CYBER SECURITY

Mahima Sharma, Piyush Kumar Verma*

ABSTRACT:
In today's world, we all use the internet. Using the internet is interesting as well as it plays a vital role in our daily life. The internet is transforming our lifestyles; it is connecting everyone to everything. The number of issues today have been created more concern within this dynamically changing landscape than cyber security. There won't be a single person who doesn't use the internet as we all have a device in our pocket, it's called smart phones. Modern trends like growing dependence on the cloud, more personal information on the internet, usage of personal devices on corporate networks, are some of the major causes behind data breaches. The terms and conditions are a set of guidelines which help in permitting personal details. Besides various measures, cyber security is still a very big concern to many. Does it describe what these terms and conditions mean? Do these terms and conditions talk about authorising our detail? Do we know what kind of details do they ask from us while accessing their websites or their product? They ask for our personal details. They basically use the data so that they can keep track of our activities for their gains. They only monitor activities which they feel would be a misuse of their website or products. This paper critically analyse the Indian laws and regulations based on cyber security and cyber crimes. This paper also focuses on challenges faced by cyber security on the latest technologies. It also focuses on the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: Cyber security; Laws and policies.

INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data is being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today the Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of mankind. In 1996, only 36 million people, or about 1% of the world's population, used the Internet. By the beginning of 2017, 3.7 billion people, or nearly half the world's population, were online. But due to these emerging technologies, we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. People around the world are becoming increasingly connected with smart devices. Sending and receiving massive amounts of data back and forth, we rely on the transfer and storage of data on a daily basis. Hackers and cyber attackers know this and know how to steal data for their profit. Our job as an information security specialist is to defend our company's data, implementing preventative and protective measures and monitoring our data and systems. Meanwhile, with a plethora of information available, it can be difficult for businesses to know where to begin when it comes to taking measures to reduce the risks of becoming a cyber-attack victim. For businesses large and small, it is vital to be able to identify cyber security risks and effectively manage threats to information systems.

Figure 1: Digital Population Growth

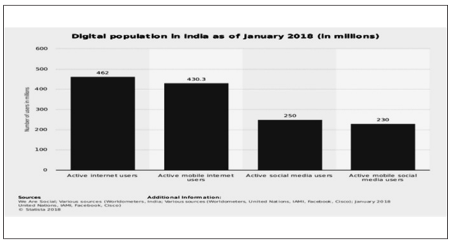
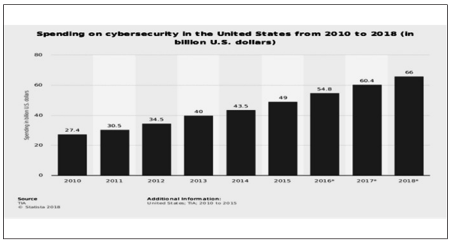


Figure 2: Money Spent by Countries on Cybersecurity



The concept of Cyber Security- Cyber security refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cyber security strategies include identity management, risk management and incident management. The term cyber security refers to a wide range of problems that were not a major concern among the small community of researchers and programmers who developed the Internet. Cyber security is a very broad category which encompasses numerous hardware and software

* *Students, Asian Law College*

technologies and can be applied on any level, including personal, corporate or governmental devices or networks. Passwords are a cyber security tool that people encounter nearly every day. Other common cyber security tools include:

1. Anti-virus/anti-malware software
2. Software patches
3. Firewalls
4. Two-factor authentication
5. Encryption

A cyber security plan is critical for any company with highly sensitive information. Many companies now appoint a chief security officer (CSO) or chief information security officer (CISO) to oversee their cyber security. Most of the businesses have a Chief Information Security Officer (CISO) who is responsible to implement the necessary defence mechanism to protect the organization from external and internal data thefts.

