itsa 2018 India
India's IT Security Expo & Conference
www.itsa-india.com

Knowledge Partner Deloitte.

AN OVERVIEW OF THE CYBER-SECURITY INDUSTRY IN INDIA

NÜRNBERG MESSE

TABLE OF CONTENTS

EVOLUTION IN THE INDIAN CYBER SECURITY LANDSCAPE

Information and Communication Technologies (ICT) is fundamental to the economic growth of a nation in today's world. The rapid and unprecedented development of ICT and media has ushered in the digital age and has become the driver for economic progression. India's drive towards digital economy is fostered by key national initiatives such as Digital India, Smart Cities, National Broadband Network are changing the digital landscape, rapidly with direct impact on governance, transparency and accountability.

Technology and Information are the cornerstones of digital transformation. This transition to digital era has ushered in a new security paradigm at a national level and has brought to fore the challenges of cyber security. As India continues to aggressively pursue the Digital India vision, we continue to see significant data breaches and cyberattacks across all sectors. Prevention is possible, and that means prioritising our risks and focusing efforts to minimize those risks.

This white paper highlights our country's cyber security landscape in light of the changing threats, government initiatives, business priorities and investment opportunities.

Cybersecurity landscape in India has changed significantly in the past decade. Previously, basic virus protection and security controls were sufficient to deter threats. However, in the present times advanced security analytics tools are deployed to prevent advanced persistent threats (APTs) and tackle malicious insiders. Attackers too have evolved with time. Well-funded and technically adept attackers have the capability to bring an entire enterprise or sector to a halt – something that was unimaginable a decade or two ago.

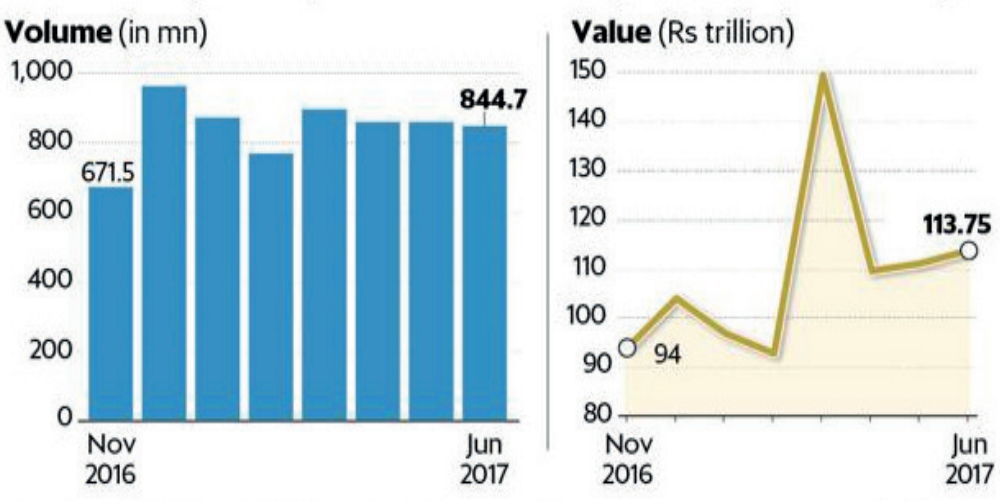
In this evolving digitally interconnected landscape, India is witnessing an increase in targeted attacks including state sponsored attacks against Indian businesses and enterprises of all sizes in the last 5 years. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), security incidents have increased from 44,679 in 2014 to 50,362 in 2016. In the first half of 2017 (till June) 27,482 cyber security incidents were already reported.

2016 has been a roller coaster ride in the Indian cyber security space. For instance, cyber breach news on debit cards, hack of recent social media accounts of known personalities and the security of personal data is in question. Post demonetization, while the use of online payment platforms have gone up so has the fraudulent misuse of payment networks including data theft.

The emergence of new services and applications, advanced technologies including cloud and IoT, is proving further impetus to the changing threat landscape in India. The National Association of Software and Services Companies (NASSCOM) reported that India aims to capture 20% of the market share in Internet of Things (IoT) by 2020 which is estimated to be worth USD 300 billion. Also, the big data sector is expected to reach a value of USD 16 billion by 2025, with India expected to be having a 32 percent share in the global market. This is driving companies to adopt more of analytical approach to predict, detect and effectively manage cybersecurity.

