Cyber Attack Concerns

What is the issue?

\n\n

Indian banks and capital market participants have cyber risk management plans at an institutional level.

\n\n

What are the cyber risks faced by capital market?

\n\n

\n
- Emerging technologies and waves of digitisation have brought in their wake new challenges and exposed organisations to new risks.
\n
- It is estimated that cyber-attacks cost companies an estimated $500 billion in damages every year.
\n
- The primary concern facing organisations is that security breaches to technology and physical infrastructure could lead to data loss, financial losses, regulatory sanctions, reputational damage, operational disturbances, among other things.
\n
- Increasing global interconnectedness and the complexity of systems make large-scale cyber-attacks on financial market infrastructure even more pertinent and threaten the stability of financial markets.
\n

\n\n

What measures are planned to address such issues?

\n\n

\n
- The strategies adopted for cyber risk management currently focus on reducing the risk of a cyber-attack and minimising the impact of a breach.
\n
- There are also plans for building resilience, that is, detecting and

recovering quickly from the impact of a breach.
\n
- Globally, organisations are investing in developing a comprehensive set of cyber risk management capabilities that cover the entire value chain and ensure the risk is efficiently managed across the ecosystem.
\n

\n\n

What measures were taken by government in this regard?

\n\n

\n
- Indian regulators have focused on cyber security as a core concern for several years now.
\n
- Securities market regulator, the Securities and Exchange Board of India, issued guidelines on cyber security and cyber resilience to market infrastructure providers in 2015 and developed guidelines for registrars in 2017.
\n
- In 2016, the RBI released a comprehensive set of requirements for internal cyber security frameworks.
\n
- The government has also undertaken initiatives including the Information Technology Act, 2000.
\n
- It has set up the nodal cyber security agency, CERT-In, to respond to computer security incidents.
\n
- The National Critical Information Infrastructure Protection Centre, is the central agency to facilitate safe, secure and resilient information infrastructure for critical sectors of the economy.
\n

\n\n

What measures Indian Industries must take?

\n\n

\n
- Traditional approaches to cyber risk mitigation have failed thus far and organisations are investing in identifying new approaches that include the use of advanced cloud-based SaaS services and platform-based

approaches to security risks.
\n
- Many of India’s leading banks and capital market participants have a well-defined plan for cyber risk management at the institutional level.
\n
- However, Indian Industries can take a few steps to ensure greater effectiveness of cyber security plans.
\n
- Industries should also consider the adoption of a common set of standards by capital market participants.
\n
- They should continuously strengthen IT governance, review policies, processes and systems to keep pace with changing risks and attack vectors.
\n
- Apart from these measures it is important to increase the collaboration among financial institutions.
\n

\n\n

\n\n

Source: Business Standard

\n