International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Information Security : Need of Digital India

Deepak Jyoti
HOD, PG Department, Computer Sc. & IT, Shanti Devi Arya MahilaCollege, Dinanagar

Abstract: ***This paper highlights the need of information security in modern and digital India.While both Smart Cities and Digital India will create new economic and social opportunities, they will also be creating an increasingly large attack surface for cyber criminals. The Digital India program envisions the creation of a digitally empowered economy and e-governance and services on demand to improve access of information as well as resources for citizens. Lack of online safety leads to things like cyberbullying, which has surfaced with alarming figures.The government initiative that seeks to transform the country into a connected economy can be successful only when security of the connected devices is assured. India is also in the process of setting up national cyber security architecture. The architecture will provide a framework for designated agencies to monitor, certify and fortify India's networks in accordance with the law.***

Keywords: Digital India, Cyber-Security, Aadhar, Smart Cities, Technology.

I. INTRODUCTION

'Digital India and 'Make in India' are two initiatives launched by the Government of India. 'Digital India' aims to transform India into a 'digitally empowered society and knowledge economy' whereas 'Make in India' is 'to facilitate investment, foster innovation, enhance skill development, protect intellectual property and build best in class manufacturing infrastructure'. The Indian government has embarked on a programme to turn the country into a digital economy. It has unveiled a series of initiatives—from introducing Digital Locker, which eliminates the need for people to carry hard copies of documents issued by the government, to demonetization, which has spurred the use of digital payments across the country. Together, these will strengthen the brain and brawn of India respectively, leading to a prosperous and healthy India.While both Smart Cities and Digital India will create new economic and social opportunities, they will also be creating an increasingly large attack surface for cyber criminals

"I dream of a Digital India where cyber security becomes an integral part of our national security... The world is so worried about cyber security. One click can change a lot of things," said Prime Minister Narendra Modi at the launch of Digital India Week on July 1, 2015.

The move towards a digital economy is likely to help trigger a fresh wave of economic growth, attract more investment, and create new jobs, across multiple sectors. The Digital India program envisions the creation of a digitally empowered economy and e-governance and services on demand to improve access of information as well as resources for citizens. It is important to understand that the generation of data is directly proportional to the number of people using a particular service, which means that more the adoption of services from the Digital India umbrella, more will be the data generated. For instance, the Aadhar (UID) initiative now stores biometric data of over 73 crore citizens. Any security breach in the initiative will raise major concerns about privacy and security of confidential data. However, it also poses a big challenge, that of cyber security. It is a well-known truism that the world over that the young embrace and adopt newer technology of almost any kind faster and India is no different. A recent study called Teens and Technology 2014, conducted by Intel's security arm McAfee, examined the online behaviour and social networking habits of Indian tweens (8-12 years) and teens (13-17 years). As many as 92% of the Indian youth was found to have shared private information online despite being aware that this is risky. 80% of youngsters trust the virtual world and interact with strangers, and as many ofthem polled did not care about their online privacy at all, according to the report. Lack of online safety leads to things like cyberbullying, which has surfaced with alarming figures. According to the report, two out of three polled youngsters had some experience with cyberbullying and an overwhelming number said they would not know what to do if they were harassed online. The median age of our country is 27 years, and therefore it is critical that cyber security is integrated tightly into the digital literacy training that is imparted to Indian citizens.

II. CHALLENGES IN DIGITAL INDIA

With the move towards a digital economy, increasing amount of consumer and citizen data will be stored digitally and a large number of transactions will be carried out online, by companies, individuals as well as government departments.Cashless society is not possible until we bring awareness in rural and poor people. But being cashless society is a good one for country. Thirty two lacs debit cards were in danger because of lack of internet security. At that time some banks changed their customers's ATM cards and some others changed their pin code. Hacking groups can hack banking system and any other site information. Actually security softwares in india don't get updated regularly because of which

International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

hackers find penetration hole to attack the information.But when your country has an internet security very less then how do you expect the people to go for cashless society. It can be used by practically any person anywhere, without any fear of being cheated or looted. So, there are chances of malpractices.

