THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Cybersecurity Reboot: *Sine Qua Non* For Digital India

Dr. Sudesh

Assistant Professor Vaish College of Education, Rohtak, Haryana, India

ABSTRACT

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. 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. 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.

While the advent of digital technology has fueled new business models and opportunity, it has also brought an element of risk as valued assets become less tangible, more distributed, and more vulnerable to cyber threats. It also poses a big challenge, that of cybersecurity. Like any other technology, IoT has its own used and challenges. For instance, IoT can be used for smart grids, smart cities, e-health, etc and thereby reduce their cost of operation and improve their productivity. However, IoT also has civil liberties and cyber security challenges to manage. Cyber criminals have already started abusing IoT controlled devices for launching malicious cyber attacks. As the technology protocols for IoT are still evolving, it is very difficult to avoid such cyber attacks. Today, many different types of cyber attackers threaten organizations, from individuals working alone ("lone wolves") to highly organized, well-sponsored teams-for-hire capable of breaching the most sophisticated cyber security systems target personal, corporate or state secrets. Cyber security in India has come a long way in the past few years and has gained huge importance in recent times with the thrust on Digital India, e-commerce and mobile payments. Cyber security has been identified as one of the key areas of development by Prime Minister Narendra Modi. "Can we secure the world from the bloodless war? I'm talking about cyber security. India must take the lead in cyber security through innovation. I dream of Digital India where cyber security becomes an integral part of national security," he has said recently. With rapidly growing interconnected business operations and increasing digitisation, cyber security challenges are bound to intensify. Effective measures need to be taken to ensure protection against cyberattacks and threats. Cybersecurity today must include a rethinking of the nature of security, and a shift from an approach that stresses protecting vulnerable assets to one based upon strengthening assets, making them more resilient and part of a holistic cybersecurity process that delivers greater value to the enterprise. Cybersecurity needs to be part of a larger value framework that includes both risk management and the development of digital trust. This paper is an attempt to develop a theoretical background on the digital space and related cyber crimes. Also deliberations are made on the how cyber space can be rebooted to create a safe and secure digital platform.

1. INTRODUCTION TO DIGITAL INDIA

Over the past few decades technology has begun to play a very important role in our day to day lives. Our internet enabled gadgets have changed the way we work, play or even carry out daily chores. Throughout the world, information and communication technologies (ICT) continue to proliferate at incredible speed. Digitalization is one of the most fundamental period of transformation we have ever witnessed. Digital India was a flagship programme launched by the Prime Minister of India Narendra Modi on 1 July 2015 - with an objective of connecting rural areas with high-speed internet networks and improving digital literacy. The vision of this programme is to transform India into a digitally empowered society and knowledge economy. It is one of the biggest step by government of India to motivate the citizen of the country and connect Indian economy to knowledge savvy world. Digitalization impacts almost everything from personal lives, education, health, business and trade, physical infrastructure, governance to national security. Information and communications technology has become indispensable to the modern life, we critically depend on information and communication infrastructure in governing our personal lives, our societies, conducting business and running critical infrastructure

India is committed to the task of promoting the spread of Information & Communication Technology. The key role of ICT as an important element of national development is also well recognized. The ICT system needs to be infused with new vitality if it has to play a crucial & beneficial role in advancing the well being of all

