20th Dec 2022 :: 11.15-12.45

Introduction to Incident Handling

- K S S Murali Krishna

1st PCP-ADCSDPL
NALSAR University of Law, Hyderabad

Data Protection Laws (DPL)

- EU & GDPR
- IT Act 2000 / 2008
- DPL in Singapore, USA, Canada

Threats & Vulnerabilities

- Cyber warfare
- Cyberspace & Vulnerabilities

Issues around DPL

- Cybercrimes (Tech & law)
- Challenges in compliance
- Cybercrimes vs IT Act 2000
- International Data Protection
- Indian Data Protection Bill
- Crimes in Social media

Indicate the requirements

Indicate the nuances and constraints

Specific use cases

- Electronic contracts
- Cybersecurity & cryptography
- IT in Banking
- Mobile security

Cybersecurity Management

- Cyber Crisis Management
- ISO 27000 – ISMS
- Cert-In & NIC guidelines
- Cyber Forensic Investigation

Influence

Incident Management

- Incident handling
- Incident Forensic Analysis

Quality of Evidence

An effective **cybersecurity attorney** helps to develop

- the statements of work for new contracts,
- negotiating information-sharing agreements,
- advising on legal risks associated with day-to-day decisions of securing networks, and
- managing the response during an incident.

- CISA (USA)

One of the **key jobs of cybersecurity attorney** is

- to translate legal requirements (such as obligations imposed by regulations) into design requirements and
- to understand the technical details enough to ask probing questions, spot legal issues and translate risks to organizational leadership.

Therefore, the attorney needs to understand the basics of technology, or at least have a curiosity and drive to learn.

Cyber incidents

"Cyber Security Incident" means any

- **real or suspected adverse event** that violates cyber security policy
- resulting in
  - unauthorised access,
  - denial of service or disruption,
  - unauthorised
    - use of a computer resource for processing or
    - storage of information or
  - changes in data, information without authorisation.

Cybersecurity-related attacks are

- increasing
- becoming diverse (new attack types)
- more damaging
- disruptive

Defences

- Preventive activities
  - risk based
  - can reduce but not eliminate incidents
- incident response capability
  - to rapidly detecting incidents,
  - minimizing loss and destruction,
  - mitigating the weaknesses, and
  - restoring IT services

Essential information about the incident:

- Current Status of the Incident Response
- About of the Incident
  - Description of the incident (e.g., how it was detected, what occurred)
  - Description of affected resources (e.g., networks, hosts, applications, data), including systems' hostnames, IP addresses, and function
  - Incident category, vectors of attack associated with the incident, and indicators related to the incident (traffic patterns, registry keys, etc.)
  - Cause of the Incident (e.g., misconfigured application, unpatched host)
- Incident Handling Actions
  - Evidence collected, secured and retained
  - Record of analysis, decisions and actions taken by all handlers
  - Contact information for all involved parties
  - List of evidence gathered
  - Chain of custody (in case of forensic analysis / investigation)
- Cost of the Incident
- Business Impact of the Incident

Prosecution:

- evidence may need to be retained until all legal actions have been completed (several years)
- evidence that seems insignificant now may become more important in the future.
  - For example, attacker uses knowledge gathered in one attack to perform a more severe attack later

Data retention costs (issues like due care, technology obsolescence, licences, skills, etc) and associated costs

We can stop the attack. Minimize impact

- Network & Perimeter defences
- Malware Protection
- Secure Configuration
- Security Incident / Crisis Management
- User Training, Education and Awareness
- User Access Controls
- Security Monitoring
- User Training, Education and Awareness

Survey

- **Find technical, procedural, physical weaknesses**
- **NW scanning, public information, social networks**

Identify potential Vulnerabilities

Delivery

- **Select delivery path**
- **Phishing, remote access, false website**

Gain initial foothold

Breach

- **Exploit vulnerability, modify operation, access online accounts, achieve full-control**

Exploit the vulnerabilities & gain unauthorized access

Affect

- **Expand access, retain admin access for future, persistence, exfiltrate, modify, disrupt, etc**

