An Introduction to Incident Handling

Ram G. Singh, Scientist
Indian Computer Emergency Response Team(CERT-In)
(r.govind@meity.gov.in)

Outline

- Cyber Incident
- Necessity of Incident Handling/ Incident Response
- Computer Security Incident Response Team (CSIRT)
- Setting a CSIRT
- Incident Handling Process
- Indian Computer Emergency Response Team (CERT-In)
- Incident Handling Tools
- References

“Incidents transpire, as nothing is hidden over the internet”

What is Cyber Incident?

- “Incident” = “Adverse event”
- The NCSC defines a cyber incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

Picture courtesy: logsign.com

Cyber Incident

- CERT-In- Any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information systems, services or networks resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource, changes to data or information without authorization; threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

Picture courtesy: logsign.com

Cyber Security Incident?

- Any real or suspected adverse event event **in relation to cyber security** that violates an explicitly or implicitly applicable security policy resulting in authorized access, denial of service or disruption, unauthorized use of a computer resource for processing of storage of information or changes to data, information without authorisation

- **Role:** Individual, organization, Govt Organization, LEA, Security researchers

Picture courtesy: logsign.com

Example of Cyber Incidents

- DoS (Denial of Service)/DDoS attack
- Unauthorized access/Hacking (Website, Database, AD server)
- Defacement of public website (intrusion)
- Worm that infects workstation on a network
- Scanning/ Network Probing
- Malware attacks, APTs
- Ransomware Attack
- Data Breaches
- Insider threat (e.g. data loss, data exfiltration)

Understanding of different types of cyber threat is essential before responding to an incident

Incident Happens!!!

- **Despite of several effort attack happens!** (Even the best security infrastructure can not guarantee that attack will not happen.)
- Possible attacks- botnet, exploit kit, 0-day, APT etc
- In worst case, **it can impact your organization, customer, your country (critical infrastructure)**

Learning

- We summarize the following questions:
  - How we have to handle it?
  - What is the impact?
  - To whom we should contact?
  - What should be prioritized?
  - How we should respond it.
  - Who will handle what?
- .

Framing the Problem

- What needs to be done?
  - Proper steps and procedure to respond and handle the incident (incident response/incident handling)
  - It must be managed in order to limit the damage, recovery, and prevent from further recurrences
  - Establishment of CSIRT/CERT team to handle cyber incidents

The speed with which an organization can recognize, analyze, and respond to an incident limits the damage done and lowers the cost of recovery.

Incident Handling/Incident Response

- **Incident Handling/Incident Response (IR)** is a organized process by which **a person or organizations defend themselves against security incidents/attacks**.
- Actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occur, with well defined procedures which involves several stages.
- It involves all the activities used before, during, and after a computer security incident occurs on a host, network, site, or multi-site environment

What is CSIRT?

- **Computer Security Incident Response Team (CSIRT)** is a name given to expert groups that handles computer security incidents.
- It is an organization or team that provides, to a defined constituency, services and support for both preventing and responding to computer incidents.

CSIRT..

- Assists the organizational constituency and general computing community in preventing and handling computer security incidents Control and containment of incident.
- Provides a **single point of for reporting problem**
- Reporting the network abuse **directly to specialized team**.
- Perform unbiased investigation of all incident
- Share information and lessons learned with other CSIRT/response teams and appropriate organizations and sites.

Basic Framework for a CSIRT

- **Mission statement** (what to do ?): A high level definition of what the team will do.
- **Constituency** (for whom ?) : Whose incident are we going to handling and responsible for.
- **Relationship with others**: At what extents relation to other teams; whom to cooperate with ? whom to trust ?
- **Services**

Establishment of IRT

- **Components**
  - Understanding of constituency
  - Education of constituency
  - Centralized communication
  - Expertise in requisite technology
  - Links to other groups assisting in incident handling, as needed
    Establishment of IRT
- **Technical support**
  - Organization-wide/ Nationwide reporting facility for incidents
  - Rapid communications
  - Secure communications for incidents involving national security

