IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

January-2018 Volume 5, Issue-1

Email: editor@ijermt.org www.ijermt.org

IMPRESSION OF THE CYBER-SECURITY INDUSTRY IN INDIA

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

-- A Definition of Cyberspace

Alok Kumar Gupta
Research Scholar
Noida International University
Greater Noida

Dr. Mayank Singh
Supervisor
Noida International University
Greater Noida

ABSTRACT

The present situation with regard to cyberspace is similar. The development of the Internet and low-cost wireless communication is the contemporary equivalent of what airplanes were a hundred years ago. Their use in economic, social and political transactions has increased at a rate that far exceeds the growth in airplane use over the last century. These technologies already play an important part in military operations in the traditional spheres of land, sea, air and the newer one of space. There are signs that they have been used for aggressive purposes by some states. There is also ample evidence of their use by criminals and terrorist groups. It is only a matter of time, like air power a hundred years ago, before cyberspace becomes an independent theatre of war.

Key words: Cyberspace, economic, social and political transactions

INTRODUCTION

There is one important nuance in the treatment of cyberspace as a fifth potential theatre of war along with land, sea, air and space. The use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks (NWs), telecom exchanges, routers, data servers, and so on. Protecting or attacking these is in the domain of the traditional arms of the military. Cyberspace as an independent theatre of war is about attacks that compromise the capability to use these facilities: they cannot be prevented by the security services in isolation. The defence of cyberspace necessarily involves the forging of effective partnerships between the public organisations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens.

The defence of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest. It is not possible for a country to ignore what is happening in any part of this space if it is to protect the functionality of the cyberspace relevant for its own nationals. Moreover, a key part of this space, the global Internet system, is still under the control of one country. Hence national defence and international cooperation are inevitably intermeshed. This means that a country's government must ensure coherence between its security policy and the diplomatic stance taken by it in multilateral and bilateral discussions on matters like Internet and telecom governance, human rights related to information freedoms, trade negotiations on infotech services, and so on.

There is another feature of cyberspace that complicates the design of security structures and policies compared to the other theatres of conflict. In cyberspace it is very easy for an attacker to cover his tracks and even mislead the target into believing that the attack has come from somewhere else. This difficulty in identifying the perpetrator makes it difficult to rely on the capacity to retaliate as a deterrent. Whom will you penalise when the perpetrator cannot be clearly identified? Moreover, the costs of mounting an attack are very modest. These two factors make cyberspace an ideal vehicle for states and non-state actors who choose to pursue their war aims through clandestine means. In this situation effective security policy for cyberspace requires a high priority for early warning, intelligence and preemptive defence.

The technologies that are used in cyberspace are still very new and are evolving rapidly. Hence investing in technological capacities to keep track of global developments, developing countermeasures and staying ahead of the competition is as central to the defence of cyberspace as the more conventional security measures.

EVOLUTION IN THE INDIAN CYBER SECURITY:

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.

CHANGING THREAT LANDSCAPE IN INDIA:

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.

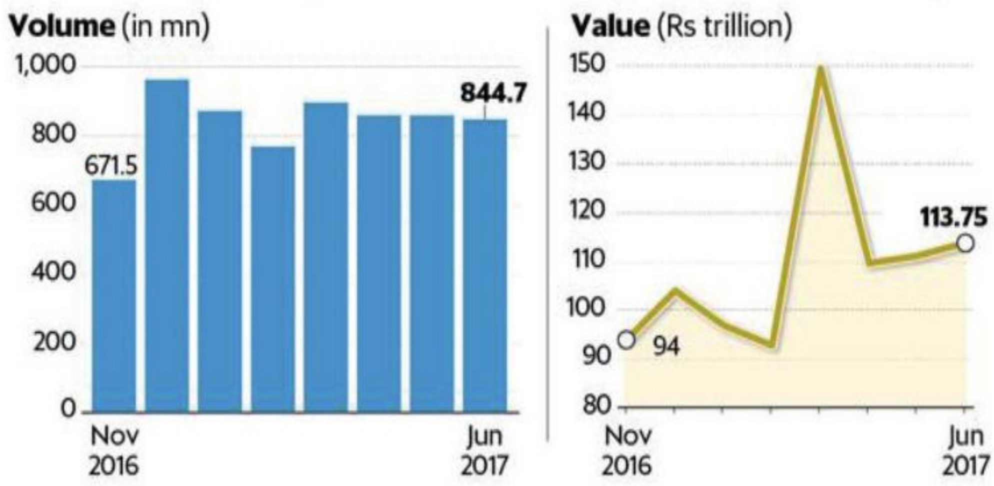
The emergence of new services and applications, advanced technologies including cloud and IoT, is proving further impetus to the changing threat landscape in India. The National Association of

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 cyber security.

EFFECTS OF NEW REGIME AND POLICIES:

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

National Cyber Security Policy:

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 cognizance 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.

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.

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.

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:

1. Albert Marcella & Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd ed., Auerbach Publications, Taylor & Francis Group,UK, 2018.
2. Loader Brian and Thomas Douglas, Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age, Routledge Publication, London, 2000.
3. Michael Chissick & Alistair Kelman, Electronic Commerce - Law and Practice, Sweet & Maxwell, London, 2016.
4. Chris Reed, Internet law, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2014.
5. Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, 2010.
6. F. Lawrence Street and Mark P. Grant, Law of the internet, LexisNexis Matthew Bender, New York, 2018.
7. Gregory J. Battersby, Charles W. Grimes, and Leonard T. Nuara, Drafting internet agreements, Wolter Kluwer (India) Pvt. Ltd., New Delhi, 2010.
8. Heather Ann Forrest, Protection of geographic names in international law and domain name systems policy, Kluwer Law International, Netherlands, 2017.
9. Ian Walden, Chap. 9,“Computer Crime” in Chris Reed (Ed.), Computer Law, 3rd Ed. Oxford University Press, 2017.
10. J. F. Dunnigan, The Next War Zone: Confronting the Global threat of Cyberterrorism. New York: Citadel Press, 2003.
11. K. D. Mitnick, & W. L. Simon, The Art of Deception: Controlling the Human Element of Security, Wiley Publishing, 2018.
12. Nandan Kamath, Law Relating to Computers, Internet and E- commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., 2012.
13. Pedro Letai, Cyber law in Spain, Kluwer Law International, Netherlands, 2014.
14. Tyson Macaulay, Critical Infrastructure: What, Who Cares, and Why, Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies, CRC Press, Florida, 2018.
15. Uta Kohl, Juridiction and the internet, Cambridge University Press, Cambridge, U.K. 2007.
16. Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, Bangalore, 2010.
17. Walter B. Wriston, The Twilight of Sovereignty - How the Information Technology Revolution is Transforming Our World, Maxwell Macmillan International, New York, 2014.