Cyber Forensics

Lesson 14

KEY CONCEPTS

■ Crime ■ Cyber Crime ■ Data Attack ■ Masquerading ■ Spear Phishing ■ Whaling ■ Vishing ■ Spamming ■ Smishing ■ Salami Attack ■ Web Jacking ■ Digital Forensics ■ Data Extraction ■ Ethical Hacking

Learning Objectives

To understand:

- The concept of cybercrime
- The classification of cybercrime
- Types of cybercrime such as Email spoofing, Hacking, Data Diddling etc.
- International guidance to cyber forensic laws
- The concept of digital forensics cyber laws
- What is Data Extraction
- The Concept of digital forensics and cyber crime
- What is Ethical Hacking?
- What is Digital Incident Response and the steps involved in it?

Lesson Outline

- Background to Cybercrime
- Meaning of Cyber Crime
- Types of Cyber Crime
- International Guidance to Cyber Forensics Laws
- Digital Forensics and Cyber Laws
- Data Extraction
- Digital Forensics and Cyber Crime
- Ethical Hacking
- Digital incidence response
- Case laws: Indian and International
- Lesson Round-Up
- Test Yourself
- List of Further Readings

BACKGROUND TO CYBERCRIME

It is a matter of pride that India has the second largest internet connection in the world. While having greater connectivity promises large-scale progress, it also leaves the citizens of our country exposed to new online vulnerabilities.

Cybercrime refers to criminal activities that are carried out using the internet or other forms of digital communication technology. Cybercriminals use these technologies to commit a wide range of criminal activities, including hacking, identity theft, phishing, cyber bullying, and online scams.

The development of digital technologies has led to the growth of the internet, social media, and other digital platforms that have become essential components of modern life. Criminals have found new ways to exploit vulnerabilities in these technologies.

The rise of the internet and digital communication technologies has led to a corresponding increase in cybercrime, which has become a major concern for Governments, Businesses, Corporates and Individuals around the world. They may target individuals, businesses, or even Governments to gain access to sensitive information, financial data, or intellectual property.

The consequences of cybercrime can be severe and wide-ranging. Victims may suffer financial losses, damage to their reputation, or even physical harm. Governments and businesses may also be affected, with cyber-attacks leading to the loss of confidential information, disruption of critical services, and other serious consequences.

The proliferation of digital technologies has created new opportunities for criminals to carry out their activities. For example, hackers can use the internet to gain unauthorized access to computer systems and steal sensitive information.

Phishing scams can be used to trick people into providing personal or financial information, while online scams can be used to defraud people of their money. Cyberbullying is also a growing problem, with individuals using digital technologies to harass, intimidate, or threaten others.

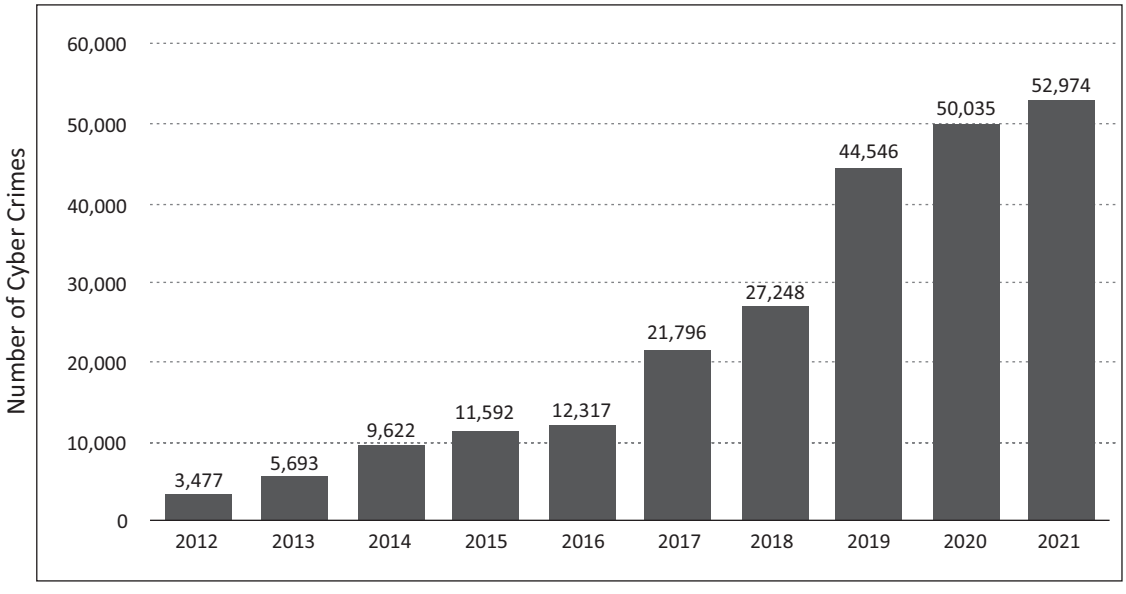
The rapid growth of the internet and digital communication technologies has also made it difficult to track and prosecute cybercriminals. Many cybercriminals operate across national borders, making it difficult for law enforcement agencies to coordinate and investigate crimes. Additionally, the nature of digital communication technologies makes it easy for cybercriminals to conceal their identities and location, further complicating law enforcement efforts.

As a result, there is a growing need for greater collaboration and cooperation between Governments, law enforcement agencies, and the private sector to combat cybercrime.

This includes the development of new technologies and strategies for preventing and detecting and responding to cybercrime by Governments and organisations, as well as increased investment in law enforcement and intelligence capabilities. It also involves greater public awareness and education about the risks and dangers of cybercrime.

These can include cybersecurity protocols, data protection laws, and the establishment of specialized law enforcement agencies. Preventive steps that individuals and organizations can take to protect themselves from cyber threats. However, the constantly evolving nature of cybercrime means that these measures must continually be updated and improved to stay ahead of the latest threats.

Number of cybercrimes reported across India from 2012 to 2021



https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

India saw a significant jump in cybercrimes reported in 2021 from the previous year possibly due to Covid pandemic forcing most of the citizens to transact online. That year, over 52 thousand cybercrime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. A majority of these cases were registered under the Information Technology Act, 2000 with the motive to defraud, or sexually exploit victims.

Roles and Responsibilities of the Board of Directors and Company Secretaries

Covid -19 pandemic has forced most of the entities across the world to innovate by initiating work from home and shifting to digital space to ensure business continuity. This has created an opportunity for online fraudsters and cybercriminals to exploit the vulnerability in networks as employees work from home. Today, a company's board of directors has a role in promoting overall organisational cyber health.

Key roles and responsibilities of the Board of Directors include: Cybersecurity Risk Oversight, Allocating sufficient manpower and financial resources, Proritising the material cyber risks, formulating risk mitigation plans. Board members have to take responsibility for the breaches and failures of the company's cyber security systems.

The Company Secretary is responsible for supporting the board and the Governance process, providing advice and guidance to the board on Information Technology Act and the appropriate regulations, company's own cyber security policies and ensuring best practice in Cybersecurity risk oversight.

MEANING OF CYBERCRIME

What is Crime?

Crime is defined as "an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law that makes the offender liable to punishment by that law" (Webster Dictionary).

What is Cybercrime?

Cybercrime as per European Commission 2007 has been defined as "criminals acts committed using electronic communications networks and information systems or against such network or systems".

Cybercrime is "a crime of any illegal activity committed either on or with a computer and the internet to steal personal identity, gaining unauthorised access to computer systems, sell contraband online or stalk victims online or disrupt operations with malevolent programs".

Through the medium of internet fraudsters' gain valuable sensitive information of companies, firms, individuals, banks and so forth. It can also lead to intellectual property crimes like stealing new product launch plans, new product description and marketing plans, list of potential customers, selling illegal articles, pornography/child pornography etc.

It is done using methods such as Phishing, Spoofing, Spamming, Pharming and so forth. Phishing refers to "an attack using mail programs to deceive internet users into disclosing confidential information that can be then exploited for illegal purposes".

