domain names.

7.List of host-based IOCs: Track any characteristic necessary to form a well-defined indicator

8.List of compromised accounts: Ensure you track the scope ' of the account's access, local or domain-wide,

9.List of ongoing and requested tasks for your teams: During our investigations, We usually have scores of tasks pending at any point' From requests for additional information from the ancillary teams,
to forensic examinations, it can be easy .to let something fall through the cracks if you are not organized.

3.3.5 Reporting

All' incident response activities will be documented to include<artifacts> obtained using methods consistent with chain of Custody and confidentiality requirements. Incidents will be prioritized and ranked according to their potential to disclose restricted data.As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of resources incidents will be reviewed post-mortem to assess whether the Investigational process was successful and effective. Subsequent adjustments may be made to methods andprocedures and by other participants to improve the incident response process. Artifacts obtained during the course of an investigation may be deleted after the conclusion of the investigation.

3.4 Incident Response Methodology

For the perfect way to organize a process; we are always on an exploration. To define phases of the process, we search for the right way and also look for bright-line separation of phases to avoid murky areas. To illustrate the process, we try to make the perfect flowchart and organize the phases, so the process can be applied to the generic cases. It is quite a challenge to form a straightforward image of the process, whereas maintaining a helpful level of accuracy as a result of the incident response process will involve numerous variables and factors that may have an effect on its flow. However, we tend to feel that we have developed an event response method that is straightforward, correct, and actual.

Computer security incidents are for the most part, complicated, multifaceted problems. We use a "black box" approach with any complex engineering problem to solve it. We distribute the larger problem of incident resolution into components and survey the inputs and outputs of each component. Figure 3.2 illustrates our approach to incident response.

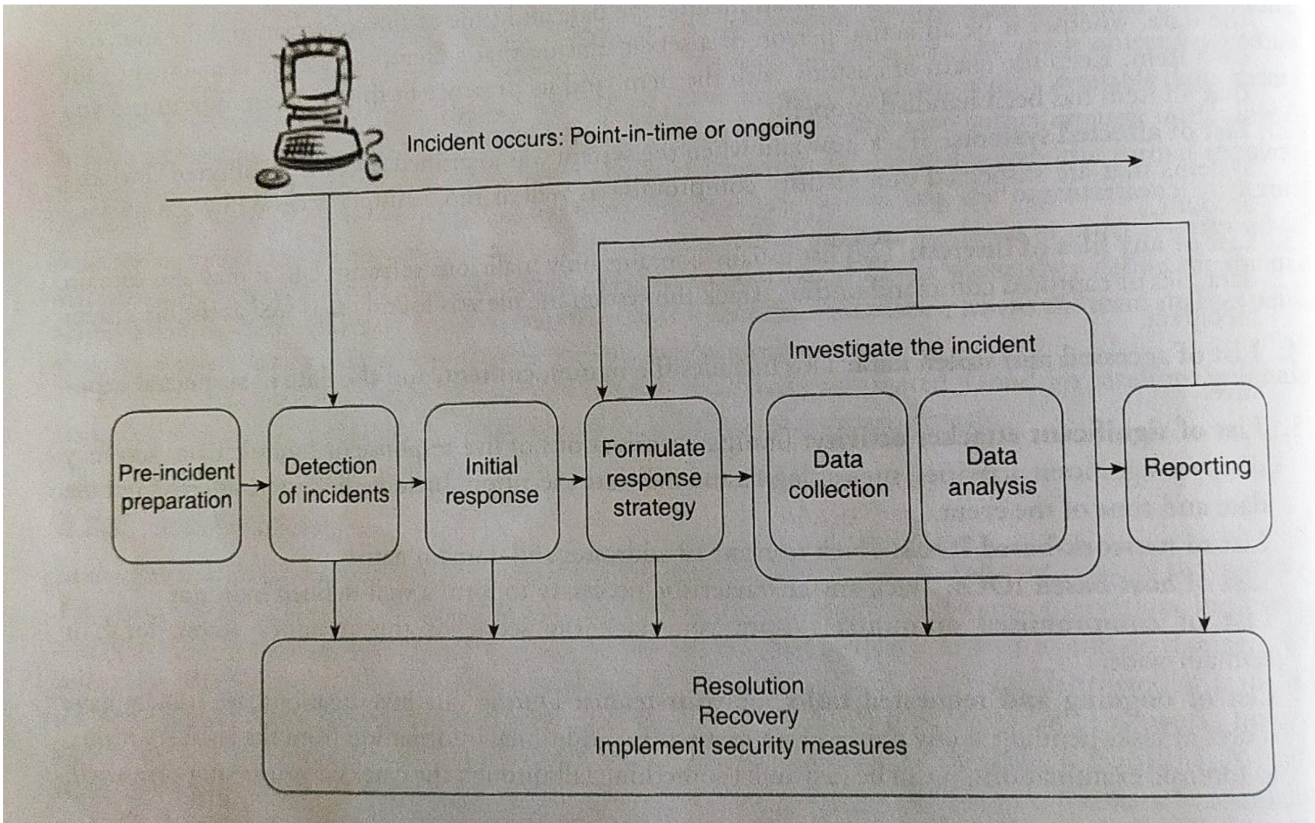


Figure 3.2 Incidence response methodology.

In incident response methodology, there are seven major components of incident response:

I, Pre-incident preparation: Before an incidence occurs, take necessary actions to prepare the organization and the CSIRT,

2. Detection ofincidents: Recognizing a probable computer security incident.

3.Initial response: recording the basic particulars of surrounding the incident, collecting the incident response teams and informing the individuals who need to know about the incident/ the. initial response team performs initial investigation.

4.Formulate response strategy: Regulate the best response team and gain the management approval based on the outcomes of all the known facts, On the basis of to regulate the civil, criminal, administrative, or other actions which are appropriate to be drawn from the investigation,

5.Investigate the incident: Perform a comprehensive collection of data, to determine what happened, when it happened, who did it, and how it can be Prevented in the future.

6.Reporting: Flawlessly report information about the investigation in such a manner that if becomes useful to decision makers,

7.Resolution: Various resolutions must be taken such as employing security measures and procedural changes, recording Of lessons learned and development of long-term fixes for any problems identified.

3.4.1 Pre-incident Preparation

Planning leads to successful incident response. Your organization needs co-operate both the organization itself and the CSIRT members, prior to responding to a computer security incident during this phase.

We recognized that computer security incidents are outside our control. We have no clue when the next incident will arise, as an investigator. Moreover, we often have no control or access to the exaggerated computers before an incident happens. Even though having no control does not mean we should not attempt to position an organization to encourage a fast and fruitful response to any incidents.

Incident response is vulnerable in nature. The pre-incident preparation phases include the only preemptive measures the CSIRT can pledge in order to safeguard that an organization's possessions and information are safe and conserved.

Preferably, preparation involves not just obtaining the tools and developing techniques to respond to incidents it also includes taking up the actions on the systems and networks that will be part OF any incident that you need to investigate. There are a variety of steps you can take now to save time and effort later, if you are fortunate enough to have any level of control over the hosts and networks that you will be asked to investigate.