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

sections of our society. The nation continues to be firm in supporting ICT in all facets. It recognizes ICT's central role in raising the quality of life of the people of the country, particularly the vulnerable section of society including rural masses and women community in creating wealth for all, in making India globally competitive, in utilizing natural resources in a sustainable manner, in protecting the environment and ensuring the national security. ICT has enabled citizen participation in governance through more eff ective interaction between the government and the citizens making a closer partnership between the two. But undoubtedly, there is a massive digital divide in the country based on income, education, residence and use of ICT which are correlated with economies, political and cultural power. To overcome the problem, the eff ective solutions should be found out for using ICT for inclusive growth, promoting gender inclusivity and ensuring balanced regional growth. Now world is in the midst of a knowledge revolution, complemented by opening up of entirely new vistas in communication technologies and recent development in the fi eld of information and communication technology (ICT). Since ICT is meant for everyone and doesn't discriminate between rural and urban, man and woman, both can take the equal benefi ts off ered by it. It has the potential to reach and empower women and encourage them to participate in economic and social progress and help them make informed decisions about issues that aff ect them. The government has attempted to involve, encourage and empower the citizens of the country in the decision making process to ensure their participation at local and district levels of governance. Digital India is an initiative of Government of India under the leadership of our visionary Prime Minister for transforming India into a digitally empowered society and knowledge economy. The objective of the project is to integrate the government departments and the people of India by ensuring the government services are made available to citizens electronically by reducing paperwork with the plans to connect rural areas with high speed internet networks. The three core components of this project that are: digital infrastructure as a utility to every citizen, delivering services digitally in governance & service on demand and digital empowerment of citizens with digital literacy; deserve full support from the people of the society at a large. The Govt. of India organisation Bharat Broadband Network Limited which executes the National Optical Fibre Network Project shall be the custodian of digital India project and it has ordered United Telecoms Ltd. to connect 250000 villages in the fi rst phase and it is expected to be completed by 2017. With the eff ective activation & inclusion of nine pillars of digital India such as broadband highways for all, universal access to phones, Public Internet Access Programme, e-Governance as the tool for reforming government through technology, electronic delivery of services, Information for all, electronic manufacturing, Information Technology for Job creation and early harvest Programmes like wi-fi - for all Universities, secured email within government etc.; shall refl ect its impact by 2019 such as broad band in 2.5 lakh Villages, universal phone connectivity, zero Import of IT equipments by 2020, 4 lakhs public internet access points and job creation (1.7 crore direct & 8.5 crores indirectly) and projecting India as a leader in IT use in services like health, education, banking, agriculture, water resources, etc.

2. CYBERSECURITY : A BIG CONCERN

"Cyber-attacks by hostile organizations, nations and criminals are on the rise, along with increase in cases of threat to governments, businesses and individuals by attempting to extract technical, financial, and national security information.

Gulshan Rai, Director General, Govt. Of India, Department of IT

The recent attack by 'WannaCry' ransomware had left several organisations and countries locked-in. The ease with which this ransomware has spread across several countries raises big questions on cybersecurity issues. This worrisome situation also raises questions on security and safety aspects on initiatives like 'Digital India' that aim at transforming India into a digitally empowered society and expect to further accelerate awareness, availability and adoption of digital technologies. Year after year, cyberattacks continue to escalate in frequency, severity and impact. Prevention and detection methods have proved largely ineffective against the increasingly adept assaults, and many organisations don't know what to do, or don't have the resources to combat today's highly skilled and aggressive cybercriminals. The asymmetric nature of cybercrime incentivises it; the cost of committing cybercrimes to intercept and/or modify information, degrade performance of assets, gain unauthorised access to systems, get information for personal gain or bring harm to an organisation is negligible compared to the investments required to safeguard against attackers. Underestimating the level of risk an organisation is exposed to is usually a fatal mistake. Cyber security impacts all organisations, from fledgling start-ups to billion-dollar multinationals. Notable cyber incidents over the past year, such as that of the Indian music streaming service that compromised the records of more than 10 million users, or the vulnerability found in the routers of a popular networks company which allows attackers to spy on traffic, testify this.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through siloed ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialised has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as an NW created by academics for the use of the military, it has now become a global social and economic and communications platform. The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which the number of Internet users has doubled between 2005 and 2010 and surpasses two billion. Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage. The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other. Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information — they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property. Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in Õve years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty — in fact, because of it — we need to be clear about the type of security controls needed

3. CYBER THREATS

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets: cyber espionage, cyber warfare, cyberterrorism, and cyber crime. Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day. It includes the following