Cybercrimes lead to financial loss, reputational loss, legal consequences, sabotage and theft of IPR. Human being is the weakest link and hence any negligence of human beings enables criminals to commit cybercrimes. Cybercrimes are now committed using mobile phones, tablets, Personal Digital Assistants (PDA) which has connectivity to internet.

Cybercrimes can cross borders in fractions of a second and impact several people in different countries at the same time. Melissa virus triggered havoc across the countries.

Melissa virus- On March 26, 2009, Microsoft Word 97 and Microsoft Word 2000 propagated virus via e-mail attachments. Its widespread attack affected a variety of sites throughout the internet. In Melissa attack, the email attachment is a .DOT Word document that contained a piece of malicious micro code. If an infected document in Word 97 or Word 2000 is opened, the embedded micro code will infect the Normal.dot template and cause any documents referencing this template to be infected with this macro virus.

Melissa virus is not the only virus that propagates itself through email attachments. Other viruses such as I Love You Virus (year 2000) and My Doom (year 2004) also propagates itself through email attachments.

Traditional white collar crime and Cybercrime

Traditional white collar crimes include Bribery, Corruption, Embezzlement or theft Forgery, Money laundering, Financial statements fraud, Identity theft, Procurement and contract fraud, Siphoning of funds and so on.

In both crimes there is no bloodshed and are perpetrated against individuals, society, organisations and the governments. The main difference lies in the modus operandi since in the case of cybercrime physical presence at the venue of the crime is not required.

In both the crimes fraud trail is left as an evidence which can be only detected by trained forensic experts. Let us understand how a computer can be a target and also used as a tool for committing cybercrime.

Computer as a Target

The computer system/ information stored on the computer are the target of the crime. Hackers broke into the system of Citibank in USA on June 9th 2011 and accessed the data of its customers, gained access to the online banking platform and viewed customer account numbers, contact information.

There are other cybercrimes using computer as a target like virus/worm attacks, Distributed Denial of Service (DDoS), Pornography etc.

Computer as a tool

The computer system/ or information stored on the computer system constitutes an important tool for committing the crime. Computer fraud, forgery like counterfeit currency notes, mark sheets, stamp papers, degree certificates can be done using sophisticated computers, printers and scanners , distribution of child pornography etc.

Motive and Reasons for Cybercrimes

Greed, Power hunger, Publicity, Revenge, Adventure or thrill seeking, Destructive mindset, Desire to access forbidden information have been observed as the motive and reasons for all Cybercrimes in the world.

Classification of Cybercrimes

Against Individuals – E-mail spoofing and other online frauds, Phishing, Spear Phishing, Vishing, Smishing, Spamming, Cyber defamation, Cyberstalking, Computer sabotage, Password sniffing, Pornographic offences and transmitting virus. These crimes are directed against individuals for various reasons ranging from greed to personal dispute.

Against Organisation- Hacking, Password sniffing, Denial of Service attack under section 43 of Information Technology Act,2000, E-mail bombing, Salami Attack/ Salami technique, Trojan Horse, Data Diddling, Industrial espionage, Software privacy, Cyber terrorism by rogue actors against any organisation.

Against Society and Governments- Hacking, Forgery (printing of counterfeit currency, forging passports, sale of illegal articles, online gambling, fake Stamp papers (Telgi scam) Cyberterrorism, Webjacking are directed against the society at large.

Against Property – Intellectual property, Credit card frauds, Internet time theft. Property refers also to software, computer source codes. These types of crimes are generally targeted against the society.

Accordance to the Information Technology Act, 2000 a Cyber Crime can be defined as "an act or omission that is punishable under the Information Technology Act, 2000". This however is not an exhaustive definition as the Indian Penal Code also covers certain cyber-crimes, such as email spoofing and cyber defamation, sending threatening emails, etc.

Cyber offences under the Act are tabulated below:

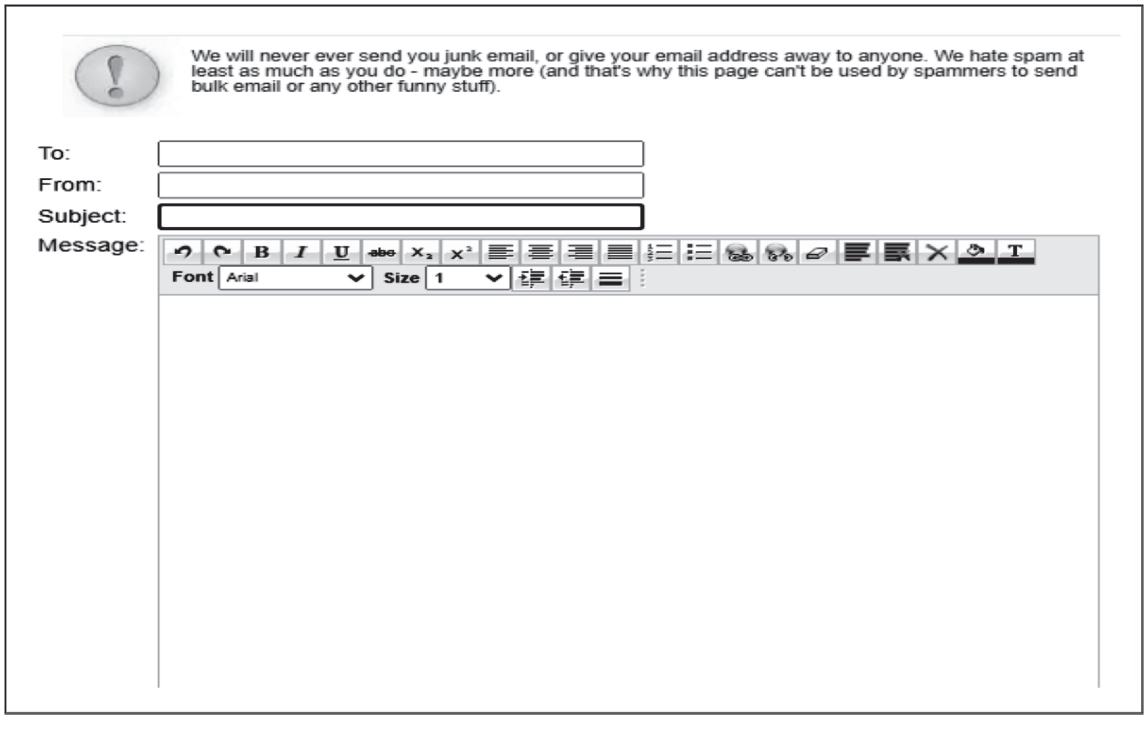
Section	*Offence*	*Description*
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.
66	Hacking with computer system	If a person 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 it injuriously by any means, commits hack.
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.

Section	Offence	Description
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.
70	Securing access or attempting to secure access to a prote	The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.

TYPES OF CYBER CRIME

E-mail spoofing/ Phishing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. Free website are available to send fake emails. Anyone can fill any email address with the intention of deceiving the recipient of the email. When gullible receiver reads the mail/ he or she would think that the e-mail has been sent by legitimate sender based on the IP address indicating that the message has come from a trusted host. Phishing is an alternative of fishing, means to fish for information.



Source: http://deadfake.com/Send.aspx

The term Phishing was used in 1994-95 by hackers who were stealing American Online internet accounts by scamming passwords without the knowledge of AOL users (netizens). It is also an example of social engineering techniques used to deceive netizens. This was done using www.ao1.com instead of www.aol.com

Phishing is done to steal valuable personal and financial data like credit card details, passwords, PIN, social security numbers and bank account numbers by luring the victim to provide the account details and other personal information unwittingly.

E-mail spoofing is dealt under sections 416,417, 419, 463, 465 of Indian Penal Code.