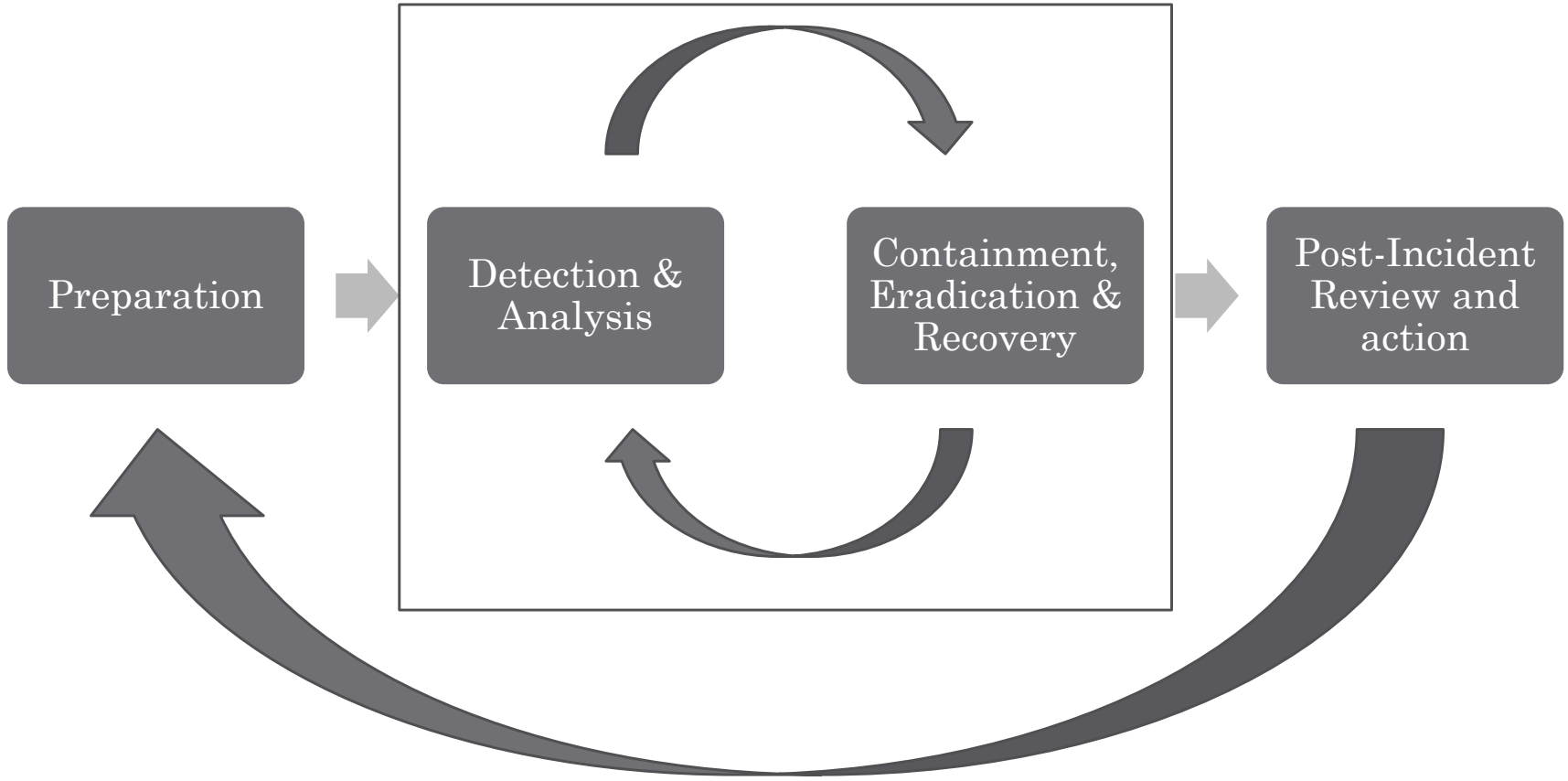
Activities to achieve attacker's goals

Incident handling is the process of **detecting** and **analysing** incidents and **limiting the incident's effect**.