I. Preparing the organization; Developing all of the corporate-wide strategies you need to employ to get better position of your organization for incident response is what all is required for preparation.

Preparation of an organization includes:

(a) Host-based security actions should be implemented.

(b) Network-based security procedures should be implemented. (c) Training for eventual Users,

(d) Intrusion detection system (IDS) should be active,

(e) Formation of strong access Control,

(f) Performance of timely weakness assessments,

(g) Safeguarding backups which are achieved on a regular basis,

2. Preparing the computer security incident response team: During the pre-incident preparation phase, the CSIRT is defined. Your organization needs Co assemble a team of experts to handle any incidents that occur, Preparing the CSIRT includes;

(a) TO investigate computer security incidents, hardware is needed»

(b) To investigate computer Security incidents; software is needed,

(c) TO investigate computer security incidents; documentation (forms and reports) are needed.

(d) To implement your response 'strategies; thereu Should be appropriate policies and operating procedures:

(e) To perform incident response in such a manner that it promotes successful forensics, Investigations, and remediation; train your staff or employees.

After an incident occurs, you would not want to acquire essential resources, Anyhow, you cannot afford unnecessary delays when attempting to resolve an incident, We will go into detail about the hardware, software, documentation, policies, and training required to prepare your organization and CSIRT before an incident occurs.

3.4.2 Detection of Incidents

It cannot be successful in response to incidents if an organization cannot notice or sense incidents success_ fully Therefore, one of the most important features of incident response is the detection of incident's phase (Fig. 3.3). It is also one of the most disjointed phases, in which incident response proficiency has only slight control.Suspected incidents may be detected in innumerable ways. Whew someone suspects that •an unauthorized, unacceptable, or unlawful event has occurred involving an organization's computer networks or data-processing equipment, computer security incidents are normally identified. Initially, the incident may be reported by a user, detected by a system administrator, identified by IDS alerts, or detected by some othermeans.

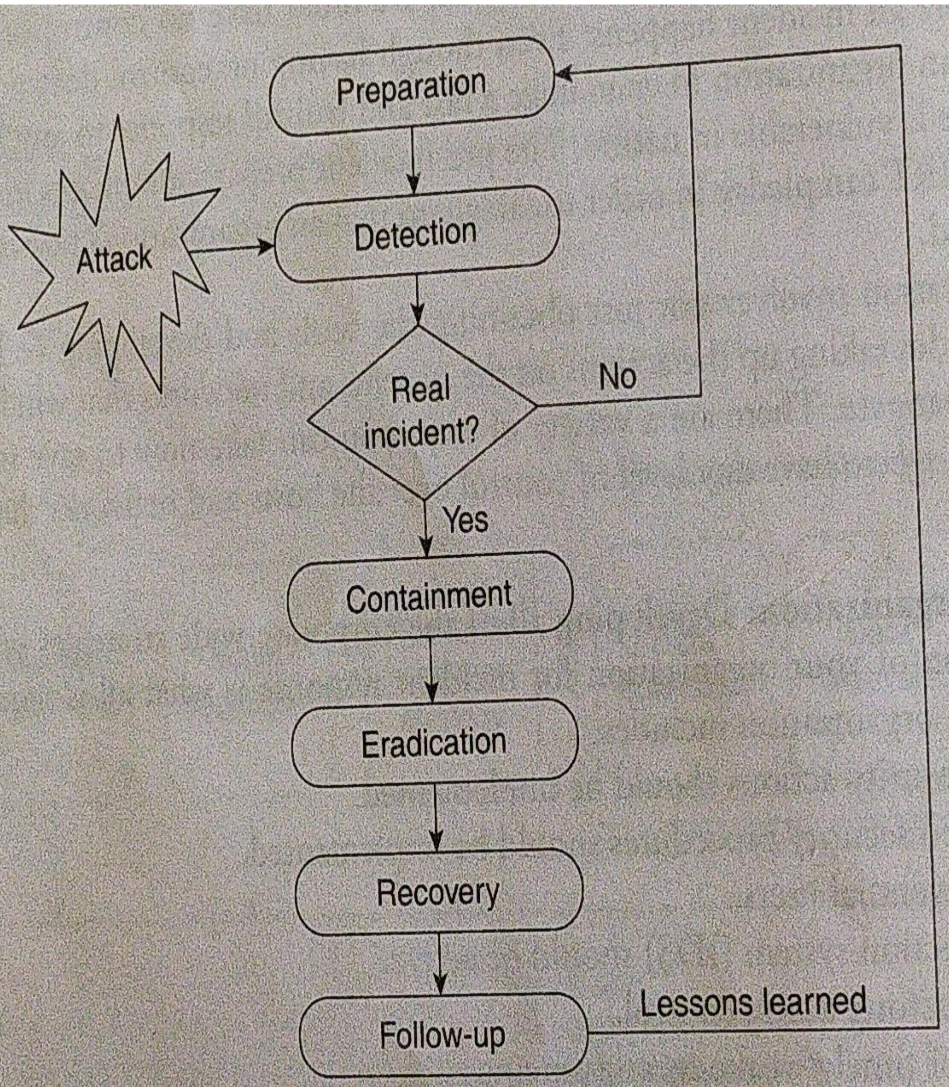


Figure 3.3 Detection of incidence.

In most organizations ultimate users may report an incident through one of three avenues. These three avenues maybe their immediate supervisor, the corporate help desk (or local Information Technology department if there is no formal helpdesk). ok an incident hotline managed by their information Security entity Typically, employee-related to a supervisor directly to the local Human Resources department? While end users report technical. Issues to the help desk.

It is important to record all the known details, no matter how you detect an incident. To make sure you record the relevant facts, we suggest using an initial response checklist. After an incident is detected, the initial response checklist should account for many details, not all of which will be readily recognizable immediately. Also. record the known facts. Some of the details which are critical include:

1. Prevalent time and date.
2. Report of the incident such as who/what.
3, Description of the incident.
4. Incident occurrence.
5. Involvement of hardware/software.
6. Points of contact for involved human resources.

The CSIRT should be activated and appropriate people contacted after completing the initial response checklist. This team will use the information from the initial response checklist to begin the next phase of the response process—initial response.

3.4.3 Initial Response

One of the first steps of any investigation is to determine an appropriate response by obtaining enough information. The initial response phase involves assembling the CSIRT, collection of network-based and other data. It also involves determining the type of incident that has occurred and assessing the impact of the incident. To begin the next phase, the idea is to gather enough information, which is used in developing a response strategy. The other motive of the initial response phase is to document steps that must be undertaken. When an incident is detected, this approach prevents "knee-jerk" reactions and panic, allowing your organization to implement a methodical approach in the middle of a stressful situation.

Computer security incidents can be detected in innumerable ways. The Department of Justice conducted one of the largest economic surveillance investigations that began with non-technical indicators. An employee of a large telecommunications company spotted another employee placing proprietary hardware into a gym bag. It was commonly accepted that the programs which were developed by them could also be worked on their specialized equipment by employees who worked at home. However, the employee noticed that this particular employee continued to "sneak" proprietary components out of the organization in a gym bag.