The concept of Cyber Crimes- Cyber crimes are the criminal activities carried out by means of using digital devices like computers through the internet. Basically, a crime committed by using the internet is called a cyber-crime. Cybercriminals often exploit less developed countries due to less attention og government in this issue and then use these exploitations to target more developed countries to gain access to big multinational companies. Cybercrime is an attempt to destroy or infect computer networks in order to extract or extort money or for other malicious intentions such as procuring necessary information. Cyber crimes alter computer code, data or logic via malicious code resulting in troublesome consequences which can compromise the information or data of the organizations to make it available to cybercriminals. Cyber crimes consist of various attacks which are hacking, D.O.S, Virus Dissemination, Credit Card Fraud, Phishing or Cyber Stalking. It's the new boardroom discussion. Since we are living in the most technologically sophisticated threat environment ever, companies are paying attention to the cyber security domain. With the increasing amount of data businesses and its customers are producing comes an increasing number of people maliciously trying to obtain it. In relevant previous years, we saw increases in ransomware attacks, financial fraud and massive data breaches. It was a busy year for security practitioners, and 2019 will be no different, with new global regulations, redesigned threats to new devices, and ways to combat those threats. International Chamber of Commerce (ICC) also leverages its worldwide reach to strengthen cyber capacity and expertise globally, sharing business recommendations and experience with intergovernmental organisations and relevant forums addressing cyber security risks and management. However, business managers, including executives and directors, must recognise that cyber risk management is a continual process with no end solution. But improving cyber security is possible via a risk management process that puts heavy emphasis on management. It is difficult to take action and ensuring information security best practices are adopted within enterprises. One of the institutions the ICC Cyber security developed a guide for business, a pragmatic guide to starting a cyber security conversation between information technology specialists and company management.ICC global digital appendix of cyber security resources was created as an evolving digital appendix of resources that serves as a living database and provides localized advice from standards of practice to technical standards.

CHALLENGES IN INDIA

Cybercrimes are crimes specifically dealt with computers and networks, such as hacking, phishing and processing traditional crimes through the use of computers (such as child pornography, hate crimes, telemarketing/internet fraud). Some common cybercrimes are briefly discussed below:

1. Hacking: Hacking in simple terms means an illegal intrusion into a computer system and network. There is an equivalent term to hacking i.e. cracking, but from Indian legal perspective there is no difference between the term hacking and cracking.
2. Child Pornography: The internet is extensively accessed and used for sexual abuse of children's. While children access and use the internet to become the victim of Paedophiles. Paedophiles (a person who is sexually attracted to children) lure the children by distributing pornographic material and then pursue them for sexual exploitation.
3. 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. Cyberstalking can be defined as the repeated acts of harassment or threatening behaviour of the cyber-criminal towards the victim by using internet services.
4. Denial of Service: This is a technology-driven cyber intrusion, whereby the influencer floods the bandwidth or blocks the user's emails with spam emails depriving the user, access to the internet and the services provided therefrom.
5. Data Diddling: It involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
6. Dissemination of Malicious Software (Malware): Malware is defined as software designed to perform an unwanted illegal act via the computer network. It could be also defined as software with malicious intent

and it can be executed through the virus, worms, Trojans horse programme, hoax and spyware.

7. Web Jacking: Web Jacking occur when someone forcefully takes control of a website (by cracking the password and later changing it)
8. Phishing: It lures users to a phoney website, usually by sending them an authentic appearing e-mail. Once at the fake site, users are tricked into divulging a variety of private information, such as passwords and account numbers.
9. Credit Card Frauds: It is theft and security of data of cardholder facing the payment problem.
10. Password Sniffing: Password Sniffers are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents.
11. E-Mail Bombing/Mail Bombs: E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's Email account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider).
12. Identity Theft: Identity theft is a fraud involving another person's identity for an illicit purpose.
13. Data Related: It encapsulates the data interception, data diddling and data theft etc.
14. Network Related: It includes Network interference, Data Security Network sabotage.

According to Economics Times out of the top 10 most targeted countries by cyber attackers, India ranks third and cyber security defenders are facing a lot of threats from these cyber criminals. A Cyber crime is an illegal activity and is continuously increasing in India for financial loots. India is rapidly moving towards a digital ecosystem. The number of connected devices is only increasing and the Internet is penetrating the remotest of areas, but have we covered all our bases? There are huge gaps in India's cyber-security infrastructure. India might be ready for a digital future but is it truly prepared to handle the security risks that tag along