Example : when an attacker breaks in the incident handling process should

- detect the security breach
- analyse the data and
- determine seriousness of the attack
- select and prioritise the action
- arrest further progress of the damage
- return to normal operation as soon as possible

Incident Response Life Cycle



Source : NIST

Incident Response (good practices)

Step 1:

collect and remove for further analysis:

- Relevant artifacts,
- Logs, and
- Data.

Step 2:

implement mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.

Step 3:

consider soliciting incident response support from a third-party IT security organization to:

- Provide subject matter expertise and technical support to the incident response,
- Ensure that the actor is eradicated from the network, and
- Avoid residual issues that could result in follow up compromises once the incident is closed.

Incident Handling effectiveness depends on many factors…

Is it an incident? Which policies are violated?
What capabilities (people, tech.,processes) exist to detect / investigate

- Logs, baselining (profiling / anomalies), monitoring, event correlation
- Precursors of incident and other related/preceding incidents (prev. attack)
- Indicators of incident / compromise
- Indicators of attack

Which evidences (logs, artefacts) to be collected, stored, secured and retained?
What would be the strategy(s) to contain, eradicate and recover?
Whom to report to, how to prioritise the action, strategy to choose?
How would the team analyse and validate the incident?
What capabilities exist to prevent or contain the impact?
Which additional tools / skills needed (including forensics/investigations)
What are the external dependencies and preparedness?
How to communicate, coordinate and share information?

- Legal, regulatory and contractual obligations to fulfil.
- Entities involved (roles / responsibilities), contracts / agreements and enforcement.

Sources of information

- Intrusion Detection and Prevention System logs
- Security Information and Event Management Systems analysis, alerts
- Anti-Malware software (virus, spyware,..) logs, alerts
- File integrity checking software
- Third-party monitoring services
- Operating system, services and application logs
- Network device, firewalls, gateway device logs
- Network flows
- Information on new vulnerabilities and exploits
- People (internal, external)

Threat: The potential source of an adverse event.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Malware: A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Intrusion Detection and Prevention System (IDPS): Software that automates the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents and attempting to stop detected possible incidents.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Event: Any observable occurrence in a network or system.

Precursor: A sign that an attacker may be preparing to cause an incident.

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Indicator: A sign that an incident may have occurred or may be currently occurring.

Baselining: Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Cyber Incidents - CERT-In directions

u/s 70B (4) IT Act 2000
CERT-In will be national agency for cybersecurity for:

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

u/s 70B (6) of the IT Act, 2000

CERT-In is empowered to (w.r.t. cybersecurity)

- call for information and
- give directions to

the service providers, intermediaries, data centres, body corporate and any other person

Deficiency:

CERT-In observed that the requisite information is not found or readily not available with service providers/data centres/body corporate.

This is hampering analysis, investigation and coordination as per the process of law

No. 20(3)/2022-CERT-In

Government of India

Ministry of Electronics and Information Technology (MeitY)

Indian Computer Emergency Response Team (CERT-In)

Electronics Niketan,
6 CGO Complex,
New Delhi-110003

Dated: 28 April, 2022

Subject: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

CERT-IN directives dt 28 April, 2022
(effective after 60 days)

organisations should comply with the following:

- Report to CERT-IN within six hours of cybersecurity incidents in the prescribed format.
- Synchronise time with NIC's Network Time Protocol server.
- Enable logs of all ICT systems.
- Retain logs for 180 days.
- Nominate a Point of Contact for communicating with CERT-IN.

The incidents can be **reported to CERT-In** via

- email (incident@cert-in.org.in),
- phone (1800-11-4949) and
- fax (1800-11-6969)

Evidence / Records

Applicable entity shall **mandatorily**

- **enable logs** of all their ICT systems (IT, OT, IoT, IIoT, IoMT) and
- **maintain** them securely **for** a rolling period of **180 days** and
- maintained within the **Indian jurisdiction**.