Rather than approaching and alerting the employee, the witness was smart enough to report the incident to the appropriate people. The witness recognized that the stolen hardware may be a manifestation of something much more devastating: the theft of the company's prized source code. The witness fostered excellent incident response by not alerting the employee. To determine whether the employee was also pilfering the source code, the organization was able to implement steps to collect additional evidence.

Actually, the beginning of the initial response phase is the involvement of individuals detecting an incident' Whoever detects the incident or an individual who has notified that the incident may have occurred, the crime scene has been documented (e.g., help desk or security personnel). To take advantage of the team's experience, control of the response should be forwarded to the CSIRT early in the process. The more steps in the initial response phase performed by the CSIRT, the better it is.

Typically, touching the affected system(s) will not be involved in the initial response. The data collected during this initial response phase includes reviewing of network-based and other evidence. Initial response phase involves:

1.Interviewing system administrators of an incident who might have an understanding of the technical details.

2.Interviewing business unit human resource that may provide a context for the incident, which

3.To identify data-reviewing intrusion detection reports and network-based of the incident should support that an incident has occurrence

4.To if any avenues of attack can be ruled out, review the network topology and access lists of an incident.

The team first verify that an incident has actually occurred, and which systems are directly or indirectly affected. It should also verify the users involved and the potential business impact. For the actual response be appropriate, the team should verify enough information about the incident. In order to simply that an incident has occurred, it, becomes necessary to initiate network monitoring at this stage. Before formulating your overall response strategy, the key here is to determine how much information is enough The answer depends on many factors, which have been discussed in later sections.

At the end of the initial response stage, you will know whether or not an incident has occurred. This phase will give you a good idea of the systems affected; the type of incident, and the potential business impact. With the basis of this information, you are now ready to make a decision on how to handle incident.

3.4.4 Formulate Response Strategy

To determine the most appropriate response strategy, the circumstances of the incident is the main goal of the response strategy formulation phase. The political, technical, legal, and business factors that surround the incident should be considered into strategy. For selecting the strategy, the objectives of the group or individual with responsibility should be taken on which the final solution depends.

1. Considering the totality of the circumstances: Based on the circumstances of the computer security incident, the response strategies will vary. While deciding how many resources are needed to investigate an incident, whether to create a forensic duplication of relevant systems, whether to make a criminal referral, whether to pursue civil litigation, and other aspects of your response strategy, the following factors are needed to be considered:

(a) How much are the affected systems critical?

(b) How sensitive is the compromised or stolen information?

(c) Who are the potential perpetrators?

(d) Is the incident known to the public?

(e) What is the level of unauthorized access attained by the attacker?

(f) What is the attacker's apparent skill?

(g) Involvement of system and user downtime.

(h) The overall dollar loss.

From virus outbursts to theft of consumers' credit card information, the incidents may differ extensively. A typical virus outburst usually results in some idle times and lost productivity. The theft customer's credit card information could put an inexperienced dot.com operation out of business. The response strategy for each event will fluctuates: consequently. A virus outburst is usually swept under the theft of credit card information is just like a five-alarm -fire— compelling a response that includes the Public Relations department, the CEO, and all available technical resources.

During the initial response, the details obtained can be critical when choose a response strategy For example, a Denial of Service attack originating from a university may be handled differently how an equivalent Denial of Service attack that originates from a competitor is handled. It may necessary to reinvestigate details of the incident before the response strategy is chosen.

The response strategy is also important in a large organization because it provides future update for new CSIRT team to determine technical resources, political considerations, legal constraints, and business objectives. The detailed discussion of these factors will be discussed later.

2. Considering appropriate responses: You should be able to arrive at a viable response strategy armed with the circumstances of the attack and your capacity to respond. It shows some common situations with response strategies and potential outcomes. The response strategy determines how you proceed from an incident to an outcome. As shown in Table 3.1, which explains some examples of Incident and its response strategy as well as its expected outcome.