- **Cyber Warfare :** There is no agreed definition of cyber warfare but it has been noticed that states may be attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. The attacks on the websites of Estonia in 2007 and of Georgia in 2008 have been widely reported. Although there is no clinching evidence of the involvement of a state in these attacks, it is widely held that in these attacks, non-state actors (e.g. hackers) may have been used by state actors. Since these cyber attacks, the issue of cyber warfare has assumed urgency in the global media In the latest official military doctrine, the US has declared cyberspace to be the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. The issue whether cyber attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated.
- **Cyber Crime** : The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber crime being in billions of dollars worldwide. cyberspace is increasingly being used for various criminal activities and different types of cyber crimes, causing huge financial losses to both businesses and individuals. Organised crime mafia have been drawn to cyberspace, and this is being reflected in cyber crimes gradually shifting from random attacks to direct (targeted) attacks. A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets. The vast amounts of money lubricating this ecosystem is leading to increased sophistication of malicious codes such as worms and trojans. The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars. At the other extreme, components of critical infrastructure such as Programmable Logic Control (PLC) and Supervisory Control and Data

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Acquisition (SCADA) systems were targeted by the Stuxnet malware that attacked supposedly secure Iranian nuclear facilities. Stuxnet exploited five distinct zero-day vulnerabilities in desktop systems, apart from vulnerabilities in PLC systems, and exposed the grave threat to critical infrastructure such as nuclear plants and other critical infrastructure. Cyber criminals are using innovative social engineering techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber crime, as evinced by the increasing number of complaints on consumer complaint forums. The low levels of computer security are also apparent in recurring statistics that show that India is the third-largest generator of spam worldwide, accounting for 35% of spam zombies and 11% of phishing hosts in the Asia-Pacific-Japan region. Over 6,000,000 computers were part of bot NWs. India ranked first in the Asia-Pacific region and contributed 21% to the regional total. A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average. According to CERT-In, India sees an average of 788 bot-infected computers per day. With regard to web-based attacks, India has seen a significant increase and has ranked seventh, with 3% of the world attacks, and second in the Asia-Pacific region

- **Cyberterrorism** Cyberspace has been used as a conduit for planning terrorist attacks, for recruitment of sympathisers, or as a new arena for attacks in pursuit of the terrorists' political and social objectives. Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes. From that perspective, the challenge of non-state actors to national security is extremely grave. The shadowy world of the terrorist takes on even murkier dimensions in cyberspace where anonymity and lack of attribution are a given. The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities, especially in the aftermath of the terrorist attack in Mumbai in November 2008. Parliament passed amendments to the IT Act, with added emphasis on cyberterrorism and cyber crime, with a number of amendments to existing sections and the addition of new sections, taking into account these threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements. While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyberterrorism both in terms of methods and end goals.
- **Cyber Espionage :** Instances of cyber espionage are becoming quite common, with regular reports of thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and NWs of both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. It may also be that theft of intellectual property from private enterprises is not an issue here because R&D expenditure in India is only 0.7% of GDP, with government expenditure accounting for 70% of that figure. Companies are also reluctant to disclose any attacks and exfiltration of data, both because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public. As far as infiltration of government NWs and computers is concerned, cyber espionage has all but made the Official Secrets Act, 1923 redundant, with even the computers in the Prime Minister's Office being accessed, according to reports. The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult; governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive NWs, and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exfiltrated.

4. TOOLS OF CYBER ATTACKS

Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware.

1. Bluetooth hijacking – (also called "Bluejacking") is an attack conducted on Bluetooth-enabled mobile devices, such as cellular telephones, smart phones, and PDAs.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