Denial of Services/ Distributed Denial of Services

It is an attack to make a computer or network resource unavailable for the users either temporarily or permanently. DoS attackers target sites or services hosted by banks, airlines, hotel, credit card payment gateways etc. Cybercriminals prevent an internet site form functioning temporarily or even permanently.

Another Bot is a *spambot*, which gathers valid email addresses, so mailing lists can be created to send SPAM. Bots are particularly dangerous when they're deployed to large collections of computers, called *botnets*. Once a computer is infected, the bot can lay dormant until an attacker chooses to activate them. At this point, the

attacker has control of targeted computer (now called a *zombie*) and all the other computers in the botnet (also called a *zombie army*). The attacker can send a signal to have these computers distribute viruses, or send messages to a particular server in a coordinated attack called a *Distributed Denial of Service* attack.

It results in enormous financial and reputation loss as a result of such denial of service attack. It also leads to significant loss of time and money for the victim organisation as they have to rebuild from scratch.

There have been a number of instances of DoS attacks against India.

Distributed denial-of-service (DDoS) attacks are growing significantly across the world, and India ranks second as the largest source of Hypertext Transfer Protocol or HTTP-based DDoS attack traffic in July-September this year after China. China replaced the US as the main source of HTTP DDoS attack traffic in Q3.

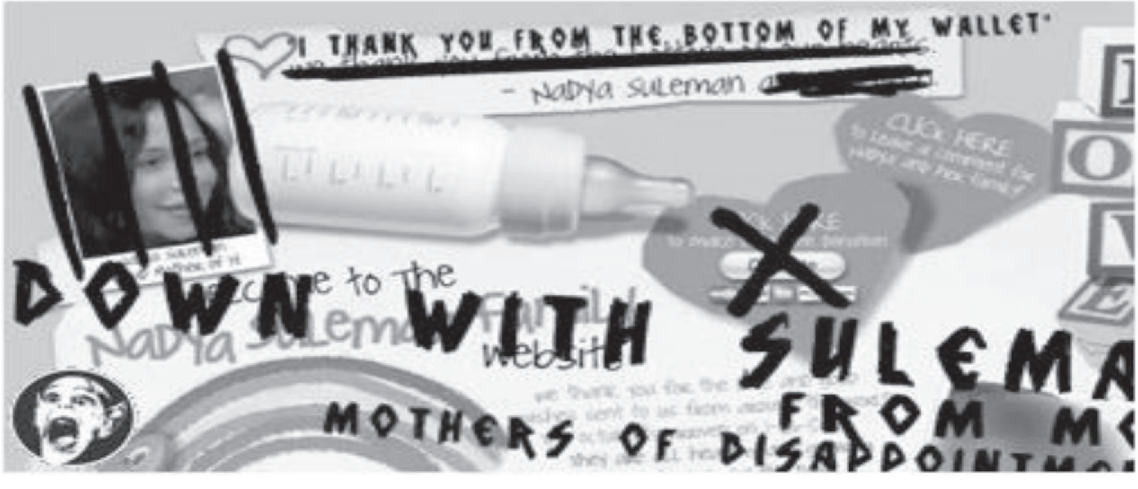
Hacking

It was at Massachusetts Institute of Technology the word "Hack" was used in the late 1950's. In the 1960's the term seems to have migrated from the MIT to computer enthusiasts and in time, it has become an essential part of their lexicon. The meaning of hacking at that time was "fussing with machines".

Major reasons for hacking has been identified as: Greed, publicity, revenge, adventure and destructive mindset, strong desire to access forbidden and highly confidential information. Hackers write or use ready-made computer programs to attack the target computer and get enjoyment out of destruction. They exhort money from corporates threatening them that they will publish their stolen information. Government websites are always on hacker's target and attacks on the Government websites get wide publicity.

Every act committed towards breaking into computer and/or network is hacking and Hacking with intent or knowledge is an offence under section 66 of Information Technology Act, 2000 with a Fine of Rs.2 Lakhs and imprisonment for 3 years.

Real world examples of hacking

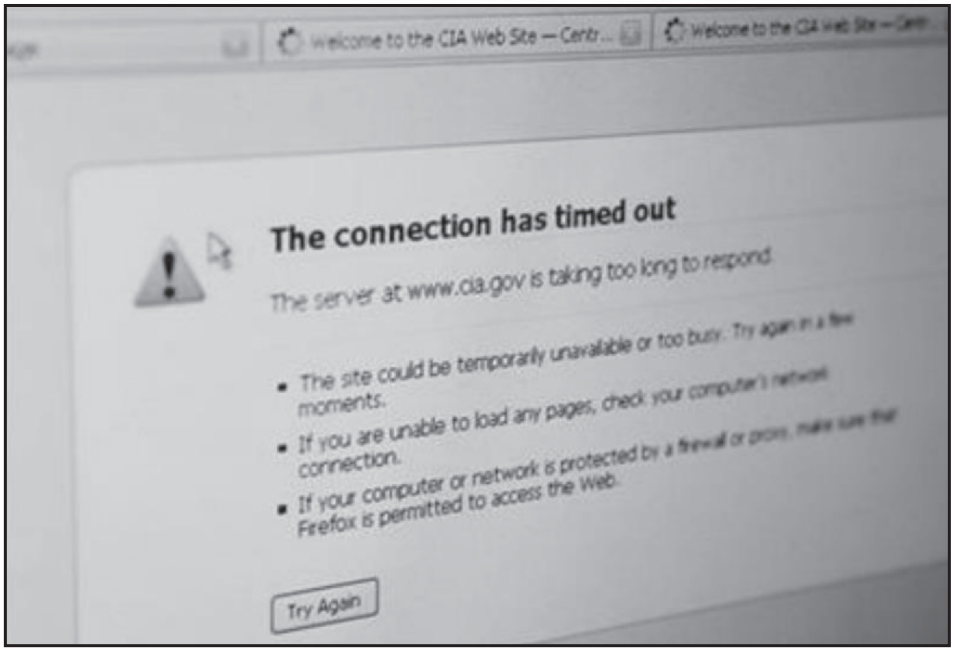


Nadya Suleman –Octomom's defaced website

Source: https://weeklyworldnews.com/headlines/6233/nadya-sulemans-website-hacked/

The public website of the Central Intelligence Agency went down on 15th June 2011 evening as the hacker group Lulz Security said it had launched an attack.

Source: https://www.reuters.com/article/us-cia-hackers-idUKTRE75E6JC20110616



The website of the U.S. Central Intelligence Agency (CIA) is unresponsive and unavailable after reports that the website had been attacked by internet hackers in Washington June 15, 2011. The Lulz Security group of hackers said in a Tweet that it had launched an attack on the public website of the U.S. Central Intelligence Agency. The site, www.cia.gov, was unavailable for a few minutes on evening, immediately after the group announced the attack via Twitter.

Data Attacks

According to 2022 Verizon Data Breach Investigation Report (DBIR) 5,212 breaches were analysed, 23,896 security incidents were reviewed. 82% breach involved the human element including social attacks, errors and misuse, 13% increase in Ransomware breaches which is more than in the last 5 years combined and 62% of incidents in the system intrusion pattern involved threat actors compromising partners. Over 50% of breaches involved use of either remote access or web applications. About 66% of breaches involved Phishing, stolen credentials and/or Ransomware.

The four key paths to data breaches are: Credentials, Phishing, Exploiting vulnerabilities and Botnets. No organisation is safe without a way to handle them.

Source: Verizon Data Breach Investigation Report, 2022

Data Diddling

It is one of the oldest form of computer crimes since the advent of electronic data processing. Data Diddling is changing of data either before or during entry into the computer system. Examples include forging or counterfeiting documents used for any data entry and replacing valid disks and tapes with tampered or modified disks and tapes. One of the earliest data diddling fraud was Equity Funding Corporation of America.

The NDMC Electricity Billing Fraud took place in 1996.The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and payment in the bank were exclusively left to a private contractor who was a computer professional.