As per some data, India currently has 319 million internet users and mobile internet users are projected to be increase. In fact, more than 50% of shopping happen on the mobile online. Now a days, Android phones can be hacked with a single text message. In the context of Digital India, we anticipate that a majority of citizens will be accessing their e-government services with mobile computing device which is why mobile security needs to be taken very seriously. When you talk to the visiting heads of the technology giants about the government's ambition of Digital India and Smart Cities, usually the focus is only around the scale of the ambition, capacity to do it but soon the mission will move to the subject of cyber security. Nowadays security is the major feature. While both Smart Cities and Digital India will create new economic and social opportunities, they will also be creating an increasingly large attack surface for cyber criminals to exploit as an initial foothold or vector into otherwise well-protected IT environments. The current government mission is to transform the country into a connected economy which can be successful only when security of the connected devices is assured.

"As Digital India and the concept of Smart Cities takes shape, security needs to be considered as integral part rather than an afterthought. Securing data at all the times, protection of citizen's information at large and security of critical infrastructure need to be ensured through strict compliance with the security policy and using modern techniques, tools and processes," Tarun Kaura, director—Technology Sales, India, Symantec, told FE.

Generally, across the globe, government and businesses have been reluctant to invest in security because they have too many other project to execute and security does not become the priority. But now there is need for change, security should be at higher priority task in the age of Digital India.in the finanacial year of 2015-16, ATM and Debit cards frauds increased by 6585 whereas in the previous years it was lessi.e 1307. So the fraud rates in online transactions increased by 73.24%.In October 2016, what is being touted as the 'biggest ever breach of financial data in India', as many as 3.2 million debit cards were compromised. Of the cards breaches, at least 2.6 million were on the Visa and MasterCard platform while 600,000 were on the RuPay platform. State Bank of India (SBI), India's largest bank, which has over 13000 branches was worst hit. The bank blocked and re-issued around six lakh debit cards to customers.

The report of the breach also indicated that a malware-related security breach took place in a non-SBI ATM network. On 7th February 2017, Hitachi Payment Services confirmed that the malware had originated in the ATM network. India at 16.9% was among the five countries that included China and Pakistan, at the risk of being exposed to cyber-attacks. India also ranked fourth globally among the countries most affected by ransomware. As per government data, The National Crime Record Bureau (NCRB) registered a total of 16458 cybercrime cases in the year 2015-16, recorded data was 9500 reported in 2013-14. Similarly data for the year 2016-17 is again more than previous years. The highest number of cases was reported in Uttar Pradesh and Maharashtra, which has cyber police stations in every city. NCRB does not give us the actual cybercrime data. One of the senior NCRB officer said that they will plan to start counting cybercrimes complaints to give accurate data. The RBI has also registered a total of 8,689 cases of frauds involving credit cards, ATM/debit cards and internet banking during the year 2017. Interestingly, the reported incidents have increased in the last few years in India. The cost of cyber-attacks in India currently stands in excess of Rs25,000crore ($4billion). It is important to note that there are many cyber-attacks that go undetected and unreported as well, so this number could be much higher. One of the biggest reasons behind this is the limited awareness of the impact and importance of cyber security currently. Many companies do not treat it as a strategic agenda, but rather as a small issue for their IT departments. In fact, 90% of cybercrimes incidents go unidentified and hence, unreported

"There has been dramatic changes in India. Indian government and enterprises' willingness to look into the challenge of cyber security has substantially increased," said Stephen DuBravac, executive vice-president, Security Weaver. Bruce Schneier, the noted American cryptographer, who says, "Security is not a product, but a process."

III. EFFORTS ON CYBER SECURITY

In 2017's Union Budget, finance minister, Arun Jaitley, announced plans by the Indian government to enhance India's digital footprint. The government's mission is to achieve a target of 2,500 crore digital transactions for 2017-18 through UPI, USSD, Aadhar Pay, IMPS and debit cards. It is for all the above reasons that we at Intel believe that India needs a properly structured and well thought through security and cyber wellness plan that's integral to the Digital India vision. Security and cyber wellness need to be addressed at the policy and

architecture level as the government and industry work towards designing solutions and building the country's digital infrastructure. Security and data privacy need to be the foundation of all process flows that get designed for Digital India. The citizenry at large needs to be educated about the do's and don'ts of security as part of the digital literacy training that's imparted to make one person per house hold e-literate. Also, in the back-end, a strong, intelligent and solid detection system needs to be in place that can identify any potential threats and trigger the appropriate corrective action. People should not share their ATM/credit cards numbers and their passwords with any one. Online transactions is more secure on http sites as compare to www. Passwords of your cards should be change monthly. One should have SMS alert about transaction and check the bank statements regularly.