Governments across the globe are gearing up through policy enactments and necessary investments to fight the menace of rising cybercrimes. These policies and investments also assure citizens of their privacy rights in the cyber space.

Similarly India, with its economy pegged at INR 152.51 Lakh Crore (or USD 2.34 Billion) and 7.11 % GDP growth rate in 2016-2017 (expected GDP in 2017-18 fiscal being 7.2% and 7.7% in 2018–19) is rapidly integrating itself with Internet Economy, where transactions are predominantly carried out electronically. Digital payments have grown 55% by volume and 24.2% by value in 2016-2017. Cashless transactions are likely to reach the estimated target of 25 billion digital transactions in 2017-2018. While the Internet offers new means for expanding economic and business avenues, it is, subject to ever increasing dangers of cybercrimes. Individuals need legal protection to protect their personal rights and secure their transaction in cyber space.



Data in graphic till June 2017; figures include some of the payment systems managed by NPCI

Source: Reserve Bank of India

This requires setting up of an ecosystem that is capable of understanding new age complexities and offering swift response mechanisms. The ecosystem for cyber security and data protection necessitates and calls for a strong legal framework, proactive government initiatives, active involvement of and contribution by the industry and effective law enforcement.

To this effect, there are multiple initiatives embarked upon and key policies put in place by the Indian Government and Regulators in sectors such as Banking and Financial Services to meet the rising challenges of the Cyber Security. Some of the key elements for building an eco-system for cyber security and data protection are as follows:

GOVERNANCE AND POLICY INITIATIVES:

National Cyber Security Policy: 2013

The Government of India took the first formalized step towards cyber security in 2013, vide the Ministry of Communication and Information Technology, Department of Electronics and Information Technology's National Cyber Security Policy, 2013. The policy is aimed at building a secure and resilient cyberspace for citizens, businesses and our government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber-attacks, and minimize damages through coordinated efforts of institutional structures, people, processes, and technology.

Legal Framework for Cyber Security and Data Protection

The Indian IT Act 2000 provides a legal framework for electronic governance which was further amended in 2008. A set of data privacy rules were introduced in 2011 and appended to the Indian IT Act 2008.

On August 24, 2017 Honourable Supreme Court of India delivered a historic judgment that privacy is constitutionally protected right. Indian Constitution, through Article 21, guarantees its citizen right of privacy. In various judgments, Supreme Court of India upheld individual rights about privacy and fixed liability of offenders, and recognized constitutional right to privacy against unlawful government invasions. This brings India to the league of countries that have a legal regime for cyber security and privacy.

Regulatory Authorities

Taking into cognisance the increased risk exposure to cyberattacks due to the rapid technological developments, banking regulatory authority i.e. Reserve Bank of India (RBI) has issued the Cyber Security Framework guidelines for building a resilient cyber security framework.

In 2017, RBI issued guidelines urging the Non-Banking Finance Companies (NBFCs) to put in place a robust Information Technology framework, to ensure adequate IT preparedness on a continuous basis. Following suit, other regulatory bodies in the financial sector including Insurance Regulatory and Development Authority (IRDA) and Securities and Exchange Board of India (SEBI) have highlighted the urgent need to put in place cyber resilience framework including developing a cyber security policy for insurers and exchanges along with registrars (RTAs) respectively. This will ensure adequate cyber security preparedness among the organizations on a continuous basis.

Telecom Regulatory Authority of India (TRAI) released 'TRAI consultation paper' on August 9, 2017 focused on privacy, security and ownership of data in the telecom sector. Telecom Regulatory (TRAI) through its 'Do Not Call Registry' assures protection to consumers from telemarketers that potentially infringe the privacy of telecom customers.

Data Security Council of India (DSCI) is an industry body on data protection in India, setup by NASSCOM committed to making cyberspace safe, secure and trusted by establishing best practices, standards and undertaking initiatives in cyber security and privacy.

ROLL OUT OF INITIATIVES – BY BOTH GOVERNMENT AND PRIVATE SECTOR:

Government Initiatives:

Some of the initiatives undertaken by the government in the cyber security space have been listed below:

Computer Emergency Response Team, India (CERT-In) - Government of India has set up CERT-In as a nodal agency for incident management. This agency, through a dedicated infrastructure, monitors threats that affect computer systems, collaborates internationally for the incident response, tracks incidents affecting both public and private sector and issues security guidelines. CERT-In has signed MoUs with counterparts and similar organizations in other countries such as the United Kingdom, Korea, Canada, Australia, Malaysia, Singapore, Japan and Uzbekistan.