JUDICIAL ACTIVISM

- Kumar v. Whiteley (2009): In this case the accused gained unauthorized access to the Joint Academic Network(JANET) and deleted, added files and changed the passwords to deny access to the authorized users. Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and made an alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.
    - Verdict: The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offence)
- State of Odisha v. Jayanta Das (2017): For the first time in the judicial history of Odisha, a local Friday held guilty one person in a cyber pornography case and sentenced him to six years of imprisonment.The Puri sub-divisional judicial magistrate court convicted Jayanta Kumar Das, a known RTI activist, for uploading a photo of a married woman on a pornographic website in 2012. The sdjm, Shibasis Giri, while sentencing six-year imprisonment also slapped an Rs-8,000 fine on Das.The cyber cell of the Odisha crime branch police had registered a case following a complaint by a local journalist. After an investigation, the crime branch had arrested Das on September 18, 2012, under section 66(c) and 67(a) of the Indian Information Technology Act 2008 and under sections 292, 465, 469, 500 of the Indian Penal Code. Das used to send obscene photos and messages to the wife of the journalist by opening fake account in order to teach a lesson to the journalist who had once written against him sentenced to six years' imprisonment and a fine on charges of forgery, identity theft and cyber pornography for creating a fake profile on a pornographic website in the name of the complainant's wife.
- Shankar v. State (2010) (see "Electronic theft" above): a case was also made out that by downloading, copying and causing the publication of confidential information, the accused diminished the value and utility of such information and affected it injuriously.
- Bhim Sen Garg v. State of Rajasthan (2006): fabrication of an electronic record, or committing forgery by way of interpolations in a CD; and
- Dr Prakash v. State of Tamil Nadu (2002): The appellant stands convicted and sentenced by the learned Additional Sessions Judge holding that the alleged guilt against the appellant, he was proved beyond

a reasonable doubt

  - ○ Verdict: - He was convicted under section-67 of Information Technology Act and sentenced to imprisonment for posting nude pictures of female patients online in contravention of Section 367 of Indian Penal code and under section 4 read with section 6 of Indecent Representation of Women (Prohibition) Act, 1986.

- IDRISHBHAI SAIFUDDINBHAI HATHI V STATE OF GUJARAT & 2 : The petitioner is an agriculturist. He possesses savings bank account No.210910100002143 in Bank of HC-NIC Created On Sun Mar 13 22:05:12 IST 2016 R/SCR.A/1410/2016 ORDER India at Pisawada Branch.It is the sway of the petitioner that on 16.2.2015 when he went to ATM,SBI, Bazar Branch to withdraw Rs.1000/-, the machine was not working properly. He managed to get the amount of Rs.1000/- after inserting the card twice or thrice with the help of some persons. It is his say that to his shock he realized that sum of Rs.50,000/- had been deposited from his account on 16.2.2016. Therefore, he rushed to his bank to find out the truth of the matter only to find another shock that the card, which he was carrying was not that of his but that of a third person. His card had been taken away by those who camouflaged to help him. He, therefore, had lodged a complaint of cheating by giving a representation to P.I.Dholka police station and as no FIR is lodged,
  - ○ Verdict:-This Hon'ble Court may be pleased to grant such other and further relief's as deemed fit and proper in the interest of justice."Learned advocate Mr.M.A.Saiyed appearing for the petitioner has urged that this not only concerns the offence of fraud and cheating but also relates to cyber-crime. He has also placed in service, a communication shot by the Police Commissioner, Ahmedabad on 5.5.2012 to emphasize that every time there is a question of cyber-crime, ordinarily, no complaint is being registered.

Surveys

Internationally, businesses are intimately familiar with the need for data protection. Yet 2017 has taught us that even some of the largest businesses holding some of the most sensitive consumer data are still vulnerable—and at times, poorly secured. Around the world, hackers increasingly targeted businesses and governments. Small Business and even hospital learned the hard way that enterprise businesses are not the only ones who need to be concerned.

- 32 per cent of U.S. organizations were victims of cybercrime in 2016, with 34 per cent expecting to become victims in the next two years. (Source: PWC)
- In 2016, adware affected around 75 per cent of organizations in 13 countries. (Source:Cisco)
- In the first half of 2018, the industry with the highest number of reported DDoS attacks was the wired telecommunications carrier industry, with almost 800,000 attacks during that period.

