Strengthen cyber security the right way

Why in news?

Indian Computer Emergency Response Team (CERT-In) has issued directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under Section 70-B(6) of Information Technology Act 2000.

What are the new directions issued by CERT-In regarding Cyber security?

- Synchronisation of computer clocks to the network time protocol set at the National Physical Laboratory and National Informatics Centre (NIC).
- Mandatory reporting of all cyber incidents within 6 hours of noticing or being brought to their notice in the prescribed format.
- Designating point of contact and notifying CERT-In.
- Perform the actions notified by CERT-IN for cyber security mitigation.
- Maintain all logs of all ICT systems up to 180 days within Indian jurisdiction.
- Data centres, virtual private network service providers, cloud service providers and virtual private server providers has to maintain all records of their users and usage for a minimum of 5 year even after the cancellation or withdrawal of registration.
- The virtual asset industry too will have to maintain all KYC records and details of all financial transactions for five years.

Why new directions are issued?

- CERT-IN has been struggling to get information and incident reporting from service providers, intermediaries as per section 70B(4) of the IT Act.
- This was impacting its responsibility as a collector, analyser and disseminator of information on cyber incidents as well as coordinating incident responses and emergency measures.

What are the concerns raised regarding these new directions?

- **Unrealistic deadlines -** A window of 60 days has been provided before implementation of these compliances begins. Given the scale of the revamp, this might be too short a window.
- Multiple companies even from the MSME sector will take time to set up systems for compliances.
- Recruitment of additional manpower for compliance may take far longer.
- Also penalty for non-compliance is stiff (including up to one year of imprisonment and monetary fines).
- **Additional data storage requirement -** At present, most entities maintain logs for around 30 days. To maintain logs for 180 days, the additional data storage device cost would be huge.
- To maintain the data for 5 years the compliance cost is going to rise substantially.

- **Data localisation -** Many entities having offshore servers have to shift their servers geographically in line with the government's objective of localising data storage.
- **Privacy concerns -** VPNs and virtual asset wallets are being asked to store and share KYC and transaction data. This raises privacy concerns.
- VPNs have been successful for corporates as well as individuals because they address privacy concerns.
- **Incidents to be reported -** The directions do not differentiate between the scales and nature of the incident to be reported.
- An organisation might receive hundreds of phishing emails and the effort to notify each would drastically increase their compliance cost.
- In the absence of data protection law there is ambiguity on which information can be held back or how his sensitive personal information is being protected.

Reference

https://indianexpress.com/article/opinion/columns/strengthen-cyber-security-right-way-7920843/