Cyber Crimes and Investigation Procedures

Lesson 4

KEY CONCEPTS

■ Investigation ■ Cyber Crime ■ Cyber Forensics ■ Digital Evidence ■ Security Audit

Learning Objectives

To understand:

- Status of Cyber Crimes in Indian Scenario
- Government Initiatives to Regulate and Control Cyber Crimes
- Tools and Techniques Used to Commit Cyber Crimes
- Reporting of Cyber Crimes
- Investigation of Cyber Crimes and Process under Indian Laws
- Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes
- Steps of Conducing Investigation of Cyber Crimes
- Prosecution of Cyber-Crimes
- Computer Forensics
- Digital Evidences
- Security Audit

Lesson Outline

INTRODUCTION

As discussed in the previous chapters that use of Internet and rapid deployment of information and communication technologies in recent years have bought various changes in the world both at individual level as well as organization level. Right from the way we communicate to the way we buy our groceries, each and every activity of human life is revolutionized with the help of information and communication technology. Crime is not an exception to this revolution brought by information and communication technologies. On one hand wherein the pattern of crime has been altered by misusing the tools and techniques of information and communication technology, on the similar hand, historic trends and practices in criminal investigation has also been revolutionized. This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails. Among the obstacles were legal, technical and operational challenges, but these are not the total extent of the difficulties faced; rather, they have been recognized as the main issues to be addressed in order that law enforcement agencies are able to meet the emerging challenges of cybercrime. Traditional law enforcement government agencies are now called upon to investigate not only real-world crimes, but also crimes on the Internet. For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code, 1973 and the Evidence Act, 1872 have been amended. Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation. Hence, this chapter aims to provide the understanding on the following:

- Overview of Cyber Crimes and Indian Scenario
- Initiatives to Regulate and Control Cyber Crimes: Governmental and Law Enforcement Agencies
- Tools and Techniques Used to Commit Cyber Crimes
- Reporting of Cyber Crimes
- Investigation of Cyber Crimes and Process under Indian Laws
- Case Study: Steps of Conducing Investigation of Cyber Crimes
- Cyber Forensics
- Digital Evidences
- Security Audit.

OVERVIEW OF CYBER CRIMES[1]

In simplest words, cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.[2] Cybercrime can be carried out by individuals or organizations. As per Britannica Dictionary – "*Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.*" Hence any crime conduced with the use of computer and computer network will fall under the category of cybercrime.

> In any statute, the term cybercrime is not defined. Any unauthorized/ unlawful act, commissioned with the use of a computer or computer network or communication device, to commit or facilitate the crime is called cyber-crime.

1 Students to Note: Cyber Crime and Types of Cyber Crime are discussed in detail in chapter 2 and 3 of this study material.

2 Kaspersky (2021) What is Cybercrime? How to protect yourself from cybercrime.

CYBER CRIME *VIS-À-VIS* INDIAN SCENARIO

As is being seen world over, cyber-crimes are on the rise in India also and so are the arrests made in cyber-crimes cases. India has been a favorite hub for cybercriminals, mostly hackers and other malevolent users who misuse the Internet by committing crimes. Data Security Council of India in their Cyber Crime Investigation Manual[3] in 2011 have quoted *Crime in India 2009 report published by National Crime Reporting Bureau (NCRB)*, and that point in time there has been an increase of over 45% in the number of cyber-crimes reported under The Information Technology Act 2000 (IT Act) in 2009 over the corresponding figures for 2008. In 2021 also cyber-crimes in India saw the rise of 6% in comparison to previous year.[4] As per the data revealed by Statista[5] "*India saw a significant jump in cyber-crimes reported in 2021 from the 2020. That year, over 52 thousand cyber-crime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. The northern state of Uttar Pradesh had the highest number of cyber-crimes compared to the rest of the country, with over six thousand cases registered with the authorities in 2018 alone. India's tech state, Karnataka, followed suite that year. A majority of these cases were registered under the IT Act with the motive to defraud, or sexually exploit victims*." As per the report it was estimated that in 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cyber-crimes. However, these were estimates based only on reported numbers. In a country like India, it is highly likely that the actual figures could be under-reported due to a lack of cyber-crime awareness or the mechanisms to classify them. Recent government initiatives such as a dedicated online portal to report cyber-crimes could very well be the main factor behind a sudden spike in online crimes from 2017 onwards. Such an increase in the number of cyber-crimes cases could pose serious economic and national security challenges.

As per 2019 Norton Life Lock Cyber Safety Insights Report, 63% Indians do not know what they will do if their identities are stolen, even though 70% are worried that identities will be stolen. 4 in 10 consumers in India have experienced identity theft.[6] Cyber-crimes know no borders and grow at a pace at par with emerging technologies.

India is the 80th most targeted country worldwide in cybercrime: Report[7]

It is stated in an article of The Hindu, with the rise of AI use and the consistent digital payment adoption here, it has become imperative for organizations to continuously improve their cybersecurity posture to protect their assets and maintain stakeholder trust.

As per the Report published on recording the cyber incidents, India was placed on the 80th position in a report focusing on local threats in the year 2023. The position is based on the malicious programs found directly on users' computers or removable media connected to them (flash drives, camera memory cards, phones, external hard drives) or that initially made their way onto the computer in non-open form, including programs in complex installers or encrypted files.

Additionally, nearly 34% of users in India were targeted by local threats, amounting to some 74,385,324 local incidents being blocked by one of the leading antivirus companies.

India's cybersecurity market reached USD 6.06 billion in 2023. However, according to IDC, a global marketing intelligence firm, the alarming increase in sophisticated external cyber threats and cybersecurity attacks is one of the biggest challenges for the majority of enterprises in establishing organizational trust.

---

3 Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte

4 https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

5 Basuroy Tanushree (October 13, 2022) Number of Cyber Crimes reported in India 2012-2021

6 https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019survey/articleshow/75093578.cms#:~:text=Rs%20131.2%20million%20is%20the,the%20global%20average%20being%2067%25

7. Reproduced from The Hindu. Available at https://www.thehindu.com/sci-tech/technology/india-the-80-most-targeted-country-worldwide-in-cybercrime/article67869960.ece

Almost 67% of Indian enterprises are reportedly looking to outsource key areas of security landscape to managed security service providers in the next three years.

The following four major categories of crimes reported in India as per NCRB constitutes nearly 90% of the cyber-crimes:

a. Hacking of Computer System

b. Forgery / counterfeiting using Computers

c. Publication / Transmission of obscene information in electronic form i.e. Pornography

d. Breach of Trust / Frauds.

According to Director CBI, "The use of modern technology has resulted in traditional crime becoming global. This has made the task of investigation more difficult and complex. There are several examples of kidnapping, terrorist attacks, economic crimes, bank frauds and financial scams being committed with the help of computers"[8]. Thus, the task before the law enforcement authorities is going to grow in complexity and, urgent focus is needed to build capacity to tackle this growing menace.

Tools and Techniques used to Commit Cyber Crimes[9]

On one hand where we are witnessing the advancement of information and communication technology; on the similar end, we are seeing the new tools and techniques of committing cybercrimes. In general, cyber criminals make use of various tools and techniques yet the following are the most common tools and techniques used recently to conduct cybercrimes.

It is to be noted that many of these tools (*used for the commission of the cyber-crimes*) are installed on the victim's systems through exploitation of the vulnerabilities in the systems / networks or by surreptitiously gaining access to the victim's systems which may include physical access or by making use of the intermediary systems or by deceiving the victim to allow access to his system or by gathering the victim information.

- **Buffer overflow:** The condition when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- **Cracking:** Cracking is breaking into someone else's computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this either for profit, or maliciously, or for some altruistic purpose or cause.
- **Data Didling:** Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.
- **Malware**: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
- **Phishing:** Using spoof E-mails or directing the people to fake web sites to deceive them into divulging personal financial details so that criminals can access their accounts.
- **Rootkit**: A set of tools that enables continued privileged access to a computer, while actively hiding its

8 http://www.cbi.gov.in/speech/nasscom_20101122_dcbi.php

9 Source: Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte

presence from the administrator. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

- **Salami Attack:** A programmed attack which is implemented in small (meant to be unnoticeable) increments. This attack involves making alteration so insignificant that it is easily concealed and would go completely unnoticed. Attacks are used for commission of financial crimes.
- **Sniffer**: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate net-work management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.
- **Social Engineering:** A hacker term which involves non-technical intrusion for deceiving or manipulating unwitting people into giving out information about a network or how to access it.
- **Spoofing:** Refers to a situation in which the incoming information from an attacker is masqueraded as one that appears to come from a trusted source to the recipient or to the recipient network. Often the messages from the fraudster appearing to be from a genuine source (like bank), seeks personally identifiable information to perpetrate fraud on the victim.
- **Spyware:** It is a type of malware that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.
- **Steganography**: The art and science of writing hidden messages in such a way that no one, apart from the sender and in-tended recipient, suspects the existence of the message An image file may contain hidden messages between terror groups, which will be known only to the intended recipient and the sender.
- **Trojan:** A malicious program that masquerades as a benign application and can take complete control of the victim's computer system.
- **virus:** A self-replicating program that runs and spreads by modifying other programs or files.
- **Worm**: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
- **Zombie**: A program that is installed on a system to cause it to attack other systems.

INITIATIVES TO REGULATE AND CONTROL CYBER CRIMES: GOVERNMENTAL AND LAW ENFORCEMENT AGENCIES

The discussion above confirm that India is facing the growing threat of cybercrimes. This has led government of India to channelize the effective ways in enhancing the level of cyber security. This in consolidation has resulted to various initiatives and programs for Cyber Security under the Department of Information Technology along with enactment of the Information Technology Act, 2000. The Act was also amended in the year 2008 retrofitting newer crimes. The Act heralded the legal recognition of electronic documents, digital signatures and transactions done using computers and internet. Further, the Act described the punishment and penalty for criminal offences and contraventions.

Many law enforcement agencies including the Central Bureau of Investigation have created separate units/ cells for handling cybercrimes. The IT capital of India i.e., Bangalore has even led to establish country's first Cyber Crime Police Station. As on date, all the states and almost all the cities have created Cyber Crime Police Stations and, Cyber Crime Cells to handle the menace of growing cybercrimes.

Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes[10]

The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs). To strengthen the mechanism to deal with cyber-crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

- The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) to deal with all types of cyber-crime in the country, in a coordinated and comprehensive manner.
- Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber-crime hotspots/ areas having multi-jurisdictional issues by on boarding States/ UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.
- National Cyber Forensic Laboratory (Investigation) has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) have provided its services to State LEAs in around 9,000 cyber forensics like mobile forensics, memory forensics, Call Data Record (CDR) Analysis, etc. to help them in investigation of cases pertaining to cyber-crimes.
- The 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber-crimes, with special focus on cybercrimes against women and children. Cyber-crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, an amount of more than Rs. 1200 Crore have been saved in more than 4.7 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.
- The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber-crime investigation, forensics, prosecution etc. along with certification. More than 76,000 Police Officers from States/UTs are registered and more than 53,000 Certificates issued through the portal.
- Till date more than 3.2 lakhs SIM cards and 49,000 IMEIs as reported by Police authorities have been blocked by Government of India.
- I4C has imparted cyber hygiene training to 6,000 officials of various Ministries/ Departments of Government of India.
- I4C has imparted cyber hygiene training to more than 23,000 NCC cadets.
- The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 crores under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs. So far, more than 24,600

10. Reproduced from Increase in Cyber Crime (February 07, 2024), Information was given by Minister of State for Home Minister in a written reply to Rajya Sabha, Press Information Bureau. Available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505

LEA personnel, judicial officers and prosecutors have been provided training on cyber-crime awareness, investigation, forensics etc.