Figure 3: Attacked users on Malware

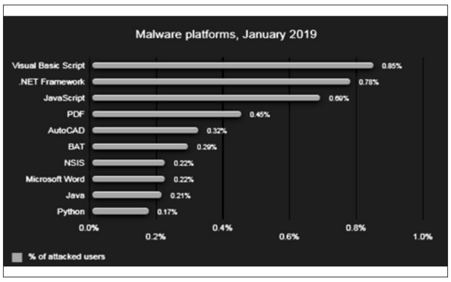
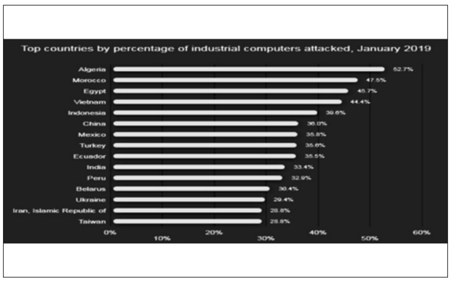


Figure 4: Cyber Attacks Percentage



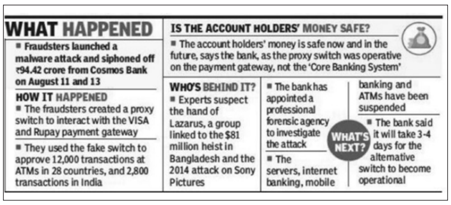
Cyber Attack on Cosmos Bank

A daring cyber attack was carried in August 2018 on Cosmos Banks Pune Branch which saw nearly 94 Crores rupees being siphoned off. Hackers wiped out money and transferred it to a Hong Kong situated bank by hacking the server of Cosmos Bank. A case was filed by Cosmos bank with Pune cyber cell for the cyber attack. Hackers hacked into the ATM server of the bank and stole details of many visa and rupee debit cards owners.

In July 2018 fraudsters hacked into Canara bank ATM servers and wiped off almost 20 lakh rupees from different bank accounts. The number of victims was over 50 and it was believed that they were holding the account details of more than 300 ATM users across India. The hackers used skimming devices on ATMs to steal the information of debit card holders and made a minimum transaction of INR 10,000 and the maximum of INR 40,000 per account. On 5 August 2018, two men were arrested in New Delhi who was working with an international gang that uses skimming activities to extract the details of a bank account.

- India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA
- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm ”Symantec Corp”

Figure 5: Cyber Attack at Cosmos Bank, Pune



WHAT HAPPENED

■ Fraudsters launched a malware attack and siphoned off ₹94.42 crore from Cosmos Bank on August 11 and 13

HOW IT HAPPENED

■ The fraudsters created a proxy switch to interact with the VISA and Rupay payment gateway

■ They used the fake switch to approve 12,000 transactions at ATMs in 28 countries, and 2,800 transactions in India

IS THE ACCOUNT HOLDERS' MONEY SAFE?

■ The account holders' money is safe now and in the future, says the bank, as the proxy switch was operative on the payment gateway, not the 'Core Banking System'

WHO'S BEHIND IT?

■ Experts suspect the hand of Lazarus, a group linked to the $81 million heist in Bangladesh and the 2014 attack on Sony Pictures

WHAT'S NEXT?

■ The bank has appointed a professional forensic agency to investigate the attack

■ The servers, internet banking, mobile banking and ATMs have been suspended

■ The bank said it will take 3-4 days for the alternative switch to become operational

72 Per cent of Indian Companies Faced Cyber Attack in 2015

Incidences of cybercrime in India shot up drastically in 2015, with 72 per cent companies in the country falling prey to online attacks this year, a survey report said.“Around 72 per cent of Indian companies faced cyber crimes this year alone. 94 per cent respondents indicated that cyber-crime is a major threat faced by organisations, but surprisingly only 41 per cent indicated that it forms part of the board agenda,” the KPMG Cybercrime Survey Report 2015 prepared by KPMG in India, a professional services firm, said. The survey report was released in the presence of Mumbai Police Commissioner Ahmed Javed today. 83 per cent respondents of the 250+ C-suite executives that participated in the survey indicated that there is usually external involvement in cyber-attacks with directors/management being most vulnerable according to 64 per cent, the report said adding, “It was also alarming to note that 54 per cent indicated that spend on cyber defences is less than five per cent of the IT spend.” City police commissioner urged the companies to approach police instead of leaving such incidents to go unreported. “The reason for this (incidents being unreported), usually, is that the company is afraid of its reputation being spoilt in the market or his shares might come down,” said Commissioner Javed. Also, the advancement and adoption of technology have enabled criminals to leverage upon it to carry out crime, he said. The Mumbai police have a dedicated cyber police station and are continuously strengthening itself by undertaking training to deal with cyber-crime cases, he informed. “It is critical for the citizens, both corporates and individuals, to be aware of cyber risks and not fall prey to the phishing scams. We are undertaking a drive to educate and create awareness among citizens with reference to cyber-threats,” Mr Javed said.

