Cyber Security

For Prelims: Cyber Surakshit Bharat Initiative, Cyber Swachhta Kendra, Online cybercrime reporting portal,

For Mains: Issue of Cyber Security, Steps that needs to be taken.

Why in News?

Recently, CERT-In has **asked all government and private agencies** to **mandatorily report cyber security breach incidents to it within six hours of noticing them.**

- CERT-In is empowered under **Section 70B of the** Information Technology Act to collect, analyse and disseminate information on cyber security incidents.

What is CERT-IN?

- **Computer Emergency Response Team** - India is an organisation of the Ministry of Electronics and Information Technology with the objective of securing Indian cyberspace.
- It is the nodal agency which deals with cybersecurity threats like hacking and phishing.
- It collects, analyses and disseminates information on cyber incidents, and also issues alert on cybersecurity incidents.
- CERT-IN provides Incident Prevention and Response Services as well as Security Quality Management Services.

What are the Mandates of the CERT-In?

- **Mandatorily Enable Logs:**
  - It **mandates all service providers,** intermediaries, data centres, corporates and government organisations to mandatorily enable logs of all their ICT (**Information and Communication Technology**) systems.
    - The service providers **has to maintain the logs securely for a rolling period of 180 days**, and the same shall be maintained within the Indian jurisdiction.
      - The log **should be provided to CERT-In along with reporting** of any incident or when directed by the computer emergency response team.
- **Connect and Synchronize all ICT systems:**
  - To ensure the chain of events is accurately reflected in the time frame, service providers have been asked **to connect and synchronize all their ICT systems clocks to the Network Time Protocol (NTP)** Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL).
    - NTP is a protocol used for reliably transmitting and receiving accurate time sources over TCP/IP-based networks.

        - It is used for synchronizing the internal clock of computers to a common time source.
- **Requires Maintaining Records:**
    - It also require **virtual asset, exchange, and custodian wallet providers to maintain records on KYC and financial transactions for a period of five years.**
        - Companies providing cloud, virtual private network (VPN) will also have to register validated names, emails, and IP addresses of subscribers.

What is the Need of Such Initiative?

- **Address the issue Hindrance:**
    - It will address the issue of hindrance in the analysis of breach incidents in handling cyber incidents.
- **Streamline the Date Records:**
    - There have been **cases in the past where cases of non-storage or availability of data** and proper records with intermediaries and service providers have been identified.
        - These guidelines **will streamline the date records** to be maintained and proper reporting of security incidents to CERT-In.
- **Address the Users Right to Know:**
    - End-user has the right to know if their data is loaded so that an individual can protect himself from fraud transactions, fake loans, ID misuse etc.
        - Government should also force companies to inform their users within 24 hours of the incident.
    - Many users are still unaware if their **KYC (Know Your Customer)** and financial data is safe or not.

What are Government Initiatives for Cyber Security?

- Cyber Surakshit Bharat Initiative
- Cyber Swachhta Kendra
- Online cybercrime reporting portal
- Indian Cyber Crime Coordination Centre (I4C)
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- **Information Technology Act, 2000**
- **National Cyber Security Strategy 2020**

Way Forward

- India is the **one of the fastest digital adapters** among 17 of the most-digital economies globally, and rapid digitisation does require forward-looking measures to boost cybersecurity.
- It is **important for the corporates or the respective government departments to find the gaps in their organisations** and address those gaps and create a layered security system, wherein security threat intelligence sharing is happening between different layers.
- There is a **need for an apex body to ensure operational coordination** amongst various agencies and ministries.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Ans: (d)

- According to section 70B of the Information Technology Act, 2000 (IT Act), the Union Government by notification should appoint an agency named Indian Computer Emergency Response Team (CERTIn) to serve as the national agency for incident response.
- The Union Government under section 70B of the IT Act, 2000 established and notified rules of CERT-In in 2014. According to Rule 12(1)(a), it is mandatory for service providers, intermediaries, data centers and corporate bodies to report cyber security incidences to CERT-In within a reasonable time of occurrence of the incident. Hence, 1, 2 and 3 are correct. Therefore, option (d) is the correct answer.

Source: TH