- National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber-crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.
- To spread awareness on cyber-crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@Cyberdost), Facebook(CyberDostI4C), Instagram (cyberdostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.
- CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
- CERT-In, through RBI, has advised all authorized entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empaneled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.
- CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM[11]

Recently, as an initiative to provide easy resolution to financial cybercrimes, a new feature "Citizen Financial Cyber Fraud Reporting and Management System" has been activated for prevention of money loss in case of Cyber Financial Fraud. Under this initiative, an immediate reporting the complainant can be made by the victim, which ensures timely action and resolution of the cybercrime.[12]

Reporting of Cyber Crime

The Government of India had launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature. The Central Government has launched a scheme for formulating of Indian Cyber Crime Coordination Centre (I4C)[13] to handle the cybercrime incidents in India, in an inclusive & coordinated manner.

The said scheme has following seven components:

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Forensic Laboratory (NCFL)
- National Cybercrime Training Centre (NCTC)
- Cybercrime Ecosystem Management
- Platform for Joint Cybercrime Investigation Team

11 Source: How is cyber-crime investigation conducted (2020) iPleaders.

12 More details can be accessed from 'Citizen Manual' under "Resources Section" at www.cybercrime.gov.in.

13 https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067

- National Cybercrime Reporting Portal
- National Cyber Research and Innovation Centre (NCR&IC).

The government is also planning to set up Regional Cyber Crime Coordination Centers at respective States/UTs.

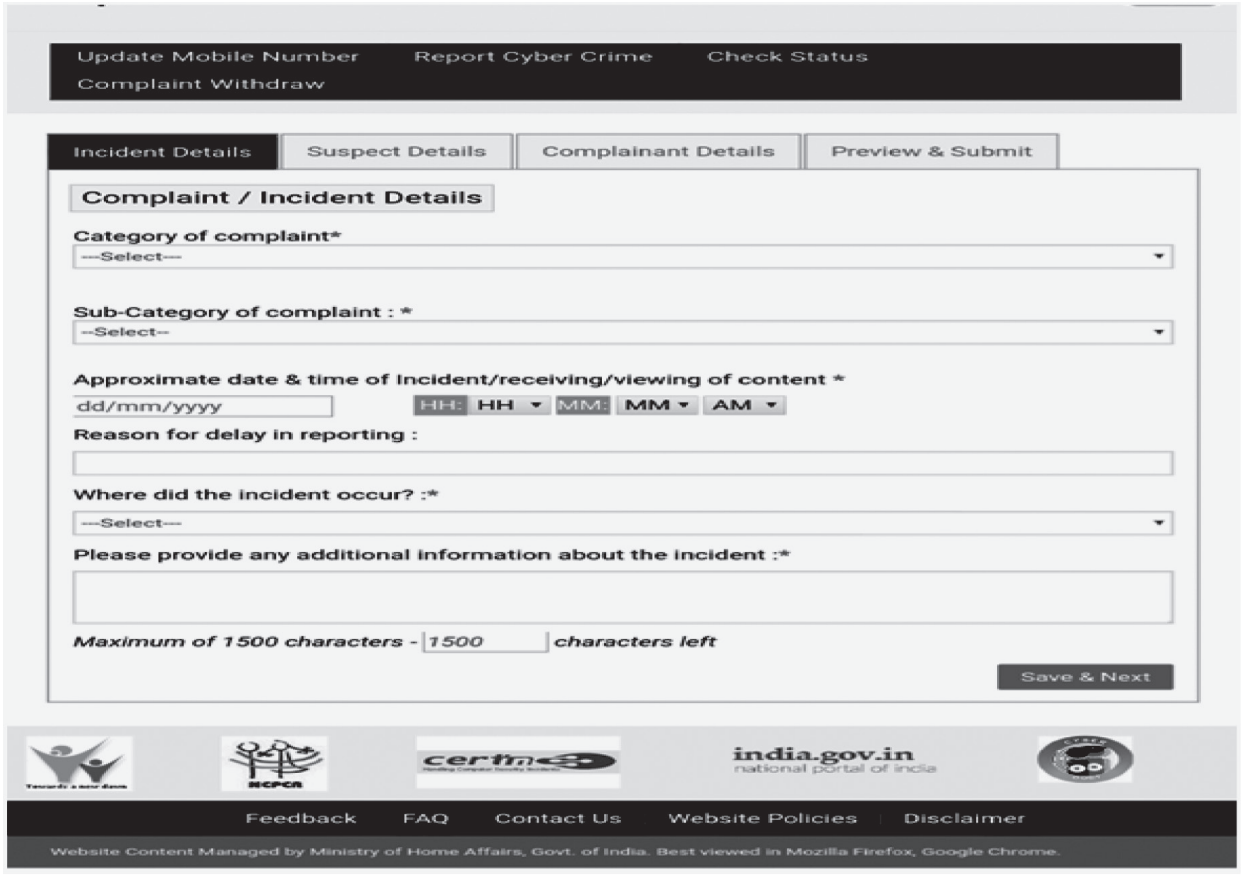
PROCESS OF REPORTING A CYBER CRIME[14]

A Cyber-crime can be reported online as well as offline i.e., in physical form

***A. Online Reporting of Cyber Crime*:** By following below-mentioned steps, one can report a cyber-crime online:

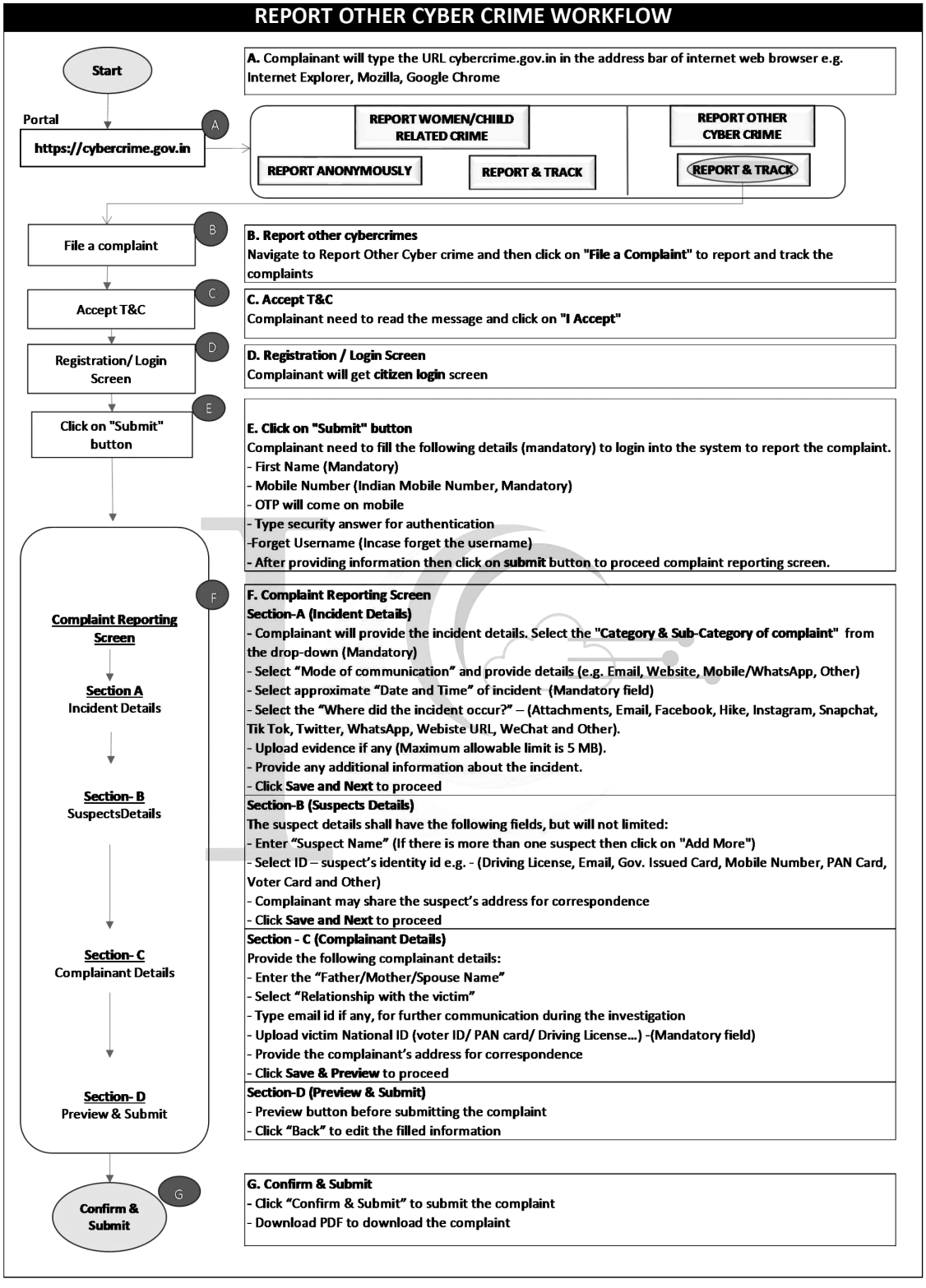
1. Step 1: Go to https://www.cybercrime.gov.in/Accept.aspx.
2. Step 2: Click on 'Report Other Cyber Crimes' on the menu.
3. Step 3: Create 'Citizen login'.
4. Step 4: Click on 'File a Complaint'.
5. Step 4: Read the conditions and accept them.
6. Step 5: Register your mobile number and fill in your name and State.
7. Step 6: Fill in the relevant details about the offence.

It is important to note that one can also report the cyber-crime anonymously.



14 *This portion of the chapter is reproduced from article titled - How is cyber-crime investigation conducted (2020) iPleaders.*

Work Flow for Reporting a Cyber Crime[15]



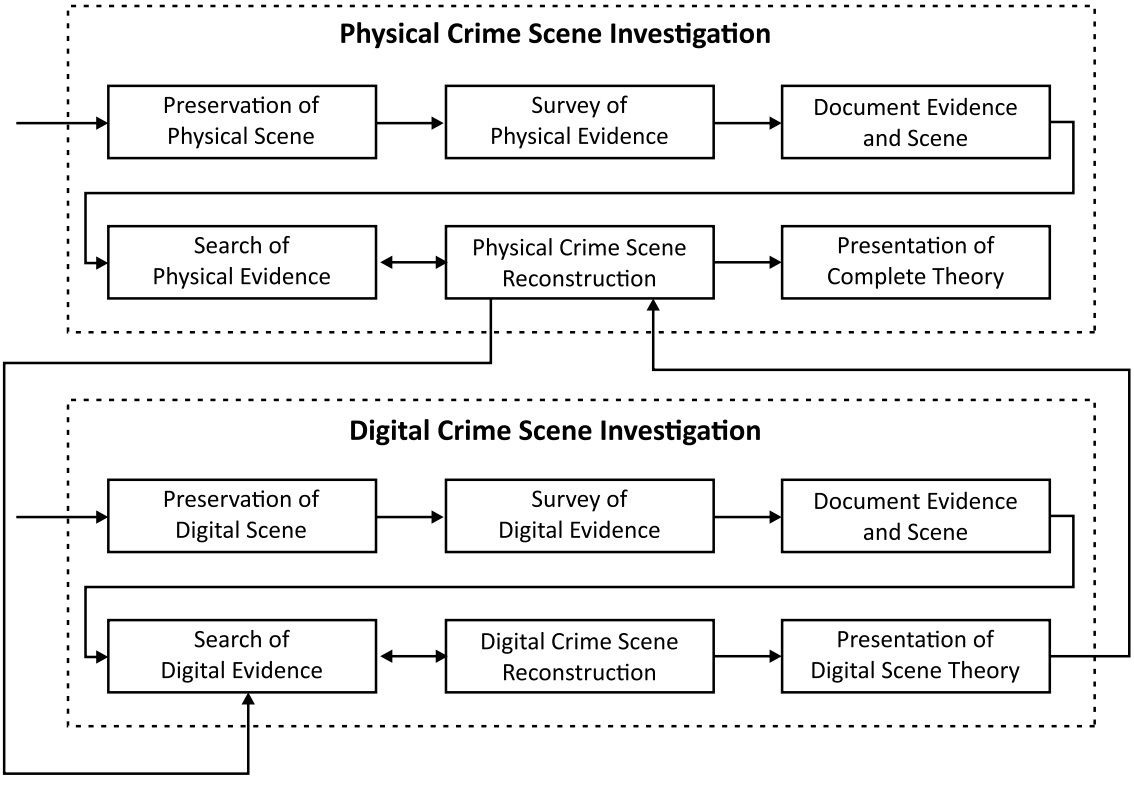
15 Source: https://www.cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