STATUTORY FRAMEWORK GOVERNING CYBER SECURITY IN INDIA

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) Introduction of a computer contaminant/virus; and

(ii) Damage to any computer, computer system or computer network or any data, database or computer program residing therein (Sec. 43(c) and (d), ITA).

The above offences are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession of any plate (including negative duplicating equipment, block, mould, etc.) for making infringing copies of copyrighted work is punishable with imprisonment of up to two years and a fine (Sec. 65, Copyright Act).

Dishonestly receiving stolen computer resources or communication devices is punishable with imprisonment of up to three years or a fine of up to INR 100,000 (Sec. 66B, ITA).

Identity theft or identity fraud (e.g. in connection with access devices):- Publication of electronic signatures: (i) that are fake; or (ii) for fraudulent/unlawful purposes, is punishable with imprisonment of up to two years or with a fine of up to INR 100,000 or with both (Secs 73 and 74, ITA).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement);- The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) Downloading, copying or extracting data/information from a computer resource (including any removable storage medium) (Sec. 43(b), ITA); and

(ii) charging services availed of by a person to the account of another person by tampering with/manipulating any computer (Sec. 43(h), ITA).

The above is punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Violation of privacy by intentionally or knowingly publishing/transmitting a private image of a person without his/her consent is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 66E, ITA).

Disclosure of personal information obtained while providing contractual services, with the intent/knowledge that wrongful loss/gain will result, is punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 72A, ITA).

Criminal copyright infringement (i.e. with knowledge): knowingly using an infringing copy of a computer program, and infringement and passing off of trademarks, is punishable with imprisonment of up to three years and a fine of up to INR 200,000. In each case, an enhanced penalty is invoked upon subsequent convictions (Sec. 63 and Sec. 63B, Copyright Act and Sec. 104 of the Trade Marks Act).

Theft, cheating, fraud, dishonest misappropriation and criminal breach of trust provisions under the IPC may also be invoked

Other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

1. Destroying, deleting, injuring, altering or diminishing the value/ utility of information residing in a computer resource; and
2. Stealing, concealing, destroying or altering computer source code (including computer commands, design and layout, program analysis, etc.) with an intention to cause damage (Sec. 43(i) and (j), ITA).

The above is punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Knowingly or intentionally tampering (concealing, destroying or altering) with computer source documents required to be kept/maintained by law is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 65, ITA)

Laws, rules and regulations those are applicable in Indian jurisdiction. This may include, for example, laws of data protection, intellectual property, breach of confidence, the privacy of electronic communications, information security, and import/export controls, among others.

1. Information technology laws
   a. Information Technology Act, 2000 (“ITA”);
   b. IT (Certifying Authority) Regulations, 2001;
   c. IT (Security Procedure) Rules, 2004;
   d. IT (Procedure and safeguards for an interception, monitoring and decryption of information) Rules, 2009 (“Decryption Rules”);
   e. IT (Procedure and safeguards for blocking for access to information by the public) Rules, 2009;
   f. IT (Procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009;
   g. IT (Intermediaries Guidelines) Rules, 2011 (“Intermediary Rules”);
   h. IT (Guidelines for Cyber Cafe) Rules, 2011;
   i. IT (Electronic Services Delivery) Rules, 2011;
   j. IT (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013 (“CERT Rules”); and
   k. National Cyber Security Policy, 2013.
   l. In addition, relevant offences under the Indian Penal Code, 1860 (“IPC”) may also be added to offences under the ITA at the time of prosecution.