Different Types of CSIRT

- Type of activities scope and capabilities may be different
- Example:
  - National CSIRT (e.g. CERT-In)
  - Regional CSIRT (e.g. states CERT, probably every state)
  - Vendor CSIRT
  - Financial CERT (FinCERT), Health Sector CERT, Power Sector CERT
- Communication and information sharing CSIRT

Terminologies

- CSIRT: Computer Security Incident Response Team
- CERT or CERT/CC: Computer Emergency Response Team/Coordination centre
- CIRC: Computer Incident Response Capability
- CIRT: Computer Incident Response Team
- IRC: Incident Response Center /Capability
- IRT: Incident Response Team
- IHT: Incident Handling Team
- IMT: Incident Management Team
- SERT: Security Emergency Response Team
- SIRT: Security Incident Response Team

World CSIRTs:

US-CERT	AUSCERT	SingCERT	CERT-In
CAIS/RNP	Cisco PSIRT	HP SSRT	CERT-Army
APCERT	FIRST	CERT/CC	JPCERT/CC

Key People in IRT

- Incident Response Team may comprise:
  - **System administrators :** provide the knowledge and expertise of system resources, including data backups, backup hardware available for use, and more.
  - **Network administrators :** provide their knowledge of network protocols and the ability to reroute network traffic dynamically.
  - **Information security experts:** Information security personnel are useful for thoroughly tracking and tracing security issues as well as performing a *post-mortem (after the attack)* analysis of compromised systems.
  - **Others:** Executive management, Legal, Public relations, IS management, Human resources, CFO, financial auditor

Point of Contact

- The service providers, intermediaries, data centres and body corporate shall designate a Point of Contact (**PoC**) to interface with CERT-In.
- Chief Information Security Officer (**CISO**)

CSIRT Services

- **Proactive services:** Designed to detect & prevent attacks before there is an actual impact on the production systems. In this category of services, the information generated by the CSIRTs gets disseminated to their constituency and partners for protecting their assets and avoid being target of an attack.
- **Reactive services:** Consist in post incident reports from constituency or other events related to threats or attacks such as compromised hosts, malware, vulnerabilities or other type of similar incidents.
- **Other Services:** Demanded by the constituency for review and improvement of the security posture of their organizations. This category of services are not time dependent and are usually demanded by the constituency which makes the request to their CSIRT.

CSIRT Services

- **Proactive**
  - to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected.
  - main goals are to avoid incidents and to reduce their impact and scope when they do occur.
- **Announcement**
  - Announce intrusion alerts and security advisories to protect systems against newly found problems before they can be exploited
- **Technology Watching**
  - Up to date, catch up the latest situation
- **Security Audit/Pentests, Tools development, Intrusion Detection, Threat intelligence sharing**

CSIRT Services

- **Reactive**
  - To respond to requests for assistance
  - Alerts & warnings
  - Reports of incidents from the constituency, and any threats or attacks against CERT systems.
- **Incident Handling**
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- **Vulnerability handling**
- **Artifact handling**

CSIRT Services

- Security Quality Management
- Risk Analysis
- Security consulting
- Awareness Building
- Education/ Training
- Product Evaluation/ Certification