B. Offline/Physical Reporting of Cyber Crime

One can report a cyber-crime by:

- Filing a written complaint in nearest, any Cyber Cell
- Lodging an F.I.R (First Information Report)
- Filing a complaint at https://www.cybercrime.gov.in/Accept.aspx

After filing of a complaint / F.I.R., the process of investigation, is hereby diagrammatically presented below:



Source: http://www.dynotech.com/articles/images/crimescene.jpg

CASE STUDY

Case Study on Cyber Crime Reporting: SONY.SAMBANDH.COM CASE[14]

India saw its first cybercrime conviction in 2013. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

16. Reproduced from "Important Cyber Law case studies by Cyber Laws and Information Security Advisors".

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint about online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated, and Arif Azim was arrested. Investigations revealed that Arif Azim while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless headphone, in this one of its own kind of cyber fraud case. In this matter, the CBI had evidence to prove their case, and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

State Nodal Officer and Grievance Officer

In case the response has not been appropriate then the complainant can write to State / UT Nodal Officer and Grievance Officer, the details of which can be accessed at https://www.cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx.

INVESTIGATION OF CYBER CRIMES UNDER INDIAN LAWS

For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code and the Evidence Act, have been amended. Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation.

Who can investigate?

The power to investigate the accused in regard to the cyber offences, has been entailed in Section 78 of the IT Act, which says that "notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act". Nevertheless, the IT Act is not sufficient to meet the necessity, therefore the Criminal Procedure Code, 1978 and the Indian Penal Code, 1860, were also amended accordingly to introduce cyber-crime under their ambit. This gives power to the Inspector to register and investigate the cyber-crime as like another crime.

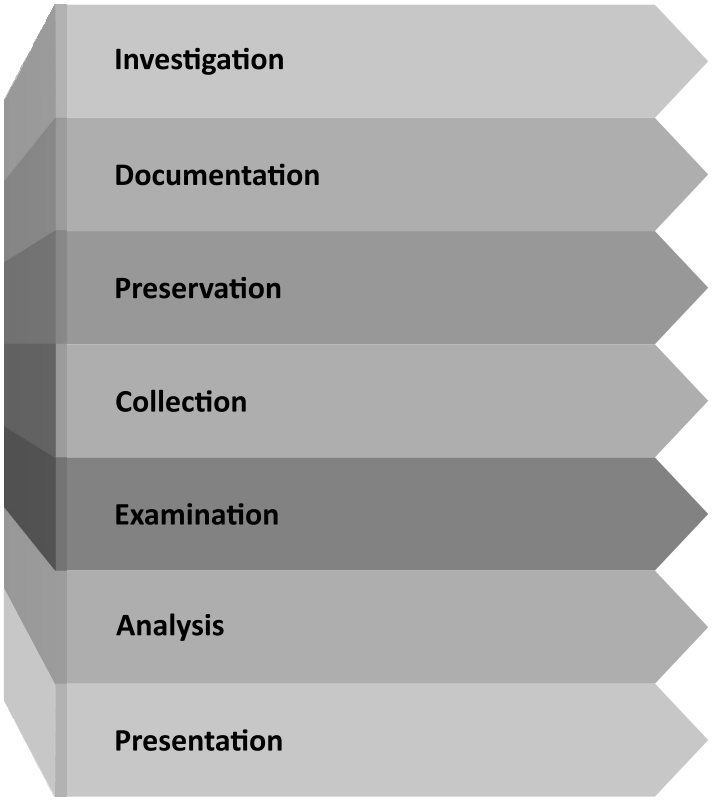
Process of search & arrest

The power of the police office and other officers to enter, search etc. is entailed in Section 80 (1) of the IT Act, which says that, notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of the Inspector or any other officer of the Central Government or State Government authorized by the Central Government in this regard, may enter any public place, search and arrest without warrant any person, who is reasonably suspected of having committed or of committing or about to commit an offence under the IT Act.

Pursuant to Section 80 (2) of the IT Act, any person who is arrested under sub-section (1) by an officer other than a police officer then such officer shall, without any unreasonable delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Case Study[17]: Steps in Investigation of Cyber-Crime *(Example Data Breach)*

Following are the major steps in conducting the investigation in a cybercrime. Let us understand the same in a cyber-crime of data breach.



Identification: Identify the incident that happened and determine the type of incident, in this case, the incident was a data breach that stolen 500 million identities and got sold in the dark web. The type of the incident could be data breach and data theft. The breach includes personal information like email address, contact information, name etc. The Investigation and/or the forensic examiner should identify the size of the attack (data breach), how the attack happened, method used in stealing the data etc.

The investigation should look for the answers the following questions,

- Check who is involved.
- Find what happened.
- When this happened.
- Where did this incident happen?
- How this incident happens?

By finding the answers to these questions, the investigator can get idea how to proceed with the case. Also, the investigator cannot miss the essential device that might be affected to this investigation. Costs can be estimated

17 See Jayasekara CM (2022) Cyber Crime and Forensic Investigation: Case Study Analysis, Researchgate.

in advance and be prepared for the actual needs. Identify the related evidence such as desktop, smartphones, printers, digital cameras, etc. And try to identify the suspect's characteristics.

There are many factors that may be noticed when identifying,

- Whether there is an administrator that can identify these devices?
- Number of devices that can be involved with this and types of devices.
- If there are any devices that have any remote login capabilities.
- Operating systems that may involve with.
- Power of sources of the suspected devices to operate.

Documentation

Last stage in this identification phase would be documenting every critical thing and revise them if it's necessary. In documentation, we can include, where these devices are found or removed, the information regarding the interview like name ad titles, and the number of devices that are found, where they founded or removed etc.

With this investigator may also continue the investigation process, which may help the business to identify the vulnerabilities and accordingly to adopt modalities to improve their network and security.

Preservation

In this stage, investigator should work in isolation, securing and preserving the physical and digital evidence. This helps to maintain the integrity of the digital evidence and protect the digital evidence from the modifications. Investigator should be responsible and must demonstrate that the evidence should be preserved through all steps in the process like in collection phase, examine phase, analyze phase, etc.

Preservation of the digital and physical evidence should be done by trained and skilled staff members that possess the required techniques and the knowledge of using appropriate tools.

Methods to preserve the Digital Evidence

Following methods need to be considered for preserving the digital evidence by forensic investigator:

- ***Drive Imaging:*** Imaging the drives can help to keep the evidence side and use the images for the analysis. To perform this imagining, professional make a duplicate of the drive with completing the evidence sector by sector.
- ***Making copies of the Evidence:*** Copies of the evidence could also help to retain the evidence. Copies should be encrypted with hash values in the label of the copies so can distinguish from Original. Along with that, critical information like name of the personnel, the date and time and place would be added with. This helps to verify the authenticity and helps to protect the integrity. These hash values could be useful in the court case.
- ***Chain of custody***[18]: When investigator extracts the media from the business and transfer the media if required, then the investigator should document all the transfer on a form called Chain of Custody (CoC).

This stage is crucial because once if the evidence not being preserved properly, this might be invalid in court case. From global perspective, it is to be noted that non-preservation of data and evidences may attract fines under GDPR.

18 Students to Note: Chain of Custody is an important pillar of Digital Evidence and the same is discussed in detail in the later pages of this chapter. See title – Digital Forensics

Collection:

In a cybercrime, there are high probabilities of having certain physical evidences also. Hence along with imaging, duplicating, or copying of the digital evidence, the investigator shall focus on collecting physical evidence also that relates to the crime scene. The investigator shall also collect documents which contain information of the evidence like, name, model, made year etc. Also, the audio recording, photographs, and other visual forms of the crime scenes should be collected and documented. Digital evidence such as desktop, smartphones, printers, digital cameras, etc. should be collected, in addition to the physical evidence. Other relevant evidence may include notes like passwords, suspect's documents, suspect's dairy etc. If the breach initiated within the perimeter, it's required to containment the crime scene, preform the specialized procedures like if the device was ON or OFF when found. If the computer is found OFF, investigator can take the photos of the computer, labelling cables, etc.

For an organized investigation, the investigator should follow some procedures during the collection process such as:

- Separate the electronic evidence from magnetic evidence.
- Keep the evidence in the required temperature.
- Should prepare proper packaging forms like bubble wrap depending on the type of evidence to avoid damages like shock etc.
- Do not store the evidence more than given amount that it should be stored (lifespan of batteries, lifespan of hard disk, etc.).
- Store all acquired evidence in secure manner (e.g.: proper storage)
- Avoid the loss of the dynamic data such as a lists of network connections, personal digital assistants (PDA's), data collected in cell phones, etc.
- During the collection and duplicating the digital evidence, hash values can be used to verify that it is an exact duplicate.

When investigators collecting the digital evidence, they need to care about the volatility and ensure to collect the evidences in, parts in sequence or order of volatility. It's a best exercise to collect the parts from highly volatile to the least volatile.

Order of volatility in a standard document.

- Registers, cache, and peripheral memory (Most Volatile)
- Main physical memory
- Virtual memory
- Network state
- Running processes
- Disk
- Floppies, backup media
- Archival media (CD, USB drives etc.) (Least Volatile)

Examination

This phase would be important for investigator to answer the legal questions and prove the case in court. This involves with in-depth systematic search of evidence that related to the crime scene. The goal of this phase is

to locate, analyze, and extract the digital evidence to refurbish the crime scene, analyze and extract refers, to interpret the data that extracted from the media and placing into the different logical format. Investigation uses lots of techniques while examining and interpret those crucial data into useful formats so that it helps to preserve the integrity and the chain of custody that are required to present in the court. The ways of examination can vary according to the types of devices and the personnel who doing examination must be skilled and trained.

Examination process can be done with two steps:

- Prepare to work on media where evidence files are stored that can be take out and used to prepare documentation for recording all the details of the examination process.
- Preparing a registry can helps to proceed the examination process and track everything by making double check.

Extraction of Data and/or Digital Evidences

Extracting can be done in two different ways such as physical and logical. Physical refers the extraction of the data from the physical level evidence and logical extraction refers the extracting from the file system that present in the drive like active files, etc. After the extraction, they can used to construct the crime scene to get a bigger picture of the incident. Things that might be worth to extract:

- File systems and Applications - using forensic tools, examiner can extract the important metadata like timestamp, directories, authors, etc.
- Registry files – example: in a Windows OS, Windows registry is where contains information like device information, configuration settings, etc.
- Temporary files like cookies, temporary worker/.tamp files, batch files (.bat) etc.
- Unallocated spaces and unused partitions that may expose some important information of deleted files.
- Scanning for the backdoors using tools like THOR and other free open-source forensic tools and monitor the network for data packets seizures.

