Response to cyber incident

Point of view on the cyber security directions released by Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (Cert-In)

June 2022

home.kpmg/in

The context

Cyber risk and associated incidents have increased significantly in the past 18-24 months, which is also clubbed with rapid adoption of digital technologies.

Considering these developments, there is a need to establish a robust cyber resilience and response framework.

Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY) has recently shared a notification highlighting the need for and importance of information security practices, procedures, prevention, response and reporting of cyber incidents for a safe and trusted environment.

Applicability

The directions released by CERT-In are mandated to comply under IT Act 2000 for service providers, intermediaries, data centres, body corporate, Virtual Private Servers (VPS), cloud service providers, Virtual Private Network Service (VPN) providers and government organisations. This is applicable for all ICT environments, including on-premises systems, systems that are hosted and managed by third party, cloud service providers, data centres, etc.

Key areas for cyber incident management

Reporting cyber incident

CERT-In notification has included reporting of cyber incidents within six hours of incidents being brought to notice. Subsequently, when required by CERT-In, information about protective and preventive actions taken, for the purpose of cyber incident response, will have to be furnished.

As part of incident reporting process, a Point of Contact should be provided to CERT-In. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the Point of Contact.

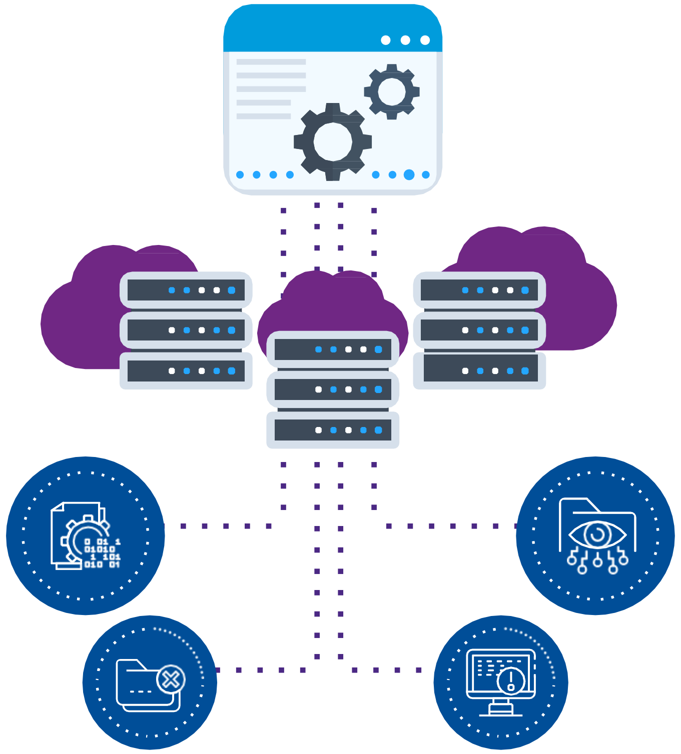
Key measures to be considered

- Review existing cyber crisis management plan and incident response plan to better understand coverage to relevant threat scenarios, having appropriate communication plan and reporting management.
- Enhance/prepare cyber incident communication plan, including processes for real time and periodic reporting of incidents to internal and external stakeholders, including CERT-In.
- Establish technical operating environment to monitor security incidents for timely identification of cyber incidents.
- Defined roles and responsibilities for cyber crisis management team.
- Understand the cyber security monitoring capabilities across your network infrastructure to make sure that strong incident detection and prevention capabilities are in place and have adequate coverage of your business, ICT systems and data. This should also cover systems hosted on cloud, third party environment, etc.
- Establish/refresh cyber incident playbooks, including collection and preservation of relevant logs and data, that may be required for submission at CERT-In.
- Perform regular cyber threat hunting exercise to identify specific indicator of compromise (IOC) based on tactics, techniques and procedures (TTP) linked to various threat actors and organised cyber crime groups.
- Perform table-top simulation exercise to assess response and preparedness to manage and respond to cyber incidents.

Information to be provided during cyber incident response

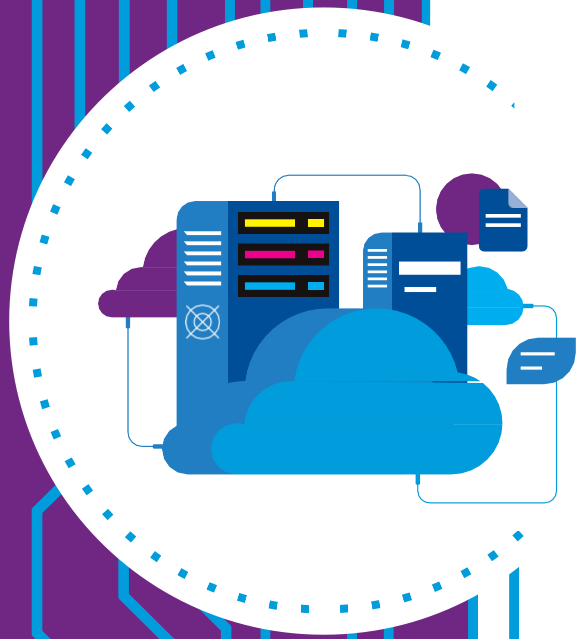
CERT-In notification has included to enable logs of all ICT systems and maintain them securely for a rolling period of 180 days.

