Exploring Cyber security threats on society

***Nagasri Vanga**

Assistant Professor (MCA)
Aurora PG College,
Punjagutta, Hyderabad.

***Abstract*: Cyber security is crucial to society as protecting information, computer networks, databases, and software programs has become one of the biggest challenges in the current day situation using countermeasures for cybersecurity. So, to ensure security, software, antivirus, firewalls, other technological tools are essential for safeguarding personal and sensitive data. As our governing bodies are building cybersecurity policies and infrastructure, all technical savvies and educated people should compliance with the cyber infrastructure. The information security triad confidentiality, integrity and availability are ensured for the information systems by reducing the damage done by cyber-attacks. An intrusion detection system (IDS) is a software application which scans and monitors networks for any suspicious activity or a policy breaching and issues alerts if any such are found. Cybersecurity, ethics, and cyber safety and cyber threats are need to be integrated with the education to reduce the risks associated with them. New approaches are finding their way to ensure cyber security. This paper focuses on emerging trends of cybersecurity using technologies like social-networking, cloud computing, e-commerce.**

***Keywords*: cyber safety, e-commerce, intrusion detection system, cyber security, cyber safety.**

Introduction

A remarkable transformation was possible in India due to the diffusion of technology to the grass root level and same happened with the computers with internet connection. Everything happened so suddenly and rapid delivery of information increased productivity and decreased cyber security. India stands fifth in worldwide ranking of countries affected by cybercrime [1]. Among the Indian organizations, which responded to KPMG's [2] Cybercrime survey report 2014, 89 % considered cybercrime as a "major threat" (p, 3). Much of the vulnerability is because of computer illiteracy and pirated software.

Internet is one of the fastest –growing areas of technical infrastructure development [1]. Since the degree of digitization of economic activities is tightly linked to the probability of experiencing cyber-attacks [3] , India's massive digitization efforts deserve mention. More than 80% of commercial transactions are done online today. As a consequence, there is an increasing cybersecurity concern among organizations, individuals and government agencies. Cyber Security plays an important role in the development of information technology, as well as internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being[1]. Society has become dependent on cyber systems across the full range of human defense[2]. Internet users are worried that they give away too much of personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information.

And hence since 2006, concern for personal information has increased. Due to the country's lack of indigenous technology and patents related to cyber security, the GoI has announced that it would provide financial incentives to Indian firms to acquire Foreign firms with high-end cyber security technology [4].

Cyber Security wholly depends on the care people take, when they install, maintain and use computers and Internet. Social-networking sites are the most vulnerable targets to steal personal data. According to a study by a US cyber tech firm CrowdStrike, on an average, companies across the world take seven days to respond to cyber security breaches, in contrast, Indian companies take around nine days. These statistics push India to the bottom of the list when it comes to dealing with the cyber security threats and attacks.

Current Strategies To IT – Security

The onset of the pandemic resulted in heavier dependence on technology, coupled with a deeper adoption of inter connected devices and hybrid work environments.

India Stress Test

Indian Computer Emergency Response Team (CERT).

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security. It Collects, analyzes and disseminates information on cyber incidents. Forecasts and issue alerts of cyber security incidents. It coordinates with the response actions of cyber activities. It issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents. Data Security Council of India (DSCI), is a not-for-profit industry body on data protection in India, set by NASSCOM, committed to make cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. The main challenge now for India is to train and equip its law enforcement agencies and judiciary, particularly outside big city like Delhi, Mumbai and Bangalore. Training must expand to cover the whole country says Bajaj, at DSCI, we have developed training and investigation manual for police officer. We have trained more than 9,000 personnel of local education authorities and the judiciary on cyber security.

Most IT security management approaches consist of checklists which decision makers use to develop a coverage strategy; these generally are little more than a triage approach to categorizing threats. One popular approach for risk visualization has been the construction of a risk cube, where each axis or dimension represents one of the three components of risk (threats, assets, and vulnerabilities),and the volume of the cube represents the amount of risk[6].models have been developed which attempt to deal with risk analysis in a qualitative manner. Mark Egan (the then CTO for Symantec) in his book The Executive Guide to Information Security introduced a very simple tabular model which allows users to rate threat severities into one of three categories/columns (low, medium, and high) and then to average across columns. This simple triage approach to subjective threat impact analysis, though insightful, is notable to capture system uncertainty. Alberts and Dorofee developeda system called OCTAVE which also utilizes qualitative information to assess risk. Others have tried approaches that quantify IT security risk analysis. Beauregard applied the Value Focused Thinking (VFT) approach from general risk analysis to assess the level of information assurance within the Department of Defense units [7].

Cloud computing

Cloud computing is the delivery of various hardware and software services over the internet, through a network of remote servers. These remote servers are busy storing, managing, and processing data that enables users to expand or upgrade their existing infrastructure. The capabilities and breadth of the cloud are enormous. The IT industry broke it into three categories to help better define use cases. (i). Software as a service (Saas), (ii) Infrastructure as a service (IaaS), (iii) Platform as a Service (PaaS).