Analysis:

It is significant to note that all the collected evidences are arranged and analyzed properly, so that specific conclusions can be drawn in solving the cyber-crime. This helps to understand the incident very well by reconstructing the crime scene.

Fundamentally, there are three kinds of ways to reconstruct:

- Temporal Analysis,
- Relational Analysis, and
- Functional Analysis.

Temporal analysis helps to find the factors that are likely to cause this incident and who shall be held responsible for. Relative analysis refers finding the baseline of the crime scene by corresponding the actions of the victim and functional analysis is about finding the actions that caused this.

During this phase, analyst gathering all evidence and present the cruciality of the evidence by using different analysis mechanisms depending on the nature of case.

- *Data hiding analysis*: Recovering the data can be hidden in these digital items could give the examiner a chance to know the significant information that may give the idea about the ownership, etc.

- *Log files analysis*: This analysis uses logs to get the idea of the behavior of system pre crime and find out the possibilities that lead to this crime. Analyzing some important log files like Intrusion Detection system logs and scan the security events are one of examples of log files analysis.
- *Time frame analysis*: The goal of this analysis is to get the idea of when this crime happened with analyzing the events on the digital systems by reviewing the time and data that has embedded into the files as metadata.
- *File analysis*: Analyzing the metadata that embedded in the files and the applications and other information may contain some hints leading to the crime scene like getting idea of the behavior of the user.

Presentation

This is final stage of any investigation which presents the results containing conclusions and summary of the investigation process. The information that provides with this presentation must be clear and precise so the business and victims can understand very well and get better knowledge how to avoid such another destruction in future.

In the presentation, any documents that had taken in each step in the process should be engaged with the audience. Reporting is the significant part of the presentation. A professionally written and clear report can increase the chances to prove the case very well in the court and win the case. In a good report should include the case logs, videos and other media, technical report, non-technical report, Chain of Custody (CoC), etc.

Also more importantly, the report should provide the aims and objectives, detailed steps of every log and technical and non-technical qualifications of the personnel who conducts the process would add more information to presentation.

Last but not the least, investigator and its team should work with the business/victim closely to understand the crime very well and provide the business/victims with all information on how crime committed, their probable loss and how the security system shall be implanted to protect the victim from cyber-crimes. For example, in this case, investigators shall inform the business/victim with the risks involved in the loss/beach of data. With such information the business can take suitable legal step for saving themselves the huge financial loss. However, the business should be aware of the steps that needs to avoid another data breach in the future and protect the customers from further destructions. Also, it is important that business should have tools to briefly address the destructions like data breach to get the depth and scope of the attack. One of the best steps to avoid is to implement more advanced security frameworks involving with the policies and regulations so business can be prepared to avoid attacks in future.

Some of the common cyber-crimes of 2023-2024[19]

- **FedEx Scam**

  How it works: It all starts when someone gets a call from a stranger pretending to be from 'FedEx.' The caller says a package in the person's name, heading to Macau or another country, got seized by Mumbai customs for having illegal stuff. After that, the victim is linked to a "police officer," often from the Mumbai Crime Branch or Anti-Narcotics Unit.

  Protect yourself: Verify the legitimacy of such messages/calls by contacting FedEx directly using official contact information.

- **YouTube Like Scam**

  How it works: Criminals are using WhatsApp and Telegram to approach potential victims with offers for part-time work from home or part-time jobs. In these fraudulent schemes, scammers are enticing users to engage with videos on YouTube by liking and subscribing.

19. Reproduced from Cyber Digest (2024), Indian Cyber Crime Coordination, Ministry of Home Affairs. Available at https://i4c.mha.gov.in/cyber_digest/jan_2024/I4C%20Daily%20Digest-%2029.01.2024%20.pdf

Protect yourself: Avoid clicking on links in suspicious messages. Verify notifications directly on the official YouTube website or app.

- **Online Shopping Scam**

  How it works: Fraudsters make fake websites that seem like real online stores. These sites usually tempt people with attractive discounts on popular products to trick them. When people enter their payment details, the scammers take their money and vanish.

  Protect yourself: Stick to well-known online stores, check reviews, and be wary of deals that appear too good to be true. Opt for secure payment options, and ensure the website has a secure connection before making any purchases.

- **Identity Theft Scam**

  How it works: Identity theft occurs when someone dishonestly obtains another person's important personal and financial information. They then use this information for various fraudulent activities, posing a significant risk to the victim.

  Protect yourself: Create strong and unique passwords, turn on two-factor authentication, be careful about sharing personal details on the internet, and routinely keep an eye on your accounts for any unusual activities.

- **Scholarship and Grant Scam**

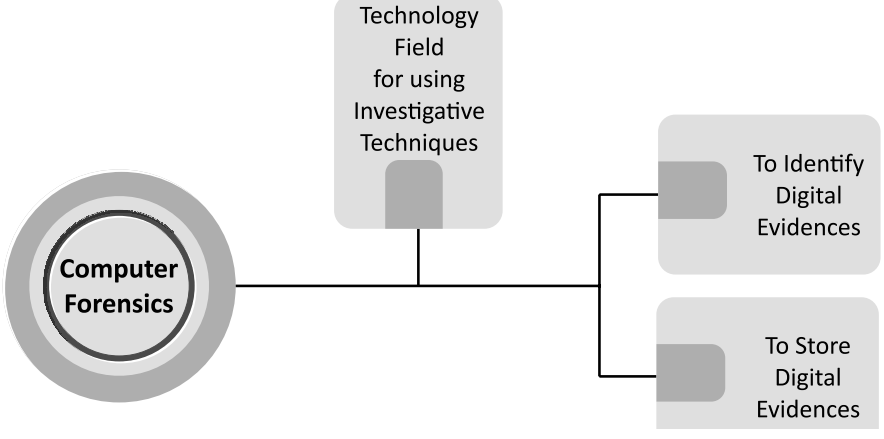
  How it works: Be wary of scammers pretending to be organizations offering scholarships or grants. They might ask for upfront fees or personal information without any intention of actually providing financial assistance.

  Protect yourself: When searching for scholarships, make sure to thoroughly research your options, confirm the legitimacy of organizations, and be cautious if asked for payment or sensitive information. Legitimate scholarships usually don't involve upfront fees.

COMPUTER FORENSICS AND DIGITAL EVIDENCE

What are Computer Forensics?

In general parlance, computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device.

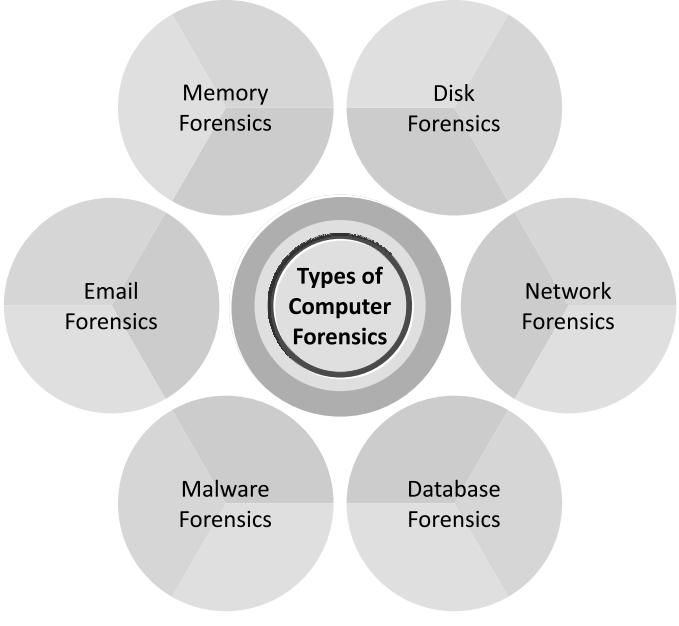


Often, computer forensics is used to uncover evidence that could be used in a court of law. Computer forensics also encompasses areas outside of investigations. Sometimes professionals in this field might be called upon to recover lost data from drives that have failed, servers that have crashed or operating systems that have been reformatted.

Use of Computer Forensics

Computer forensics is primarily used for two separate purposes, investigation and data recovery. To be precise, it can be called that computer forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Types of Computer Forensics[20]



Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.

- ***Network Forensics:*** It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- ***Database Forensics:*** It deals with the study and examination of databases and their related metadata.
- ***Malware Forensics:*** It deals with the identification of suspicious code and studying viruses, worms, etc.
- ***Email Forensics:*** It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- ***Memory Forensics:*** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.
- ***Mobile Phone Forensics:*** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

20 Source: Introduction of Computer Forensics (2023) Geeksforgeeks.

Role of Computer Forensics

- ***Identification:*** Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- ***Preservation:*** Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- ***Analysis:*** Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- ***Documentation:*** A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- ***Presentation:*** All the documented findings are produced in a court of law for further investigations.

COMPUTER FORENSICS VIS -A- VIS CYBER SECURITY

Both computer forensics and cyber security deal with criminals and computers, hence many a times they are considered rather similar. Despite this initial similarity, the function of computer forensics and cyber security greatly differs from each other.

To be precise, cyber security is majorly concerned with providing security/defence against the possible cyber-crime/cyber threat. Cyber security aims to build networks and systems that are secure from potential attackers. Sometimes hacking is also used to test networks, systems or the networks of a client to find areas of weakness and bolster them.

On the other hand, the computer forensics comes into picture when a cyber-crime is already committed and hence cyber forensic focuses largely on data recovery. The data recovered is often used as evidence in criminal trials, but sometimes is recovered for companies after a data loss incident. Additionally, the criminals that computer forensics professionals investigate are not always cybercriminals. Because almost everyone uses a computer, there is often valuable information on their personal device that can contribute to an investigation.

Investigations vide Computer Forensics

Computer forensics can be an essential facet of modern investigations. When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.

When a suspect has been identified and their personal computer or cell phone taken into evidence, a computer forensics professional goes searching for data that is relevant to the investigation. When searching for information, they need to be careful to follow detailed procedures that allow their findings to be used as evidence. The information they uncover, whether it be documents, browsing information or even metadata, may then be used by prosecution to create a compelling case against the suspect.

- ***Procedure***

  The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizure of the evidence which leads to the seizure of the evidence. The evidence are then transported to the forensics lab for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidence are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidence.

The analysis is then done on the copied evidence for suspicious activities and accordingly, the findings are documented in a nontechnical tone. The documented findings are then presented in a court of law for further investigations.

- ***Data Recovery***

  Aside from working to collect evidence, computer forensics professionals can also work in data recovery. When it comes to data recovery, forensics professionals can take broken hard drives, crashed servers and other compromised devices and retrieve the data that was previously lost. This is valuable for anyone who has lost important data outside of uncovering criminal evidence, such as businesses who have experienced a system crash.

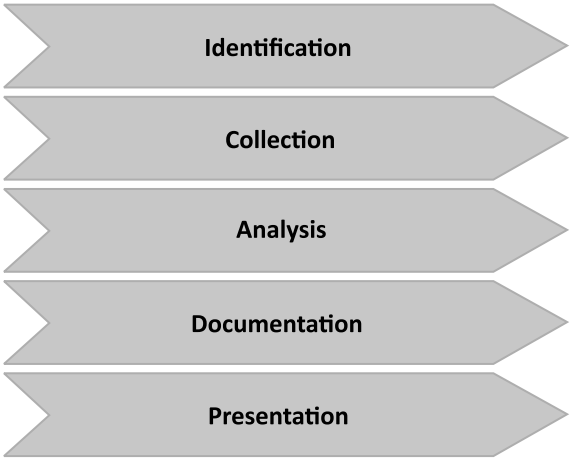
DIGITAL FORENSICS/DIGITAL EVIDENCES[21]

Digital forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.