Incident Handling Process

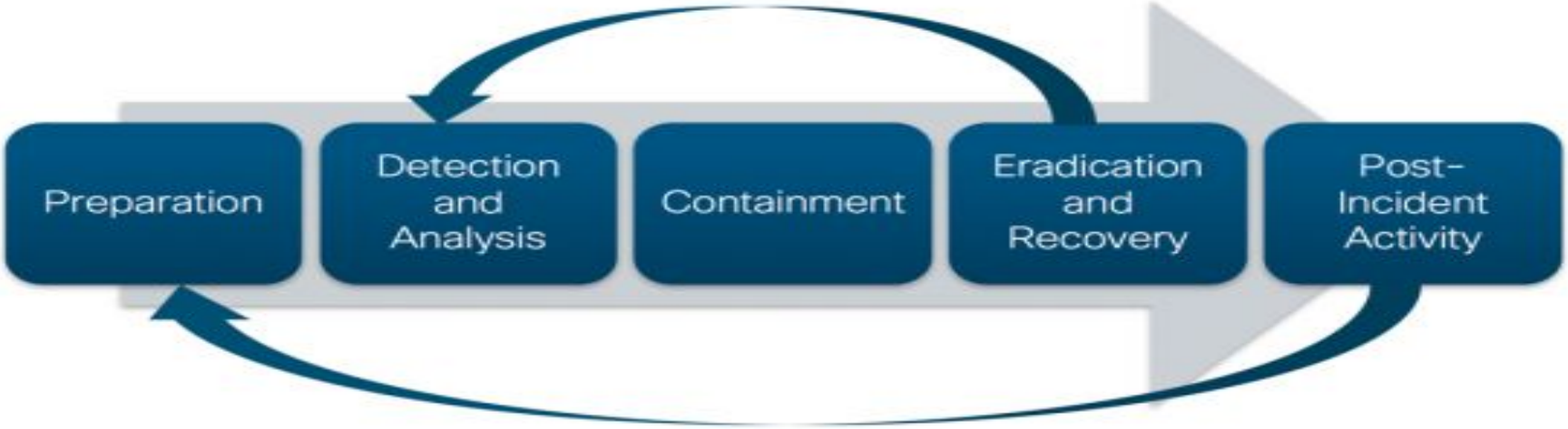
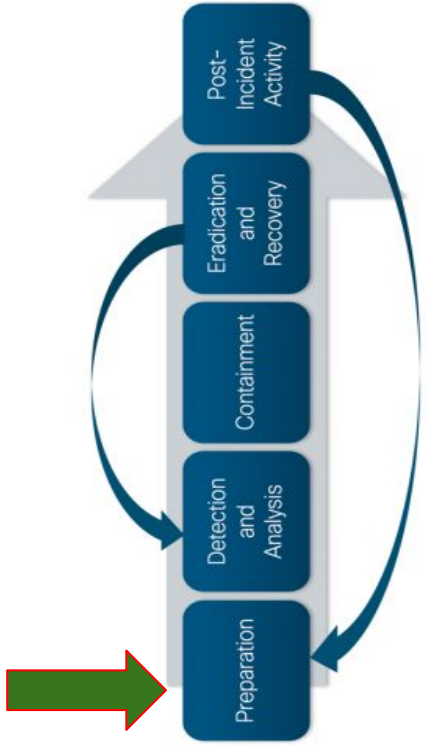


Figure: Incident Handling Process

Picture courtesy Cisco-Blogs

Preparation: Incident Prevention

- Security control
  - Host and network
- Risk assessment
  - System and asset inventory
  - Critical and high value asset identified
  - Vulnerability critical path
- Awareness and training
  - Organizational security policies
  - Acceptable use
  - Incident reporting
  - Changes in policy



Detection and Analysis

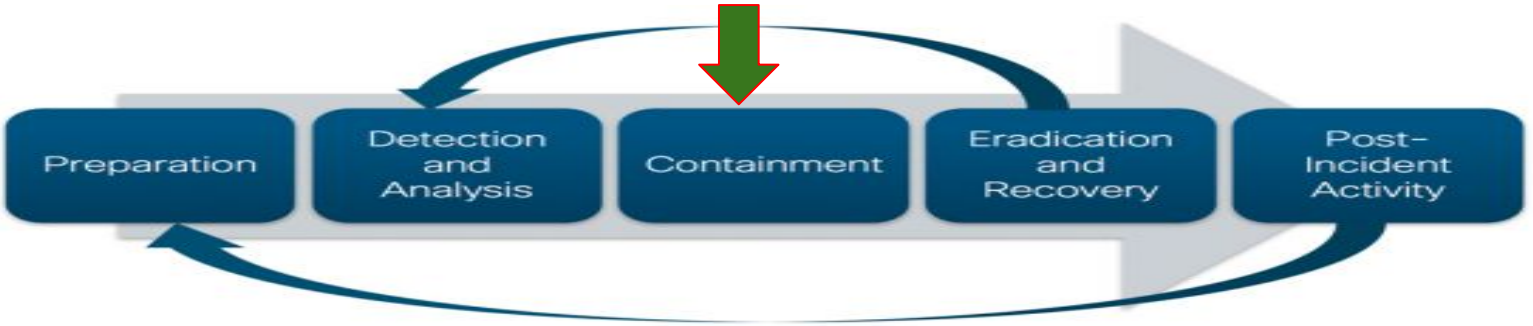
- **Detection**
  - **Goal :** accurate detection and analysis of incident
  - **Approach:** manual and automated data analysis
  - **Detection: sensing data, and established method for data collection and analysis**
  - **Data:** event, log, people**; Methods:** Signature, anomaly, hybrid approach
  - Incident reporting channel: telephone, email, sms IDS alert, IPS alert, SIEM alert