These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

ICT **system clocks** of applicable entities should be **synchronised** with Network Time Protocol (NTP) Server of

- National Informatics Centre (NIC) or
- National Physical Laboratory (NPL) or
- their associated servers

Entities having ICT systems over **multiple geographies** may use NPL and NIC, or any other without deviating from NPL and NIC.

Applicable entities : All service providers, intermediaries, data centres, body corporate and Government organisations. Individual citizens are **NOT** covered by these Directions.

Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to

- register the accurate information about their customers/subscribers and
- maintain the information for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration

Details about customer : validated names, period of hire with dates, IP addresses allotted, Email address and IP address and time stamp used at the time of registration / on-boarding, purpose for hiring services, validated address and contact numbers, ownership pattern of the subscribers / customers

The **virtual asset** service providers, virtual asset exchange providers and **custodian wallet** providers (as defined by Min. of Finance) shall **mandatorily maintain for a period of 5 years**

- all information obtained as part of Know Your Customer (KYC – RBI/SEBI/Dept of Telecom) and
- records of financial transactions

while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets

Accurate transaction records shall be maintained

- in such a way that individual transaction can be reconstructed
- along with the relevant elements comprising of, but not limited to, information relating to
  - the identification of the relevant parties
  - IP addresses along with timestamps and time zones,
  - transaction ID,
  - the public keys (or equivalent identifiers),
  - addresses or accounts involved (or equivalent identifiers),
  - the nature and date of the transaction,
  - and the amount transferred.

Where multiple entities are associated then any entity which notices the cyber security incident, shall report to CERT-In. The obligation of reporting of cyber incident is neither transferrable nor indemnified or dispense with.

At present, the reporting of vulnerability as a standalone or in isolation, unconnected with the cyber security incident is not mandatory.

Processes in CERT-In Rules, 2013 are followed to ensure chain-of-custody of information provided

Penalties

The **failure to furnish** the information **or non-compliance** with CERT-In directions, may invite punitive action under sub-section (7) of the section 70B of the IT Act, 2000 and other laws as applicable

(**punishable with imprisonment up to one year or with fine up to one lakh rupees or with both**)

Mandatory Reporting

Types of Incidents

Applicable entities shall **mandatorily report** cyber incidents in **prescribed format** to CERT-In **within 6 hours** of noticing such incidents or being brought to notice about such incidents.

Additional needs of CERT-In:

Applicable entities are **mandated to**

- take action or
- provide information or
- any such assistance to CERT-In,

which may contribute towards cyber security **mitigation actions** and enhanced cyber security **situational awareness**.

Applicable entities shall designate a **Point of Contact** to interface with CERT-In. Entity should share the details of the contact with CERT-In.

All communications from CERT-In seeking information and providing directions for compliance shall be **sent to Point of Contact**

Types of cyber security incidents mandatorily to be reported :

i. Targeted scanning/probing of critical networks/systems
ii. Compromise of critical systems/information
iii. Unauthorised access of IT systems/data
iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.

v. Malicious code attacks such as spreading of virus/ worm/ Trojan/ Bots/ Spyware/ Ransomware/ Cryptominers

vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers

vii. Identity Theft, spoofing and phishing attacks

viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

ix. Attacks on Critical infrastructure, SCADA (Supervisory Control And Data Acquisition) and operational technology systems and Wireless networks

x. Attacks on Application such as E-Governance, E-Commerce etc.

xi. Data Breach

xii. Data Leak

xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers

xiv. Attacks or incident affecting Digital Payment systems

xv. Attacks through Malicious mobile Apps

xvi. Fake mobile Apps

xvii. Unauthorised access to social media accounts

xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems /servers /software / applications

xix. Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual (digital) asset exchanges, custodian (crypto) wallets, Robotics, additive manufacturing (3D printing), and 4D Printing (3D printed polymer objects able to morph into different forms in response to environmental stimulus like temp., humidity, voltage, etc), Drones

xvii. Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence (such as visual perception, speech recognition, decision-making, and translation between languages) and Machine Learning

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

THANK YOU