Security risks of cloud computing have become the top concern in 2018 as 77% of respondents stated in the referred survey. Proper IT governance should ensure IT assets are implemented and used according to agreed-upon policies and procedures; ensure that these assets are properly controlled and maintained, and ensure that these assets are supporting your organization's strategy and business goals. One of the risks of cloud computing is facing today is compliance. That is an issue for anyone using backup services or cloud storage. Every time a company moves data from the internal storage to a cloud, it is faced with being compliant with industry regulations and laws. Cloud-based services involve third-party for storage and security. Can one assume that a cloud-based company will protect and secure one's data if one is using their services at a very low or for free? They may share users' information with others. Security presents a real threat to the cloud.

Threats in Mobile devices and computing: Mobile devices can be attacked at different levels. This includes the potential for malicious apps, network-level attacks, and exploitation of vulnerabilities within the devices and the mobile OS. As mobile devices become increasingly important, they have received additional attention from cybercriminals. As a result, cyber threats against these devices have become more diverse. While some intrusions may not result in an immediate impact on the operation of a cyber-systems, as for example when a ―Trojan Horse‖ infiltrates and establishes itself in a computer, such intrusions are considered cyber-attacks when they can thereafter permit actions that destroy or degrade the computer's capacities [9]. Often, the focus of cybersecurity is on top-layer software, but lower levels of the software stack can contain vulnerabilities and be attacked as well. With mobile devices – like computers – vulnerabilities in the mobile OS or the device itself can be exploited by an attacker. Often, these exploits are more damaging than higher-level ones because they exist below and outside the visibility of the device's security solutions.

Countermeasures of Private Organizations

Private and Non-governmental entities play major roles in the cyber security arena. Technical standards for the internet (including current and next-generation versions of the Internet Protocol) are developed and proposed by privately controlled Internet Engineering Task Force (―IETF) [8]; The World Wide Web Consortium (W3C) is an international organization committed to improving the web. It is made up of several hundred member organizations from a variety of related IT industries. W3C sets standards for the World Wide Web (WWW) to facilitate interoperability and cooperation among all web stakeholders. It was established in 1994 at Cambridge, Massachusetts, US .Other privately controlled entities that play significant operational roles on aspects of cyber security include the major telecommunications carriers, internet Service Providers (–ISPs), and many other organizations, including:

- The Forum of Incident Response and Security Teams (FIRST), which attempts to coordinate the activities of both government and private Computer Emergency Response Teams (CERTs) and is also working on cybersecurity standards;
- The Institute of Electrical and Electronics Engineers (IEEE), which develops technical standards through its Standards Association and in conjunction with the U.S. National Institute of Standards and Technology (NIST);
- The Internet Corporation for Assigned Names and Numbers (ICANN), which operates pursuantto a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN the technical management of the Domain Name System[11].

Countermeasures of Governments

Many national governments have adopted laws aimed at punishing and thereby deterring specific forms of cyberattacks and exploitation. The U.S., for example, has adopted laws making criminal various forms of conduct, including improper intrusion into and deliberate damage of computer systems. These laws have little or no effect, however, on individuals, groups, or governments over whom the U.S. lacks or is unable to secure regulatory or criminal jurisdiction.US national security experts almost exclusively emphasize the need for national measures for enhancing cyber security [2]. More effective defenses and responses to cyberattacks and exploitation developed through government-sponsored research and coordination pursuant to cyber security plans. The GAO's July 2010 report details the specific roles being played by many U.S. agencies in efforts to enhance global cybersecurity, but ultimately concludes that these efforts are not part of a coherent strategy likely to advance U.S. interests[12]

International Countermeasure

Governments of other countries often cooperate with each other informally by exchanging information, investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and even arranging for the rendition of individuals to a requesting state. States have also made formal, international agreements that bear directly or indirectly on cyber security. [13]. International agreements that possibly bear upon cyber-security activities also include treaties(the UN Charter and Geneva Conventions) and universally accepted rules of conduct (customary law).International law also provides policies related to the use of force during armed conflict that presumably apply to cyberattacks, including for example requirements that noncombatants and civilian institutions such as hospitals not be deliberately attacked, and that uses of force be restricted to measures that are only necessary and compatible.[2].

Requirement and importance Of Cyber Security

Our dependency on the internet has become immense. And that provides enough opportunities to the fraudsters to dupe you of your money or other crucial data if you are not cautious.

Information is the most valuable asset with respect to an individual, cooperate sector, state and country. With respect to an individual the concerned areas are:

- Protecting unauthorized access, disclosure, modification of the resources of the system.
- Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
- Security of accounts while using social-networking sites against hijacking.
- One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses [5].
- Need of separate unit handling security of the organization.
- Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness [14].

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

- The requirement to notify those affect as soon as possible
- Let the government know as soon as possible
- Pay some sort of fine

California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim. In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered [15].With respect to state and country

1) Securing the information containing various essential surveys and their reports.
2) Securing the data basis maintaining the details of all the rights of the organizations at state level.

