Cyber Security

What is the issue?

\n\n

McKinsey report says, "Despite years of effort, and tens of billions of dollars spent annually, the global economy is still not sufficiently protected against cyber attacks and it is getting worse".

\n\n

What is the cyber scenario in developing countries?

\n\n

- Cyber crime has been called one of the biggest risks to data and security.
- UNESCO says that the increased threat of cyber attacks puts critical infrastructure, like the information systems of hospitals, air traffic control facilities, factories, police and military, of developing nations at risk.
- Developing nations which are in the throes of a technological revolution are catching up on modern technology, but the infrastructure for cyber security and cyber laws are either archaic or non-existent.
- Countries like India are bringing millions of people online, but the **security infrastructure is just not ready.**
- For emerging digital economies, another risk is that hacking attacks and online fraud can **deter people from using e-commerce or e-payments.**
- Added to that is the fact that Indian data protection laws are inadequate and only address some security, and privacy issues. Meanwhile cyber crime in the country is on a rise.
- The National Crime Records Bureau (NCRB) said in its 2016 report, that 11,592 cases of cyber crime were registered in India in 2015.

\n\n

What need to be done?

\n\n

\n
- We need to work fast on **building a security infrastructure** to insulate the billion strong population from cyber threats.
\n
- **A national level programme:** for cyber security and a budget for implementation. We need to develop standards and guidelines, and build capacity for laws and enforcement.
\n
- **Public and private institutions:** They must identify what their information assets are and which ones need protection.
\n
- **Cyber experts:** Have to be employed to understand the threat landscape and take a risk-based approach to identify impact. They will have to understand the functioning of departments and businesses, and prioritize information assets in need of protection.
\n
- **Preparedness:** Defence mechanisms need to be tested continuously to improve incident response. The Sony hack of 2014 for instance is a big lesson on the lack of preparedness.
\n
- **Educate users:** Users are known to click on links that they should not click on, or choose insecure passwords.
\n

\n\n

What is the way ahead?

\n\n

\n
- As a country, the biggest challenge to implement data security is to acknowledge that this is an issue for both the government and private sector.
\n
- At an organisational level it has to be **understood as a management issue and not just a tech issue.**
\n

\n\n

\n\n

Source: Live Mint

\n