Challenges to India’s Cyber Security

For Prelims: Hacking**,** Phishing, Cyber Security, Computer Emergency Response Team, India (CERT-IN), Information Technology (IT) Amendment Act 2008, **SWIFT system**, UPSC CSE PYQ.

For Mains: Challenges related to India’s Cyber Security.

Source: TH

Why in News?

A critical vulnerability that exposed the personal details of VVIPs, including top industrialists, celebrities and sports personalities in the country, has been fixed by the Ministry of Corporate Affairs 10 months after a cybersecurity expert flagged the issue.

- The cybersecurity flaw was initially identified by a Cybersecurity Expert who reported the issue to the **Computer Emergency Response Team, India (CERT-IN).**
- Despite the alert, the vulnerability persisted for several months, raising concerns about potential data theft or misuse.

What is CERT-In?

- **About:**
  - CERT-In is the national nodal agency responsible for **handling cyber security threats,** such as Hacking **and** Phishing. **It operates under the Ministry of Electronics and Information Technology.**
  - CERT-In has been operational since January 2004.
- **Functions of CERT-In:**
  - According to the **Information Technology (IT) Amendment Act 2008**, CERT-In has been designated to serve as the national agency to **perform the following functions 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, procedures, prevention, response and reporting of cyber incidents.
    - Such other functions relating to cyber security as may be prescribed.
- **Importance for India:**
  - CERT-In is important for India because it helps to protect **the country’s critical information infrastructure** and digital assets from cyber-attacks.
  - It also helps to enhance the cyber resilience and readiness of the country’s various sectors, such as government, defence, banking, telecom, etc.
  - It also contributes to the national security and economic development of the country by

promoting a safe and secure cyber environment.

What is Critical Information Infrastructure?

- **About:**
    - The **Information Technology Act of 2000** defines **Critical Information Infrastructure as a computer resource, the incapacitation or destruction of which shall have debilitating impact on national security,** economy, public health or safety.
    - The **government, under the IT Act of 2000, has the power to declare any data,** database, IT network or communications **infrastructure as CII** to protect that digital asset.
    - Any person who secures access or attempts to secure access to a protected system in violation of the law can be punished with a jail term of up to 10 years.
- **Protection of CIIs in India:**
    - **NCIIPC as Nodal Agency:**
        - Created in January 2014, the **National Critical Information Infrastructure Protection Centre (NCIIPC)** is the nodal agency for taking all measures to protect the nation's critical information infrastructure.
    - **Mandate of NCIIPC:**
        - It is mandated **to guard CIIs from unauthorised access, modification,** use, disclosure, disruption, incapacitation or distraction.
        - It will **monitor and forecast national-level threats to CII for policy guidance,** expertise sharing and situational awareness for early warning or alerts.
        - In the event of any threat to **critical information infrastructure the NCIIPC may call for information** and give directions to the critical sectors or persons serving or having a critical impact on Critical Information Infrastructure.

What are Challenges to India's Cybersecurity?

- **Critical Infrastructure Vulnerability:**
    - Power grids, transportation systems, and communication networks are **susceptible to cyber-attacks,** posing a threat to essential services and national security.
    - The attempted cyber attack on the **Kudankulam Nuclear power plant** in October 2019 highlights the potential risks to critical infrastructure.
- **Financial Sector Threats:**
    - The financial **sector is at a high risk of cyberattacks,** with cybercriminals targeting banks, financial institutions, and online payment systems.
    - Malware attacks, such as the one on City Union Bank's **SWIFT system** in March 2020, can result in financial losses, identity theft, and damage trust in the financial system.
- **Data Breaches and Privacy Concerns:**
    - As India transitions to a digital economy, the increased storage of personal and government data online raises the risk of data breaches.
    - The compromise of sensitive information, as seen in the **leak of Common Admission Test (CAT) data** in May 2021, can have severe consequences for privacy and security.
- **Cyber Espionage:**
    - India is a target for cyber espionage activities that aim to steal confidential information and gain a strategic advantage.
    - **Examples** include **Operation SideCopy in 2020,** where a Pakistani threat actor targeted Indian military and diplomatic personnel with malware and phishing emails.
- **Advanced Persistent Threats (APTs):**
    - APTs, characterised by **sophisticated and prolonged cyber attacks**, pose a challenge as they are difficult to detect and counter.
    - The targeting of **India's power sector by a China-linked APT group in February 2021,** with potential implications for power outages, underscores the severity of this threat.
- **Supply Chain Vulnerabilities:**

    - Weaknesses in software or hardware components used by government and businesses create supply chain vulnerabilities.
    - The **global cyberattack on SolarWinds in December 2020 affected Indian organizations, including** the National Informatics Centre **(NIC)** and the Ministry of Electronics and Information Technology **(MeitY).**

What are the Initiatives Taken for Cyber Security?

- **National Cyber Security Policy**
- **Cyber Surakshit Bharat Initiative**
- **Indian Cyber Crime Coordination Centre (I4C)**
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)**
- **Defence Cyber Agency (DCyA).**

Way Forward

- India's primary legislation governing cyber crimes is the **Information Technology (IT) Act of 2000,** which has been amended several times to address new challenges and threats.
- However, the **IT Act still has some gaps and limitations**, such as the lack of clear definitions, procedures, and penalties for various cyber offences, and the low conviction rate of cybercriminals.
- India **needs to enact comprehensive and updated laws** that cover all aspects of cyber security, such as cyber terrorism, cyber warfare, cyber espionage, and cyber fraud.
- **India has several initiatives and policies to improve its cyber security,** such as the **National Cyber Security Policy**, the **Cyber Cells and Cybercrime Investigation Units**, the **Cyber Crime Reporting Platforms**, and the **Capacity Building and Training programs.**

UPSC Civil Services Examination, Previous Year Questions

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

1. Service providers
2. Data centers
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)

Exp:

- 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.