Detection and Analysis

- **Analysis**
  - **Triage**: extracting the information for incident analysis
  - **Information gathering**: logs, file, system registry, malicious emails, network activity etc
  - **Timeline analysis**
  - **Log analysis:** web server log, email server, database, error, firewall logs,

Containment

- The primary purpose of this phase is a function that assists **to limit and prevent further damage** from happening along with ensuring that there is no destruction of forensic evidence that may be needed for legal actions against the attackers later.
- Containment should be a **Strategy**. Once a containment strategy is defined, the respective tools & technologies can be selected to participate in the fulfilment of the strategy.



Containment..

- **Examples of Perimeter & Extended Perimeter Strategy:** Stop the outbound communication from infected machine, block inbound traffic, IDS/IPS Filters, Web Application Firewall policies, null route DNS, fail-over to backup link, switch to secondary data centre etc.
- **Examples of Internal Networks Strategy:** Switch based VLAN isolation, router based segment isolation, port blocking, IP or MAC Address blocking, ACLs etc.
- **Examples of Endpoint Strategy:** Disconnecting the laptop/desktop, powering off the servers, blocking rules in Desktop firewall, HIPS etc
- **Short term containment**
- **Long term containment**
- **System backup (FTK)**

Eradication

- Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
  - **Actual removal of infection and restoration of affected systems.**
  - **Re-Imaging**
  - **Preventing the root cause**
  - **Scan for the malware, disarming malware**
  - **Disabling compromised accounts**
  - **Patching devices**
  - **Applying basic security best practices**

Recovery

- The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.
  - **Defining time and date to restore operations**
  - **Test and verifying**
  - **Monitoring**
  - **Do everything to prevent another incident**

Post Incident Activity(Lesson Learned)

- The CSIRT should compile all relevant information about the incident and extract lessons that can help with future incident response activity.
  - **Perform post Incident Review (PIR)**
  - **Consideration of what can be improved**
  - **Sharding of threat intel with other communicating team (other CERT, National CERT)**
  - **Advisories and alerts**
  - **Lesson learned, Future planning**