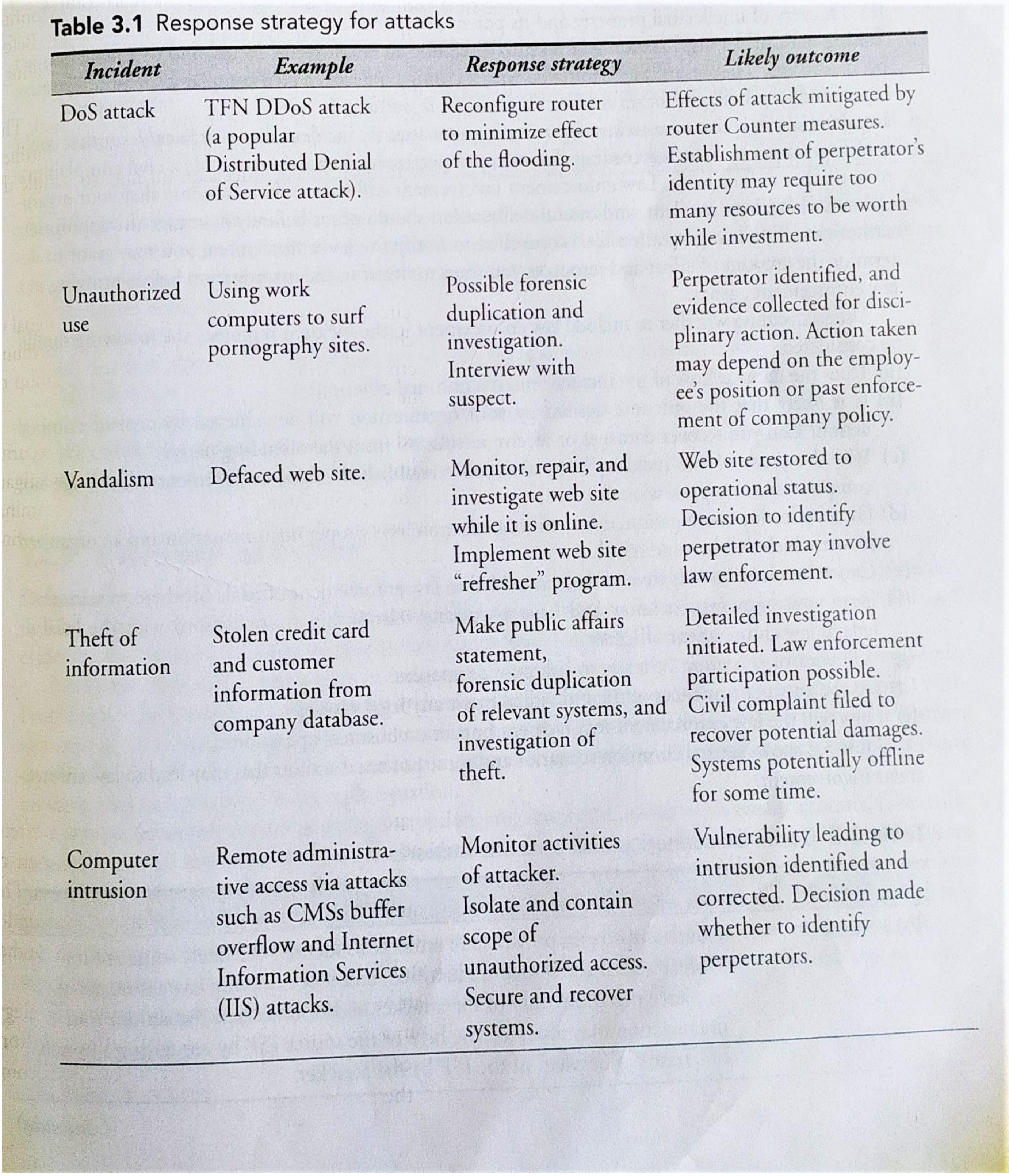


Table 3.1 Response strategy for attacks

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 Counter measures. Establishment of perpetrator's identity may require too many resources to be worth while 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 the employee's position or past enforcement of company policy.
Vandalism	Defaced web site.	Monitor, repair, and 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, and investigation of theft.	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 CMSs 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.

The response strategy must take into consideration your organization's business objectives. The response strategy should be approved by the top management and because of the potential impact to your organization The response strategy options should be quantified with pros and cons related to the following, since the top management and TCP/IP discussions are usually oil and water:

(a). Evaluated dollar loss.

(b). The impact to operations and network downtime.

(c). The impact to operations and user downtime.

(d). Is your organization or not legally compelled to take certain actions?

(e). Public disclosure of the incident and the impact of it on the organization's reputation/business.

(f). Thievery of intellectual property and its potential economic impact.

3.Taking action: An organization will need to discipline an employee or to respond to a malicious act by an outsider. The action can be initiated with a criminal referral, a civil complaint, or administrative reprimand or privilege revocation when the incident is warranted.

4.Legal action: It is common to investigate a computer security incident that is actionable, or that could lead to a lawsuit or court proceeding. The two prospective legal choices are to file a civil complaint or to notify law enforcement. Law enforcement involvement will reduce the autonomy that your organization deals with an incident, and careful deliberation should occur before you engage the appropriate authorities. If your organization feels compelled to notify the law enforcement, you may want to determine the amount of effort and resources you want to invest in the investigation before bringing in a law enforcement agency.

When deciding whether to include law enforcement in the incident response, the following should be considered:

(a). Doesthe damage/cost of the incident merit a criminal criterion?

(b). Isit likely that the outcome desired by your organization will be achieved by civil or criminal action? Can you recover damages or receive restitution from the offending party?

(c). Was the cause of the incident been reasonably established?' (Law enforcement officers are not computer security professionals.)

(d). Foran effective investigation, does your organization have proper documentation and an organized report which will be conducive?

(e). Can substantial investigative leads be provided to law enforcement officials for them to act on?

(f). Does your organization know and have a working relationship (prior liaison) with the local or federal law enforcement officers?

(g). Will your organization be ready to risk public exposure?

(h). Do the past performances of the individual merit any legal action?

(i). How will the law enforcement involvement impact on business operations?

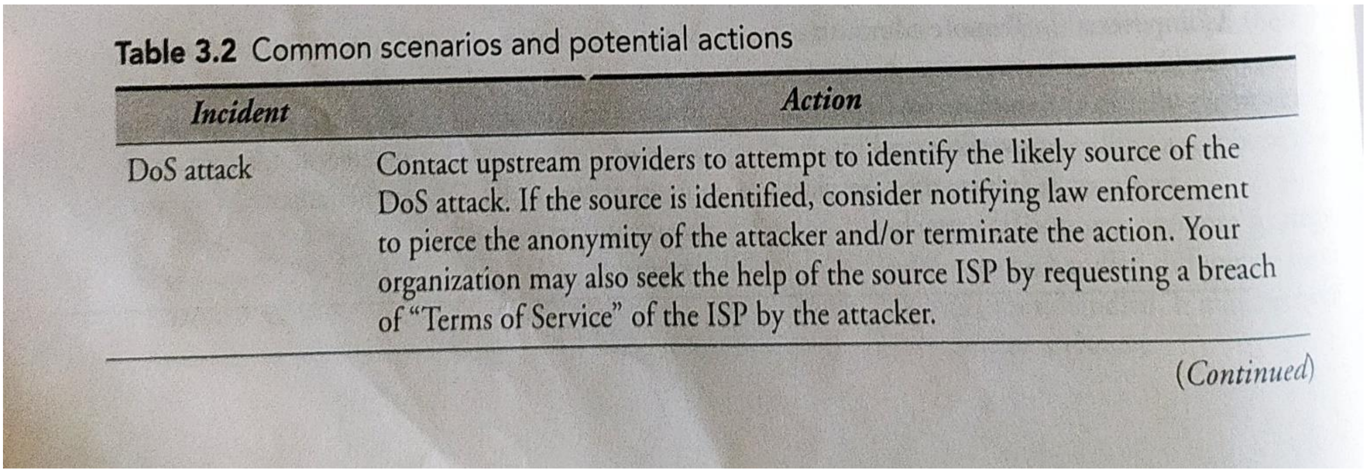


Table 3.2 Common scenarios and potential actions

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.

(*Continued*)