He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

Section 66 [i] and 43(d) [ii] of the Information Technology Act, 2000 covers the offence of Data Diddling.

Masquerading

When a perpetrator pretends to be someone he is actually not by creating fake email ids, or uses someone else's user ID and password.

How is it done?

Cybercriminals browse the Facebook profiles and identify those posting profile pictures in police uniform and download profile picture and other photos. They also download the contact names of friends. They create fake account in the same name by using the downloaded photos from original social media account. They then send friend request to contact list and asks for money later. Fraudsters want money to be transferred to them through Google Pay, Paytm, PhonePe etc.

A fake Facebook account was created in the name of Raman (name changed), a sub-inspector of a rural police station, and messages were sent from it to his multiple Facebook friends, requesting money. One of the friends, without crosschecking, sent Rs 7,000 to the account mentioned in the message. There are many such instances of impersonating police officers across India for financial gain.

Spear Phishing

Any highly targeted e-mail attack that a scammer sends only to people within a small group. E-mail sent by the scammer appears genuine to all employees or members within the company or a Government department. Phishing scams are designed to steal information from individuals, Spear Phishing aims to gain access to an organisation's entire computer system. E-mail message might appear to be genuine, but if the recipient responds to it, he or she might put himself or herself and the employer at huge risk.

In Spear Phishing, targets are carefully chosen, and emails are carefully crafted with the specific target in mind. Few examples are given below:

---------- Forwarded Message: ----------
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000

citi

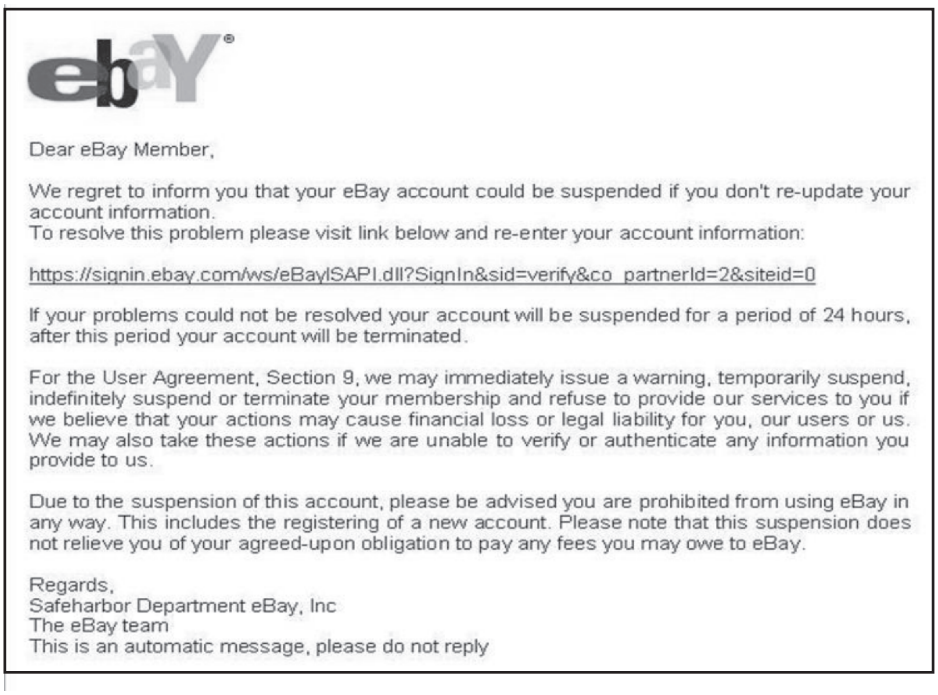
This is a Security Alert you requested to help you protect your account.

Your account has been blocked.
219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please your account

Thank you for your cooperation.

Sincerely Yours,
Letha Cox
Letha.Cox@citibank.com



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

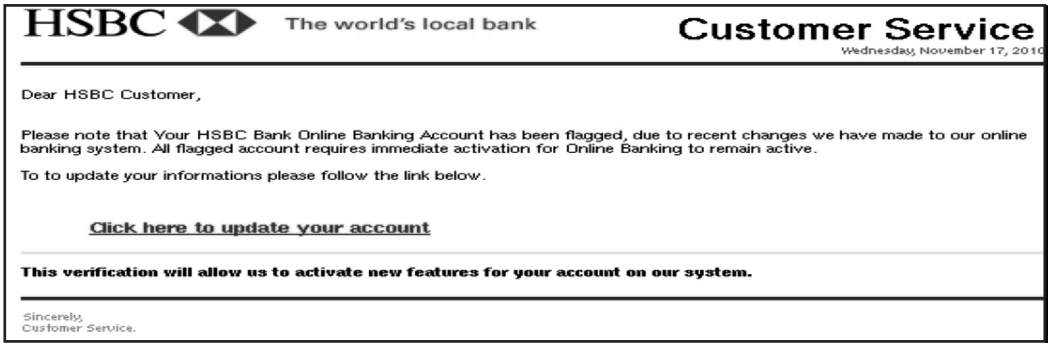
Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Whaling

This form of Spear Phishing targets top management C- Suites executives with the help of information obtained through Spear Phishing by installing malware for keylogging or other backdoor access mechanisms. E-mail is sent in the Whaling scam showing a sense of falsified urgency to transfer funds urgently and is meant to be tailored for executives as per example below:

Vishing

The term is a combination of V-voice and Phishing and is usually used to steal credit card numbers or related data used in ID theft from individuals. Using a spoofed phone number and caller ID, the cybercriminal pretends to be calling on behalf of the victim's bank. The caller says that there has been unusual activity on the victim's account and asks the victim to confirm their bank account details, including their mailing address, for updating proof of identification (KYC) by sending a link. This information is then used by the cybercriminal to commit online banking fraud.


HSBC The world's local bank

Customer Service

Wednesday, November 17, 2010

Dear HSBC Customer,

Please note that Your HSBC Bank Online Banking Account has been flagged, due to recent changes we have made to our online banking system. All flagged account requires immediate activation for Online Banking to remain active.

To to update your informations please follow the link below.

Click here to update your account

This verification will allow us to activate new features for your account on our system.

Sincerely,
Customer Service.

Many examples are: Scammers offering to help the account holders with bank KYC updating by asking them to download an app and also by sharing the OTP. They also ask the victim to share the debit card details and OTP by claiming that the call is from the Bank.

Spamming

Spam is abuse of electronic message systems by sending unsolicited bulk messages indiscriminately. Spamming is difficult to control since it is difficult to hold senders accountable for their mass mailings.

Botnet Email spam– though email is seen today as an older path for attack, spam botnets are some of the largest in size. They are primarily used for sending out spam messages, often including malware, in towering numbers from each bot. The Cutwail botnet founded in 2007, can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.

Smishing

The term is derived from SMS + PHISHING. The pretender hides the purpose and/or identity to get the personal information/ sensitive data about another individual. The criminal impersonates a legitimate entity such as an IT service/security admin, a bank, a government agency, an e-commerce site, a package delivery service, etc.

Cyber-defamation

It occurs when defamation takes place with the help of computers and internet. If someone publishes a defamatory matter about someone on a website or posts any defamatory message on any digital media.

India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

Section 499 of Chapter XXI of the Indian Penal Code defines Defamation:

Whoever by words either spoken or intended to be read or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm or knowing or having reason to believe that such imputation will harm the reputation of such person is said except in the case hereinafter expected to defame the person.

Cyber-stalking

It is the use of internet and/ electronic communication devices by an individual or groups of individuals to harass another individual or groups of individuals or an organisation by false accusations, monitoring, transmission of threats, damage to data or equipment and gathering information for harassment. Online stalkers aim to start the interaction with the targeted victim directly through internet. Email and Chatrooms are the most common form of medium used to connect with the victim.