In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. It includes the area of analysis like storage media, hardware, operating system, network and applications.

Steps in Digital Forensics

It consists of following five (s) steps:



21 Reproduced from Geeks for Geeks on Digital Forensics in Information Security, June 16, 2022.

Identification of Evidence: It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.

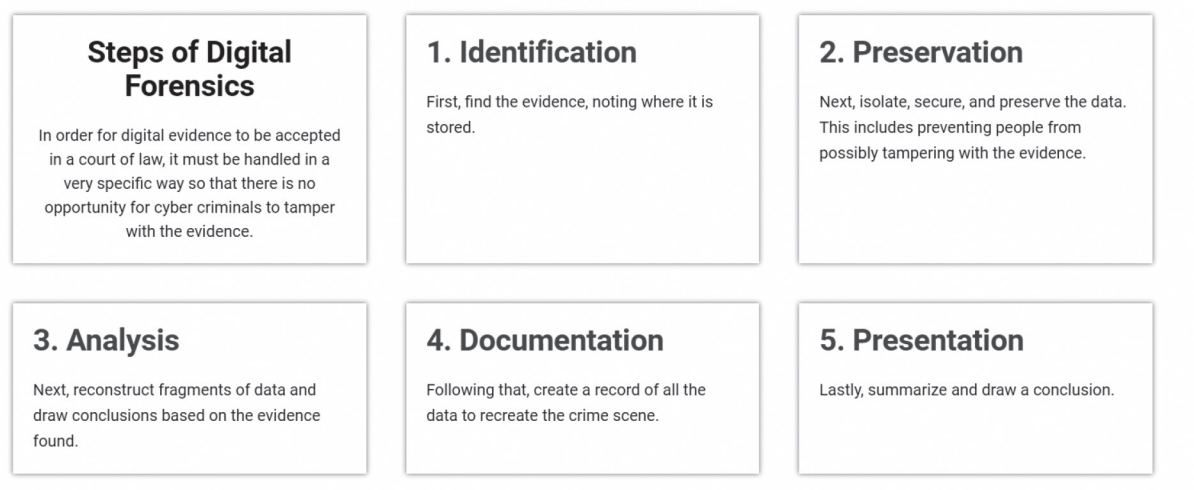
Collection: It includes preserving the digital evidences identified in the first step so that they don't degrade to vanish with time. Preserving the digital evidences is very important and crucial.

Analysis: It includes analysing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.

Documentation: It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.

Presentation: It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

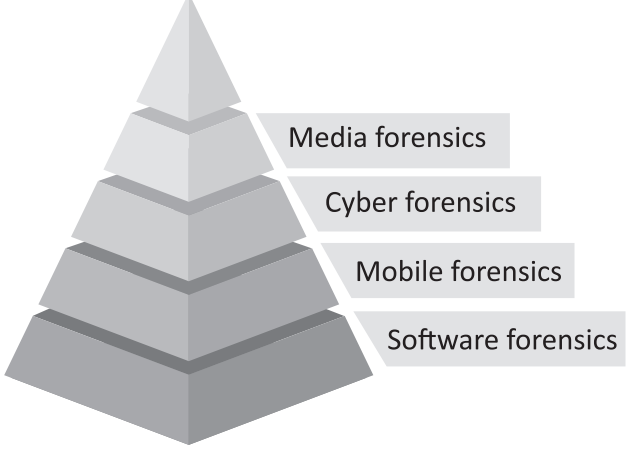
For the purpose of acceptance of Digital Evidence in the court of law, the EC Council has identified following steps of Digital Forensics/Evidence.



Source: https://www.eccouncil.org/what-is-digital-forensics/

Branches of Digital Forensics:

Following are the main branches of digital forensics:



Media forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.

Cyber forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cybercrime.

Mobile forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.

Software forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to software only.

Steps in Preserving Digital Evidence

(Source: Geeks for Geeks)

Following critical steps that need to be followed to prevent loss of data before bringing to the forensic experts. Time is highly important in preserving digital evidence.

- Do not change the current state of the device: If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
- Power down the device: In the case of mobile phones, if it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
- Do not leave the device in an open area or unsecured place: Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
- Do not plug any external storage media in the device: Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
- Do not copy anything to or from the device: Copying anything to or from the device will cause changes in the slack space of the memory.
- Take a picture of the piece of the evidence: Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
- Make sure you know the PIN/ Password Pattern of the device: It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
- Do not open anything like pictures, applications, or files on the device: Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.
- Do not trust anyone without forensics training: Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
- Make sure you do not shut down the computer, if required Hibernate it: Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

DIGITAL FORENSICS - CHAIN OF CUSTODY[22]

The digital evidence and digital chain of custody are the backbones of any action taken by digital forensic specialists. Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential and in case any step is missed, then the evidence may be rendered inadmissible in the court of law. Thus, we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.

What the Chain of Custody (under the perspective of Digital Cyber Forensics)

The chain of custody in digital cyber forensics is also known as the paper trail or forensic link, or chronological documentation of the evidence.

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.

Digital evidence is acquired from the myriad of devices like a vast number of Internet of Things (IoT) devices, audio evidence, video recordings, images, and other data stored on hard drives, flash drives, and other physical media.

Significance of maintaining Chain of Custody

A. Importance to Examiner:

- To preserve the integrity of the evidence.
- To prevent the evidence from contamination, which can alter the state of the evidence.

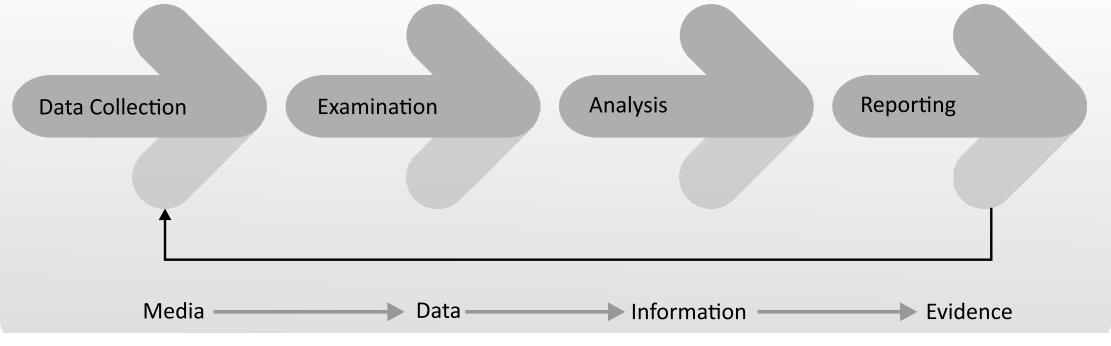
In case you obtained metadata for a piece of evidence but unable to extract any meaningful information from the metadata. In such a case, the chain of custody helps to show where possible evidence might lie, where it came from, who created it, and the type of equipment used. This will help you to generate an exemplar and compare it to the evidence to confirm the evidence properties.

B. Importance to the Court:

If not preserved, the evidence submitted in the court might be challenged and ruled inadmissible.

Process of Chain of Custody:

In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid any probability that the evidence has been compromised in any way.



Source: geeksforgeeks

22 *Reproduced from Article titled – Chain of Custody of Digital Forensics, Geekforgeeks.org*

- *Data Collection:* This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.
- *Examination:* During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
- *Analysis:* This stage is the result of the examination stage. In the analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.
- *Reporting:* This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:
  - Statement regarding Chain of Custody.
  - Explanation of the various tools used.
  - A description of the analysis of various data sources.
  - Issues identified.
  - Vulnerabilities identified.
  - Recommendation for additional forensics measures that can be taken.

The CoC form must be kept up-to-date. This means every time the best evidence is handled off, the chain of custody form needs to be updated.

Procedure to establish the Chain of Custody

In order to assure the authenticity of the chain of custody, a series of steps must be followed. It is important to note that the more information forensic expert obtains concerning the evidence, the more authentic is the created chain of custody. Following procedure is trailed according to the chain of custody for electronic devices:

- Save the original material.
- Take photos of the physical evidence.
- Take screenshots of the digital evidence.
- Document date, time, and any other information on the receipt of the evidence.
- Inject a bit-for-bit clone of digital evidence content into forensic computers.
- Perform a hash test analysis to authenticate the working clone.

Documentation/Authentication of Chain of Custody:

During the process of examination, it is important to document all such information that is beyond the scope of current legal authority and later brought to the attention of the case agent. A comprehensive report must contain following sections:

- Identity of the reporting agency.
- Case identifier.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.

- Descriptive list of items submitted for examination: This includes the serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during the examination: For example- string searches, graphics image searches, and recovering erased files.
- Results.

SECURITY AUDIT[23]

In general, security audit is a systematic evaluation of the security of a company's information system by measuring how well it adheres to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

Security audits are often used to determine compliance with regulations such as Information Technology Act, 2000 and other rules and regulations applicable on the IT environment of a particular organization. It majorly specifies how organizations have dealt with the information and data available in the organization.

Meaning of Audit

In order to catch the glimpse of security audit in totality, it also become significant to know and understand the meaning of Audit.

Audit in general refers to the examination or inspection of various books of accounts by an auditor followed by physical checking of inventory to make sure that all departments are following documented system of recording transactions. It is done to ascertain the accuracy of financial statements provided by the organization.[24]

Audit can be done internally by employees or heads of a particular department and externally by an outside firm or an independent auditor. The idea is to check and verify the accounts by an independent authority to ensure that all books of accounts are done in a fair manner and there is no misrepresentation or fraud that is being conducted.

All the public listed firms have to get their accounts audited by an independent auditor before they declare their results for any quarter.

As per *English Oxford Dictionary*, Audit means an official inspection of an organization's accounts, typically by an independent body. It also states a word of cautions that many a times, audits are not expected to detect every fraud.

Cambridge Dictionary refers that Audit is a systematic process to make an official examination of the accounts of a business and produce a report.

English Oxford Dictionary	***Cambridge Dictionary***
Audit means - ● An official inspection of an organization's accounts, ● Typically, by an independent body, ● It also states a word of cautions that many a times, audits are not expected to detect every fraud.	Audit refers as - ● Systematic process, ● To make an official examination of the accounts of a business, and ● To produce a report.

With the analysis of these definitions, it is apt to state that an audit is a systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern.

It also attempts to ensure that the books of accounts are properly maintained by the concern as required by law.

23 Students to note: As one of the major purposes of this paper is to understand law and practice related to Cyber Security, hence the Security Audit herein refers to cyber security audit in specific.