Crisis Management Plan - India has prepared a Crisis Management Plan (CMP) for countering cyberattacks and cyber terrorism for preventing the large scale disruption in the functioning of critical information systems of government, public and private sector resources and services.

'Cyber Swachhta Kendra' - To combat cyber security violations and prevent their increase, Government of India's CERT-in launched 'Cyber Swachhta Kendra' in February 2017. This initiative is a bot-net cleaning and malware analysis centre established to help detect bot-net infections in India and prevent further infections by notifying, enable cleaning and securing systems of end users.

National Critical Information Infrastructure Protection Centre (NCIIPC) - Article 70A (IT Act 2008) mandates the need for a special agency that will look at designated critical infrastructure and evolve practices, policies and procedures to protect them from a cyber-attack. To this effect, the NCIIPC was established and placed under the technical intelligence agency called the National Technical Research Organization (NTRO). Its primary objective is, to roll out counter-measures in cooperation with other security agencies and private corporate entities that man critical sectors.

National Cyber Coordination Centre (NCCC) – NCCC is an operational e-surveillance and cyber security agency in India. This has been set up primarily for cybercrime prevention strategy, cybercrime investigation training, review of outdated laws, etc.

Cyber Security Awareness - Looking at the growing importance of Information Security, Department of Information Technology (DIT) has formulated and initiated the Information Security Education Awareness (ISEA) program. This program relies on the education exchange program, security research in engineering and PhD program, train system administrators/ professionals, and train government officers.

Cyber Forensics - Under the Directorate of Forensic Science, a part of Ministry of Home Affairs, three Central Forensic Labs (CFSLs) have developed capabilities in cyber forensics. Also, there are 28 State Forensic Labs (SFSLs), now acquiring capabilities in cyber forensics techniques and skills. Resource

Centre for Cyber Forensics (RCCF) at Thiruvananthapuram has been established with the objective to develop cyber forensic tools and to provide technical support and necessary training to Law Enforcement Agencies in the country.

Cyber Policy Research Centre – Is a global think tank funded by the government/ Industry, for studying all facets of cyberspace and making policy recommendations to the government. The Cyber Policy Research Centre has the following objectives:

- Conducting Research and Publishing papers on important issues concerning cyberspace;
- Suggesting public policies to address the above issues;
- Disseminating balanced information on cyber issues;
- Initiating public debate on important cyber issues; and
- Organizing seminars, training sessions and conferences on cyber issues.

Private Sector Initiatives:

Indian businesses can no longer evade the truth that Digital has become the need of the hour and the most effective enabler for creating a differential and unique competitive advantage. Organizations are still struggling with the complexity that comes with deploying digital initiatives in spite of the intent shown towards the digital vision.

For any organization, the digital touch points typically comprises of four main components – customer, employee/business partners/ third party, data and assets. The interaction of these components in an enterprise is through websites, social media, mobile devices, cloud, Internet of Things (IoT) and advanced technologies. As per Deloitte , organizations are channelizing their spends to address the key risk areas in the digital ecosystem i.e. strategic, technology, operations, third party, regulatory, forensic, cyber, resilience, Data leakage and privacy.

Organizations are spending on initiatives including developing skill sets in some of the key areas using a combination of in-house, cloud service and consultants. Few of these key areas are highlighted as follows:

- Application Security;
- Compliance to regulatory requirements including changing privacy laws;
- Data Security to ensure protection of data across the digital ecosystem at various stages of data; life-cycle i.e. data in use, data in transit and data at rest;
- Training and Awareness to employees as well as third parties;
- End point administration and Incident Response; and
- Intelligence/analytics.

Cyber threats have evolved swiftly from virus attacks to sophisticated malware and advanced denial of service attacks. India will continue to face increasingly sophisticated and destructive cyber threats as compared to the disruptive attacks that are currently adding up to 200 plus million malware-related intrusions in any given week. Sectors high on the priority list of cyber criminals are banking, energy, telecom and defence, along with the government, account for three-fourths of all cyber-attacks. Some of the key focus areas for organizations across all industrial sectors in 2017 is as follows:

India's scenario on security

Key focus areas for organizations across all industrial sectors in 2017

1

Cyber Security Awareness
Many board of directors and the C-Suite have begun to address cyber security as a serious risk oversight issue that has strategic, cross-functional, legal and financial implications and have taken necessary steps in providing cyber security awareness among employees.

