FAQs

Cyber attacks

Q What is the context ?

A The Ministry of Electronics and Information Technology is likely to come out with new cyber security regulations which will put the onus on organisations to report any cybercrime that may have happened against them, including data leaks.

Q What are damages inflicted by the cyber crimes ?

A

- Apart from private firms, government services, especially critical utilities, are prone to cyber attacks and breach incidents.
- The ransomware attack against the nationwide gas pipeline in 2021 in the U.S. virtually brought down the transportation of about 45% of all petrol and diesel consumed on the east coast.
- If it were measured as a country, then cyber crime — which is predicted to inflict damages **totalling $6 trillion globally in 2021** — would be the world's third-largest economy after the U.S. and China.

SRIRAM'S IAS®

Q What are provisions for reporting the cybercrime ?

A

- **Clause 25 in the Data Protection Bill 2021** says that data fiduciaries should report any personal and non-personal data breach incident **within 72 hours of becoming aware of a breach.**
- **Clause in EU GDPR:** Even the golden standard for data protection, namely the **European Union General Data Protection Regulation (EU GDPR),** has a clause for reporting data breach incidents within a stringent timeline.
- This, in principle, is likely to improve cyber security and reduce attacks and breaches.

Q Why reporting cybercrime is important ?

A

- **Alerting other organisations:** If incidences are reported, the **Indian Computer Emergency Response Team** and others can alert organisations about the associated security vulnerabilities.

FAQs

- **Precautionary measures:** Firms not yet affected can also take precautionary measures such as **deploying security patches** and improving their cyber security infrastructure.
- **Why firms are reluctant to notify the crime?** Any security or privacy breach has **a negative impact on the reputation** of the associated firms.
- An empirical study by Comparitech indicates that the share prices for firms generally fall around 3.5% on average over three months following the breach.
- So, firms **weigh the penalties** they face for not disclosing the incidents versus the potential reputational harm due to disclosure, and decide accordingly.

Q What are Possible solutions ?

A

- **Periodic cyber security audits:** How will the regulator come to know when a firm does not disclose a security breach?
- It can be done only through **periodic cyber security audits.**
- Unfortunately, the regulators in most countries including India **do not have such capacity to conduct security audits** frequently and completely.
- **Empanel third-party auditors:** The government can empanel **third party cyber security auditors** for the conduct of periodical cyber security impact assessments, primarily amongst all the government departments, both at the national and State level, so that security threats and incidents can be detected proactively and incidents averted.
- **Evaluation and Certification of cyber security:** The Ministry, as part of cyber security assurance initiatives of the Government of India, to evaluate and certify IT security products and protection profiles, has set up Common Criteria Testing Laboratories and certification bodies across the country.
- These schemes can be extended towards cyber security audits and assessments as well.
- **Security command centre:** Much like IBM, which set up a large cyber security command centre in Bengaluru, other large firms can also be encouraged to set up such centres for protection of their firms' assets.
- Such measures will also pass the muster of the EU GDPR, thereby moving India closer to the set of countries that have the same level of cyber security and data protection as that of EU, for seamless cross-border data flow.

SRIRAM's IAS®