24 Definition of Audit, The Economic Times.

Significance of Security Audit

As discussed above that audit is conducted to reflect the true and fair value of certain concern, hence the security audit implies the true and fair value of security of computer, computer network, information and data. To be precise, security audits will help protect critical data, identify security loopholes, create new security policies and track the effectiveness of security strategies. There are several reasons to do a security audit and collectively include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

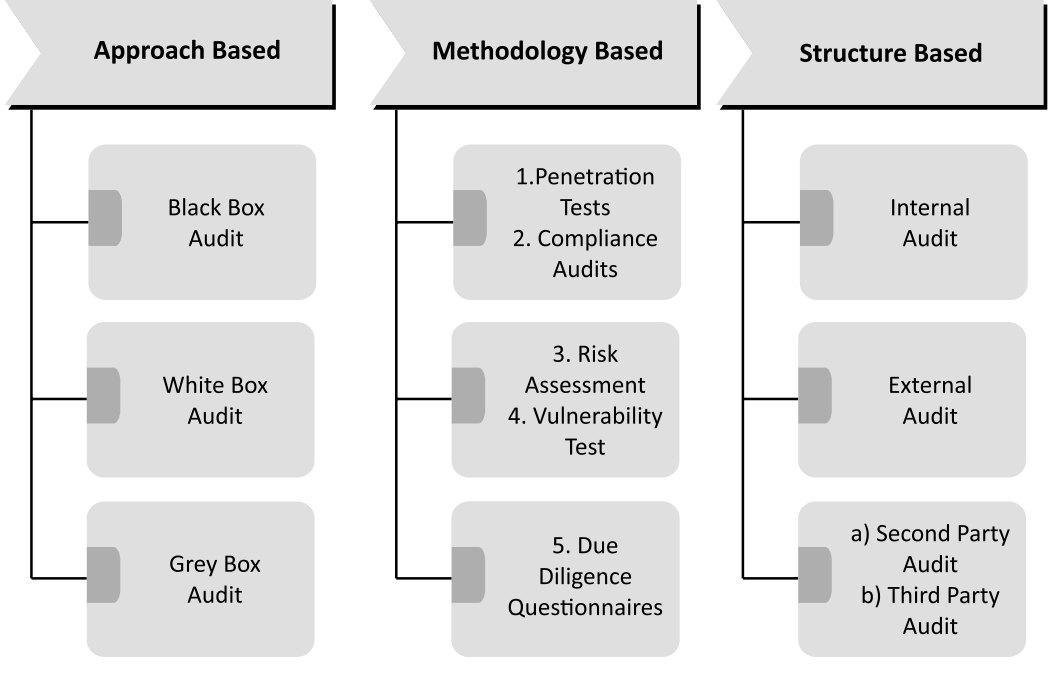
Advantages of Security Audit

As mentioned above, the security audit reveals underlying vulnerabilities and security risks in an organization's information technology assets. The identifying risks through security audit has following advantages:

- Weighs the security structure and protocols of the organization and helps it to define a security standard for organization with the audit results.
- Mitigates hacker-risks by discovering potential hacker entry points and security flaws well in advance.
- Verifies how compliant IT infrastructure is with top regulatory bodies, regulations, laws and rules applicable to certain sector/service. Accordingly helps the organization to stay compliant in accordance.
- Finds lag in organization's security training and awareness and helps you make informed decisions towards its betterment.

Types of Security Audit

Different types of audits based on approach, methodology and structure can be discussed as under.



Approach Based

- **Black Box Audit:** In this type of security audit, the auditor only knows about the info that is publicly available regarding the organization that is to be audited.
- **White Box Audit:** In this type of security audit, the auditor is provided with detailed info (i.e. source code, employee access, etc.) regarding the organization that is to be audited.
- **Grey Box Audit:** In grey box audit, the auditor is provided with some info, to begin with, the auditing process. This info can also be gathered by the auditors themselves but is provided to save time.

Methodology Based

- **Penetration Tests:** The auditor tries to break into the organization's infrastructure.
- **Compliance Audits:** Only certain parameters are checked to see if the organization is complying with security standards.
- **Risk Assessments**: An analysis of critical resources that may be threatened in case of a security breach.
- **Vulnerability Tests*:*** Necessary scans are performed to find possible security risks. Many false positives may be present.
- **Due Diligence Questionnaires:** Used for an analysis of existing security standards in the organization.

Structure Based Audit

Security audits come in two forms, internal and external audits that involve the following procedures:

- **Internal audits:** In these audits, a business uses its own resources and internal audit department. Internal audits are used when an organization wants to validate business systems for policy and procedure compliance.
- **External audits:** With these audits, an outside organization is brought in to conduct an audit. External audits are also conducted when an organization needs to confirm it is conforming to industry standards or government regulations.

There are *two subcategories of external audits: Second and Third Party Audits*. Second Party audits are conducted by a supplier of the organization being audited. Third Party audits are done by an independent, unbiased group, and the auditors involved have no association with the organization under audit.

Steps – On Conducting Security Audit:

Step 1: Preliminary Audit Assessment

This stage is used to assess the current technological maturity level/status of the company and helps to identify the required time, cost and scope of an audit. Firstly, one need to identify the minimum-security requirements, which are as below:

- Security policy and standards
- Organizational and Personal security
- Communication, Operation and Asset management
- Physical and environmental security
- Access control and Compliance
- IT systems development and maintenance

- IT security incident management
- Disaster recovery and business continuity management
- Risk management.

Step 2: Planning & Preparation

The auditor should plan a company's audit based on the information found in previous step. Planning an audit helps the auditor obtain sufficient and appropriate evidence for each company's specific circumstances. It helps predict audit costs at a reasonable level, assign the proper manpower and time line and avoid misunderstandings with clients.

An auditor should be adequately informed about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern
- Review the current IT organization chart
- Review job descriptions of data center employees
- Research all operating systems, software applications, and data center equipment operating within the data center
- Review the company's IT policies and procedures
- Evaluate the company's IT budget and systems planning documentation
- Review the data center's disaster recovery plan.

Step 3: Establishing Audit Objectives

In the next step, the auditor outlines the objectives of the audit after that conducting a review of a corporate data center takes place. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Following is a list of objectives the auditor should review:

- Personnel procedures and responsibilities, including systems and cross-functional training.
- Change management processes are in place and followed by IT and management personnel.
- Appropriate backup procedures are in place to minimize downtime and prevent loss of important data.
- The data center has adequate physical security controls to prevent unauthorized access to the data center.
- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding.

Step 4: Performing the Review

The next step is collecting evidence to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and within the data center. The following review procedures should be conducted to satisfy the pre-determined audit objectives:

- *Data Center Personnel* – All data center personnel should be authorized to access the data center (key cards, login ID's, secure passwords, etc.). Data center employees are adequately educated about data center equipment and properly perform their jobs. Vendor service personnel are supervised when doing

work on data center equipment. The auditor should observe and interview data center employees to satisfy their objectives.

- *Equipment* – The auditor should verify that all data center equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
- *Policies and Procedures* – All data center policies and procedures should be documented and located at the data center. Important documented procedures include data center personnel job responsibilities, back up policies, security policies, employee termination policies, system operating procedures and an overview of operating systems.
- *Physical security / environmental controls* – The auditor should assess the security of the client's data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted-down equipment, and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data center equipment. These include Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
- *Backup procedures* – The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure.

Step 5: Preparing the Audit Report

After the audit examination is completed, the audit findings and suggestions for corrective actions can be communicated to responsible stakeholders in a formal meeting. This ensures better understanding and support of the audit recommendations. It also gives the audited organization an opportunity to express its views on the issues raised.

Writing a report after such a meeting and describing where agreements have been reached on all audit issues can greatly enhance audit effectiveness. Exit conferences also help finalize recommendations that are practical and feasible.

Step 6: Issuing the Review Report

The audit review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as per the completion of the auditor's inquiry and procedures. It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

Typically, a security audit review report consolidates the entirety of the audit. It also offers recommendations surrounding proper implementation of physical safeguards and advises the audited organization on appropriate roles and responsibilities of its personnel. Generally, the audit report include:

- The auditors' procedures and findings.
- The auditors' recommendations.
- Objective, scope, and methodologies.
- Overview/conclusions.

The security audit report may optionally include rankings of the security vulnerabilities identified throughout the performance of the audit and the urgency of the tasks necessary to address them. Rankings like "high", "low", and "medium" can be used to describe the imperativeness of the tasks.

Concluding Remarks

The above discussion confirms the signification of security audit for fortifying the IT infrastructure of a company as well as the minimize the probability of cyber-attacks. A well conducted security audit ensures the following:

- Identify potential threats including the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- Evaluate security and risks. Apart from assessing the risk of each of the identified threats happening, it also guides on how well the organization can defend against them.
- Determine the needed controls by Identifying what security measures must be implemented or improved to minimize risks.
- Helps the organization in ensuring compliance with the applicable laws and regulations related to the IT infrastructure and requirement of the company.

Hence, it will be apt to state that periodic security audit is directly proportionate to the growth of the organization.

Cyber Security Audit: A Snapshot[25]

A cybersecurity audit involves a comprehensive analysis and review of your IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices.

Significant benefits of IT security audits are:

- Risk assessment and vulnerability identification
- Strengthened security measures
- Compliance with regulations and standards
- Incident response preparedness
- Safeguarding sensitive data and customer trust
- Proactive threat detection and prevention

Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security posture. They aim to identify vulnerabilities, risks, and threats that may affect the organization. These audits cover various areas, including:

- **Data Security** – involves reviewing network access control, encryption use, data security at rest, and transmissions.
- **Operational Security** – involves a review of security policies, procedures, and controls.
- **Network Security –** a review of network & security controls, anti-virus configurations, security monitoring capabilities, etc.
- **System Security** – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- **Physical Security** – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Beyond these, a cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

25. Reproduced from Chinnaswamy Vinugayathri (2023), What Is Cyber Security Audit and How Is It Helpful for Your Business? Indusface. Available at https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business/#:~:text=A%20cyber security%20audit%20involves%20a,Risk%20assessment%20and%20vulnerability%20identification

Source: https://blueteamresources.in/cyber-security-audit-checklist/

Cyber Attacks in Middle East

With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported by the NIPC (National Infrastructure Protection Centre) in October of 2000 to U.S. Officials. The attacks were a volley of e-mail floods, DoS attacks, and Ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah.[26]

India and Pakistan Conflict

As tensions between the neighbouring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Center which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy's Website.[27]

Retribution by China

In May 1999 the accidental bombing of a Chinese embassy in Yugoslavia by U.S. Bombers, led to a massive website defacement and email bombardment attack on American companies and agencies. Pro Chinese hackers and political groups executed the attacks to gain sympathy for Chinese cause. US Government sites such as the US department of energy and the interior and the National Park Service were all hit and had website defaced along with the White House website. The sites were downed for three days by continual e-mail bombing. Although the attack was rather random and brief and affected a small number of U.S. sites, the effects could have been worse.[28]

Cyber attack by Tamil Tigers

In 1998, with surges of violence committed in Sri Lankan over Several years, attacks in cyber-space were the next area to target. The group known as the Tamil Tigers, a violent guerrilla organization bombarded Sri Lankan embassies with over 800 e-mails a day. This was carried out over a two week period. The attack by the e-mail message conveyed the message, "We are the Internet Black Tigers and we are doing this to disrupt your communications." After the messages created such major disruption the local Intelligence authorities were dispatched to investigate. The authorities declared the attack as the first known attack on the Sri Lankan by the terrorists on any computer system in the nation.[29]

Yugoslavia Conflict

When NATO[30] air strikes hit Former republic of Yugoslavia in Kosovo and Serbia, NATO web servers were

26. "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber- assault-931 (Accessed on 14th February, 2016)

27. "Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (Accessed on 14th February, 2016)

28. Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventional- terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

29. Cyber Terrorism – "Testimony before the Special Oversight Panel oil Terrorism"- Dorothy E Denning - May 23, 2000. also at https://www.sans.org/reading- room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

30. The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its

subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to "ping saturation", Distributed Denial Of service assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks cause serious disruption of NATO communications infrastructures.