In order to further ensure consistency and reliability in correlation of logs, it has included to connect to the Network Time Protocol (NTP) server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all ICT systems clocks.



Key measures to be considered

- Most of the organisations in today's time have a complex set of ICT environment, which includes an ecosystem of cloud service provider, vendors for ICT management, third parties providing critical systems and digital channels leading to proliferation of data. In such an environment, it is important for organisations to have a clear view on:
  - Asset inventory and classification of critical ICT system
  - Network designs and security architecture
  - Logging, auditing and storage capability, within Indian jurisdiction
  - System privilege levels, root and administrator permissions
  - Security baseline configuration
  - Standard operating procedures and IR playbooks
  - Integrated cyber crisis management plan
  - Continuous monitoring, vulnerability management and reporting capability
  - Cyber security incident awareness.
- Dependence on critical suppliers, vendors and cloud service providers should be obtained. Also, these providers should be able to provide logging of respective system for a pre-defined period (as per CERT-In, it is 180 days).
- Configure systems, and network devices to generate relevant logs that are required for detailed incident response, analysis, cyber investigation and root cause assessments.
- Security management system to co-relate security incidents based on the system logs and automated remediation measures.
- Design log storage capability (on-line and off- line) to ensure availability of logs for the period of 180 days.
- Design a NTP server stratum hierarchy based on network topology, type of devices and geography/regions that require synchronous clock time.
- Implement secure NTP servers with built-in resilience in NTP stratum 1 which synchronises its system clock directly with the 'reference' clock that resides at stratum 0 in NIC or NPL as external public source of time.
- Other devices on the ICT systems such as workstations, servers and network devices synchronise their system clock with the clock on a stratum 1 server.
- Continuous monitoring of NTP server outages, out of sync alarm, general attack and exploits to NTP servers such as abuse attempt, unauthorised NTP reply packets, bogus packet, zero origin packet, etc