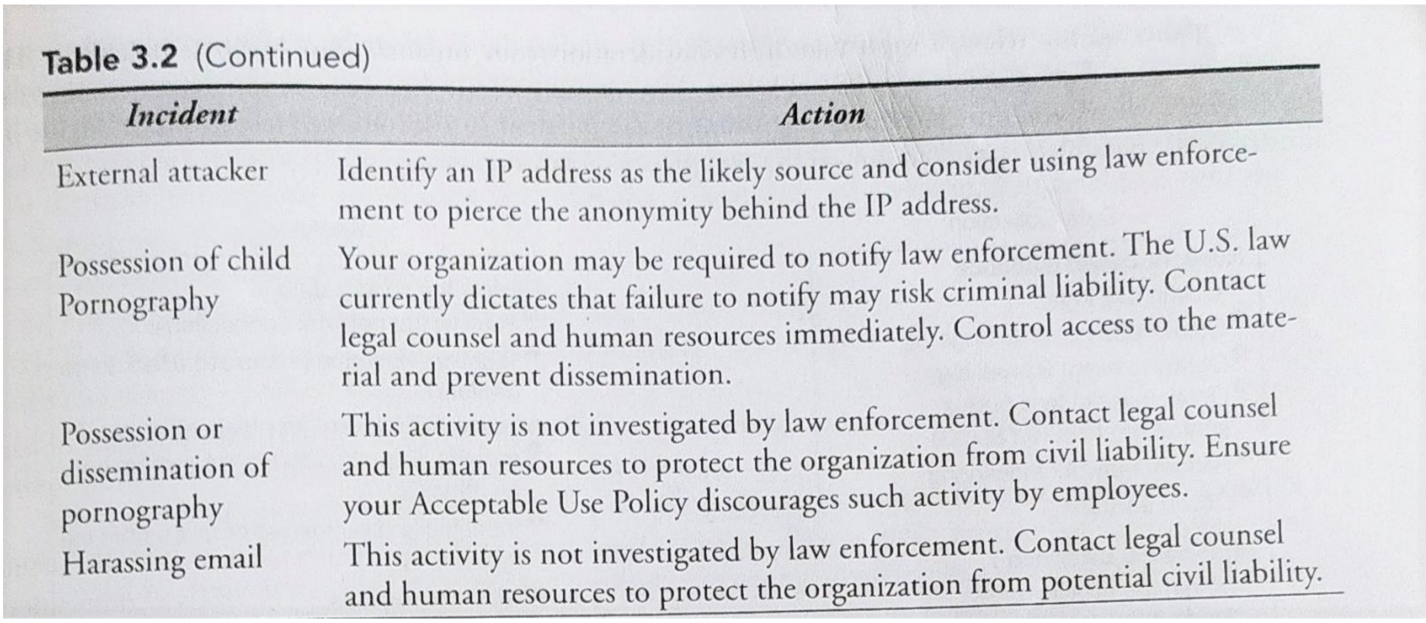


Table 3.2 (Continued)

Incident	*Action*
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. The 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.

5. Administrative action: Currently, more common than initiating civil or criminal actions is disciplining or terminating employees via administrative measures. To discipline internal employees, some administrative actions that can be implemented includes:

(a) Letter of reproof

(b) Immediate discharge.

(c) Leave of absence for a specific length of time (paid or unpaid) is mandatory.

(d) Job duties should be reassigned (diminished responsibility).

(e) Temporary reduction in pay to interpret for losses/damage.

(f) Public/private apology for actions regulated.

(g) Withdrawal of certain advantages such as network or web access.

3.4.5 Investigate the Incident

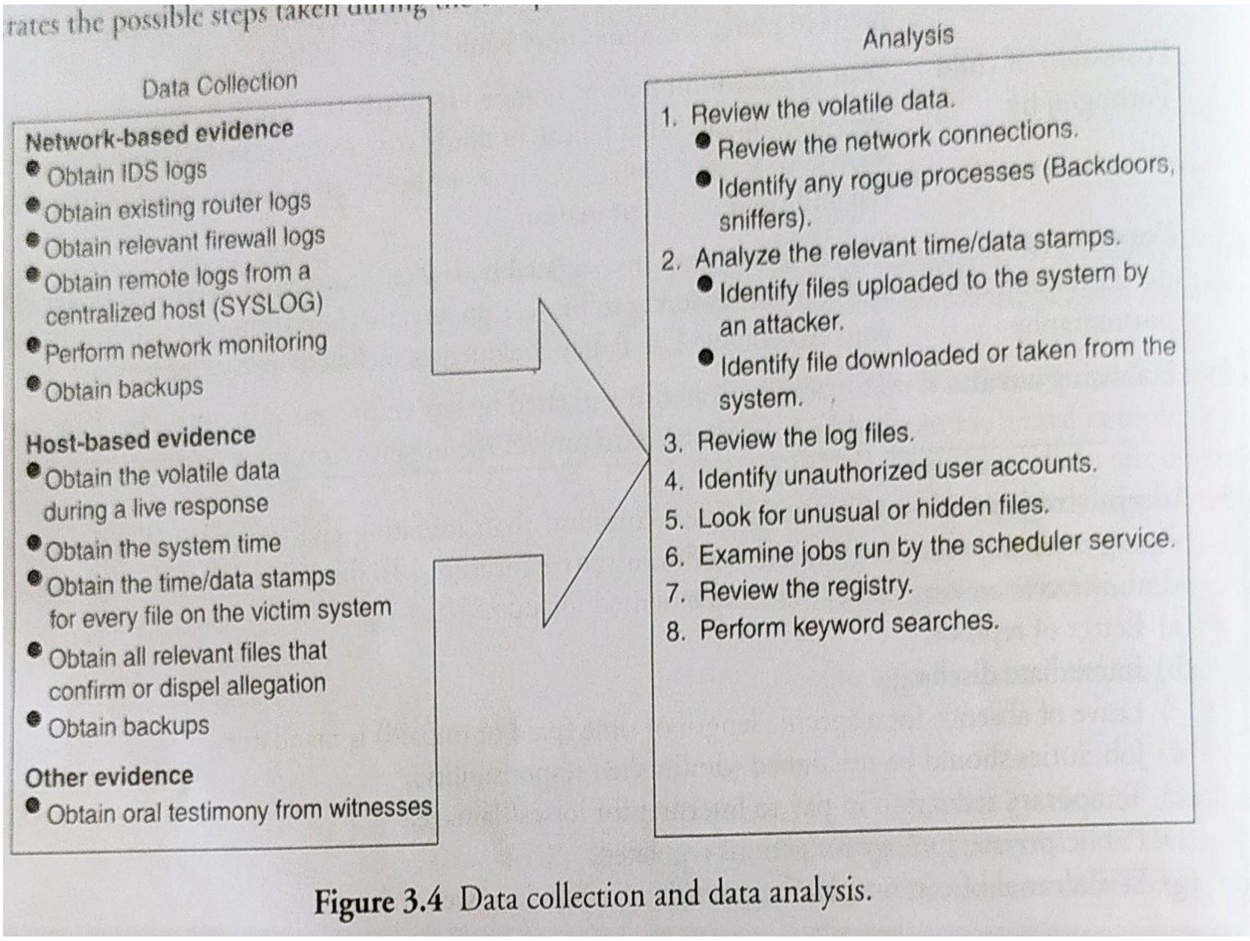
Determining the who, what, when, where, how, and why surrounding an incident is involved in the investigation phase. You need to conduct your investigation, reviewing host-based evidence, network-based evidence, and evidence gathered via traditional, nontechnical investigative steps.

No matter how you conduct your investigation, you need to respond to an incident caused by people. People cause the incidents by using things to destroy, steal, access, hide, attack, and hurt other things. With any type of investigation, the key is to determine which things were harmed by which people. However, establishing the identity behind the people on a network is increasingly difficult because a computer crime incident adds complexity to this simple equation.

Users are becoming experts at using encryption, steganography, anonymous email accounts, fake mails, spoofed source IP addresses, spoofed MAC addresses, masquerading as other individuals. The other means to mask their true identity in "cyberspace" is also one of the factors. The identification of an attacker who brought down your web sites can be so time-consuming that, in fact, most companies may elect not to even try. Establishing identity can be less of a concern to the victim than the things harmed or damaged; since many organizations choose to focus solely on what was damaged, how it was damaged, and how to fix it. The two phases for computer security investigation can be:

1. Data collection
2. Forensic analysis

You gather all the 'relevant information needed to resolve the incident in a manner that meets your during the, data collection phase, you examine all the data collected co determine the who, when, *fid bow information relevant to the incident in the forensic analysis phase, Figure illustrates tbc possible steps taken during the two phases of investigation.



rates the possible steps taken during the

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/data 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/data stamps.
   - Identify files uploaded to the system by an attacker.
   - Identify file 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.