2. Botnet- A botnet (a contraction of the term "RoBOTNETwork") is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. E.g. distribute malware, spam, and phishing scams etc. a. Network of compromised computers that are remotely controlled by malicious agents. They are used to send massive quantities of spam e-mail messages, co-ordinate distributed denial-ofservice attacks (DDOS).
3. Browser hijacking - is the unintended modification of a web browser's settings by a malware. The term "hijacking" is used as the changes are performed without the user's permission. Some browser hijacking can be easily reversed, while other instances may be difficult to reverse. Various software packages exist to prevent such modification.
4. Cyber Stalking : This term is used to refer to the use of the internet, e-mail, or other electronic communications devices to stalk another person. Cyber stalking can be defined as the repeated acts of harassment or threatening behaviour of the cyber-criminal towards the victim by using internet services.
5. Data interception –Hijacking e-mails, interference of an intermediary in the network, may be a prelude to another type of computer crime, typically data modification.
6. Data diddling: –Usually done in conjunction with data interception, valid data intended for a recipient is hijacked or intercepted and then is replaced with an erroneous one. This could also apply to illegal tapping into database and altering its contents. Basically, any form of alteration without appropriate authorization falls under this category.
7. Data theft -outright stealing of most commonly classified or proprietary information without authorization. This could be the result of data interception. It might also be the unlawful use or possession of copyrighted works such as songs, pictures, movies or other works of art.
8. Network interference -any activity that causes the operation of a computer network to be temporarily disrupted. Interference implies something momentarily such as Denial of Service Attacks that causes delays in data transmission by using up all available bandwidth. Distributed denial of service, ping of death and smurf attacks also fall under this category.
9. Data Security Network sabotage – causing permanent damage to a computer network such as deleting files or records from storage.
10. Cyber Defamation: Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking). After the popularity of the printing press, one witnessed the increase in libel. With the advent of information technology and the Internet, libel has become much more common and of course, easier. In simple words, it implies defamation by anything which can be read, seen or heard with the help of computers/technology. Since the Internet has been described as having some or all of the characteristics of a newspaper, a television station, a magazine, a telephone system, an electronic library and a publishing house, there are certain noticeable differences between online and offline attempt of defamation which makes the online defamation more vigorous and effective.
11. Corporate Cyber Smear : Harmful and defamatory online message has been termed as corporate cyber smear. It is a false and disparaging rumour about a company, its management or its stock that is posted on the Internet. This kind of criminal activity has been a concern especially in stock market and financial sectors where knowledge and information are the key factors for businessmen.
12. Digital Forgery : Forgery is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. Digital forgery implies making use of digital technology to forge a document. Desktop publishing systems, colour laser and ink-jet printers, colour copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.
13. Online Gambling : Gambling is in many countries illegal. Computer is a medium for the purposes of online gambling. The act of gambling is categorised as an offence in some countries and has a legal sanctity in others. The main concern with online gambling is that most virtual casinos are based offshore making them difficult to regulate. It is in this situation that the Internet helps the gamblers to evade the law. Anyone with access to a personal computer and an Internet connection can purchase lottery tickets or visit gambling sites anywhere in the world. The world of online gambling, due to its

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

anonymity, unfortunately has many other hazards like danger of illegal use of credit card or illegal access to bank account.

14. Denials of service (DoS) - an attack that prevents or impairs the authorized use of information system resources or services.These attacks are used to overwhelm the targeted websites. Attacks are aimed at denying authorized person's access to a computer or computer network.
15. Distributed denial-of-service (DDoS) - is a variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
16. E-mail address harvesting - obtaining an electronic mail address using an automated means from an Internet website or proprietary online service operated by another person.
17. E-Mail Related Crime - Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff. a. Cyber criminals are using innovative social engineering techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. E.g. Nigerian email asking bank account to transfer lots of money. Tempting emails of user winning lottery or in some luck draw have been few famous tricks.
18. Exploit tools - publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain access into targeted systems.
19. Hacking - The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing tempest attack, password cracking and buffer outflow facilitates hacking, Identity theft.
20. Logic bomb - a computer program, which may perform some useful function, but which contains hidden code which, when activated, may destroy data, reformat a hard disk or randomly insert garbage into data files.
21. Identity theft - Obtaining and unlawfully possessing identity information of someone with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime.
22. Keyboardlogging - is a software that captures and "logs" every keystroke typed on a particular keyboard.
23. Macrovirus – is a program or code segment (can be called a Virus) written in the application's internal macro language.
24. Malware - (a concatenation of malicious software)a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting
25. Pharming – is a method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
26. Phishing - refers to a social engineering attack, where someone misrepresents their identity or authority in order to induce another person to provide personally identifiable information (PII) over the Internet.
27. Root kit–is a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
28. Skimming – is the act of obtaining data from an unknowing end user who is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus.
29. Sniffer - (also called a packet sniffer) is asoftware tool for auditing and identifying network traffic packets.
30. Spamming - unsolicited commercial e-mail (UCE) sent to numerous addressees or newsgroups.
31. Spoofing - the ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database.
32. Spyware- technologies deployed without appropriate user consent and/or implemented in ways that send away the information about user activity without his/her acknowledgement.
33. SQLinjection - is a way to cause database commands to be executed on a remote server. Such command execution can cause information leakage.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