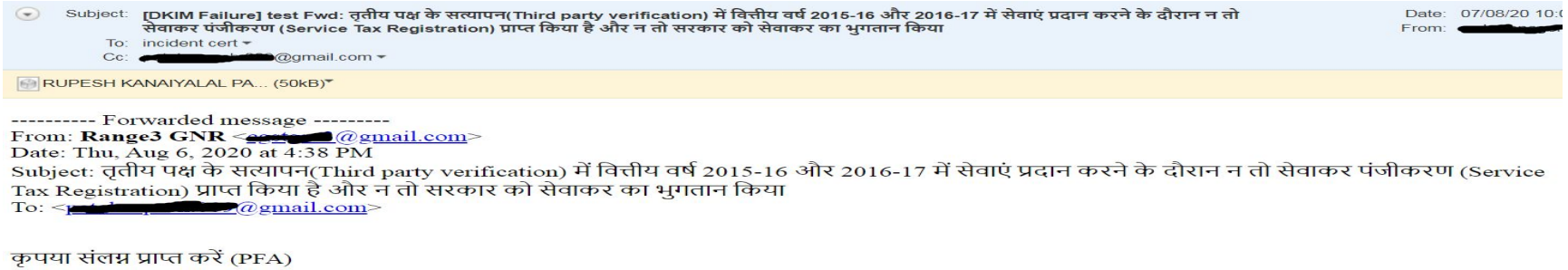
CERT-In

- **Indian Computer Emergency Response Team** (**CERT-In)** is the national nodal agency for responding to computer security incidents as and when they occur.
- In the recent Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform following function in the area of cyber security:
  - Collection,analysis and dissemination of information on cyber incidents.
  - Forecast and alerts of cyber security incidents
  - Emergency measures for handling cyber security incidents
  - Coordination of cyber incident response activities.
  - Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices cyber incidents.
  - Such other functions relating to cyber security as may be prescribed

CERT-In

- Functioning 24*7
- Constituency: Indian cyber community
- Communication: mail, phone
- Services
- Reporting incident to CERT-In
- Incident form
- Verification
- Triage
- Incident handling

A Phishing Incident



Subject: [DKIM Failure] test Fwd: तृतीय पक्ष के सत्यापन(Third party verification) में वित्तीय वर्ष 2015-16 और 2016-17 में सेवाएं प्रदान करने के दौरान न तो सेवाकर पंजीकरण (Service Tax Registration) प्राप्त किया है और न तो सरकार को सेवाकर का भुगतान किया

Date: 07/08/20 10:

From: [redacted]

To: incident cert

Cc: [redacted]@gmail.com

RUPESH KANAIYALAL PA... (50kB)

---------- Forwarded message ---------

From: **Range3 GNR** <[redacted]@gmail.com>

Date: Thu, Aug 6, 2020 at 4:38 PM

Subject: तृतीय पक्ष के सत्यापन(Third party verification) में वित्तीय वर्ष 2015-16 और 2016-17 में सेवाएं प्रदान करने के दौरान न तो सेवाकर पंजीकरण (Service Tax Registration) प्राप्त किया है और न तो सरकार को सेवाकर का भुगतान किया

To: <[redacted]@gmail.com>

कृपया संलग्न प्राप्त करें (PFA)

- A suspicious mail has been received by a user having an attachment “rupesh kanaiyalal patel.zip”. What will be your approach to verify and handle this incident?
- **Incident Prevention:**
  - Verify the genuineness of the file form open search analysis tools such as virustotal using hashes (MD5, SHA-1, SHA-256).
  - Block emails containing suspicious extension “.exe‘, “.bat”, “dll” etc.
  - Generate warning over the received emails containing an attachment.
  - Block IoCs like IPs, domain, port, received from threat sharing.

Responding a Phishing Incident

1. **Detection & Analysis:**
   - Perform analysis of reported phishing emails: email header analysis, url analysis, malware analysis (suspected malware); whether email server is compromised (if phishing email come from own server)?
   - Phishing site analysis: phishkits? Phishing site take down; isolation of infected systems; What data has been stolen?
2. **Containment/ recovery**
   - who all are infected?
   - removal/suspension/ isolation of other infected systems.
   - browser notification to prevent further recurrences/propagation
   - Credential "Stolen": notify the relevant users
3. **Report/Escalation**
   - advisories and alerts, preparation of incident reports
4. **Lesson Learned**

Responding a Malware Incident

- Different types of malware: Botnet, Exploit kit, Data stealing Trojan-RAT CRIMSON-RAT, APT.
- **Ask the following questions:** what network connections does the malware generate? Does the malware connect to any domains? What files are created on disk? What running processes are created? Are there any unique registry keys that have been created? What Data exfiltrated?
- **What we have to handle:**
  - List of Infected computers
  - Artifact analysis, malware analysis (behavior analysis)
  - Infection points (c&c, IPs, websites)
  - Take down effort of the organization
  - Steps taken to prevent future attacks.
  - Writing of advisory
  - Contacting with law enforcement agencies

