Are we prepared for cyber attacks?

Why cyberspace is getting more vulnerable?

\n\n

\n
- The shortage of cash happened due to demonetisation has forced people to migrate to online transactions even for their smallest needs.
\n
- This **sudden uptake of online transactions** has exposed the existing security gaps in the system which make organisations as well as customers vulnerable to cyber attacks at this critical time.
\n

\n\n

How the term ‘security’ is often viewed?

\n\n

\n
- Security is seen as **just another layer to transact hassle-free** but it is imperative that security becomes embedded by design rather than as **a bolted add-on for payment gateways.**
\n

\n\n

In what ways can the cyberspace be exploited?

\n\n

\n
- The existing security gaps are ready ground for cyber-criminals to exploit. There are various ways of doing this:\n\n
\n
  - by introducing a malicious bug into the system that can skim through privileged information.
\n
  - by introducing rogue applications to lure customers into downloading them.
\n
  - by intensifying hacking attempts and phishing attacks etc.,

\n
\n
\n

- According to research on strategic national measures to combat cybercrime, mobile frauds are expected to grow by to about 65% in India by 2017. About 46% complaints of online banking are related to credit or debit card fraud.
\n
- In the **absence of a proper understanding of the security infrastructure** and the right policies and assets to protect, businesses and organisations are at a risk.
\n
- India’s premier security agency, CERT, has already cautioned bankers and customers to adopt high-end security encryption.
\n

\n\n

In what ways can the cyberspace be strengthened?

\n\n

\n

- The data security infrastructure along with customer-redress mechanisms will have to be well thought of and the purview of IT laws for cybercrimes will have to be expanded to include mobile-wallet payment systems.
\n
- E-wallet firms will need to invest in the latest technologies to safeguard their gateways against cyber attacks which are quite sophisticated and advanced.
\n
- It is imperative that organisations develop a **comprehensive “business-driven” security model** that fully integrates with the security requirements keeping in mind the overall business goals and objectives of the company.
\n
- Such a model will help organisations chose their security investments to create the best possible balance between customers’ ease of use and cyber security.
\n

\n\n

What are the current policies and laws?

\n\n

\n

- **We already have strong cyber security guidelines in place** but they are not followed stringently, leading to a ‘gap of grief’.
\n

- The Government is mulling over the almost 15-year-old Information Technology (IT) Act to further strengthen cyber security infrastructure, following demonetisation.
\n
- The RBI has also recently sent out a cyber security framework to be followed by banks, covering best practices.
\n
- To help the Government achieve its goal of Digital India, the RBI has ordered all prepaid payment instrument issuers, which includes all RBI-authorised banks and NBFCs, to **get a special audit done of their systems by auditors of CERT-In** and comply with the audit report recommendations immediately.
\n
- CISOs (chief information security officers) along with the board of directors now need to take tough decisions to address the business impact of a cyber-attack.
\n

\n\n

Conclusion:

\n\n

\n
- It is evident that the **threat landscape is evolving continuously** and the complex layers make cyber security a challenge.
\n
- The Government's push for stronger cyber security infrastructure is a welcome move, although we still have a long way to go. The illusion of protection from cyber attacks is a thing of past, no one is secure.
\n
- How we minimise the impact with continuous monitoring, early detection and quick response is the key in the world of digital economy. An attack is imminent. It is now up to the organisations to prioritise their cyber security needs and act on it.
\n

\n\n

\n\n

Category: Mains | GS – III | Internal Security

\n\n

Source: Business Line

\n