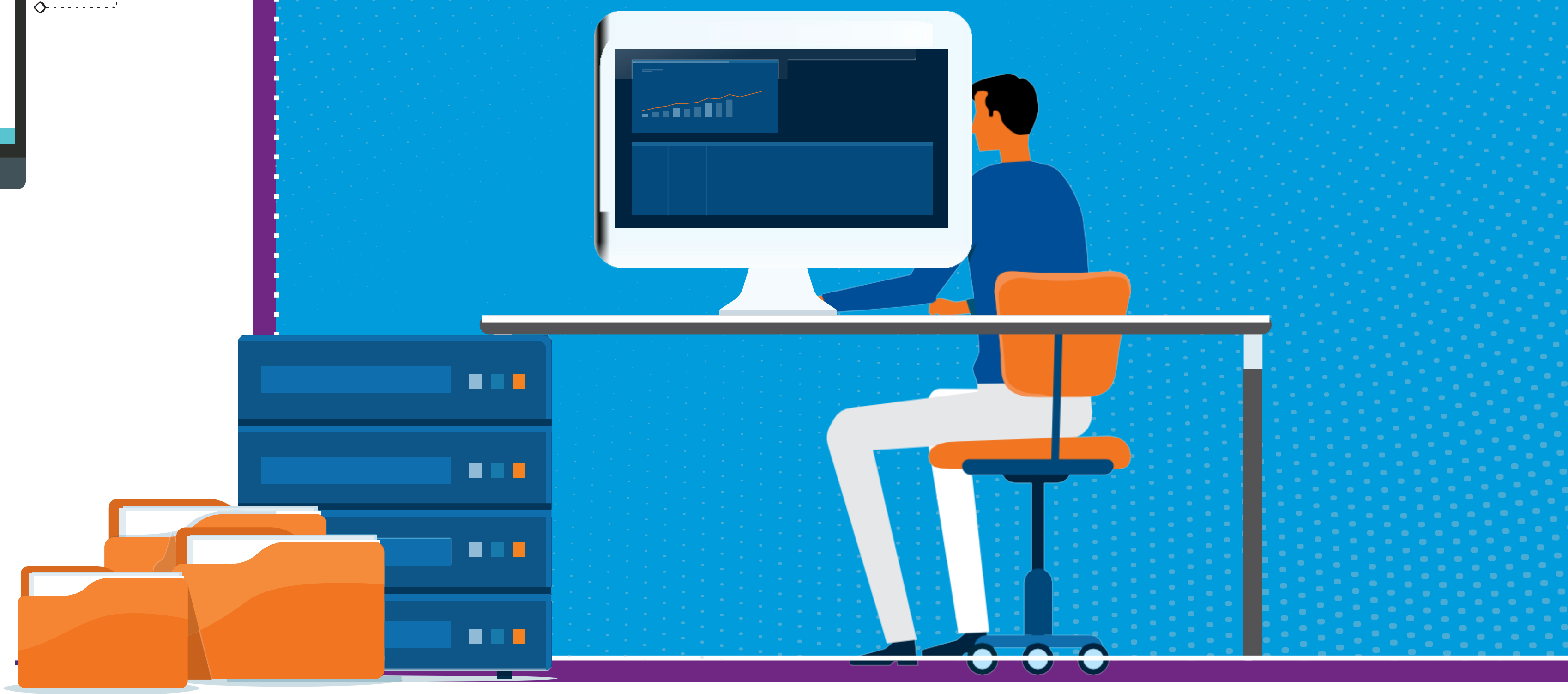


Customer information

As per the CERT-In notification, data centres, Virtual Private Server (VPS) providers, cloud service providers and Virtual Private Network service (VPN service) providers are required to register accurate information of validated subscribers/customers, and it must be maintained for a minimum for period of five years after any cancellation or withdrawal of the registration.

Key measures to be considered

- Data centres, CSP, VPS, VPN service providers should review availability and secure storage of following information:
  - Validated names of subscribers/ customers hiring the services
  - Period of service (including dates)
  - IP details
  - 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 hiring services.
- Review the storage capacity requirement to retain, manage and maintain subscriber/ customer information for more than five years.
- Implement technology for automatic storage, validation, back-up and restoration testing of information.
- Secure the supporting customer/ subscriber information applications and ICT assets



Retaining KYC and transaction information

The virtual asset service providers, virtual asset exchange providers and custodian wallet providers shall mandatorily maintain all information obtained as part of Know Your Customer (KYC), including records of financial transactions for a period of five years.

Key measures to be considered

- Secure the supporting applications and ICT assets that hold and process customer KYC information and financial transactions
- KYC guidelines to be complied upon (based on industry):
  - Reserve Bank of India (RBI) Directions 2016
  - Securities and Exchange Board of India (SEBI) circular dated 24 April 2020
  - Department of Telecom (DoT) notice 21 September 2021
- Ensure availability of transaction records, containing information relating to the identification of the relevant parties, IP addresses, timestamps, 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.
- Review storage capacity of records and logs, including testing and periodic restoration for a period of five years., including methods for automatic secured back-up.

Way forward

The regulators globally have been emphasising on the importance of cyber incident response planning and with the recent notification from CERT-In, it has further set forth minimum requirements to be followed by organisations.

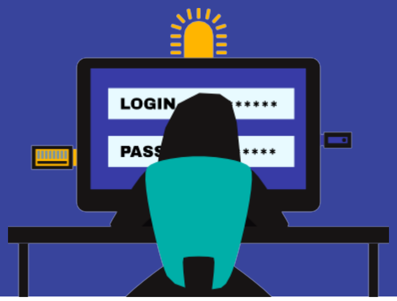
Consequently, it is imperative to enhance cyber incident response capability across the entire ICT environment (including operational technology). The overall cyber response framework needs to have policies and supporting technology environment to enable organisations to respond effectively.

Communication strategy with clear roles and responsibilities is extremely important to respond effectively to cyber incidents and also to various regulatory requirements.

Regular cyber drills, red teaming activities, threat hunting and table-top activities ensure that cyber response plan is current and also effective.

KPMG in India's cyber response team works with organisations to help prevent, detect and respond to cyber incidents. We offer a wide array of services on managing cyber incidents and building cyber resilience, including retainership services that could be utilised during an incident scenario.

Have a cyber emergency? Contact our 24X7 cyber response hotline : : +91 9176471471



KPMG in India contacts:

Atul Gupta
Partner
Head of CyberSecurity
M: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
M: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Associate Partner M:
+91 98181 99432
E: mtembhurkar@kpmg.com

B V, Raghavendra
Partner
M: +91 98455 45202
E: raghavendrabv@kpmg.com

Chandra Prakash
Partner
M: +91 99000 20190
E: chandraprakash@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011, Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only. (007_FLY0522_AR)