Responding a Compromised Website Incident

- Website compromise may lead to defacement or abused for other kind of attacks
- An organization may also targeted in mass defacement or in pre announced attacks.
- **What we have to handle:**
  - Contacting with website administrator/owner of the website
  - Find the source of attack
  - Find the cause and vulnerabilities
  - Find the data exfiltereted? Inform to the users.
  - Fixes and patches
  - Sharing of findings

Data Breach

- Thousand or millions of users credential (e.g. username and password) and are being exposed and shared publicly
  - Either by accidently or by an adversary
- **What we have to handle:**
  - Contact owner of the credential
  - Contacting to owner of system where credentials are being dumped
  - Implementing higher security 2FA
  - Removing the credentials

Responding a Ransomware Incident

- Ransomware malware program encrypt all the files in your system ask money to decrypt it.

- **What we have to handle:**
  - List of infected systems, Isolate infected systems
  - Performing root cause analysis/patches/fixes
  - Find the root cause of vulnerability exploited
  - Issuing advisory not to pay ransom
  - Promoting regular backup of the systems

Incident Response Tools

- **CSIRTs daily work relies more and more on tools and platforms, open source tools.**
- Open source malware/file/URL analysis tools
  - Hybrid analysis [https://www.hybrid-analysis.com/
  - Cuckoo Sandbox [https://cuckoosandbox.org/]
  - Virus Total https://www.virustotal.com/gui/
- Spam and Email Header Analysis: MX Toolbox [https://mxtoolbox.com/]
- Web Defacement [http://www.zone-h.com/?hz=1]
- Whos is and Passive DNS Query
  - CentralOPS [https://centralops.net/co/]
  - WhoIs Domain Tools [https://whois.domaintools.com/]
  - Passive DNS

Incident Response Tools

- **Malware Domain List:** [https://www.malwaredomainlist.com/mdl.php]
- **Disk Image Creation Tools:** AccessData FTK Imager, Bitscout, GetData Forensic Imager, Guymager, Magnet ACQUIRE
- **Memory Analysis tool:** Volatility, KnTList, Evolve, VolDiff
- **Incident Response Tool:** Belka Evidence, CIRTKit, CyberTriage, Digital Forensics Framework
- **Network tools:** Wireshark, Networkminer, nmap, nessus
- A detailed list: [https://gbhackers.com/cyber-incident-response-tools/]

Collaboration and Information Sharing

- Report incident to CERT-In (Defacement, malware, vulnerabilities, data breach, data leak, ransomware etc).
- Collaborate with other organization for services; Define trusted organization.
- Association with other CERTs e.g. National CSIRT, Regional CSIRT, PSIRT.
- Getting information on different sources e.g. Shadow server, Team Cymru, Honeypot project; open source threat intel, open source phishing, open source malware.
- Participate in global take down process.
- Help and promoting best practices.
- Making awareness of cyber security/ recent attack/vulnerabilities
- Participate in cyber security exercises.
- Sharing of compliance

References

- Incident handling step by step, SANS; [http[:]//index-of.es/Hack/SANS%20Incident%20Handling%20Step%20by%20step.pdf]
- The Incident Handlers handbook, SANS; [https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901]
- Dfir intro – By Scott J. Roberts
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response – Richard Bejtlich's book on IR
- Setting up CSIRT, Adli wahid [https://pt.slideshare.net/apnic/setting-up-csirt]
- Most Important Cyber Incident Response Tools List for Ethical Hackers and Penetration Testers, BALAJI N, GBhackers [https://gbhackers.com/cyber-incident-response-tools/]
- https://www.cert-in.org.in/s2cMainServlet?pageid=AUTHORITY
- https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf
- https://www.cert-in.org.in/PDF/Addition_of_Mandated_Activity.pdf

Thank You

Queries??

incident@cert-in.org.in/ (r.govind@meity.gov.in)