Deloitte.

NASSCOM®

Cyber Security:

Are digital doors still open?

November 2017

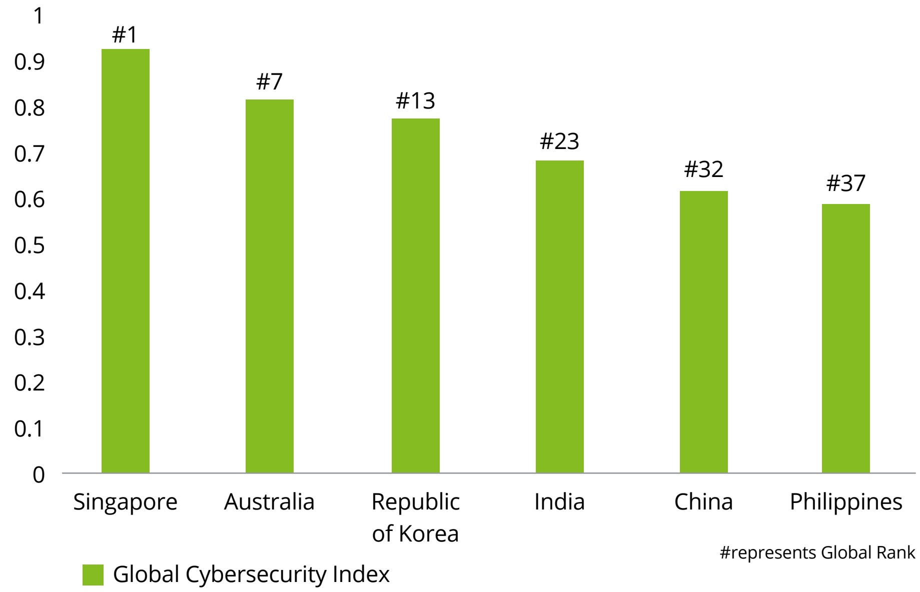
Introduction

Security is becoming a rapidly evolving and complex issue that various organizations are contending with today. It continues to be one of the most pressing challenges faced by Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) today. With the increasing impact of social media, smart devices and mobility, organizations are becoming more vulnerable to fraud and privacy breaches. Globally, security has risen to be one of the top concerns in almost all areas from defence, corporate organization, smart cities, etc.

With the increasing volume of data generated by organizations, instances of cyber-attacks, loss of sensitive information, and security breaches are becoming increasingly common. Increasing internet penetration is leading to expansion of cyber space which in turn is leading to increasing attacks on sensitive intellectual property. This has resulted in the transformation of the IT landscape at a very rapid pace.

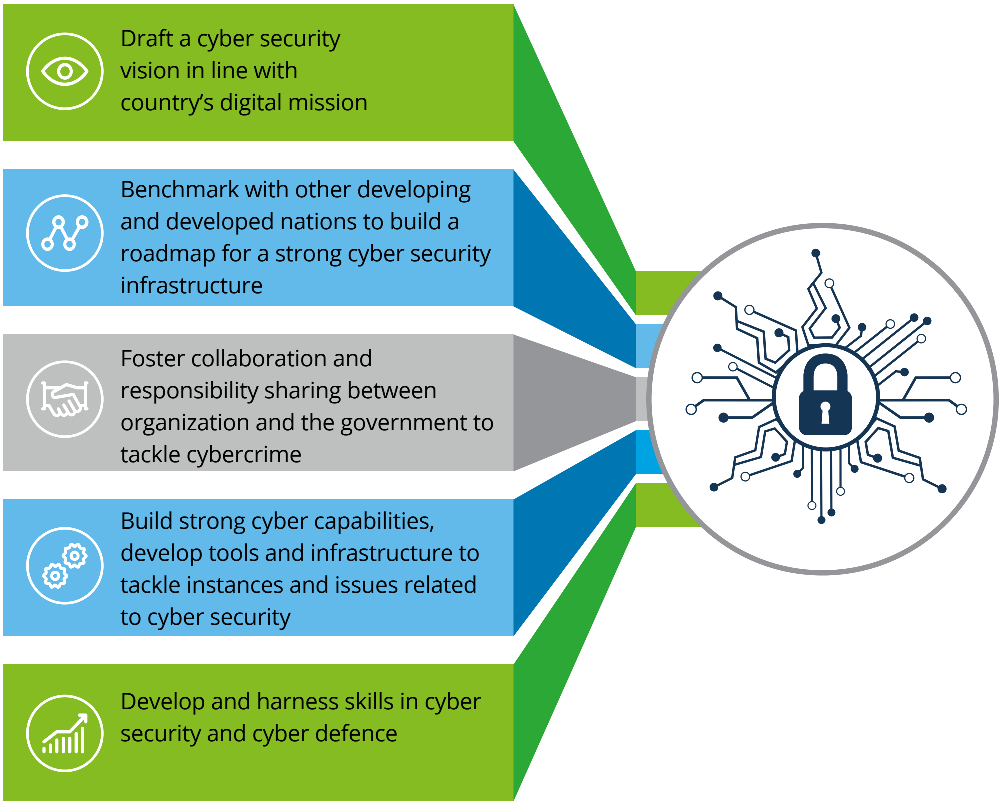
According to The Global Cyber Security Index released by the UN telecommunications agency International Telecommunication Union (ITU) in 2017, only about half of all countries have a cybersecurity strategy or are in the process of developing one. The index, which saw India at 23rd position, was topped by Singapore at 0.925. India has also been ranked fourth globally among the countries most affected by ransomware.

