Cyber Security Service Providers Invest in Technologies to Prevent Attacks

With cyber threats rising rapidly, there is an increase in demand for cybersecurity service providers and their products.

- The security service providers are investing in the latest technologies such as machine learning to predict and prevent attacks.
- There is also more focus on mobile security solutions as the penetration of smartphones has increased.

Background

> According to the 'State Of Endpoint Security Survey', 90 per cent of the businesses in India have been either hit or are expected to be hit by ransomware.

NOTE: Ransomware is a form of malicious software (or malware) that could take over and affect a system usually by denying access to the owner's data. The attacker demand service or ransom, usually in the form of payment from the victim, to restore access to the data. Some examples of ransomware are wannacry, Petya etc.

- The survey also found that traditional security is no longer enough to protect against the evolving ransomware threats.
- Large enterprises are now investing almost 10-15 per cent of their IT spend on cybersecurity.
- The cybersecurity market, estimated to be Rs 1,000 crore is projected to grow at the rate of 19 per cent between 2018-2023.
- However, challenges also exist as evolving technologies give rise to new business models that increase the level of cyber attacks.

Way Forward

> Firms and cybersecurity providers must invest more in infrastructure and use advanced technologies such as Artificial Intelligence (AI) and machine learning (ML) to trap more malwares.

Artificial Intelligence (AI) is the ability of machines to learn and reason through analogy, analyse, interpret information, recognise speech, visual perception and take decisions. In other
words, AI is the application of human intelligence by the machines.
Machine learning is the ability to get computers to act without being explicitly programmed. For instance, machines like computers can analyze and interpret information and derive logical inferences and the outcomes are self-driving cars, practical speech recognition, effective web search etc.

> Using technologies such as AI and ML to use the past data to learn the different patterns of cyber attacks and also incorporate the global attack pattern will help in making the detection more precise and intelligent.