

Suggested Cyber Security Solutions

R.Ramamurthy, Chairman,

Cyber Security & Privacy Foundation

15.12.2015

Cyber threats

Identity theft

- Data theft
- Phishing
- Social media abuses
- Cyber terrorism
- Compromised digital certificates
- Advanced Persistent Threats
- Hactivism, botnets, supply chain attacks
- Distributed denial of service DDOS
- Compounded threats concerned with mobile devices and smart phones, virus attacks

Key drivers

- Information & Communication Technology
- Nanotechnology
- Biotechnology
- Cognitive science
- Internet of Things
- Virtualisation
- Cloud Computing
- Big Data
- 3D printers

NATIONAL CYBER SECURITY POLICY

- PROTECT INFORMATION AND INFORMATION STRUCTURE
- BUILD CAPABILITIES TO PREVENT AND RESPOND TO CYBER THREATS.
- REDUCE VULNERABILITIES AND MINIMIZE DAMAGE FROM CYBER INCIDENTS.
- THROUGH A COMBINATION OF INSTITUTIONAL STRUCTURES, PEOPLE, PROCESSES, TECHNOLOGY AND COOPERATION.

Key issues

- Need – 5,00,000 of cyber security professionals are needed in India by 2018, which is planned to be done by capacity building, skill development and training
- Availability – Current #s including the public and private sector is 30,000.
- Stigma attached to the word hacking
- White hat hackers are not given their due respect and recognition of their expertise.

Suggestions

- Recognition by the Govt
- Govt. should come up with cyber treaty with other countries.
- Internet should not become a base for anti-nationals & terrorists.
- Beware of Cyberwarfare invasions.
- Anonymous cyber invasions felt cost effective than traditional attacks
- Our formation of Cyber Command
- Mobile phones menace

Suggestions – contd.

- Increase Cyber-awareness among police personnel
- Corporate reticence in reporting Cyber Crimes
- Mafia and insider threats.
- Banks are shy of negative visibility
- Penetration Testing and Vulnerability audits / assessments
- Cyber Insurance must be encouraged
- Secure Coding
- More usage of Open Source programmes.
- Conclusive remarks