Figure 3.4 Data collection and data analysis.

3.4.51 Data Collection

The accumulation off acts and clues that should be considered during your forensic analysis is data collection. The basis of your conclusions is the data you collect. You may not be able to successfully comprehend how an incident occurred or appropriately resolve an incident, if you do not collect all the necessary data. Before you can perform any investigation, you must collect data.

Data collection involves several different forensic challenges:

I. You must collect electronic information in a forensically sound manner.

2.You very often collect more data than you can read in your lifetime (computer storage capacity continues to grow).

3.You must handle the collected data in such a manner that it protects the integrity (evidence handling).

these requirements describe thatspecial skills are required to obtain technical evidence. During the data collection phase, the information you obtain can be divided into three fundamental areas: host-based information, network-based information, and other information.

Host-based information: The jogs, records, documents, and any other -information that is found on a system and nor obtained from networkbased nodes are included in host-based evidence. For example, host-based information may be a system backup which harbors evidence at a specific period in time. Gathering information in two different manners—live data collection and forensic duplication—should be included in host-based data collection efforts.

In some cases, when the victim/relevant system is powered down, the evidence that is required to understand an incident is ephemeral (temporary or fleeting) or lost. When attempting to understand the nature of an incident, this volatile data can provide critical information. Therefore, the collection of any volatile information from a host before this information is lost is the first step of data collection. At the time you respond, the volatile data provides a "snapshot" of a system. You need to record the following volatile information:

(a) The date and time of system.

(b) The applications which are currently running on the system.

(c) The establishment of current network connections. (d) The recently opened sockets (ports).

(e) The applications which are listening on the open sockets.

(f) The network interface state (promiscuous or not).

Alive response must be performed in order to collect this information. When a computer system is still powered on and running, a live response is conducted. This actually means that the information contained in these areas must be collected without impacting the data on the compromised device. There are variations of live response:

(a) Initial live response: Initial live response involves obtaining only the volatile data from a target or victim system. When you have decided to conduct a forensic duplication of the media, an initial live response is usually performed.

(b) In-depth response: This obtains merely the volatile data. To determine a valid response strategy, the CSIRT obtains enough additional information from the target/victim system. Non-volatile information, such as log files, is collected to help and understand the nature of the incident.

(c) Full live response: This helps in a full investigation on a live system. All data for the investigation is collected from the live system, usually in lieu of performing a forensic duplication, which requires the system to be powered off.

You need to decide whether or not to perform a forensic duplication of the evidence media at some point (usually during your initial response). Generally, a forensic duplication is warranted if the incident is severe or deleted material may need to be recovered. While handling critical incidents, forensic duplication of the target media provides you with a "mirror image" of the target system, which is same as original the copy. For analysis, it provides a means to have working copies of the target media without worrying about altering or destroying potential evidence. Law enforcement generally prefers forensic "bit-for-bit, byte-for-byte" duplicates of target systems, if the intent is to take judicial action. It is prudent to perform a forensic duplication, if the incident could evolve into a corporate-wide issue with grave consequences.

1.**Network-based evidence**: Network-based evidence includes the following sources from which the information is obtained: (a) IDS logs

(b) Consensual monitoring logs

(c) Non consensual wiretaps

(d) Pen-register/trap and traces

(e) Router logs

(f) Firewall logs

2.**Authentication servers**: To confirm suspicions, accumulate evidence, and identify co-conspirators involved in an incident, an organization often performs network surveillance (consensual monitoring) where host-based auditing may fail; network surveillance may fill in the gaps. Network surveillance is not deliberated to prevent attacks. Instead, it allows an organization to fulfill a number of tasks:

(a)Confirm or dispel suspicions surrounding a supposed computer security incident.
(b)Accumulation of additional evidence and information.
(c)Verification of the scope of a compromise.
(d) Identification of additional parties involved.
(e) Determining a timeline of events occurred on the network.
(f) Ensuring compliance with a desired activity.

3. Other evidence: The testimony and other information obtained from people are involved in the "otherevidence" category. This is the type of collection of evidence following more traditional investigative techniques. You may think of this as the collection of evidence via nontechnical means. This is the col_ lection of personnel files, interview employees, interview witnesses, interview character witnesses, and documents of the information gathered.

3.4.5.2 Forensic Analysis

Forensic analysis consists of reviewing all the data collected. It also includes reviewing log files, system configuration files, trust relations, web browser history records, electronic mail messages and their attachments, installed applications, and graphic files. You can perform software analysis, review time/date stamps. perform keyword searches, and take any other necessary investigative steps. It also includes performing more low-level tasks, such as 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. Figure 3.5 depicts the major steps taken during forensic analysis.

the investigation. Figure 3.5 depicts the major steps

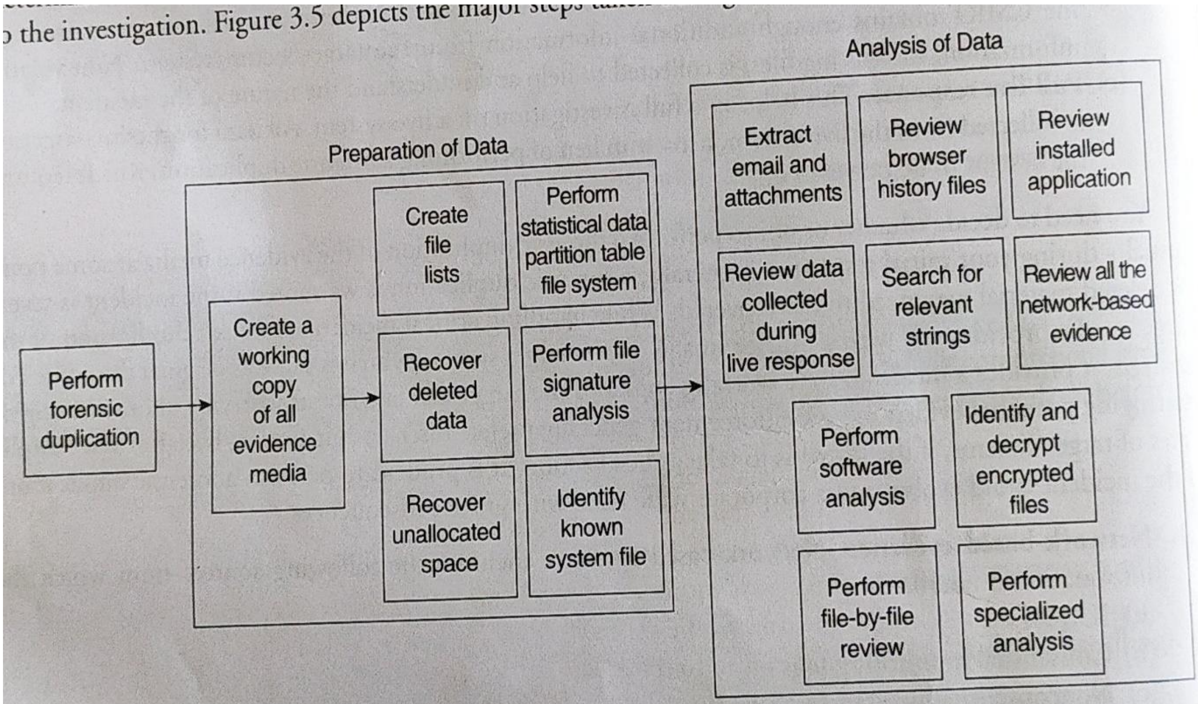

Analysis of Data
Preparation of Data
Perform forensic duplication
Create a working copy of all evidence media
Create file lists
Perform statistical data partition table file system
Recover deleted data
Perform file signature analysis
Recover unallocated space
Identify known system file
Extract email and attachments
Review browser history files
Review installed application
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

Figure 3.5 Major steps taken during forensic analysis.