34. Trojans - Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12thCentury BC.
35. Virus – A computer virus is the program code that attaches itself to application program and when application program run it runs along with it. It typically has a detrimental effect, such as corrupting the system or destroying data.
36. War-dialing– is a recursive dialing of phone numbers from a modem-enabled PC in an attempt to locate other unadvertised modems resulting in unauthorized access into a computing or Process Control System domain.
37. War-driving - is the recursive searching for wireless access points in an attempt to access a communication network resulting in unauthorized access into a computing or control system domain.
38. Worms - is a code that replicates itself and consumes the resources of a system to bring it down.
39. Zero-day exploit – is an attack against a software vulnerability that has not yet been addressed by the software maintainers. These attacks are difficult to defend against as they are often undisclosed by the vendor until a fix is available, leaving victims unaware of the exposure.

5. THE INDIAN CYBERSPACE:

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three NWs were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities. Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003. Though the rate of growth has slowed subsequently, with Internet users now approximately numbering 100 million, exponential growth is again expected as Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%.2 The target for broadband is 160 million households by 2016 under the National Broadband Plan. Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India.3 Similar figures have also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites. An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India's top e-commerce retailer, saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million).4 Even though the Indian government was a late convert to computerisation, there has been an increasing thrust on e-governance, seen as a cost-effective way of taking public services to the masses across the country. Critical sectors such as Defence, Energy, Finance, Space, Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on NWs to relay data, for communication purposes and for commercial transactions. In terms of contribution to the economy, the ICT sector has grown at an annual compounded rate of 33% over the last decade. The contribution of the IT-ITeS industry to GDP increased from 5.2% in 2006-7 to 6.4% in 2010-11 and to 12% in 2015-16. Much of the activities of the IT/BPO sector, which was responsible for putting India on the services export map, would not have been possible but for the cost-efficiencies provided through the expansion of global data NWs. The government has ambitious plans to raise cyber connectivity. There has been a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility. As in other countries, much of the infrastructure related to cyberspace is with the private sector, which also provides many of the critical services, ranging from banking, to electricity to running airports and other key transportation infrastructure. Taking telecommunications as a case in point, CII in India comprises around 150 Internet and telecom service providers, offering Internet, mobile and wireless connectivity to a user base of nearly 800 million. A major portion of data communication is facilitated by submarine cables. India has landing points for major submarine cable systems which are minimally protected. A preview of what could happen by way of these cables being disabled took place in 2008 when a series of outages and cable cuts in undersea cables running through the Suez Canal, in the Persian Gulf and Malaysia caused massive communications disruptions to India and West Asia.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Other sectors that could be subject to serious threats include the financial sector, which has largely transferred operations online. Stock exchanges in the United States and Hong Kong have reportedly been subject to cyber attacks. The electricity grid is also vulnerable with the inevitable move towards a smart grid, given the economic and efficiency factors. The protection of critical infrastructure is a complex task requiring forethought, planning, strong laws, technologies, PPP and resources. For all these reasons it needs to be given top priority by the government. The country cannot afford to wait indefinitely for a robust policy to protect this critical infrastructure. Above all, the political will needs to be mustered to take the challenge head on. The government would necessarily have to work closely with the private sector, particularly in promoting cyber security practices and hygiene.