Recent Survey Issues In Cyber Security Trends

The following list was developed from cyber security research and survey [1] [16] [17] [18].

Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device are vulnerable to security risks and they are available to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perpetual problem of lost and stolen devices will expand to include these new technologies.

Safeguarding computer systems more than information systems

The emphasis is mainly on protecting information system, not just computer systems. As internet users and their businesses are preferring to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems on the whole. Rather than focusing on developing processes for protecting the computer networks and programs than information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

Social Media Networking

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

Countermeasure for Cybersecurity

In the attempt of creating a 'cyber-secure nation' for businesses and individuals, the government of India is reportedly set to unveil its cybersecurity strategy, policy in Jan 2020 to achieve the target of a $5 trillion economy. Speaking at SKOCH event Rajesh Pant, the National Cyber security Coordinator confirmed saying, "India's cybersecurity strategy policy, which will be released in the coming year will enable the government to secure the whole nation. The government's vision of $5 trillion economy will be helped to a great extent by this effort."

He added for securing the internet, it is important to have efficient coordination between government officials who are overseeing the aspect of securing the whole nation. The two key aspects of a cybersecurity frame work are the proper formation of critical infrastructure and a seamless partnership between the public and the private. To create such a stringent framework, the country requires huge budget. Ajeet Bajpai, the Director General of the National Critical Information Infrastructure Protection Center said, "Considering the size and scale of our nation, we need approximately Rs.25,000 crore budget for the same. And, there is a need to emphasize on the need to make cybersecurity a compulsory subject in the universities for high-decibel awareness. CERT-In issues alerts and advisories regarding the latest cyber vulnerabilities and countermeasures to tackle them.

Cyber Surakshit Bharat

Targeting the strengthening of cybersecurity ecosystem in India – in line with the government's vision for a 'Digital India', the Ministry of Electronics and Information Technology (MeitY) has launched Cyber Surakshit Bharat initiative. National Critical Information Infrastructure Protection Centre: NCIIPC is a central government establishment, formed to protect critical information of our country, which has an enormous impact on our national security, economic growth, or public healthcare. This was amended as per the provisions of section 70A of the Information Technology (IT) Act, 2000. NCIIPC has broadly identified the following as 'Critical Sectors':-

(a) Power & Energy
(b) Banking, Financial Services & Insurance
(c) Telecom
(d) Transport
(e) Government
(f) Strategic & Public Enterprises

Personal Data bill Protection

The approval of Personal Data Bill Protection by the Union government is to protect Indian users from the global breaches, which focuses on data localization. The bill implies the storage and processing of any critical information related to individuals only in India. The bill also aims at making social media companies more accountable and pushes them to solve issues to the spread of offensive content.

Conclusion

This paper discussed the threat to individual privacy as it is the fundamental human right. Violation of human rights comes from the unlawful collection and storage of personal data, the problems associated with inaccurate personal data or the abuse or the unauthorized disclosure of such data. This paper includes the present day threats, issues and challenges and government measures to tackle the issues to protect the society from cyberattacks. With the increasing incidents of these attacks, building an effective intrusion detection model with good accuracy and real-time performance are essential. With the increasing use of wireless media, security problems of confidentiality, integrity and authentication are also increasing. Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work. The IT industry has been playing cat and mouse game with hackers and cybercriminals for decades. Thus there is a need for cybersecurity curriculum in the near future which should give in-built cybersecurity understanding among youth and finally the IT sector will get profound skilled professionals not only in the security sector but also in every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers.

References

[1] Ravi Sharma, Study on Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June – 2012, ISSN 2229-5518 USER @2012

[2] KPMG (2014). *Cybercrime survey report 2014*. Retrieve from www.kmg.com/in

[3] Thilla Rajaretnam Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC),International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)

[4] Thomas H. Karas and Lori K. Parrott , Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839

[5] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012

[6] Loren Paul Rees, Jason K. Deane , Terry R. Rakes , Wade H. Baker, Decision support for Cyber security risk planning, Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States

[7] S. Bistarelli, F. Fioravanti, P. Peretti, Using CP-nets as a guide for countermeasure selection, Proceedings of the 2007 ACM Symposium on Applied Computing (Seoul, Korea, 2007), 2007, pp. 300–304.

[8] Abraham D. Sofaer, David Clark, Whitfield Diffie ,Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers pg185-205
[11] Clarke and Knave, 92. The authors anticipate that –*logic bombs"*—software that erases all programming, effectively negating further use of a device—will be used in attacks and may already be in place.
[12] E.g.Fraud , Related Activity in Connection with Computers, U.S. Code 18,1030.
[13] See Convention on Cybercrime CETS No. 185 at
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=EG.
[14] Cisco, Cisco 2009 Annual Security Report: Highlighting Global Security Threats and Trends, December 4, 2009.
[15] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, –Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels,‖ September 9, 2010.