2

Securing the technology infrastructure
Hackers will look for the weakest link and exploit industries who have highly sensitive information and lower investments in security solutions.The technology is key enabler for Digital India, therefore, the protection has to be on securing the technical infrastructure.

3

Stringent on Security of their Third Party Vendors and Collaboration Partners
Organizations will be expected to put in place stricter compliance regulations on their thirdparty outsource vendors and external collaboration partners. Thirdparties pose a huge risk because they require access to systems and data to conduct business, yet there is no accountability in handling company's data.

4

Adopt Data Centric Approach
2017 will be the year that organizations acknowledge the need to secure the data itself, and not just infrastructure and devices. The focus will be on data leakage prevention.

5

IT Hygiene and monitoring mechanism
Recent ransomware attacks using Wanna Cry and Petya viruses confirmed cyber as a "Weapon of Mass Disruption" with large number of computers affected across various industry sectors i.e. health, finance, transport, ports worldwide.

India will continue to face increasingly sophisticated and destructive cyber threats. Cyber-attacks use techniques and tools that help criminals evade detection with increasing refinement, and this has led the government to recognize cyber security as a “strategic domain” and devise strategies aimed at deepening cooperation at the international level. At a national level, some of the future key initiatives to be undertaken to further strengthen our cyber security maturity level are as follows:

Security Standards, Frameworks and Audit
India needs to develop and promulgate the cyber security standards and frameworks for development and audit processes for protection of the country’s NCII. Enabling policy measures are required to encourage establishment of testing labs for managing ICT supply chain risks.

R&D product development
India proposes to take R&D initiatives in the development of safe products, discovery and analysis of vulnerabilities, fixing attribution and design of cyber weapons. Manufacturing and export of cyber security products presents a very attractive opportunity for India.

Cyber Workforce Development
This is an urgent requirement to have a national plan to develop cyber security workforce and an associated cadre.

Cyber Threat Intelligence Center
India proposes to have cyber analysis centers to collect attack on various infrastructures, financial systems, web sites and services; correlate ‘big data’ generated from government with financial and commercial data to create patterns and suggest anomalies for advance preventive actions.

In today’s digital ecosystem, development of full cyber security spectrum is a national imperative.

Key Drivers for Security Spending:

According to the latest forecast from Gartner, global information security spending will grow 7% to reach USD 86.4 billion in 2017 and up to USD 93 billion in 2018.

With an increase in the number of breaches, the need for a strong and robust cyber security framework is now more than ever. Spending on Information security products and services in India is likely to touch USD 1.5 billion in 2017 , an increase of 12 percent over 2016. Spending is expected to grow to USD 1.7 billion in 2018. In 2016, 10% of the overall IT budget of Ministries was allocated for security spend. Cyber Security is one of the top priorities of the Union Budget for 2017-2018.

India Spending on Information Security to reach USD 1.5 Billion in 2017

The changing cyber threat landscape in India along with the initiatives taken by Indian businesses and government are acting as catalyst to aid the cyber security spend in India. In this era of disruptive technologies including Internet of Things (IoT), advanced virtual reality, renewable energy, autonomous self- driving vehicles, cloud technology, artificial intelligence (AI), robotics, blockchain technology, big data, etc. Some of the key technology likely to gain momentum are as follows:

Cloud Security

As per Gartner, the investment in cloud infrastructure (IaaS) in India will exceed that in traditional data centre outsourcing in 2017 and is estimated to reach USD 667 million in 2017.

Looking at the exponential market growth in Cloud Infrastructure, it is imperative that organizations should invest in cloud security.

Companies should develop security guidelines for private and public cloud use and utilize a cloud decision model to apply rigor to cloud risks.

Technology such as 'Cloud workload protection platforms' are being looked at to provide single management console and a single way to express security policy, regardless of where the workload runs.

Blockchain Technology

Blockchain market is attracting lot of attention from enterprises, start-ups and media globally as well as in India.

The global blockchain market is expected to rise from USD 315.9 million in 2015 to be worth USD 20 billion by the end of 2024, exhibiting a whopping CAGR of 58.7% between 2016 and 2024.

The Asia Pacific market is estimated to expand at a 61.3% CAGR between 2016 and 2024 on account of the growing trend of online payment in countries such as India, China, and Japan. In addition, the recent demonetization initiative in India will further drive the growth prospects of the blockchain technology market.