Cyber Attack on Estonia

The small Baltic country of Estonia was cyber-attacked from Russia. Ever since the government of the Baltic state decided to remove a war memorial to the Red Army from a square in the capital, Tallinn, Russian outrage has ensued. This took the form of demonstrations and even riots. But then something extraordinary happened: quickly, and wholly without warning, the whole country was subjected to a barrage of cyber-warfare, disabling the websites of government ministries, political parties, banks and newspapers. Techniques normally employed by cybercriminals, such as huge remotely- controlled networks of hijacked computers, were used to cripple vital public services. NATO has sent its top cyber-terrorism experts to Tallinn, with western democracies caught on the hop over the implications of such an attack. The Estonian defence ministry said: "We've been lucky to survive this. If an airport, bank or state infrastructure is attacked by a missile, it's clear war but if the same result is done by computer's, then what do you call It. IS It a state of war? These questions must be addressed." Estonia has blamed Russia, predictably enough; which, if true, would mean this is the first cyber attack by one sovereign state upon another. The Estonian attacks were more likely to be the work of angry young Russian hackers working alone than any sort of organised blitz by the Kremlin. But either way, the implications are serious.[31]

Sony PlayStation Network, Microsoft's Xbox Live network case

In this case the confidential data of the employees and their families has been leaked in 2014. The company has faced loss in revenue due to movies being leaked, sensitive employee information was disclosed including their salaries and social security numbers, and executive emails were publicized. The attack was hatched by the Lizard Squad, an organization that refers to itself as a cyber-terrorist. Then they launched a massive Distributed denial of service attack against Sony's PlayStation Network and Microsoft's Xbox Live networks. They followed up these disruptions with an attack against the Tor Project, a network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure and network has gone down for almost Ten hours due to the attack affecting the lives of millions. Due to that many think that it is an act by the US government. However it is not but they manage to create doubts regarding purchasing the product among the consumer and people regarding the multinational companies. The Motive behind these cyber terrorist attacks is collateral damage involved and the obvious ties to geo-political situations that we see in so many attacks. The Current President Barack Obama of United States has said that "cyber- terrorism is perhaps one of the greatest threats against the U.S. today. Unfortunately, the attacks are not only here to stay, but given the utter reliance on the Internet today, they are likely to grow in a very serious manner".[32]

Indian Law & Cyber Terrorism

It is the easiest way in modern scenario is attack a country is through cyber network. India is in developing stage and the impact of cyber attack on Indian infrastructure and communication is going to be immense, because India now heavily depends on computers and information Technology.

---

member states agree to mutual defense in response to an attack by any external party. (Source Wikipedia accessed on 16th February, 2016)

31. See "Attack of the cyber terrorists" by MICHAEL HANLON Available at: http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html (Accessed on 16th February, 2016)

32. See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/ (Accessed on 16th February, 2016)

There is need of series of innovative laws and global standards on dealing with cyber crimes. The Computer/ Internet is changing the process of knowledge creation and dissemination of information as well as deeper transmission is taking place towards redefining the communication process. Thus a fine balance can be achieved between terrorism and Law enforcement with due care and consideration. Thus we have enacted Information Technology Act, 2000 to punish the cyber criminals.

Earlier there was no specific provision in the IT Act, 2000 which deals specifically with Cyber terrorism due to this, a new section 66F has been inserted by Information Technology (Amendment) Act, 2008. It is a welcome change brought by the IT Amendment Act, 2008 in view of increasing terrorist activities in India and neighbouring nations.

Punishment for cyber terrorism[33] - (1) whoever, -

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or destruction of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

For the prevention of cyber terrorism we can use the method of “Counter strike through aggressive Defence”. The concept of counter strike through aggressive defence presupposes the adoption and use of information technology to produce legitimate and legalized disabling and reasonably destructive effects. Some adopted measures completely destroys the functioning of the offending computer while others simply disable the computer for the time being by either shutting it down or making it temporarily non-functional. The technology adopted must not only be safe and effective, but it must also be “legal and law-abiding”. A counter-measure, which is not very accurate, and law abiding would be a remedy worst than the malady and hence it should be avoided. For instance, if a virus has been launched by using a public server, then by disabling that server the genuine and legitimate users will be unnecessarily harassed and they would be denied the services which they are otherwise entitled to. Thus, the countermeasure measure adopted must be job specific and not disproportionate to the injury sought to be remedied.[34]

33. Information Technology Act, 2000, s., 66F

34. Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer Crime Research Center, March 10, 2006.

In March 2013, suspected Chinese hackers breached the computers of India's top military organisation, the Defence Research and Development Organisation (DRDO), in what was touted to be amongst the biggest such security breaches in the Indian history. India has seen many such attacks on its critical installations and the misuse of social media and Internet has brought home the threat of cyber-terrorism, the country is vulnerable to such cyber- terrorism attacks with some countries and vested interest groups bent on espionage and destruction.[35]

According to Pavan Duggal the threat of cyber attacks remains "imminent", the country lacks an institutionalised mechanism of a cyber army to deal with the threat. Further stated that "the recent DRDO breach was a classical case of cyber war attack rather than mere hacking. It was an attack on India's critical information infrastructure. Cyber warfare as a phenomenon is not covered under the Indian cyber law. Clearly, India's cyber security is not in sync with the requirements of the times"[36]

Over the past few years, India has witnessed a growing number of cyber terrorist attacks, with government departments, particularly defence establishments, coming under attack. There are following cases of cyber terrorism in India.

1. In 2012, hacker group 'Anonymous' carried out a series of Distributed Denial of Service (DDoS) attacks against a number of government websites, in retaliation against the alleged Internet censorship.
2. Also in 2012, Hackers from Algeria carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments.
3. Hackers from Pakistan and terrorist organization are increasing their attacks on Indian Websites to provide a new dimension to the ongoing conflict over Jammu and Kashmir. 'GForce' a group of anonymous hackers whose members write slogans critical of India and its claim over Kashmir, have owned up to several instances of hacking of Indian sites run by the Indian government like breaking into the high security computer network of Bhabha Atomic Research Center.
4. Indian Parliament attack is one of the deadliest attacks on Indian Democracy. It is a case of cyber terrorism where accused committed cyber forgery and made passes, downloaded official logo and layout map of the parliament has been downloaded through the Pakistan service provider. They controlled the e-mail and identity system of Indian Army.
5. In March, 2016 the Indian Infrastructure was attacked by the Terror outfit with the name of Al Qaeda who, allegedly hacked a micro site of the Rail net page of the Indian Railways to show its sinister reach for the first time. The hacked page of Bhusawal division of Personnel Department of the Central Railway and part of a large intranet created for the department's administrative needs was replaced by a message of Maulana Aasim Umar, Al Qaeda chief in south Asia, for all Indian Muslims to participate in Jihad.[37]

Information Technology becomes an easy tool in hands of terrorist. They use computers and networks to communicate with their operatives all around the world in codes without detected by the enforcement agencies. Cases like Ayodhya incident, attack in Mumbai in 2006, defacement of Indian Military sites in India by hackers in July 2005, attack on American Center at Kolkata and Pathankot Terrorist Attack etc., are the major cyber terrorist attacks in India.

As per the cyber law and cyber security expert Prashant Mali "The threat landscape remains very threatening, India is awakening to the global threat of cyber warfare now. Our cyber security is still ineffective as mass awakening towards it is missing or inadequate. Even though NTRO and DRDO are mandated with cyber offensive work, only time will show effectiveness of these organisations."

---

35. http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 (Accessed on 16th February, 2016)

36. Ibid

37. http://www.ndtv.com/india-news/al-qaeda-hacks-into-indian-railways-website-leaves-message-to-join-jihad-1283023 (Accessed on 21 March, 2016)

With cyber security impacting the country's security, Shiv Shankar Menon, the national security adviser, announced that the government is putting in place national cyber security architecture to prevent sabotage, espionage and other forms of cyber threats.

Shantanu Ghosh, vice president at India Product Operations-Symantec Corporation, which developed Norton Antivirus has said that "The past few years have witnessed a dramatic shift in the threat landscape. The motivation of attackers has moved from fame to financial gain and malware has become a successful criminal business model with billions of dollars in play. We have now entered a third significant shift in the threat landscape, one of cyber- espionage and cyber-sabotage."

Rikshit Tandon, advisor to the Cyber Crime Unit of the Uttar Pradesh Police, said: "Cyber terrorism is a grave threat not only to India but to the world. It can come to any country and, yes, a proactive measure by government and consortium of countries needs to be taken as a collective effort and policy since internet has no geographical boundaries".[38]

Hacking

Hacking is labelled as amongst the most serious of all cyber crimes. It is said that hacking erodes the faith of people in information technology and the Internet. Hacking a computer system has been projected as a menace requiring harsh laws to act as deterrents. Such a general projection is somewhat misconceived.

Hacking a computer simply implies getting into another's computer without permission. Gaining unlawful access to another's computer is hacking. Unauthorized entry into a computer belonging to another is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein. Anti- hacking tools such as the 'Firewall' technology and intrusion detection systems are preventive measures that can be taken to protect a computer from being hacked. Firewall, like a wall of fire, prevents hacking. Intrusion detection systems will in addition also try to detect the source of hacking.

Hacking perse, in simple terms, is criminal trespass into a computer that is a private property. Criminal trespass under the Indian Penal Code, 1860 is simply defined as entering into property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, by unlawfully remaining there with intent thereby to intimidate, insult or annoy any such person or with intent to commit an offence.[39] Criminal trespass entails a punishment of imprisonment upto three months or fine upto rupees five hundred, or with both[40] Criminal trespass perse is thus a minor offence.

Here is a short list of great hackers of the world.

The most famous hacker in the history is Kevin Mitnick. At the tender age of 17 in 1981, he hacked into a phone exchange that allowed him to redirect subscriber calls in any way he wanted. In 1983, he accessed a Pentagon computer. In 1990s, he cracked/hacked/broke into the computer systems of the world's top technology and telecommunications companies like Nokia, Fujitsu, Motorola and Sun Microsystems. He was arrested by the FBI in 1995 and later released on parole in 2000.[41]

Gary McKinnon, an Englishman, was arrested in November 2002 on the accusation that he had hacked into more than 90 US military computer systems in the U.K.

Vladmir Levin, a Russian computer 'expert' is said to be the first to hack a bank to steal money. In early 1995,

38. Ibid

39. Indian Penal Code, 1860., s. 441

40. Indian Penal Code, 1860., s. 447

41. http://www.funonthenet.in/forums/index.php?topic=1260.0;wap2 (Accessed on 20th February, 2016)

he hacked into Citibank and robbed US$ 10 million. He was arrested by Interpol in the U.K. in 1995, after he had transferred money to his accounts in the US, Finland, Holland, Germany and Israel.

A Los Angeles radio station announced a contest that would reward the 102nd caller with a 'Porsche 944S2'. Kevin Poulsen took control of the entire city's telephone network and ensured he was the winner being the 102nd caller. He also hacked into 'Arpanet' that was the precursor to the Internet. Arpanet was a global network of computers.

US based hacker Timothy Lloyd planted a malicious software code in the computer network of Omega Engineering which was a prime supplier of components to NASA and the US Navy. Omega lost US$10 million due to the attack by which its manufacturing operations were impaired.[42]

Species of criminal trespass have been treated with more deterrent punishments. For instance, punishment for house-trespass is punishable with imprisonment upto one year.[43] House-trespass in order to commit an offence punishable with death (i.e. murder etc.) is punishable with imprisonment for life or rigorous imprisonment upto ten years.[44] House-trespass in order to commit an offence punishable with imprisonment for life is punishable with imprisonment upto ten years.[45] House-trespass, other than the above, entails punishment with imprisonment extending to two years and if the offence intended to be committed is theft, the term of the imprisonment may extend to seven years.[46] For house-trespass committed after preparation to cause hurt, assault or wrongful restraint or putting any person in such fear, the punishment prescribed is imprisonment extending to seven years.[47] Lurking house- trespass or housebreaking is punishable with imprisonment extending to two years.[48] Lurking house-trespass or housebreaking in order to commit an offence punishable with imprisonment, is liable for imprisonment upto three years and if such intended offence is theft, the term of imprisonment has been extended to ten years.[49] The punishment for lurking house-trespass or housebreaking by night is punishable with imprisonment extending to three years.[50] Grievous hurt caused whilst committing lurking house-trespass or housebreaking, is punishable with imprisonment for life, or imprisonment extending to ten years.[51] All persons jointly concerned in lurking house- trespass or housebreaking by night, are liable to be punished with imprisonment for life or extending to ten years, where death or grievous hurt is caused or attempted to be caused by any one or more of them.[52]

Another instance of an offence that has numerous species is "mischief". Every species of mischief is separately laid down in the I.P.C. with differing punishments, depending upon the magnitude thereof.[53] Many of the offences in the I.P.C. such as robbery, criminal breaches of trust, cheating etc., have their respective species that are treated differently from one another.