Global Cyber Security Index by International Telecommunications Union (ITU), 2017



#represents Global Rank

Key considerations for an effective cyber security strategy



Draft a cyber security vision in line with country's digital mission

Benchmark with other developing and developed nations to build a roadmap for a strong cyber security infrastructure

Foster collaboration and responsibility sharing between organization and the government to tackle cybercrime

Build strong cyber capabilities, develop tools and infrastructure to tackle instances and issues related to cyber security

Develop and harness skills in cyber security and cyber defence

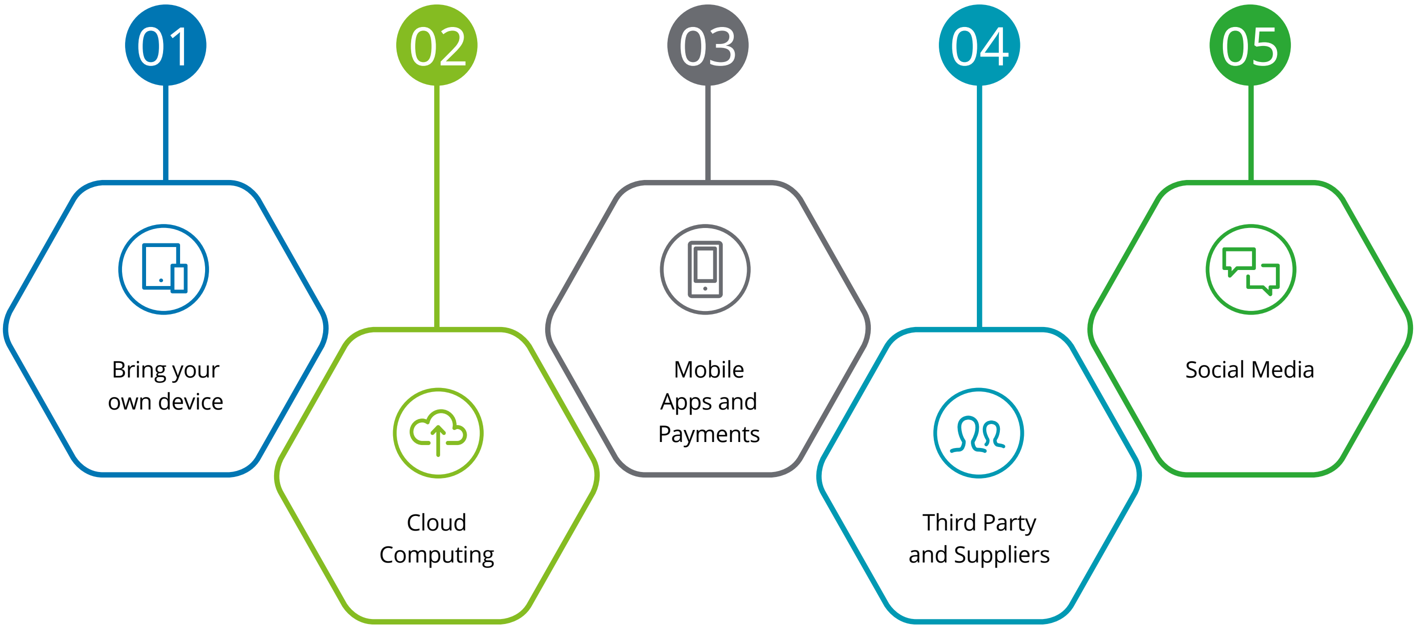
Source: Industry Reports

> "Today, it's not a question of "if," but rather "when" your network will be breached."