Big Data Analytics

The big data industry in India currently employs around 90,000 people, across various different sectors. With around 600 companies in this space, 400 being start-ups, a 100 were added in 2015 alone.

By 2025, India is estimated to have a 32 percent share in the global market. Organizations are investing in and employing big data analytics to monitor security threats, for incidence response and audit and review data to understand how it is used, by whom and when.

There is major shift from perimeter-based defence to real time information for predicting information security incidents.

Internet of Things (IoT)

India aims to capture 20% of market share by 2020.

The most important information security challenges of IoT is finding hidden or zero-day attacks (example: The Mirai Malware).

Increased IoT adoption will drive mobility. Organizations are increasingly looking to adopt the Bring Your Own Device or the BYOD model and therefore the market for devices is also poised to grow significantly.

Enterprise mobility is expected to become a USD 1,871 million market by 2017 in India.

The emergence of IoT coupled with BYOD will further enhance the attack surface with connected number of devices and applications being susceptible to Advanced Persistent Threats (APTs). Application security is expected to witness the highest Compound Annual Growth Rate (CAGR) in the global cyber security market during the period 2016–2021.

Robotic Process Automation (RPA) is another technology that seems to be taking on steam. The RPA market grew 64 percent to USD 200 million last year and is expected to grow 70 to 90 percent by 2018. Successful pilot projects involving high number of systems and high volumes of transactions or value transactions, are inspiring buyer confidence in this technology. To help processes which may be prone to error and rework and are highly predictable with limited exception handling, RPA can be considered.

With organizations undertaking digital transformation, interaction of various players of an enterprise i.e. customers, employee and business partners/third-parties through websites, social media, mobile devices, cloud, IoT and other advanced technologies is imperative and has increased the risk exposure. Data security, third party, regulatory and privacy risks are some of the risks that will be some of the key risks to be addressed.

In 2017, the threat level to Indian businesses continues to be on the rise with reports of attacks and data breaches in the media. As attackers are evolving, so should the Indian businesses and government in their ability to protect themselves from such attacks.

In an effort to make India a global hub for cyber security-related requirements, the IT industry's representative body NASSCOM and the Data Security Council of India (DSCI) launched a detailed roadmap for the next 10 years and have identified Managed Security Service (MSS), Security and Vulnerability Management (SVM) and Network Security as the emerging global opportunities.

MSS emerges as the most attractive opportunity, with the highest growth of (more than 12 per cent) and largest market size (USD 18 billion). According to NASSCOM, the Indian IT industry is set to reach a size of USD 350-USD 400 billion by 2025. The country can build a cyber security product and services industry of USD35 billion by 2025 and generate a skilled workforce of one million in the security sector

CONCLUSION

Cyber Security landscape in India has witnessed major evolution in the last five years due to emerging technologies such as Cloud computing, big data analytics, social media, mobile computing, digitization and Internet of things. With these changes in cyber security landscape, the attacks and threats have evolved, making technology vulnerable to various attacks like malware, spyware, ransomwares and data breaches. India has witnessed some of the major cyber-attacks ranging from WannaCry, Petya to data breaches. There is no doubt that the internet is one of the key drivers for the economic growth of India, especially with the Digital India initiative. Digital transformation across industries has led to rapidly changing business environment which offers exponentially augmenting opportunities for new capabilities and initiatives. Along with Digital transformation, it is imperative for organizations to also manage the cyber security risks that are introduced into the environment and its impact to the existing eco-system to drive optimum value from their digital initiatives. In an effort to deal with this changing ecosystem, both Indian businesses and the Government have established policies, are putting in place initiatives to address the security risks and challenges on an ongoing basis and focusing on key areas to enhance the cyber security posture of the nation as a whole. With this paradigm shift in the cyber security space, the cyber security market in India is set to grow multifariously.

REFERENCE:

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

http://www.sebi.gov.in/legal/circulars/jul-2015/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporation-and-depositories_30221.html

https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3118&flag=1

http://www.sebi.gov.in/legal/circulars/sep-2017/cyber-security-and-cyber-resilience-framework-for-registrars-to-an-issue-share-transfer-agents_35890.html

http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

Deloitte's point of view on Managing Risks in Digital Transformation

Source: http://www.thehindubusinessline.com/info-tech/spending-on-information-security-services-will-touch-15-bn-this-year-gartner/article9834819.ece

http://www.everestgrp.com/2017-05-robotic-process-automation-market-poised-explosive-growth-news-39759.html/


www.itsa-india.com