2. Privacy and data protection laws: - IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“Privacy Rules”):- when the Information Act 2000(hereinafter referred to as IT Act) first came in force on October 17, 2000, it lacked provisions for protection and the procedure to be followed to ensure the safety and security of sensitive personal information of an individual. This led to several other amendments and bills being passed and finally The Information Technology(Amendment) Act, 2008 inserted Sec. 43A in the IT Act which notified and Information Technology (Reasonable security practices and procedure and sensitive personal data or information) Rules, 2011(hereinafter referred as the 2011 Rules). The key features of the 2011 Rules are:-
   a. These 2011 Rules only apply to body corporates and person located in India Sec43A of the IT Act explicitly provides that whenever a body possesses or deals with any sensitive personal data or information, and is negligent in maintaining a reasonable security to protect such data or information, which therein causes wrongful gain to any person, then such body corporate shall be liable to pay damages to the person so affected
   b. A list of items has been provided which are to be treated as sensitive personal data which include passwords biometric information sexual

orientation, medical reports etc but any information which is freely available or accessible in the public domain is not considered to be sensitive personal data.

c. Anybody seeking such sensitive personal data must draft a privacy policy which has to be published on the website of the body corporate, containing details of information being collected and purpose for its use.

d. The purpose must be clear and information used only for such consent as given and data to be retained only till such time is needed.

e. The 2011 Rules also provide Grievance Office who shall be responsible to address grievances of information providers within 1 month for resolution of such grievances. Body corporates must have an audit of the security practices and procedures implemented by it by an auditor at least once in a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resources.

f. The punishment for disclosure of information in breach of lawful contract and imprisonment under the IT Act may be for a term not exceeding 3 years or with a fine which maybe Rs.5,000,000 or with both.

Thus, as can be seen, Sec 43A of the IT Act, 2011 Rules and many similar provisions are there under the GDPR but applicable only for the residents of India. However, this does mean that most companies already have a privacy policy in place which can now be further developed and extended to include and encompass the stricter regulations of GDPR so that they do not face any penalties for breaches under the GDPR.

3. The government recently released a draft Digital Information Security in the Health Care Act, which is geared towards the protection of "digital health data", "personally identifiable information" and "sensitive health-related information" ("Health Information"). This Act is currently in draft form but is intended to apply (once enforced) to all clinical establishments and entities/ individuals that generate, collect and have custody of Health Information.

4. Intellectual property ("IP") laws

   a. (i) Copyright Act, 1957.
   b. (ii) Patent Act, 1970.
   c. (iii) Trade Marks Act, 1999.

5. Credit Information Companies Regulation Act, 2005("CICRA") As per the CICRA, the credit information pertaining to individuals in India have to be collected as per privacy norms enunciated in the CICRA regulation. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. Based on Fair Credit Reporting Act and Graham Leach Bliley Act, the CICRA has created a strict framework for information pertaining to movable property has been defined as property which is not attached to anything and is not a land. credit and finances of the individuals and companies in India. The Regulations under CICRA which provide for strict data privacy principles have recently been notified by the Reserve Bank of India.

AADHAR CARD

Aadhar system a nationwide biometric identification system is being currently challenged in India with the key dispute being whether the norms for the compilation of the demographic biometric data by the Government violates the right to privacy. This card has to be applied for the individuals and in the application requires a person to provide his or her personal data. This card is provided by the Government of India. Recently, the Government of India has mandated that even foreign residents who are taxpayers in India must obtain an Aadhar Card along with the already in place of PAN(Permanent Account Number). Thus, with the recent GDPR (General Data Protection Regulation) coming into force, the information obtained by the Government of India under the Aadhar system is impacted, especially for EU(European Union) Citizens currently residing in India. The Aadhaar scheme which was first introduced as a means of targeted distribution of subsidies, is today being implemented towards a variety of purposes, including the fight against black money, transaction authentication, and 'know your customer' requirements for banks and telecom companies. Aspects of Aadhaar Act, such as (i) security of the Aadhaar system, (ii) the inability of the individual to file complaints (for violation under the Aadhaar Act) relating to theft or misuse of their data, and (iii) the inability to withdraw / delete one's data once registered with the UIDAI (government authority dealing with Aadhaar laws) is under scrutiny in the current pending litigation with the Supreme Court of India. While the judgement which delivered the decision regarding privacy as a fundamental right of individuals subject to reasonable restrictions was not directly intended to impact the use of Aadhaar card, it will now have a significant impact on the pending litigation. The outcome of this pending litigation will significantly impact data protection policies in India.