Trends Resulting in Increased Focus on Cyber Security

Security is becoming a growing concern for organizations across domains due to increasing instances of cyber-attacks and changing technology landscape, consumer behavior and regulatory requirements. Some trends which lead to increased focus on cyber security are listed below:

Trends leading to focus on Cyber Security



01 Bring your own device

02 Cloud Computing

03 Mobile Apps and Payments

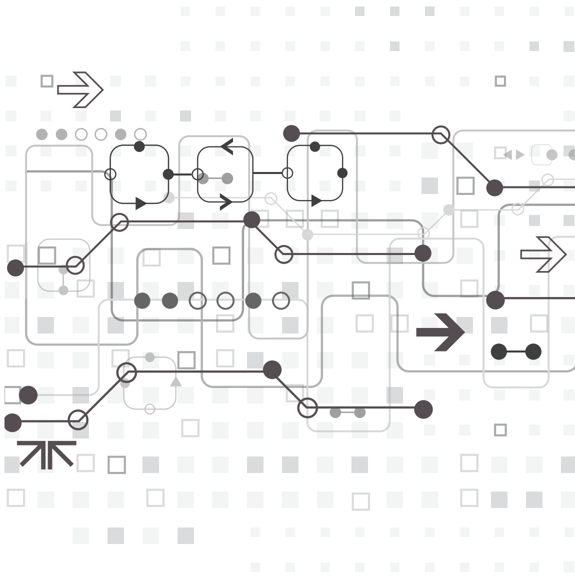
04 Third Party and Suppliers

05 Social Media

Source: Deloitte Report – Digital Revolution Forward Path for Telecom

Bring You Own Device (BYOD)
Today, employees own powerful devices (smartphones, tablets) in order to fulfill their requirement of working anytime and anywhere and handle most of the business activities related to emails, documents, spreadsheets, etc. These devices are also used for extensive use of social media and accessing data stored on cloud. Use of business data and personal applications on a single device makes the device an easy target for attackers. There is an increased risk due to these devices since a large number of them are not managed by the organization's IT department.

Cloud Computing
Many organizations make use of cloud computing for their applications and data. This may lead to ease of use but often trumps security if it is not managed well. Since it is difficult to determine the physical location of the data stored in the cloud we might not know which regulations apply to it. Applications and data managed from outside the organization through cloud increases the organization's vulnerability to security risks.



Third Parties and Suppliers

Today, in this world of outsourcing, digital supply chains and cloud computing, organizations are more dependent than ever on third parties. This results in organization’s data being shared and exposed in ways which are difficult to control. A breach in the digital supply chain undermines the security of every organization involved in the chain.