Before you begin to analyze, the data forensic analysis requires that you assemble and prepare data collected. This procedure applies to the forensic exploration of host-based media and specifically, hard

3.4.6 Reporting

The most difficult phase of the incident response process is reporting. The challenge is to create reports that are understandable to decision makers, and which can describe the details of an incident that can withstand the barrage of legal scrutiny and that are produced in a timely manner.

We have come up with some guidelines to ensure that the reporting phase does not become your CSIRT's nemesis:

1.Document immediately: It is necessary for all investigative steps and conclusions to be documented as soon as possible. To ensure that the details of the investigation can be communicated more clearly to others at any moment, writing something clearly and concisely the moment you discover evidence saves time, promotes accuracy, and if new personnel become involved or are assigned to lead the investigation.

2.Write concisely and clearly: Try to enforce the "write it tight" philosophy. Documenting investigative ansteps requires discipline and organization. You should write everything down in a fashion that is understandable to you and others. Do not use shorthand or shortcuts. Indefinite notations, incomplete ps. scribbling, and other unclear documentation can lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes made by yourself or others.

3. Use a standard format: Develop a particular format for your reports and stick to it. For creating the ful permanent data standard forms, outlines and templates of incident response should be used. This helps in report writing, saves time, and promotes accuracy.

4. Use editors: To read your forensic reports employ technical editors. This helps develop reports that are comprehensible to nontechnical people who have an impact on your incident response strategy and resolution (such as human resources personnel, legal counsel, and business leaders). Unfortunately, editors can inadvertently change the meaning of critical information, so the burden is still on you to review the final product prior to submission.

3.4.7 Resolution

To implement host-based, network-based, and procedural countermeasures to prevent an incident from causing further damage and to return your organization to a secure, healthy operational status is the goal of resolution phase. In other words, in resolution phase, you contain the problem, solve the problem, and take steps to prevent the problem from occurring again.

If you are accumulating evidence for potential civil, criminal, or administrative action, it is always a good idea to collect all evidence before you begin to implement any security measures that would alter the evidence obtained. If you rapidly secure a system by changing your network topology, implement packet filtering, or install software on a host without proper review and validation, good investigative clues—such as the state of the system at the time of the incident—are often lost!

The following steps are undertaken to resolve a computer security incident:

l. Identification of your organization's top priorities, such as which of the following is the most critical to resolve: returning all systems to operational status, ensuring data integrity, containing the impact of the incident, collecting evidence, or avoiding public disclosure.

2. In order to understand and determine the nature of the incident in enough detail how the security occurred and what host-based and network-based remedies are required to address it.

3• Determining if there are underlying or systemic causes for the incident that need to be addressed (lack of standards, noncompliance with standards, etc.).

4. Restoring any Affected or compromised systems. To ensure that the system performs as you expect it to perform, you may need to rely on a prior version of the data, server platform software, or application software as needed.

5• Applying corrections required to address any host-based vulnerability. Note that before beingapplied to production systems, all corrective techniques should be tested in a lab environment.

6.Applying the network-based countermeasures such as access control lists, firewalls, or IDS.

7.Assigning the responsibility for correcting any systemic issues.

8.If they take a significant amount of time to complete. track the progress on all corrections that arc required.

9.Validation of all remedial steps or countermeasures should be effective. This is verifying that all host based, network-based, and systemic remedies have been applied correctly.

10.To improve your response process, update your security policy and procedures as needed.

3.5Activities in Initial Response

Your will be confronted with many challenges, soon after the alert that a computer security incident may have occurred. You will need a process that fosters the following:

1. There should be rapid and effective decision making.
2. In a forensically sound manner, there should be rapid accumulation of information.
3. There should be proper escalation of the incident.
4. To assemble your CSIRT, rapid notification of the participants is required.

3.5.1 Obtaining Preliminary Information

One of the primary steps of any study is to gain enough information to determine an appropriate this is the goal of the initial response phase. It is necessary for your organization's initial response to include

1.An incident receiving the initial notification.

2.After the initial notification, record the details including an incident declaration, ifappropriate.

3.Assembling the CSIRT.

4.Perform the traditional investigative steps.

5.Interviews to be conducted.

6.Determine whether the incident is escalated or not.

Again, to develop an appropriate response strategy, the idea is to gather enough information.

3.5.2 Documenting Steps to Take

The other reason of the initial response phase is to document steps that must be taken.When an incident is

detected, organization and discipline prevent "knee-jerk" reactions and panic. A structured initial response also helps in promoting a formal reporting process and fosters maintaining good metrics.

Your organization will have an accurate number (or as near as possible) of the type that occur, their frequency, the damage caused by these attacks, and the effects these attacks metrics, has had on your organization by recording the details of an incident in an organized fashion, such for return on investment (ROT) for having a formalized incident response program, are critical.

3.6Phases after Detection of an Incident

Once the incident has been identified and detected, the following phases should be followed.

3.6.1 Recording the Details after Initial Detection

Checklist is required for implementing an organized incident response program. One such checklist is the initial response checklist for recording the details after the initial notification of an incident. If it is possible that an incident occurred, you may also declare the incident as an attack.

1.Initial response checklists: To record the circumstances surrounding a reported incident, use an initial response checklist as the mechanism. We can divide our initial response checklist into two separate sections: one for general information and one for more specific details.

2.Second section of the initial response checklist: The second part of the initial response checklist could be used by the members of the CSIRT to address the technical details surrounding the incident. To obtain and record the information, a CSIRT member will need to personally respond. Specifically, the initial response checklist can be used to address the issues.

3.6.2 Incident Declaration

In most of the cases, it will be immediately obvious whether or not the activity is actually acomputersecurity incident in which suspicious activity is reported. However, in a few cases, if an incident occurred based on the details recorded in the initial response checklist it may be difficult to determine. It should most likely be considered an incident and treated as one until your investigation proves otherwise. If it is not clear, whether the reported suspicious activity constitutes an incident, then it should most likely be considered an incident and treated as one until your investigation proves otherwise.