A report by the National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India, titled Crime in India-2014, shows a 69% increase in cases reported under the Information Technology (IT) Act in 2014 from the year before. The number of cases recorded increased from 5,693 in 2013 to 9,622 in 2014. The number of security incidents that have been handled by Indian Computer Emergency Response Team (CERT-In) over the last few years has increased exponentially. If we compare the security incidents of 2014 with 2013, there has been a marked increase of 82%. The types of incidents handled were mostly related to malicious code, phishing, website intrusion, spam, network scanning and probing and malware propagation, defacements or damages to data as well as ransomware attacks

In an interview with *Deccan Chronicle*, a spokesperson from Norton hinted that cyber criminals are looking for a target in bulk, and India suits well to them — a large, "vulnerable" population with "money".

"The financial sector in India has become an easy target for cyber criminals considering the government's demonetisation drive and the subsequent rise in digital payments," added Agarwal. "Recent examples of various cyber attacks on institutions across industries remind us of how very often security is still the weakest ink in our digital transformation."

According to Symantec's ISTR report, India ranks second highest in Asia Pacific and Japan (APJ) region. Across the globe, India stands fifth among most-affected regions beset by ransomware attacks. According to Minister of State for Electronics and IT P P Chaudhary's India witnessed more than 27,000 cyber security threat incidents in the first half of 2017. The cost of cyberattacks in India currently stands in excess of Rs25,000 crore ($4billion). It is important to note that there are many cyberattacks that go undetected and unreported as well, so this number could be much higher. The losses emanate from operational disruptions, loss of sensitive information and designs, customer churn and impact on brand image, as well as increase in legal claims and insurance premium. The issue is forecast to balloon further in the coming years, reaching as high as Rs1.25 trillion ($20 billion) over the next 10 years, as the business operations of most Indian companies become networked. Following are cyber security incidents that affected India in the past one year.

- **Mirai botnet malware**: A botnet malware named Mirai took over the Internet targeting home router users and other IoT based devices. The malware affected 2.5 million IoT devices; it's not clear how many systems were affected in India. CERT—In had also issued an advisory regarding the attack back in October 2016.
- **WannaCry**: Ransomware WannaCry swept the world in May. CERT-In immediately put out an advisory notice. Few instances of the ransomware were reported to have hit banks in India, and some businesses in Tamil Nadu and Gujarat as well during the first wave of the attack. Railwaire users were also most affected by the ransomware.
- **Petya**: India was also on the top 10 list of countries to be hit by Petya ransomware attacks, with the country faring worst among other Asia Pacific (APAC) countries, cyber security firm Symantec said in a blog post last month. Globally, India took the 7th spot with less than 20 organisations being affected as per the Symantec's analysis.
- **Data breaches**: Zomato said in May that it was affected by a data breach which led to details of 7.7 million users being stolen. The leaked information, listed for sale on a Darknet market. The company was, however, able to contact the hacker and take down the data. Reliance Jio was also affected by a data breach this month; a website called magicapk.com went up last month, allowing anyone to search for personal details of Jio customers. However, this also was taken down after the site went viral.

6. GETTING AHEAD OF CYBER CRIME

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Early warning and detection of breaches are decisive to being in a state of readiness, meaning that the emphasis of cybersecurity has changed to threat intelligence. A state of readiness to deal with cyberattacks requires behaviours that are thoughtful, considered and collaborative. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack. A state of readiness includes:

- Designing and implementing a cyber-threat intelligence strategy to support strategic decisions and leverage the value of security
- Defining and encompassing the organizations extended cybersecurity ecosystem, including partners, suppliers, services and business networks
- Taking a cyber-economic approach — understanding your vital assets and their value, and investing specifically in their protection
- Using forensic data analytics and cyber threat intelligence to analyse and anticipate where the likely threats are coming from and when, increasing readiness
- Ensuring that all the stakeholders understand the need for strong governance, user controls and accountability Governments may not be able to control when information security incidents occur, but they can control how they respond to them — expanding detection capabilities is a good place to start.