Police (Delhi) arrest a man for cyberstalking woman: A 32-year-old man created a fake social media profile with obscene descriptions and photos of a woman and sent her obscene messages and photos after she ignored his messages on social media. A case was subsequently registered under Sections 67/67A (punishment for electronically transmitting obscenity in electronic form/sexual act in electronic form) of the Information Technology Act.

Computer sabotage/ vandalism

The use of internet to obstruct the normal functioning of a computer system or networks through worms, viruses or logic bomb. Cyber vandalism is a program which performs malicious function such as extracting users' password or other confidential data or even erasing hard disk.

Password sniffers & Key logger

Password sniffers are programs that monitor and record the user id and passwords. A key logger is a type of spyware that monitors and records user keystrokes including the ability to record mouse clicks. They allow cybercriminals to read anything a victim is typing into their keyboard, including private data like passwords, account numbers, and credit card numbers. They can be installed manually or automatically without user's knowledge, such as by inserting a flash drive into a USB slot or through a rootkit.

Transmitting virus

Computer virus is a software program that can infect legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves without the knowledge or permission of the users to potentially large numbers of programs on many machines.

- **Virus can be transmitted through the internet**

  Virus is intentionally uploaded on internet server or distributed through email. The internet server and hard disk gets infected with the virus. The virus then gets downloaded onto unsuspecting user if there are no anti-virus tool kit or outdated anti-virus tool kit is in the victim's computer.

- **Virus transmits through Stand-alone computer system**

  When Virus infected pen drive or disk is loaded to the stand alone computer either intentionally or unintentionally and hard disk gets infected.

- **Virus can be transmitted through local network**

  Virus is inserted in a legitimate program code and transmitted via data communication links to another node on the network. Virus then spreads itself to another nodes on the network.

Salami Attack

To commit a financial crime, an alteration is made so insignificant that it would go unnoticed. For example, if a bank employee inserts a program onto the bank server to deduct small amount of money make an unauthorised debit to bank account holders account and credit it to his fictitious bank account, he will be siphoning off a sizeable amount every month.

Theft of computer system and Internet time theft

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer. Internet time theft occurs when an unauthorised person uses the internet hours paid for by subscriber by hacking or gaining access by illegal means without the knowledge of the subscriber.

Intellectual Property Theft

Intellectual property rights means the ownership rights in intangible assets like software, source code, trade secrets, copyrights, and trade-marks. When the rights of an owner of an intellectual property right is deprived off either wholly or partially, it is called as intellectual property theft. There are many instances of piracy in the digital world since the advent of internet revolution. Online piracy or software piracy is the practice of downloading and distributing copyrighted works digitally without permission, such as music or feature films or software.

The Hyderabad Court in a land mark judgement convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software (Parthasarathy Pati case 16th March 2003).

Web Jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

Online Frauds

Online frauds are fraudulent activities such as an identity theft, financial frauds like online games or lotteries, free vacation.

Online job frauds

It involves misleading people who require a job by promising them a better job with higher pay while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

- **SIM swapping or SIM jacking**

  It is a fraudulent way of gaining access to someone's mobile number. It happens when a criminal convinces cellular provider to transfer victim's phone number to a different SIM (Subscriber Identity Module) card, usually one in their possession. If they succeed, victim will automatically at a disadvantage.

- **Cryptocurrency frauds**

  Cryptocurrency, such as bitcoin, is different from digital currency. It uses blockchain for verification and does not run through financial institutions, so it is harder to recover from theft.

- **Fake cryptocurrency exchanges**

  Scammers may lure investors in with promises of a great cryptocurrency exchange. But in reality, there is no exchange and the investor does not know it is fake until after they lose their deposit.

- **Ponzi schemes**

  To get fresh cryptocurrency investors, cryptocurrency scammers will lure new investors with bitcoin.

- **Bitcoin investment schemes**

  As part of the scheme, the so-called investment managers claim to have made millions investing in cryptocurrency and promise their victims that they will make money with investments. To get started, the scammers request an upfront fee. Then, instead of making money, the thieves simply steal the upfront fees. The scammers may also request personal identification information, claiming it's for transferring or depositing funds, and thus gain access to a person's cryptocurrency.

Conclusion

A broad overview about cybercrime and its various types have been explained in the above paragraphs. Various types of cybercrimes existing and new types of cybercrimes are happening every second in India and other parts of the globe. As a Corporate Governance Professionals we should be aware of the latest cyber scams and cyber frauds that are happening and necessary internal controls should be designed to protect the organisation and individuals from falling victim to it. As the technology is growing at mind-blowing pace post pandemic, many more new types of cybercrimes will emerge since fraudsters are always ahead in the conning game.

INTERNATIONAL GUIDANCE TO CYBER FORENSICS LAWS

Cyber forensic laws vary widely by country, and there is no one-size-fits-all approach to international guidance on this topic. However, there are a number of international agreements, conventions, and guidelines that countries can use as a basis for their own cyber forensic laws. Few of the conventions are given below.

Council of Europe Convention on Cybercrime:

As per Council of Europe Convention, Cybercrime are offences against and by means of computer systems. It has evolved into a significant threat to human rights, democracy and the rule of law as well as to international peace and stability, and it has major social and economic impact. In addition, any crime may involve evidence on a computer system needed in criminal investigations and proceedings.

Convention on Cybercrime (also known as the Budapest Convention)

The Budapest Convention 2001 is a criminal justice treaty that provides States with

i. the criminalisation of a list of attacks against and by means of computers;

ii. procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and

iii. International police and judicial cooperation on cybercrime and e-evidence.

The Budapest Convention provides a framework for countries to establish laws and procedures for investigating and prosecuting cybercrime and in international cooperation in investigating and prosecuting cybercrime

UN Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP), have jointly drafted and launched the *Practical Guide for Requesting Electronic Evidence Across Borders*.

Both, the 2018 and 2021 editions of the Practical Guide can be accessed by registered users of the CNA Directory. Access to the CNA Directory is reserved to central and competent national authorities and Permanent Missions to the United Nations.

DIGITAL FORENSICS AND CYBER LAWS

Digital forensics and cyber laws are two closely related fields that deal with investigating and prosecuting cybercrime.

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Cyber laws, on the other hand, are a set of regulations that govern online activities, including the use of the internet, computers, and other electronic devices. These laws are designed to protect individuals, businesses, and Governments from cybercrime and other illegal activities. Cyber laws cover a wide range of topics, including data privacy, intellectual property, and online harassment. In India, Information Technology Act, 2000, Indian Penal Code are the major legislations covering Cyberlaws.

Meaning of Digital Forensics as per International Criminal Police Organization (Interpol)

Digital forensics is “a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically”.

Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations. Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.

The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

DATA EXTRACTION

Data extraction is the process of collecting or retrieving dissimilar types of data from a variety of sources such as websites, databases and documents many of which may be poorly organised or completely unstructured.

With the help of Data extraction it is possible to clean, consolidate, process, and refine the data so that it can be stored in a centralised location in order to be transformed. These storage locations may be either on-site, cloud-based, or a hybrid of the two. Data extraction is the first step in both Extract, Transform, Load (ETL) and Extract, Load, Transform processes (ELT).

Data is extracted from a variety of sources and/or systems. The extraction locates and identifies relevant data and prepares it for processing or for transformation. Extraction allows many different types of data to be combined and finally mined for business intelligence or fraud detection.

Once the data has been successfully extracted it is now ready to be refined. In the transformation phase, data is sorted, organised, and cleaned. Duplicate entries will be deleted, missing values will be removed and audit will be performed to ensure that data is reliable, consistent, and usable. The transformed high quality data is then delivered to the target location for storage and analysis.

The ETL process is used by companies and organizations in every industry for many purposes. For instance, Healthcare companies need to extract many types of data from a range of local and cloud- based sources to streamline processes and support compliance efforts. Data extraction makes it possible to consolidate and integrate data related to patient care, healthcare providers, and insurance companies.