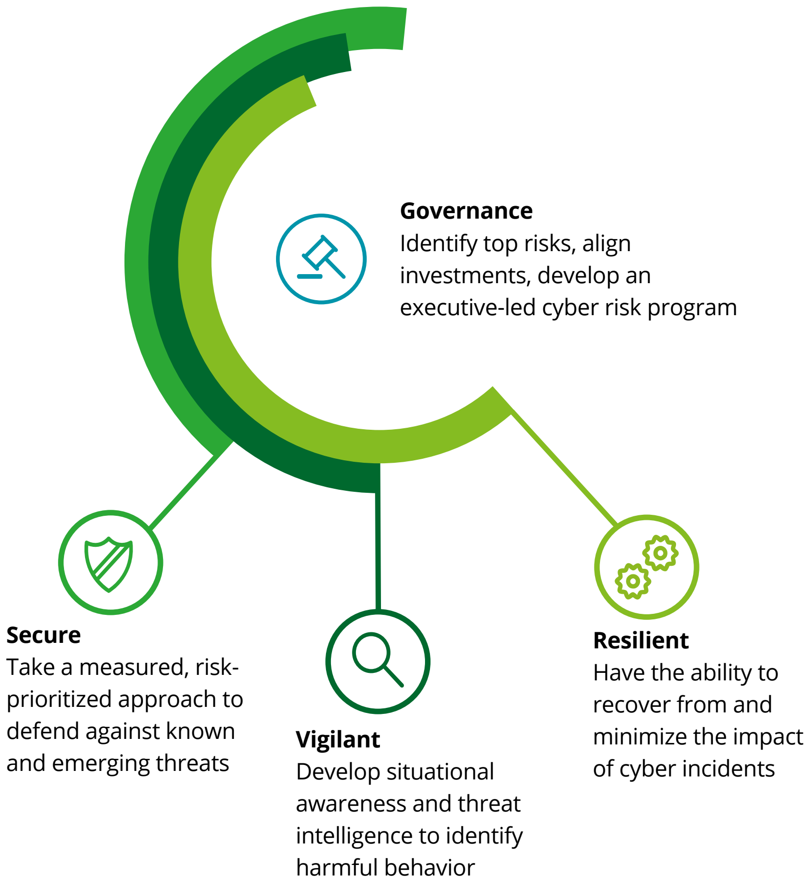
Mobile Apps and Payments

In order to grow the business, various organizations (like e-Commerce players etc.) are launching mobile applications for their users. They encourage users to make mobile payments. Authorities are promoting payment through mobile/digital means instead of cash. Though this is a valuable proposition for all stakeholders, inclusion of monetary transactions could increase the cyber risk exposure.

Social Media

Use of social media has increased drastically over the last few years. Increasing internet infrastructure and data availability, decreasing data charges and advent of cheaper smartphones have enabled the users to access social media and share information more frequently. Such increase in sharing of information has resulted in revealing sensitive information posing privacy-related issues.

Cyber Security Capabilities



Governance
Identify top risks, align investments, develop an executive-led cyber risk program

Secure
Take a measured, risk-prioritized approach to defend against known and emerging threats

Vigilant
Develop situational awareness and threat intelligence to identify harmful behavior

Resilient
Have the ability to recover from and minimize the impact of cyber incidents

Source: Deloitte Framework

Key Skill-sets

Cyber security skills landscape is large and still growing. There is high demand of cyber security professionals across domains. A diversified skill-set is required for a cyber-security professional. Some of the skills are listed below:

Cyber Security Skill Sets

Security

- IT Security
- Wireless Network Security
- Public Key Encryption Security
- Security Infrastructure
- Data Security
- Application Security
- Network Security
- Network Forensics

Data Analytics

- Big Data Expertise
- Hadoop
- SQL, SSAS, SSIS and SSRS
- SaS
- Predictive Analytics
- Machine Learning
- Stream Analytics
- Spark Streaming
- NoSQL Databases
- Data Mining

Cloud Computing

- Cloud solution architect
- Azure
- Amazon Web Services
- Kafka
- Kinesis
- Eventhub
- Cloud Native Application Development
- DevOps
- Linux
- Database Management

Networks & Architecture

- Networking Specialists
- System Architect
- LAN/WAN
- Design Modeling
- Network Capacity Planning
- Network Performance Planning
- Transmitters
- JIRA
- Confluence

Device Hardware

- Hardware Engineers
- Designing sensors and transmitters
- Experts in connectivity solutions
- Embedded Design
- ARM
- RFID Technology
- Circuit Design

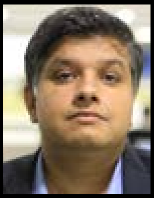
Source: Industry Reports

Conclusive Remarks

Though most organizations realize the importance of cyber security for their businesses and understand the associated risks, they often come short of a holistic, business-driven and threat-based approach to manage cyber risks. While securing assets is important, being vigilant and resilient in the face of cyber-attacks is imperative. Along with cybersecurity policies, tools, and practices, cultivating a cyber-risk aware culture across the organization will increase their ability to effectively manage emerging cyber risks.

Contacts

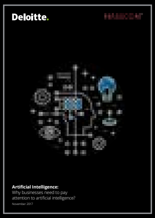
PN Sudarshan
Partner, FA
pnsudarshan@deloitte.com



Abhishek V
Partner, Consulting
abhishekv@deloitte.com

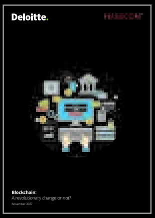
Gunjan Gupta
Director, Consulting
gunjangupta@deloitte.com

You might also like

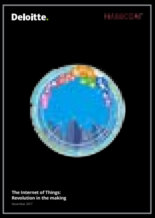


Artificial Intelligence:
Why businesses need to pay attention to artificial intelligence?

Augmented/Virtual Reality
Next Big Thing of Digital Environment



Blockchain:
A revolutionary change or not?



The Internet of Things:
Revolution in the making

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

www2.deloitte.com/in/

@DeloitteTMT