A wellfunctioning security operations centre (SOC) can form the heart of effective detection. Managing cyber threats according to strategic priorities must be the focus of the SOC. By correlating relevant information against a secure baseline, the SOC can produce relevant reporting, enabling better decisionmaking, risk management and business continuity. An SOC can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively. Governments may not be able to control when information security incidents occur, but they can control how they respond to them — expanding detection capabilities is a good place to start. A wellfunctioning security operations centre (SOC) can form the heart of effective detection. Managing cyber threats according to strategic priorities must be the focus of the SOC. By correlating relevant information against a secure baseline, the SOC can produce relevant reporting, enabling better decisionmaking, risk management and business continuity. An SOC can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively. **Possible Solutions to cyber challenges for Digital Inclusion includes the followings:**

A. **Reclaiming cyber security through innovation :** The last couple of years have witnessed the advent of the new generation security information and event management (SIEM) solutions and rise of cyber security standards. Criminals are using technology to give crime a completely new dimension. The dynamic of the cyber security threat landscape is compelling the industry to develop better systems and solutions beyond the traditional security operation centre (SOC). An effective SOC should not only contain state-of-the-art tools and technologies but also have mechanisms for threat intelligence reporting, profiling, detection and response. This need has given rise to new age Cyber Security Centerss, which fundamentally focus on integrating all internal events and global threats and provide insights or actionable intelligence, and quick and decisive remediation action. CSCs focus on providing threat intelligence by collecting and correlating information from internal and external sources and continuous strategic threat profiling through data enrichment. CSCs improve threat response capabilities by supporting forensic evidence collection, incident classification and forensic analysis and help bolster the organisation's threat management process. Technology solutions aim to use best practices to mitigate these risks. **This includes:**
    - **End-to-end encryption**
    - **Strong password policy**
    - **Up-to date firewalls,**
    - **anti-virus**
    - **Audit logs**
    - **Isolation of trusted resources from public resources (DMZ)**
    - **Implement manual over rides on all systems**

    The aim is to reduce the attack surface as much as possible and to make the surface that is visible as robust and resilient as possible.

B. **Adoption of cloudbased service model for cyber security :** Cloud computing is changing the way businesses operate by presenting new avenues for delivering services, information sharing and

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

enhancing operational efficiencies. It is also helping organisations stay cyber secure. Cloud-based models have emerged as an effective way for organisations to effectively manage cyber threat costs. A majority of survey respondents entrust a broadening range of critical services to the cloud, including real-time monitoring and analytics, advanced authentication and identity and access management. Many companies are adopting cloud-based cyber security that is delivered by managed service providers, often using private cloud architecture. Globally, cloud-based IT security solutions are also in demand, especially from small and medium businesses. As per the global survey results of PWC, 70% of respondents say that their organisations use some form of cloud-based security solutions. According to respondents based in India, cloud-based security services are being used for a wide range of solutions like threat intelligence activities, setting up of advanced identity and access management capabilities, end point encryption, etc.

C. **Move from security as a cost, to security as a plus :** Security is usually positioned as an obligatory cost — a cost to pay to be compliant, or a cost to pay to reduce risk. But moving to a model of security as risk and trust management implies looking upon security as an enabler; for example, managing public data access leverages the monetary value of the data instead of focusing on the protection of the data itself. In fact, this transformation means enabling the development of even more extended networks of networks, of more and new forms of collaboration and mobility, and of new business models. "Security as a plus" should be a mainstay of the business.

D. **Continually learn and evolve :** Nothing is static — not the criminals, not the eco system or any part of its operating environment — therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics), maintain and explore new collaborative relationships, refresh the strategy regularly and evolve cybersecurity capabilities.

E. Disaster recovery and back-up services : Data centres, either on site or off site, are at the heart of organizing looking for the security. Disaster recovery is a critical part of the data centre's architecture. If servers go down, is it important that systems are brought back online as soon as possible and, once those systems are back up and running, need to have all their previous workloads operational. It is important to identify the right level of back-up required for various services. Data back-ups should be done regularly, and according to the best practices, should be done off site. This helps in data protection in case of physical security breach at the data centre.

