Cyber Attack on Indian Agencies

Why in news?

\n\n

There was a major technical snag in NSE that forced suspension of equity trading for nearly three hours.

\n\n

What happened?

\n\n

\n
- NSE’s cash segment could not open normally in the morning due to “technical reasons”.
\n
- The derivative segment was also shut down immediately after as it is not possible to continue trading in derivatives while the cash segment is shut.
\n
- After two false starts, trading resumed mid-day.
\n
- The halt has an estimated trade loss of about 7000 crores.
\n
- This is currently being investigated on the lines of a “possible cyberattack.”
\n

\n\n

What is a cyber-attack?

\n\n

\n
- Cyber-attack is any type of offensive plan that targets computer information systems by malicious acts from an anonymous source.
\n
- It is to either steal, alter, or destroy a specified target by hacking into a susceptible system.
\n

\n\n

\n
- These can be labelled as either a cyber-campaign, cyber warfare or cyber terrorism in different context.
\n
- Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations
\n

\n\n

What are the events of cyber-attacks in India?

\n\n

\n
- 72% of Indian companies faced cyber-attacks in 2015.
\n
- There has been an exponential rise in Ransomware cases in the last one year.
\n
- In 2016, security codes of around 32 lakh debit cards were breached.
\n
- Several users reported unauthorised transactions from locations in China.
\n
- There are increasing number of data thefts among the civilians.
\n

\n\n

What are the recent attacks?

\n\n

\n
- The recent attack created cyber security threats to major Indian companies RJio, Airtel and NSE
\n
- **RJio -** Personal data such as Aadhaar details of the telecom users has been published in a website.
\n
- **Airtel -** The Radio Access Network went down for more than an hour in and around Delhi.
\n
- There was a network outage in Delhi/NCR and one of the network nodes had been corrupted.
\n

\n\n

What is the reason for the vulnerable cyber systems?

\n\n

\n
- Various telecom giants are using the telecom products which are manufactured from china.
\n
- Lack of importance given by government and private sectors in appointing cyber security professionals.
\n
- No proper understanding about the cyber space.
\n
- No ridged bilateral policies on cyber-attacks.
\n
- No Stronger framework to trace or punish the offenders.
\n

\n\n

How cyber issues can be addressed by the government?

\n\n

\n
- The Home Ministry is preparing an internal cyber security policy as it is required under the national plan.
\n
- The government already started working on a customised cyber security policy for each ministry and department.
\n
- Strong MO U’s on Cyber security should be made between various agencies and neighbouring nations.
\n
- The exchange needs to have plans to handle minor malfunctions that affect one segment of trading.
\n
- The Securities and Exchange Board of India, needs to include trading back-up, channels of communication and investor redress mechanisms.
\n

\n\n

Quick facts

\n\n

Indian Computer Emergency Response Team

\n\n

\n
- (CERT-In) is an office within the Ministry of Electronics and Information Technology.
\n

\n\n

\n
- It is the nodal agency to deal with cyber security threats like hacking and phishing.
\n
- It strengthens security-related defence of the Indian Internet domain.
\n
- They exchange information on prevalent cyber security policies and best practices.
\n
- There are MoUs signed between nations by this agency.
\n

\n\n

Ransomware

\n\n

Ransomware is a type of malicious software that threatens to publish the victim's data or eternally block access to it unless a ransom is paid.

\n\n

\n\n

Source: The Hindu, Business Line

\n