The Data (Privacy and Protection Bill), 2017:-Recently, a Bill was introduced in Parliament proposing to bring privacy under the ambit of legislation. This is not the first Bill on privacy introduced in Parliament. However, this Bill is different from the previous Bills in the sense that it seeks to make the consent of an individual for collection and processing of personal data mandatory. The Bill states that the individual will have the sole right and the final right to modify or remove personal data from any database, public or private. In the context of sensitive and personal information, the person must provide his or her express and affirmative consent for the collection, use, storage of any such data. This Bill applies not only to private corporations or body corporate but is equally applicable to state entities, government agencies or any other persons acting on their behalf. Even the definition of a "third party" under this Bill includes the public authorities. This symbolises a significant change in law from the existing regime under the IT Act and the 2011 Rules in India. However, with respect to sensitive, personal data, Section 20(2) provides that no sensitive data shall be processed for any other purpose apart from its intended use but can be used by welfare schemes and social protection laws. Hence, this would imply that the Aadhaar scheme, as mentioned earlier, would also have access to a person's personal, sensitive information. This Section is analogous with the present dispute at the Supreme Court and will continue to be subject to debate due to the existing privacy concerns. Although this Bill, which is still pending to be passed into legislation, is much more in line with the stricter GDPR norms it is unlikely to come into force until the pending litigation regarding the Aadhaar scheme comes to a conclusion regarding the use of the Government of the personal and sensitive data who resides in India

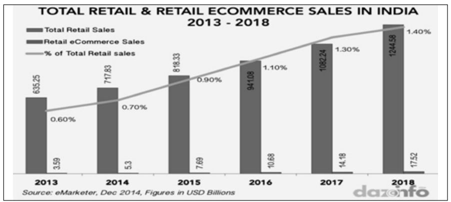
DIGITAL INDIA VIZ-A-VIZ CYBER SECURITY

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy. The journey of e-governance initiatives in India took a broader dimension in the mid-90s for wider sectoral applications with emphasis on citizen-centric services. Later on, many States/UTs started various e-governance projects. Though these e-governance projects were citizen-centric, they could make lesser than the desired impact. The government of India launched the National e-governance Plan (NeGP) in 2006. 31 Mission Mode Projects covering various domains were initiated. Despite the successful implementation of many e-governance projects across the country, e-governance as a whole has not been able to make the desired impact and fulfill all its objectives.

Need of Digital India

About one-third of India's population is internet users, and one-fourth of mobile internet users are in rural areas. But internet penetration in villages, at 8.6% compared to 37.4% in cities, has a long way to go, and this is the statistic 'Digital India' hopes to change. As per a World Bank report, a 10% increase in a country's broadband connections leads to a 1.38% rise in its gross domestic product.

Figure 6: Increase in Ecommerce



Source: eMarketer, Dec 2014, Figures in USD Billions

Figure 7: Online Transaction after Demonetization in India

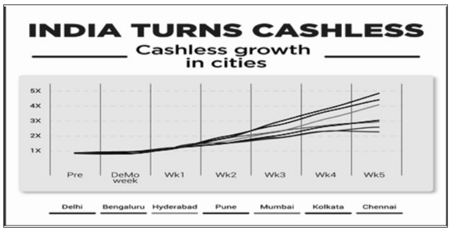
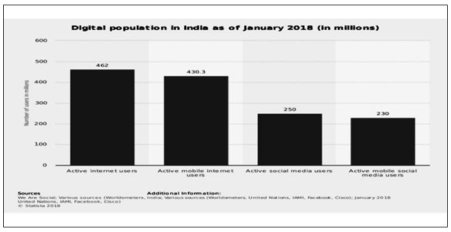


Figure 8: Digital Population in India



Government Grand Vision

Our government has emphasized the need for leveraging technology to drive the nation and bring in transparency within governance and simplifying citizens' access to public services. The vision of building 'one hundred smart cities' – which has been allocated Rs. 7,060 crore – is a major project that would rely strongly on technology, calling for a robust cloud computing backend coupled with real-time surveillance and big data analytics technologies. The Digital India programme will be implemented in phases from the current year until 2018. The vision of the government under the project includes the creation of ICT infrastructure like the high-speed Internet at gram panchayat level, on-demand availability of government services like health, education etc., and digital empowerment of citizens, especially through digital literacy. Under the programme, the government will train one person in each household digitally through ICT training to 10 lakh people with an outlay of Rs.376 crores.