Similarly, retailers may able to collect customer information through mobile apps, websites, and in-store transactions. But without a way to migrate and merge all data, its potential may be limited. To solve this, data extraction is a solution.

Many companies and organisations take advantage of data extraction tools to manage the extraction process from end-to-end. Using an ETL tool automates and simplifies the extraction process thereby precious resources can be deployed toward other priorities.

The first step in data extraction is to identify the kinds of data required for analysis. Different types of data that are extracted by any entity may include Customer Data to help businesses and organisations in understanding their customers. It can include their names, contact details, purchase histories, social media activity, and web searches etc.

Financial Data Metrics include revenue, purchase cost, operating margins, and competitor's prices. This type of data helps companies to track its performance, improve efficiencies, and for doing strategic plan.

Task or process performance data: It includes information pertaining to specific tasks or operations. A retail company may seek information on its shipping logistics, or a Health care provider may want to monitor post-surgical results or patient feedback.

Once an organisation decides on the type of information it wants to access and analyse, the next steps are

1) Finding out where it can be got; and
2) Deciding where it wants to store it.

In most cases, it means moving data from one application, program, or server into another. Migration might involve data from services such as SAP, Amazon Web Services, MySQL, SQL Server, JSON, SalesForce etc. These are few widely used applications. However, data from any program, application, or server can be migrated.

To make things easy, one may use following data extraction tools for professionals as well as beginners –

OutWitHub

OutWithub is one of the most popular web scraping tools available in the market. It usually segregates the web pages into different elements and then navigates from page to page to extract the relevant data from the website. This tool has an extension for Mozilla Firefox and Chrome which makes it easy to access and is mainly used to extract links, email ids, data tables, images, etc.

Web Scraper

This is a very simple and easy-to-use web scraping tool available in the industry. It has the unique ability to login to external pages and is mainly used by companies for document extraction, web data scraping, email id extraction, pricing extraction, contact detail extraction, image extraction, etc.

Spinn3r

This is a web service which is used to index the blogs around the world. It provides access to every blog that is published in real-time and is mainly used by organizations to get information from social media, forums, web blogs, reviews, comments, mainstream news monitoring, etc.

Fminer

This is another popular tool used by companies which mainly acts as a visual web scraping tool, web data extractor, and a macro recorder. It is mainly used for disparate web scraping, email id extraction, phone number extraction, image extraction, document extraction, etc.

ParseHub

This is one of the most well-known visual extraction tools in the market which can be used by anyone to extract data from the web. The tool is mainly used to extract images, email ids, documents, web data, contact info, phone numbers, pricing details, etc.

Octaparse

This is one of the most powerful web scraping tools which can grab all the open data from any website and also save the user the effort of copy-pasting the information or any kind of further coding. This is mainly used to extract IP addresses, disparate data, email addresses, phone numbers, web data, etc.

Table Capture

This tool is an extension to the Chrome browser which helps to capture the data from the website while navigating through the web pages without any hassles. It easily scrapes the data from an HTML table of any website copies it to a clip board and converts it into any of the data formats such as Google spreadsheets, CSV, or Excel.

Scrapy

This is an open source code development framework which performs data extraction with Python. This tool allows developers to program crawlers to extract and track information for one or many websites at once.

Tabula

This is a desktop application for Mac OSX, Windows, and Linux, which helps companies and individuals to convert PDF files into an Excel or CSV file which can be easily edited. This is one of the most used extraction tools in data journalism.

Dexi.io

This web scraping tool doesn't need any kind of download and is a browser-based tool. This tool allows you to set up crawlers and fetch web data in real-time and also allows you to save the gathered information directly in the Google Drive or export it through CSV or JSON. One unique feature of this tool is that the data can be extracted anonymously using different proxy servers.

Impact of Cloud computing and IoT on Data Extraction

The advent of cloud computing has now a major impact in the manner companies and organisations manage and store their data. In addition to changes in data security, storage, and processing, the cloud computing has made now the ETL process more efficient and adaptable. Companies are able to access data from anywhere in the globe and process it in real-time, without having to maintain their own servers or investing in data infrastructure. Through the use of hybrid and cloud-based data options, more companies are beginning to move data away from legacy on-site systems.

Internet of Things (IoT) is also transforming the data landscape. In addition to mobile phones, tablets, and computers, data is now being generated by wearables such as FitBit, automobiles, household appliances, and even medical devices. The result is an ever-increasing amount of data can be used to drive a company's competitive edge, once the data has been extracted and transformed.

Practical Case Study

Domino's Pizza – Data Extraction

We all know that Domino's is the largest pizza company in the world. The main reason is its ability to receive orders from its consumers through a wide range of technologies, like smart phones, smart watches and even social media. All these channels generate an enormous amounts of data, which with help of information technology, the company integrates to produce insights into its global operations and customers' preferences.

To consolidate all of these data sources, Domino's uses a data management platform to manage its data from extraction to integration. Running on Domino's own cloud-based servers, this system captures and collects data from point of sales (POS) systems, 26 supply chain centres, and through various channels as different as text messages. Domino's data management platform then cleans, enriches and stores data so that it can be easily accessed and used by multiple teams and the product is delivered to the right customer and at the right time.

DIGITAL FORENSICS AND CYBER CRIME

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Cybercrime is "a crime of any illegal activity committed either on or with a computer and the internet to steal

personal identity, gaining unauthorised access to computer systems, sell contraband online or stalk victims online or disrupt operations with malevolent programs".

Digital Evidence

In order to solve a cybercrime alleged to have been committed appropriate digital evidence have to be identified and collected, analysed and evaluated as to the suitability in the court of law and report have to be prepared by the digital forensic expert and submitted to those who have appointed him.

There are many other storage media and technical devices that may process and store digital evidence. Examples of these devices include media cards (ie. secure digital, SIM card, flash, memory sticks), thumb drives, optical media (ie. CD, DVD, and Blu-ray), digital cameras, MP3 players, iPods, servers, surveillance systems, gaming stations (ie. Xbox, PlayStation, Wii), and GPS devices.

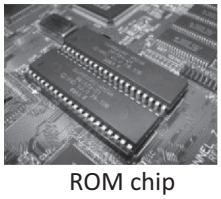
Each of these devices is capable of holding significant amount of data that could help to crack case. And each is handled in a separate way. Seizure of these items should be performed with special care. Always consider working with an experienced digital evidence analyst to collect these items.

Every sequence of events within a single computer might cause interactions with files and file systems in which they reside, other process and the programs they are executing. The files they produce and manage, log files and audit trails of various types. In a networked environment it extends to all networked devices. Evidence of an activity might be contained in a time stamp associated with a different program in a different computer as a digital forensics evidence.

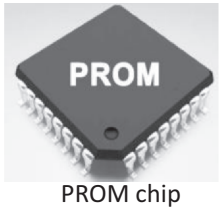
Collecting volatile data requires specific technical skills. If the computer is still on, any intelligence that can be gained by examining the applications currently open is recorded. If information is stored solely in random access memory (RAM), is not recovered before switching down.

Embedded memories inside a computer comprises of

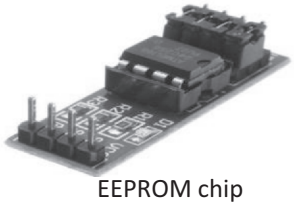
Read Only Memory (ROM) chip, Erasable Programmable Read Only Memory (EPROM) chip, Programmable Read Only Memory chip (PROM) and Electrify Erasable Programmable Read Only Memory (EEPROM) chip.


ROM chip


EPROM chip



PROM chip


EEPROM chip

Precautions to be adopted by Digital Forensics Expert

1. Take image of computer media using a write-blocking tool to ensure there is no data added or modification done to the suspected device. The process of creating an exact duplicate of the original evidentiary media is called imaging. Using hard drive duplicator or software, the entire hard disk drive is completely duplicated. The original disk drive is then securely stored to prevent tampering.

