DFA – Module 1 : chapter 16
Cyber Forensic approach, Cyber Law , IT Act

Arijit Chakraborty

Feb 14, 2022

CYBER FORENSIC

- **Digital Forensic**
- *"Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."*
- **Digital Evidence** =
- any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

Countering cyber crimes

- **Technological measures-**
- Public key
- cryptography,
- Digital signatures ,
- Firewalls,
- honey pots
- **Cyber investigation-**
- Computer forensics = process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in courts of law.
- **Legal framework-laws & enforcement**
- **Ethical Hacking** = ascertains itself from hacking by adding important elements to a process - 'consent'.

1. The Process eventually **becomes a legal activity.**
2. **Ethical Hacker seeks permission before hacking into a system** – ensure = hacking is **performed legally** & hacker **doesn't have any malicious intent**

IT Act 2000

- Enacted on 17th May 2000-
- India is **12th nation** in the world to adopt cyber laws
- The original Act = 94 sections, divided into 13 chapters and 4 schedules.
- The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law
- Introduced by - Pramod Mahajan, Minister of Communications and Information Technology
- Amended by - IT (Amendment) Act 2008

Objectives of the IT Act

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 commerce"
- To facilitate electronic filing of documents with Government agencies and E-Payments
- To amend the Indian Penal Code, Indian Evidence Act,1872, the Banker's Books Evidence Act 1891,Reserve Bank of India Act ,1934
- Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

IT Amendment Act (ITA2008)

- An Act to provide **legal recognition for transactions** carried by EDI
- Act is administered by **Indian Computer Emergency Response Team** (CERT-In).
- Amended by IT Amendment Bill passed in LS on Dec 22nd and in RS on Dec 23rd of 2008.

- Facilitate **e- filing of documents**
- Facilitate **electronic storage of data**
- Give **legal sanction & facilitate e- transfer of funds b**etween banks & FI
- **Amendment =**
- introduced Section 66A which penalized sending "offensive messages".
- Introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
- introduced provisions addressing - pornography, child porn, cyber terrorism

Offences-
Cybercrime provisions

- Section 65 - Tampering with computer source documents
- Section 66 - Hacking with computer system
- Section 66 B – received stolen computer / communication device
- section 66 C- Using PW of another person
- Section 66 F – Acts of cyber-terrorism
- section 67 – publishing obscene information
- Section 67C - Failure to maintain records
- Section 68 - Failure/refusal to comply with orders
- Section 69 - Failure/refusal to decrypt data
- Section 70 - Securing access to a protected system
- Section 71 – Misrepresentation
- Section 72 – breach of confidentiality & privacy
- section 73 – publishing false DSC

Computer Related Crimes under IPC & Special Laws

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act 1985 (Narcotics, Drugs)
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

Cyber Terrorism

- *If with intent to threaten the unity , integrity , security or sovereignty of country or to strike terror in the people or for any act which may cause denial of services of computer system*

- *Punishable u/s 66F of IT act*

Phishing and Email Scams

- *Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)*

  Provisions Applicable:- section 66D of IT Act and Section 419/420 of IPC

Theft of Confidential Information (Data Theft)

- *Secret information= targeted by rivals, criminals and disgruntled employees.*
- *Provisions Applicable:- Sections 72/72A of IT Act and 406/408 of Indian Penal Code*

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- Social media intermediaries, with registered users in India above a notified threshold, have been classified as **significant social media intermediaries (SSMIs).**
- SSMIs required to observe certain additional due diligence

✓ appointing certain personnel for compliance,

✓ enabling identification of the first originator of the information on its platform under certain conditions,

✓ deploying tech-based tool on best-effort basis to identify certain types of content.

- The Rules prescribe a framework for the regulation of content by online publishers of news and current affairs content, and curated audio-visual content.
  All intermediaries are required to provide a grievance redressal mechanism for resolving complaints from users or victims.
- A 3-tier grievance redressal mechanism with varying levels of self-regulation has been prescribed for publishers.

Objective

- ‘’ *In order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users and in tune with the changing requirements, the Rules have been revised* ‘’
- **- MEITy**
- The Rules have come into effect from : date of their publication in the Gazette (i.e., 25th February, 2021).
- The threshold criteria [Ref. rule 2(1)(v)] for significant **social media intermediaries (SSMI)** was published on 26th February, 2021.
- Additional due diligence for SSMI have come into effect **from 26thMay, 2021**

National Cyber Security Strategy 2020:

Aim: To **improve cyber awareness and cybersecurity** through **stringent audits.**

- ✓ Empanelled cyber auditors – Review security features
- ✓ **table-top cyber crisis management exercises** regularly to reinforce the idea that cyber attacks can take place regularly.
- ✓ **Index of cyber preparedness,** & monitoring of performance.
- ✓ **Separate budget for cybersecurity** suggested, + synergise role & functions of various agencies with domain knowledge.
- ✓ **Most developed cyber warfare capabilities = United States, China, Russia, Israel & United Kingdom.**

CERT-In Guidelines on Cyber-Security / Forensic Audit

- Auditee and Auditing organizations needs to re-assess their risk profile and implement controls for minimizing the risk.
- Architecture changes, exposure of services, expanded organizational boundaries and changes caused = to be reviewed by Cyber Auditor
- Services exposed on adhoc and temporary basis (Pandemic) needs to be secured and properly audited. Such temporary changes to be reflected in BCP of organizations and thoroughly tested by Cyber / Forensic Auditor.
- Auditor & auditee organisation = ensure quality of audits should not be lowered in case of remote assessment = use of techniques : video calling for evidence verification, asking for snapshot of command output, online interview of process owner / suspect / witness etc
- Auditor = to maintain situational awareness & their assessments should also include tests derived from recent cyber-attacks trends