7. TIME TO REBOOT

Today Cyberspace touches almost every part of our daily life. Be it through broadband networks, wireless signals, local networks or the massive grids that power our nation. The threat from cyber attacks and malware is not only apparent but also very worrisome. One of the biggest misconceptions about cybersecurity is that cyberattacks are restricted to the financial services and banking sector. It is important to note that industrial companies are equally vulnerable. 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, organizations in India need to be proactive to ensure they foster efficiency and efficacy in cybersecurity 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. We also need to assess the assets that are most at risk. This will differ from sector to sector and organization to organisation. It is important to identify the most valuable assets, the ones which will "hit you the most", narrow down all possible attack avenues and proactively prepare mechanisms and procedures to address those risks.

It is also important that companies run regular stress tests, which simulate real-life attacks. This can help identify places in the environment (systems, data, etc.) which will be affected the most in case of attacks and assess the company's detection and response preparedness. Further, companies need to start cooperating with peers to learn from each other's experiences—identify potential attack scenarios, identify hidden threats and co-develop a security framework. Organizations also need to enlist their employees in the fight against breaches. There is a need to change the perception of cybersecurity from being a passive agent, to an active business enabler. It is a must to ensure active participation across the organization. Finally, the regulators need to ensure they are covering all aspects at their end. This includes regulations that set minimum standards on cybersecurity for companies across the country. Maybe, even some rating system that classifies companies based on their preparedness on this front. At the same time, tough laws are needed to be put in place for perpetrators of cybercrime to ensure such criminals are deterred effectively.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

India is sitting on the cusp of digital evolution. The government has overcome its detractors with an eagle-eyed focus to achieve this goal for the country. It is now up to companies to ensure they are ready and prepared to harness and exploit the opportunities this evolution will bring. The only way to do that is to ensure that cybersecurity finds its way into the boardroom agenda. There cannot be a single solution to counter such threats. A good combination of Law, People, Process and Technology must be established and then an effort be made to harmonize the laws of various countries keeping in mind common security standards.

REFERENCES

- Abhishek Poddar And Anchit Goel "Digital India Needs A Cybersecurity Reboot" Livemint, Jun 30, 2017
- Cyber Security and Related Issues: Comprehensive Coverage, Insight, Nov 26, 2014
- Digital India Programme : Importance and Impact .Retrieved from http://iasscore.in/national-issues/digital-indiaprogramme-importance-and-impact 5Digital India. Unlocking the trillion Dollar Opportunity: ASSOCHAM –Deloitte report, November 2016.Retrieved from www.assocham.org.
- Fred McCliman et al., "Identifying Cybersecurity Gaps to Rethink State of the Art" The State of Cybersecurity and Digital Trust 2016. Copyright © 2016, Accenture and HfS Research, Ltd
- Gupta Neeru and Arora Kirandeep (2015). Digital India: A Roadmap for the development of Rural India. International Journal of Business Management ,vol(2)2, pp1333-1342. Retrieved from www. ijbm.Co.in
- Kadam Avinash (2015). Why cyber security is important for digital India. Retrieved from http://www.firstpost.com/business/why-cyber-security-is-important-for-digital-india-2424380.html
- Midha Rahul (2016). Digital India: Barriers and Remedies . International Conference on Recent Innovations in Sciences, Management , Education and Technology. Retrieved from http:// data. Conference world .in/ICISMET/P256-261. Pdf.
- Moneylife Digital Team, "Ransomware, Digital India And The Growing Cyber Threats" Moneylife, May 16, 2017
- Nitin Desai et el, India's cyber security challenge, Institute for Defence Studies and Analyses, March 2012, ISBN: 81-86019-98-7
- Rani Suman (2016) .Digital India: Unleashing Prosperity . Indian Journal of Applied Research, volume-6, Issue 4, pp187-189 Retrieved from https://www.worldwidejournals.com/indian-journal-of-applied...
- Salman SH, "27,482 Cyber Security Threat Incidents In India Till June 2017: CERT-In", Https://Www.Medianama.Com/2017/07/223-Trai-Data-Security-Privacy-Telecom/
- Sanskriti Talwar, "Is India Ready To Combat Security Threats To Its Digital Push?" DECCAN CHRONICLE. Published Aug 2, 2017, Updated Aug 3, 2017,