2. Establish and maintain Chain of Custody: Chain of custody means the chronological documentation, trail that indicates the seizure, custody of digital evidence, control, transfer, analysis and disposition of evidence, physical or electronic. Digital evidence by its very nature is invisible to the human eyes and hence evidence must be developed using sophisticated tools.

   The chain of custody requires that from the moment the evidence is collected, every transfer of evidence between persons should be documented to prove that nobody else could have accessed to that evidence. If the chain of custody is broken, the defendant can ask the court to declare the evidence as admissible.

3. Document everything.
4. Use only the tools and methods that have been tested and evaluated to validate the reliability of digital evidence**.**
5. Most valuable information that can be obtained in the course of digital forensic examination will come from interviewing the users, witnesses and the suspects. It can yield valuable information about the system configuration, applications, encryption keys and methodology to access encrypted files and network servers.
6. Without legal authority and unless the owner of the digital evidence has given consent to have the media examined, special care must be taken not to seize, copy and examine the data.
7. Due to the growing use of cryptographic storage, it may be that the only copy of the keys to decrypt the storage is in computer's memory. If the computer is switched off it will cause that information to be lost.

Digital Analysis

A digital investigation may involve many formats of digital data and therefore there are several types of analysis like Media analysis, media management analysis, file system analysis, Networking analysis, image analysis done by digital forensic experts.

Reporting

Once the digital analysis is completed based on the evidence gathered, interviews a report is prepared. After extracting and analysing the evidence the results may need to be presented before law enforcement officials, technical experts, legal experts and corporate management. Depending upon the nature of the incident or crime, it may become mandatory to present the findings in a court of law.

Most forensic reports, follow the general guideline below for a table of contents:

1. Brief summary of information
2. Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
3. Repository #1 (For example A's work computer)
   a. Summary of evidence found on Employee A's work computer
   b. Analysis of relevant portions of Employee A's work computer
      i. Email history
      ii. Internet search history
      Iii. USB registry analysis
      iv. Etc.

c. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)

4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the reports.

Source: https://www.thomsonreuters.com/en-us/posts/legal/understanding-digital-forensics-report/

Testifying

This phase involves presentation and cross-examination of expert witnesses. It depends on the country and legal framework in which cybercrime is registered. Digital forensics evidence is normally introduced by expert witness. Experts have a much specialised knowledge, skill, experience, training or specialised education about specific things of import to the matter on hand. Anyone put up as an expert who has no specialised knowledge can be seriously challenged by competent experts and counsel of the defendants.

There are broadly three types of personnel involved in digital forensics.

Technicians who carry out the technical aspects of gathering evidence as they have sufficient technical skills to gather information from various digital devices, understand software, hardware and network configurations.

Policy makers must establish forensics policies that is up to date and must be familiar with computing and forensics.

Professionals acts as a bridge between the technician and policy makers. They must have extensive technical skill and good understanding of laws.

Mobile Forensics

Mobile forensics, a part of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets is done in mobile forensics. All individuals depend on mobile devices for sending data receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.

A company may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud. Businesses have been known to track employees' personal usage of business devices in order to uncover evidence of illegal activity. Law enforcement, may be able to take advantage of mobile forensics by using electronic discovery to gather evidence.

Botnet Forensics

Botnet forensics determines the scope of the breach and applies the methodology to find out the type of the infection. It is an investigation of the botnet attacks. The prime objective of botnet forensics is to measure the level of intrusions, investigate the intrusions, and provide information on how to recover from an intrusion so as to strengthen system security.

ETHICAL HACKING

Ethical hacking is the practice of using hacking techniques for the purpose of identifying security vulnerabilities in computer systems and networks. The goal of ethical hacking is to improve the security posture of an organization by identifying and mitigating vulnerabilities before they can be exploited by malicious actors.

Ethical hackers, also known as white hat hackers, use the same tools and techniques as malicious hackers, but with the permission of the target organization. They perform penetration testing, vulnerability assessments, and other security testing activities to identify weaknesses in the target system.

Ethical hacking is an important aspect of modern cybersecurity, as it allows organizations to proactively identify and address security weaknesses before they can be exploited by attackers. It also helps organizations meet regulatory requirements and maintain compliance with industry standards.

However, ethical hacking must be conducted in a responsible and ethical manner. Ethical hackers must obtain permission from the target organization before conducting any testing, and must adhere to a strict code of ethics to ensure that their activities do not cause harm or damage to the target system or data.

DIGITAL INCIDENT RESPONSE

What is an Incident?

An incident is defined as the act of violating an explicit or implied security policy. Computer security incident is any adverse event which compromises some aspect of the computer or network security.

Digital Incident Response (IR) is the process of identifying, investigating, and responding to security incidents in computer networks and systems. The goal of digital incident response is to minimize the damage caused by an incident, contain the incident, and prevent future incidents from occurring.

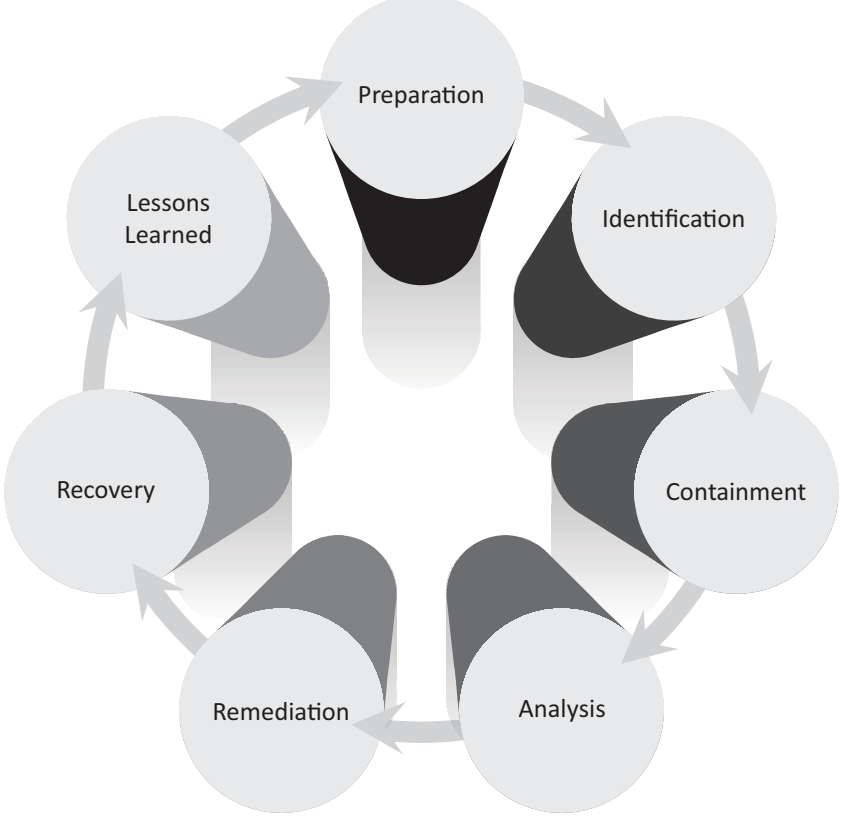
Due to frequent cyberattacks which compromise privacy of business data as well as personal privacy especially post pandemic incident response has become necessary. There have been many real incidents involving installation of malware and asking the victims to pay in cryptocurrency.

Recent case of cyberattack on AIIMS

Five servers of the All India Institute of Medical Sciences (AIIMS) were affected by the recent cyberattack in November 2022 and an estimated 1.3 terabytes of data was encrypted.

Based on the investigation it was found that the hackers had two Proton-mail addresses – "dog2398" and "mouse63209" these two addresses, 'dog2398' and 'mouse63209', were generated in the first week of November in Hong Kong. Another encrypted file was sent from Henan in China.

Digital Incidents Response Steps



The digital incident response process typically involves the following steps:

Preparation: This involves creating a plan for incident response, including identifying key personnel, establishing communication protocols, and developing a list of resources that can be used during an incident.