If you cannot immediately tell if an incident has occurred, we recommend that you assign a case or incident number making it worth investigating. Once an incident is declared, the incident has an incident number (or case number) to be used as a specific reference to that incident.

Incident numbers are often constructed in such a manner that shows chronology as well as the type of incident. You can wish to develop an incident numbering system that allows you to track the chronology of incidents you investigated and indicates the incident type.

3.6.3 Assembling the Computer Security Incident Response Team

Responding to incidents, many organizations have a CSIRT that is formed in response to a particular situation or incident rather than an established and dedicated centralized team. Therefore, the CSIRT needs to be staffed in real time after an incident is detected. Your organization must identify the types of skills and resources that are required from the rest of the organization to respond to that particular incident to staff the team properly for a particular incident. To support the incident response effort, a variety of organizational areas contributes hardware, software, technical knowledge, and manpower. One of the biggest challenges to incident response is knowing who to contact and when. However, until you are certain that an incident Occurred, you do not want to go through notification procedures and escalation of an incident.

3.6.4 Performing Traditional Investigation Steps

The investigation stage includes defining the "who, what, when, where, how, and why/' Surrounding incident. One of the finest means to streamline a technical investigation is to divide the evidence you into three categories:

1. Host-based evidence: The data is usually collected from Windows or UNIX machines, or the device actually involved in the incident (the victim system or the system used in furtherance of a crime).
2. Network-based evidence; This type of evidence is usually collected from those not directly involved in an incident such as routers, IDS, network monitors, or some network node.
3. Other evidence: Testimonial data that contributes to the case, such as motive, intent, or some other non-digital evidence are involved in this category.

3.6.5 Conducting Interviews

The first step is to start asking the "who, what, when, where, and how" questions, when your CSIRT learns of a suspected incident. These questions allow you to determine some facts surrounding the incident, such as the location of relevant systems, administrative contacts, what may have occurred and when, and so on The more answers you can obtain, the easier it will be for you to assess the situation; however, the answer to every question may not be available.

3.6.6 Formulating a Response Strategy

The most important aspect of incident response is arguably your response strategy. In this phase, you consider what remedial steps to take to recover from the incident. Your response strategy should also include initiating adverse action against an internal employee or an external attacker.

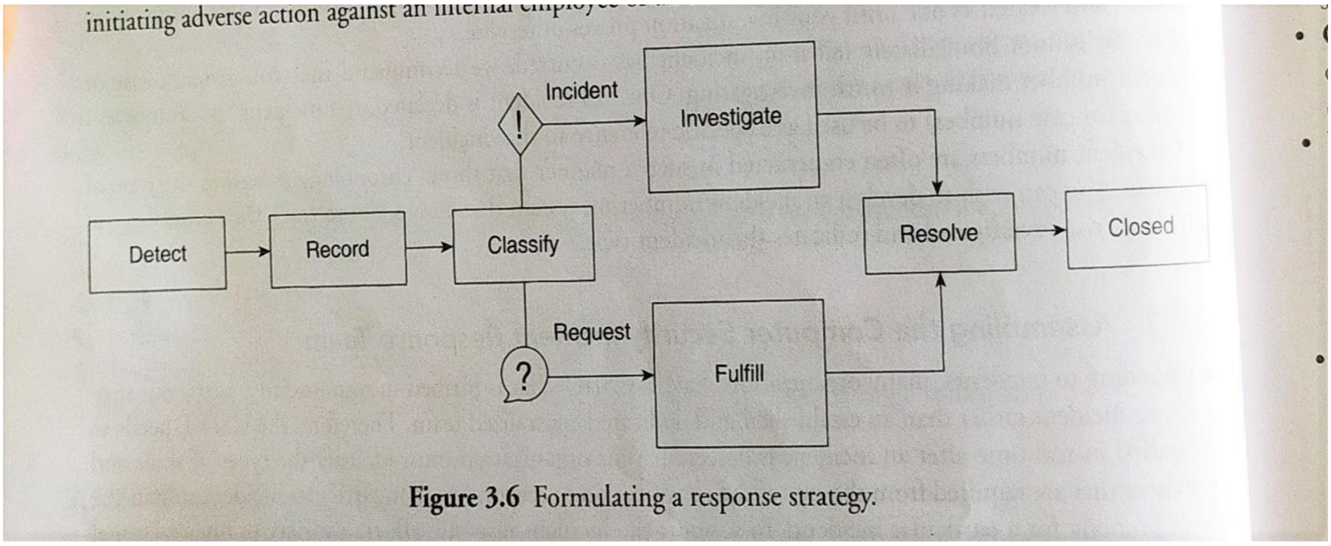


Figure 3.6 Formulating a response strategy.

Regardless of the circumstances, to determine the best way for your organization to respond you will
probably require multiple brainstorming sessions.

It consists of:

1. Response strategy considerations
2. Policy verification

A normal _procedure after detection is shown in Fig. 3.6.

Summary

This chapter highlighted the basics of the incident response process. We discussed the importance of planning with a focus on gathering information about the target of your incident response and techniques that ensure that you havethe staff and equipment resources you need on site. Understanding what a computer security incident is, what incident response defines, and the steps taken during mostresponses puts your organization in a place to best guard its properties and its standing. Wehave encountered, all too often, companies that are incapable of handling even minor computer security incidents. As attacks become craftier and more focused, your CSIRT will need to be a well-oiled, capable (with the appropriate breadth of knowledge), well-mixed (including lawyers, technical staff, and perhaps law enforcement personnel), motivated team that fully understands the flow of incident response.

Key Terms

- **Constituency:** Implicit in the purpose of a CSIRT is the existence of a constituency. This is the group of users, sites, networks, or organizations served by the team. The team must be recognized by its constituency in order to be effective.
- **Security incident**: For the purpose of this document, this term is a synonym of Computer Security Incident—any adverse event which compromises some aspect of computer or network security.
- **Constituency:**A specific group of people and/or organizations that have access to specific services offered by a CSIRT.
- **Vulnerability**: This is characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program unintentionally allowed ordinary users to execute arbitrary operating system commands in privileged mode, this "feature" would be vulnerability.
- **Computer security incident:**Any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of such events are intrusion of computer systems via the network (often referred to as "hacking").
- **CSIRT:**An acronym for "Computer Security Incident Response Team." This is a team providing

services to a defined constituency. There are several acronyms used to describe teams providing similar types of services (e.g., CSIRC, CSRC, CIRC, CIRT, IHT, IRC, IRT, SERT, and SIRT). We have chosen to use the generic term "CSIRT," as it has been widely adopted in the computer security community.

- **Liability:**The responsibility of someone for damage or loss.
- **Policy:**A set of written statements directing the operation of an organization or community with regard to specific topics such as security or dealing with the media.
- **Procedure:**The implementation of a policy in the form of workflows, orders, or mechanisms.

Review Questions

1. What is incident and incident response?

2. What are the goals of incidence response?

3.Explaintheincidenceresponsemethodology.

4. What CSIRT?

5. Explain the phases after detection of incident.