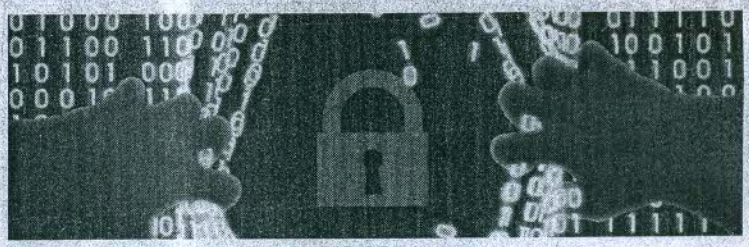
Business Standard 7 September, 2017

India needs local tools for cybersecurity

Creation of indigenous tools, niche workforce imperative to secure cyberspace: Experts



PRESS TRUST OF INDIA
6 September

India requires locally developed tools and niche workforce to protect its cyberspace, according to experts.

"Creation of indigenous tools along with building human capacity with relevant capabilities is imperative to secure India's cyberspace," a joint report by Assocham and PwC on Securing the Nation's Cyberspace said.

While the government should create a robust policy environment, and ensure adequate technology support, businesses should not limit its efforts towards cyber resilience merely for compliance, but practice self-regulation, the report noted.

"It is critical that all economic participants in a country pay attention to cyber security and develop adequate measures to identify, protect, detect, respond and recover processes and capabilities in the face of threats. "Businesses today need to urgently and proactively invest in it," Sivarama Krishnan, partner and leader — cybersecurity, PwC India, said.

Citizen participation in mitigating cyber risks is also becoming increasingly important, the report noted. Promoting a cyber safe culture within citizens for responsible cyber behaviour will be key to ensuring security of India in cyberspace, it further said.

The report stressed on the need for an inclusive approach to create a secure business ecosystem, where the Government, industry sectors, standard bodies and business all have to play their role in creating a secure environment. "Apart from the government and enterprises, India's academic institutions also have a key role to play in this fight for cybersecurity.

"Academia and industry need to collaborate to generate interest and find innovative solutions to cyber security issues. This collaboration is also needed to ensure India has the trained manpower needed to implement its cyber strategies, according to Krishnan.

DIGITAL TRENDS IN INDIA

- **1.1 bn** telephone subscribers (second largest in the world)
- **241 mn** Facebook users
- **1.15 bn** digital IDs (largest national ID programme)
- **463 mn** internet users (second largest in the world)

WHAT OTHER COUNTRIES ARE DOING

- The US Homeland Security Department has released cybersecurity guidelines for the manufacturing sector
- The Monetary Authority of Singapore has released guidelines for strengthening system security and risk management for technology-enabled systems of financial institutions
- The US has spearheaded various sectoral Information Sharing and Analysis Centres. The ISACs collect, analyse and disseminate actionable threat information to mitigate the identified risks
- South Korea's CERT and Coordination Centre have been organising cybersecurity drills for the past 10 years with the aim of testing for security

The Asian Age

7 September, 2017

CYBER | DEFENCE

Businesses need to be proactive and not just comply, says study

India needs to build local cyber security tools

Mumbai, Sept. 6: India requires locally developed tools and niche workforce to protect its cyberspace according to experts.

"Creation of indigenous tools along with building human capacity with relevant capabilities is imperative to secure India's cyberspace," a joint report by Assocham and PwC on Securing the Nation's Cyberspace said.

While the government should create a robust policy environment and ensure adequate technology support, businesses should not limit its efforts towards cyber resilience merely for compliance, but practice self-regulation, the report noted.

"It is critical that all economic participants in a country pay attention to cyber security and develop adequate measures to identify, protect, detect, respond and recover processes and capabilities in the face of threats.

"Businesses today need to urgently and proactively invest in it," Sivarama Krishnan, partner and leader — Cyber Security, PwC India, said.

Citizen participation in mitigating cyber risks is also becoming increasingly important, the report noted. Promoting a cyber safe culture within citizens for responsible cyber behaviour will be key to ensuring security of India in cyberspace, it said.

The report stressed on the need for an inclusive approach to create a secure business ecosystem, where the Government, industry sectors, standard bodies and business all have to play their role in creating a secure environment.

"Apart from the government and enterprises, India's academic institutions also have a key role to play in this fight for cyber security.

"Academia and industry need to collaborate to generate interest and find innovative solutions to cyber security issues. This collaboration is also needed to ensure India has the trained manpower needed to implement its cyber strategies, according to Mr Krishnan. — *PTI*

It is critical that all economic participants in a country pay attention to cyber security and develop adequate measures to identify, protect, detect, respond and recover processes and capabilities in the face of threats.

— Joint report by Assocham and PwC