Impact on overall economy

Analysts feel 'Digital India' has the potential to be one of most transformative programmes in recent times. Digital India Initiatives would provide the much-needed impetus to the economic growth given its focus on key social and industry sectors. Not only IT/ITeS, telecom, electronics manufacturing sectors would be benefited from Digital India, but we would see a positive impact on other industry sectors as well, like Power Sector, Banking, and Financial Services.

Implementation & Monitoring Strategy

Digital India Advisory Group (DIAG) would be created, which will be headed by Minister of Communications to supervise the implementation of the programme, advice the government on policy issues and strategic interventions necessary for accelerating the implementation of Digital India Programme across Central and State government ministries/departments. The government will appoint nodal officers at key ministries to ensure smooth implementation of 'Rs. 1 lakh crore 'Digital India' programme. The new posts of 'Chief Information Officers' (CIO) would be created in at least 10 key ministries to supervise the implementation.

Digital India Initiatives & Need for Cyber Security

We have already discussed the alarming rise of cyber crimes in India and the government's continuous struggle to cope up with the latest trends of attacks. Apart from domestic cyber threats, India also faces tough cyber-attacks from countries including Pakistan, China, UAE, US, Turkey, Brazil, Bangladesh, Algeria and nations in Europe. To counter this alarming situation, the Indian Government has aimed to step up cyber security measures under Digital India programme starting with an Rs. 800-crore centre that will help people check and clean their computer system from viruses and other malware. The programme is intending to build a capability to tell you that not only can track the malware in the computer system but will clean that infection as well. A year in the works, the National Cyber Security and Coordination Centre (NCSC) will analyze Internet traffic data scanned and integrated from various gateway routers at a centralized location. It will facilitate real-time assessment of cyber-security threats and generate actionable reports for various agencies. As a multi-agency body under the Department of Electronics and IT, the NCSC will include the National Security Council Secretariat, the Intelligence Bureau, the Research and Analysis Wing (RAW), the Indian Computer Emergency Response Team (CERT-In), the National Technical Research Organisation (NTRO), the three armed forces and the Department of Telecommunications. It is expected to subsume the work done by CERT-In as well as issue alerts in the event of a cyber-attack.

CONCLUSION

The need to develop and enforce legislation, regulations, standards and competence in the face of pervasive and dynamic digital technology and attendant security concerns. Though not all people are victims of cyber crimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they executed by a computer. The hacker's identity is ranged between 12 years young to 67 years old. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren't guns anymore; they attack with mouse cursors and passwords. As internet technology advances so do the threat of cybercrime. In times like this these, we must protect ourself from cybercrime. Antivirus software, firewall and security patches are just the beginning. To stress on the need to engage in the end to end user education on the danger of cybercrime, on the imperative of adequate cyber security, on the protection of critical infrastructure and on the need for self-reporting. Cybercrimes can be reduced by creating awareness programmes between people and developing security system of computers.

SUGGESTIONS

1. **Use Strong Passwords**
   Use different user ID/password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum of 10 characters in total) and change them on a regular basis.
2. **Secure your computer**
   a. **Activate your firewall**
   Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
   b. **Use anti-virus/malware software**
   Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
   c. **Block spyware attacks**
   Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
3. **Be Social-Media Savvy**
   Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to privacy. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
4. **Secure your Mobile Devices**
   Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.
5. **Install the latest operating system updates**
   Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. **Protect your Data**
   Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data and store it in another location.
7. **Secure your wireless network**
   Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
8. **Protect your e-identity**
   Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).
9. **Avoid being scammed**
   Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.
10. **Call the right person for help**
    Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

REFERENCES

1. A study of cyber security challenges and its emerging trends on latest technologies by G. Nikhita Reddy and G.J. Ugander Reddy : https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf
2. Cyber Security Challenges: Some reflections on Law and Policy in IndiA
3. Government initiatives https://blog.ipleaders.in/cyber-security-initiatives/
4. https://www.comparitech.com/vpn/cyber security-cyber-crime-statistics-facts-trends/
5. https://www.manupatrafast.in/pers/Personalize
6. https://www.researchgate.net/publication/331010726_Literature_review_on_Cyber_Crimes_and_its_Prevention_Mechanisms
7. http://timesofindia.indiatimes.com/articleshow/67898571.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
8. https://timesofindia.indiatimes.com/topic/cyber-crime-cases
9. International chamber of commerce https://iccwbo.org/global-issues-trends/digital-growth/cyber security/