The legal approach towards hacking should be the same as that of criminal trespass, mischief and the innumerable other offences in the I.P.C. All forms of hacking cannot be treated alike. It needs to be understood that hacking too has numerous dimensions and species like other offences.

A person who enjoys exploring computer systems is also a hacker. Many teenagers obsessed with the Internet and computers hack for fun and excitement. Excitement to make an impact, show of capability and knowledge

42. Ibid
43. Indian Penal Code, 1860., s. 448
44. Indian Penal Code, 1860., s. 449
45. Indian Penal Code, 1860., s. 450
46. Indian Penal Code, 1860., s. 451
47. Indian Penal Code, 1860., s. 452
48. Indian Penal Code, 1860., s. 453
49. Indian Penal Code, 1860., s. 454
50. Indian Penal Code, 1860., s. 456
51. Indian Penal Code, 1860., s. 459
52. Indian Penal Code, 1860., s. 460
53. Indian Penal Code, 1860., s. 425-440

of computers, fun and publicity, and the desire to explore are some of the motives of these teenagers to hack into computer systems.

Another form of hacking is by Internet security companies, to test the computer systems of their clients and potential clients, to impress them and get business assignments of setting up security systems for the clients.

Hacking is also committed to damage the business of competitors and enemies. Disruption of a computer and denial of access to a person authorized to access any computer, are some of the damages that may be caused by hacking. Hacking is also done to spy into others computer systems and for stealing information/data residing therein. Hacking is also used as a Weapon to commit other crimes such as cheating and misappropriation of funds electronically from the bank account of another.

Hacking is done at the country level too. Frequently, Pakistani hackers are accused of hacking Indian web-sites. For instance, the web-site of SEBI (Stock Exchange Board of India) was hacked whereby a link to a pornographic web-site was inserted.

Hacktivists are protestors against governments or institutions / organizations, who protest through hacking. For instance, anti-globalization protests have been made through hacking the web-site of WTO.

There are therefore numerous species of hacking, though in essence, it is the offence of criminal trespass. All forms of hacking cannot thus be treated alike. It is the intent, purpose and consequences of hacking that determine its gravity. A twelve year old, who, for excitement and playing a prank enters restricted web-sites, should not be treated as a national enemy. A terrorist organization hacking into a protected system such as the defence computer systems to steal nuclear secrets, or a criminal syndicate hacking to misappropriate huge amounts, cannot be treated on par with a teenager prying into the computer system of his best friend's girlfriend or even the CBI (Central Bureau of Investigation) for fun and excitement. The nature of the hacking determines the gravity and all forms of hacking should not be projected or legally treated in the same manner. Hacking has so many species. Hacking is a skill that can be used positively as well as negatively. A man opening locks to help people who have lost the key is a locksmith. However, a person who opens locks to steal is a thief.

The seriousness of hacking depends upon the nature, purpose, intent and the extent of loss and injury that are caused to the victim. For instance, in a reported incident in the U.S., the owner of a hobby web-site for children received an e-mail informing her that a group of hackers had gained control over her web-site. They demanded a ransom of one million dollars. The threat was overlooked as a mere scare tactic. A few days late, she discovered that the hackers had 'web-jacked' her web-site. 'Web-jacking' has been equated with hijacking an aeroplane, as forcibly assuming control of a web-site, for diverse motives. The hackers had altered a part of the web-site which said "How to have fun with goldfish". The word "goldfish" was replaced with "piranhas". Piranhas are tiny but extremely dangerous flesh eating fish. Many children visiting the web-site, purchased 'piranhas' from pet shops and tried playing with them, thereby hurting themselves badly.[54]

Hacking in various forms is already part of several offences, either as the means to their commission or as a consequence. For instance, hacking could be a tool and means to commit cheating, misappropriation, criminal breach of trust, theft, copyright violations, spying into official secrets, or as part of the conspiracy to wage war against the State, that are all well defined offences. Some of the species of hacking have been defined as contraventions as well as criminal offences in the LT. Act, 2000 as amended by the I.T. (Amendment) Act, 2008. In the original version of the I.T. Act, 2000, section 66 defined and punished hacking in the following terms:

"Hacking with Computer System - (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects is injuriously by any means, commits hacking.

54. "Hack Attack" by Shuchi Nagpal, Asian School of Cyber Laws in Indian Express Vigil, March 2002. also available at http://www.asianlaws.org/press/hack_attack.htm (Accessed on 20th February, 2016)

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both".[55]

The title of the aforesaid section 66 was a misnomer, which created confusion. It was widely believed as if section 66 was the only legal provision that dealt with the offence of hacking a computer system. This confusion has been done away with, by certain amendments made by the I.T. (Amendment) Act, 2008. The words "Hacking with Computer System" have been deleted from section 66, the scope of which has been substantially widened:

"If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both".

The various species of the offence of hacking that are provided (even though not called 'hacking' specifically) for or may have elements of hacking, in the amended version of the I.T. Act, 2000 are:

- Access to a computer.
- Downloading, copying or extraction of data from a computer.
- Introducing computer virus and contaminants.
- Causing damage to a computer.
- Causing disruption of a computer.
- Causing denial of access to a computer.
- Affecting critical information infrastructure.
- Cyber terrorism.

LESSON ROUND-UP

- As discussed in the previous chapters that use of Internet and rapid deployment of information and communication technologies in recent years have bought various changes in the world both at individual level as well as organization level.
- Right from the way we communicate to the way we buy our groceries, each and every activity of human life is revolutionized with the help of information and communication technology. Crime is not an exception to this revolution brought by information and communication technologies.
- On one hand wherein the pattern of crime has been altered by misusing the tools and techniques of information and communication technology, on the similar hand, historic trends and practices in criminal investigation has also been revolutionized.
- This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails.
- India has been a favorite hub for cybercriminals, mostly hackers and other malevolent users who misuse the Internet by committing crimes.
- On one hand where we are witnessing the advancement of information and communication technology; on the similar end, we are seeing the new tools and techniques of committing cybercrimes.
- In general, cyber criminals make use of various tools and techniques yet the following are the most common tools and techniques used recently to conduct cybercrimes.
- The discussion above confirm that India is facing the growing threat of cybercrimes.

55. Information Technology Act, 2000., s. 66

- As per the Report published on recording the cyber incidents, India was placed on the 80th position in a report focusing on local threats in the year 2023.
- India's cybersecurity market reached USD 6.06 billion in 2023.
- However, according to IDC, a global marketing intelligence firm, the alarming increase in sophisticated external cyber threats and cybersecurity attacks is one of the biggest challenges for the majority of enterprises in establishing organizational trust.
- This has led government of India to channelize the effective ways in enhancing the level of cyber security.
- The Government of India had launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature.
- The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs).
- To strengthen the mechanism to deal with cyber-crimes in a comprehensive and coordinated manner, the Central Government has taken various steps including the establishment of 'Indian Cyber Crime Coordination Centre'
- For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible.
- Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code and the Evidence Act, have been amended.
- Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation.
- In general parlance, computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device.
- Computer forensics is primarily used for two separate purposes, investigation and data recovery.
- Both computer forensics and cyber security deal with criminals and computers, hence many a times they are considered rather similar.
- Despite this initial similarity, the function of computer forensics and cyber security greatly differs from each other.
- Computer forensics can be an essential facet of modern investigations.
- When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.
- Digital forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.
- The digital evidence and digital chain of custody are the backbones of any action taken by digital forensic specialists. Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.

- Each step in the chain is essential and in case any step is missed, then the evidence may be rendered inadmissible in the court of law. Thus, we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.
- In general, security audit is a systematic evaluation of the security of a company's information system by measuring how well it adheres to an established set of criteria.
- A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.
- Security audits are often used to determine compliance with regulations such as Information Technology Act, 2000 and other rules and regulations applicable on the IT environment of a particular organization.
- It majorly specifies how organizations have dealt with the information and data available in the organization.
- The above discussion confirms the signification of security audit for fortifying the IT infrastructure of a company as well as the minimize the probability of cyber-attacks.
- Identify potential threats including the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- Evaluate security and risks. Apart from assessing the risk of each of the identified threats happening, it also guides on how well the organization can defend against them.
- Determine the needed controls by Identifying what security measures must be implemented or improved to minimize risks.
- Helps the organization in ensuring compliance with the applicable laws and regulations related to the IT infrastructure and requirement of the company.
- Hence, it will be apt to state that periodic security audit is directly proportionate to the growth of the organization.
- A cybersecurity audit involves a comprehensive analysis and review of your IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices.
- Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security posture. They aim to identify vulnerabilities, risks, and threats that may affect the organization.
- Beyond these, a cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation.)

1. Write a brief note on process of Online Reporting of Cyber Crimes in India.
2. Write a short note on the steps on conducting investigations of cyber-crimes.
3. Discuss 5 latest initiatives of Government of India in strengthening the mechanism to control cyber crime.

4. What is Computer Forensics? Mention the significance of Computer Forensics in Cyber Crime.
5. What do you mean Digital Forensics? Describe the branches of Digital Forensics.
6. Write short note on any of the following:
    - Security Audit
    - Advantages of Security Audit
    - Types of Security Audit
    - Investigation vide Computer Forensics.
6. What are the components of Checklist of Cyber Security Audit? Describe

LIST OF FURTHER READINGS

- Banoth Rajkumar et al (2023) A Comprehensive Guide to Information Security Management and Audit, ISBN 9781032344430 Published September 30, 2022 by CRC Press
- Important Cyber Law Case Studies, Cyber Laws and Information Security Advisors. Available at https://www.cyberralegalservices.com/detail-casestudies.php
- Katz Eric, Cyber Forensics: The Fascinating World of Digital Evidences, Purdue Cyber Forensic Labs
- Graeme Edwards (2020) Cybercrime Investigators Handbook, (Audio Book), Audible by Amazon
- Nelson, Phillips and Steuart (2019) Guide to Computer Forensics and Investigations 6TH edition, CENGAGE INDIA
- Sharma Nishesh (2017) Cyber Forensics in India: A Legal Perspective, Universal Law Publishing, India.

LIST OF OTHER REFERENCES

- Buckbee Michael (2020) What is an IT Security Audit? The Basics, Varonis
- Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte
- Effective Governance Risk Management, ISACA Journal. ISACA. Retrieved 2022-04-21
- Information Systems Security Audit, ISACA Journal. ISACA. Retrieved 2022-04-21
- Irwin Luke (2022) What is a Cyber Security and Why is it Important? IT Governance Blog
- Legislative Audit Division - State of Montana (2006, June). “Data Center Review” Helena, MT
- Privacy Technical Assistance Center, “Responding to IT Security Audits: Improving Data Security Practices”. PDF
- Varghese Jinson (2023) IT Security Audit: Importance, Types and Methodology, Astra.