Combat cybersecurity challenges

sanskritiias.com/current-affairs/combat-cybersecurity-challenges

(Mains GS 3 : Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security)

Context:

- India is dealing with the increase in cybersecurity threats by revamping its policies and focusing on existing systems, such as strengthening Cert-In, to address any challenges that come its way.
- Thus, the Ministry of Electronics and Information Technology is likely to come out with new cybersecurity regulations.

Report data breach:

- The essence of this regulation will be to put the onus on organisations to report any cyber crime that may have happened against them, including data leaks.
- 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.
- 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.

Continuing breach incidents:

- The new cybersecurity regulations, in principle, are likely to improve cyber security and reduce attacks and breaches.
- According to Cybercrime Magazine, 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.
- 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.
- Hence it is important that even cyber attacks on government and state-owned enterprises be reported so that corrective actions can be taken on the security of critical infrastructure of the nation.

Incidence reporting:

- Cybersecurity incidents are on the rise due to a combination of delayed awareness among people on the issue of cybersecurity, and a cybersecurity culture needs to be more developed so that more people causing [such issues] are aware of how to combat user harm.
- Thus, if incidents are reported, the Indian Computer Emergency Response Team and others can alert organisations about the associated security vulnerabilities.
- Firms not yet affected can also take precautionary measures such as deploying security patches and improving their cyber security infrastructure.

Reluctant to notify:

- Firms are reluctant to notify the breach incidents to the regulators because 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 and in the long term, breached companies underperformed in the market.
- After one year, share price of breached firms fell 8.6% on average, resulting in a poor performance in the stock market; so, firms weigh the penalties they face for not disclosing the incidents versus the potential reputational harm due to disclosure, and decide accordingly.

Enforcement of the regulation:

- The regulator came to know the important aspect of enforcement of the regulation and associated rules when a firm does not disclose a security breach.

- The periodic cyber security audits should be comprehensive enough to identify such incidents that might not have been reported by the firm.
- Unfortunately, the regulators in most countries including India do not have such capacity to conduct security audits frequently and completely.
- If either the probability of such audits is low or the probability of finding breach incidents during such audits is low, there is incentive for the firms not to disclose security attacks.

Way forward:

- Given the above complex nature of disclosure, the possible solutions apart from enacting rules are as followings-
- The government 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.
- The government can also mandate that periodic security audit reports be published by private firms and arrange to conduct surprise security audits towards enforcements.
- 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.
- 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.

IAS / PCS
Online Video Course
सामान्य अध्ययन
+
वैकल्पिक विषय
(इतिहास एवं भूगोल)
15% Discount for
Next 500 Students
Online
Learning
Programme
संस्कृति
IAS
JOIN NOW

IAS / PCS
Pendrive Course
सामान्य अध्ययन
+
वैकल्पिक विषय
(इतिहास एवं भूगोल)
15% Discount for Next
500 Students