India needs a comprehensive cyber security law to be prepared to tackle cyber security challenges more effectively.In recent times, India has launched a series of cyber security initiatives to digitally empower its citizens and safeguard cyberspace. As the Digital India initiative progresses, cyber-attacks have doubled year over year, and Indian businesses and government sites have become more vulnerable. A new cyber security law would enable India to protect critical infrastructure more effectively. It would also empower cyber security agencies to manage incidents quickly and mandate reporting of significant cyber security incidents. India appointed its first chief information security officer (CISO). The appointment underlines India's commitment to combating cyber-attacks. It will help India to develop the vision and policy to fight cybercrime and manage cyber security more effectively.

India is also in the process of setting up national cyber security architecture in collaboration with other countries. The architecture will provide a framework for designated agencies to monitor, certify and fortify India's networks in accordance with the law.

However, there is currently no strong national agency to assess the nature of cyberthreats and respond to them effectively. Some analysts recommend the creation of a National Cyber Security Agency (NCSA) as an answer to the security challenge. An NCSA would improve India's resilience and defense systems. It would also be responsible for a wide range of cybersecurity transformations in the area of policy formulation and its implementation at the national level.

India and the U.S. agreed to cooperate on cyber security issues during Prime Minister Narendra Modi's trip to the U.S. U.S and India produced Cyber Relationship Frameworkin which both countries agreed to share cybersecurity best practicesand threat information on a real-time basis. They will promote cooperation between law enforcement agencies and encourage collaboration in the field of cybersecurity research. In 2015, India and the U.K.also made a joint statement about cooperation in the cybersecurity space. The two countries agreed to work together to establish a Cyber Security Training Centre of Excellence in india for professional development. India has also entered into cybersecurity cooperation with Malaysia and the European Union. There is a strong case for India to collaborate with more countries, but in the meantime, these partnerships are a great foundation.

Cyber security and wellness is an area where strong Public Private Partnerships can benefit the country. Intel has always been a strong believer of the PPP model and is working very closely with the government in the proliferation of digital literacy in the country and most recently we've also begun working on creating awareness on cyber security and wellness In line with this, Intel launched the Digital Wellness Online Challenge along with the National e-Governance Division during the 'Digital India Week'. Digital India Week programme focus on three key vision areas of " infrastructure as a utility to every citizen" , "digital empowerment of citizens" and "governance and services on demand" . Manyevents organizedwhich are aimed to sensitize and creating a culture of digital wellness amongst people by promoting awareness on the benefits and the threats of Internet-based interactions. The January, 2017 order is surely a step in that direction. One digital quiz organized from Ist Jan to 15th Jan 2017. Additionally, Intel is relentlessly pushing the boundaries of hardware and software innovation to provide pervasive security and identity protection for individuals and businesses on all computing devices, and to supply security platforms and solutions. The implementation of a secure Digital India will need to adopt an end to end approach like never before. As a nation, we shouldn't ignore security concerns for the growth of India. Strong Internet security will help to create a new Digital India.

IV. CONCLUSION

It is time to reboot the digital India for cyber security.One of the biggest misconceptions about cyber security is that cyber-attacks are restricted to the financial services and banking sector. It is important to note that industrial companies are equally effected. At the same time, it has become clear that conventional IT systems and firewalls are increasingly becoming ineffective in preventing sophisticated hackers from creating havoc.As a result, companies in India need to be proactive to ensure they foster efficiency and efficacy in cyber security management. The vision for this has to come from the very top. It is important that the chief executive officers

make this a high priority on the management agenda and build clearly defined security road maps to have a more structured implementation in line with their security strategy.But what India definitely needs is a cyber-security vision in line with its Digital India mission. Information security awareness is an important contributing factor for a successful information security plan and should be properly assessed in order to suggest improvements. And maybe, then a time will come when we will remember, not the breach, but how it was tackled.

V. REFERENCES

[1] www.business-standard.com/.../cyber-security-critical-for-digital-india-success-11602..

[2] https://telecom.economictimes.indiatimes.com › Latest Telecom News ›

[3] www.digitalcreed.in › TRENDING › Cyber Security critical for Digital India Success

[4] www.dnaindia.com/.../standpoint-why-cyber-security-is-critical-for-digital-india-2127.

[5] https://inc42.com/buzz/cybersecurity-sacon-ciso

[6]epaperbeta.timesofindia.com/article.aspx?eid=31816&articlexml..digital-india.