Identification: This involves detecting an incident by monitoring network activity and analyzing logs for signs of suspicious behavior. Incidents can also be identified through reports from users or other sources.

Containment: This involves isolating the affected systems and limiting the damage caused by the incident. This may involve shutting down systems, disconnecting them from the network, or blocking access to certain resources.

Analysis: This involves investigating the incident to determine the cause, scope, and impact of the incident. This may involve forensic analysis of systems and data to identify the source of the incident and gather evidence.

Remediation: This involves taking steps to address the vulnerabilities or weaknesses that allowed the incident to occur. This may involve patching systems, updating software, or implementing new security controls.

Recovery: This involves restoring systems and data to their normal state and verifying that the incident has been fully resolved.

Lessons learned: This involves reviewing the incident response process and identifying areas for improvement. This may involve updating incident response plans, improving monitoring and detection capabilities, or providing additional training to staff.

Digital incident response is a critical component of modern cybersecurity, as it allows organizations to quickly and effectively respond to security incidents and minimize the impact of a security breach.

CASE LAWS: INDIAN AND INTERNATIONAL

In India, cybercrimes are covered by the Information Technology Act, 2000 ('the Act') and the Indian Penal Code, 1860. It is the Act, deals with issues related to cybercrimes and electronic commerce in India. In the year 2008, the Act was amended and outlined the definition and punishment of cybercrime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

Information Technology Act, 2000 ("the Act")

Object of the Act

It is the first cyber law to be approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Some landmark Cases

1. ***Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank (PNB), HO New Delhi & Others (2018)***

   In 2013, in one of the largest compensation awarded in legal adjudication of a cybercrime dispute, Maharashtra's IT secretary Rajesh Aggarwal had ordered PNB to pay Rs 45 lakh to the Complainant Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. A fraudster had transferred Rs. 80.10 lakh from Matharu's account in PNB, Pune after Matharu responded to a phishing email. Complainant was asked to share the liability since he responded to the phishing mail but the Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the Complainant.

Punjab National Bank has gone on appeal against the above judgement to Telecom Disputes Settlement and Appellate Tribunal.

2. Pune Citibank MphasiS Call Center Fraud

Some ex-employees of BPO arm of MPhasiS Ltd, MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cybercrime cases that raised concerns of many kinds including the role of Data Protection". The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

Information Technology Act, 2000 **("the Act")** *is versatile enough to accommodate the aspects of crime not covered by the Act but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in the Act.*

Under the Act the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs. 1 crore per victim for which the "Adjudication Process" can be invoked.

3. Cyber Attack on Cosmos Bank

In August 2018, the Pune branch of Cosmos bank was drained of Rs. 94 crores, in an extremely bold cyber-attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred. According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out. This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

4. Bomb Hoax Mail

In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

International Case Study

FTX Scam

FTX Trading Limited (FTX) was founded in 2019 by Sam Bankman- Fried (SBF) and Gary Wang is now a bankrupt company having filed on November 11, 2022 Chapter 11 bankruptcy proceedings in the US Bankruptcy Court for the District of Delaware, losing over US$ 8 Billion in client money.

FTX formerly operated cryptocurrency exchange and crypto hedge fund. FTX means Futures Exchange. SBF was arrested on multiple fraud charges in November 2022.

FTX had closed to US$9 billion liabilities compared to just US$900 million in liquid assets comprising in shares in stock-trading App Robinhood.

He is now accused of fraudulent transfer of billions of US dollars of FTX client money to prop up his hedge fund Alameda Research. He deceived investors about the true risks at the company and artificially inflated the price of FTT token to access funding from investors.

How did FTX unravel?

CoinDesk publishes a report that revealed Alameda Research – a sister company to FTX – had a balance sheet full of FTT, the cryptocurrency issued by FTX. Changpeng Zhao, the founder of Binance, said the cryptocurrency exchange would offload all of its remaining FTT tokens "due to recent revelations that have come to light." FTT prices dropped as investors began to withdraw. Binance agrees to acquire FTX. Binance pulls out of its agreement to take over FTX.

Reference

Internet web pages on FTX scandal

LESSON ROUND-UP

- Everyone is getting increasingly dependent on consistent access and accuracy of these communication channels. The internet users have increased significantly especially in the last 15 years. This clearly indicates that the impact of Information Technology is very profound.
- Both Society and the Technology are operating in a way so as to harmonize with the pace of each other's growth. With boon comes the bane and thus the World of ICT is no exception to this rule. Along with abundant opportunities that it has brought about, there are also some challenges.
- Broadly speaking, it has posed certain major concerns like privacy threat, over riding cultural impact, more reliance on technology, boycott of societal engagements, computer virus, malware, spam phishing and many more. One of the major challenges in this era of ICT is of an increasing number of cyber crimes taking place in the World today.
- Cyber-crimes are technology based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. They are organized and white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft, etc.
- Digital forensics, as a developing discipline, presents a number of opportunities for international standardisation.
- Generally when procedures are standardised, the associated costs are lower, training is simplified and consumers accept products and services more readily.
- Cybersecurity professionals understand the value of this information and respect the fact that it can be easily compromised if not properly handled and protected.
- A key component of the investigative process involves the assessment of potential evidence in a cyber-crime. In order to effectively investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases.
- Data extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration).
- An ethical hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit.

TEST YOURSELF

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

Multiple Choice Questions (MCQs)

1. Computer forensics also be used in civil proceedings.
   A. Yes
   B. No
   C. Can be yes or no
   D. Cannot say
2. *Forensic Auditors* are supposed to maintain three types of records. Which answer is not a record?
   A. Chain of custody
   B. Documentation of the crime scene
   C. Searching the crime scene
   D. Document your actions
3. Deleted files is a common technique used in computer forensics is the recovery of deleted files.
   A. TRUE
   B. FALSE
   C. Can be true or false
   D. Cannot say
4. All of the following are main type of computer forensics except:-
   A. Moral Forensics
   B. E-mail Forensics
   C. Malware Forensics
   D. Database Forensics
5. The main goal of computer forensics is:-
   A. Collect & Preserve the Data
   B. Identify the Data
   C. Analyse the Data
   D. All of the above
6. State whether True or False: Data encryption is primarily used to ensure confidentiality.
   A. True
   B. False
   C. Cannot be interpreted
   D. None

7. In which category does the lack of access control policy fall?
    A. Threat
    B. Bug
    C. Attack
    D. Vulnerability
8. Which software is mainly used to help users detect viruses and avoid them?
    A. Antivirus
    B. Adware
    C. Malware
    D. None
9. Identify the malware which does not replicate or clone through an infection?
    A. Trojans
    B. Worms
    C. Rootkits
    D. Virus
10. Choose the features which violate cyber security.
    A. Exploit
    B. Attack
    C. Compliance
    D. None

Answer:

1) A **2)** C **3)** A **4)** A **5)** D **6)** A **7)** D **8)** A **9)** A **10)** B

Practice Question

Every day, millions of computer users share files online. Shared file may be music, film, games, or software. File-sharing can give people access to a wealth of information. Your friend downloads special software that connects his computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software downloaded by the friend is free and easily accessible.

You are required to submit a detailed report on various aspects of the case based on the concepts given in this study lesson and give appropriate recommendations to your friend.

Theoretical Questions

1. What do you mean by Cyber Crime and role of forensic auditor?
2. What are the various types of Cyber Crime?

3. Write a brief note International Guidance to Cyber Forensics Laws.
4. What do you mean Data Extraction? Discuss the concept with examples.
5. Discuss the Concept of Ethical Hacking.
6. Explain the term 'Digital Forensics" along with example.
7. What is Digital Evidence?
8. What are the precautions to be adopted by Digital Forensic Expert?
9. Explain the term 'Mobile Forensics'
10. What is Digital Incident Response? Briefly narrate the steps involved in Digital Incident Response.

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann
- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's