ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

Cyber Security:
Strategy to Security Challenges- A Review

Vaishnavi J. Deshpande[1], Dr. Rajeshkumar Sambhe[2]

Abstract*— This paper is an overall study on the cyber security further explaining the needs of cyber security. Cyber security is the activity of protecting the computer, internet or the modern technology user to protect from cyber threats. It is seen that the amount of threats like data theft, phishing, and scams is increasing day-by-day. So this explains how the cyber security is important while dealing with internet. There are various cases in which it is found that the user is suffered up to much extent in the cases of online banking transactions. Not only this, it also poses a threat to nation's infrastructure. So there is a need to create awareness about cyber security and provide a protected and a safe environment to the user while providing the facilities of new and innovative technology.

***Index Terms*— Cyber security, society, challenges**

I. INTRODUCTION

Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. [1] Earlier, there was a system to send any information via letters, telegrams, etc. This system was quite time consuming and was not reliable. Later on, the development took place by invention of telephone, which helped to communicate from large distances and now there is an era of wireless technology. While doing this information exchange, it is mandatory that your information is to be safe while going through many processes. This implies the main purpose of cyber security.

Cyber security is a broad term that has evolved over time with no clear consensus on its exact meaning. [2] The incidents occurring like stealing someone else's personal id and using it with corrupt intentions, stealing money from someone else's account, etc. are cyber crimes. The aid to these problems is cyber security. Today, it is the need to build up the secured and safe cyber infrastructure to maintain national safety and the internet user's safety. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Cyber space is the domain generated from the interconnection between computers and telecommunication networks in order to store, modify, and exchange data via networked systems and associated physical infrastructures without regard to physical geography. [3] Cyber security involves the protection of our sensitive information like credit card number, ATM card pin, etc. (financial information), etc. The main reason to make user aware of his/her security through cyber security and giving user the message that while handling internet to be careful what should be shared giving preference to security, especially banking transactions. In general, cybersecurity threats are increasing rapidly, the incidents go from defaced websites to theft of large volumes of intellectual property and money, to Internet crimes. [4]

There are three core principles of cyber security: Confidentiality, Integrity, and Availability.

Confidentiality: Information which is sensitive or confidential must remain so and is shared only with appropriate users.

Integrity: Information must retain its integrity and not be altered from its original state.

Availability: Information and systems must be available to those who need it. [5]

II. IMPORTANCE OF CYBER SECURITY

The increasing volume and sophistication of cyber security threats–including targeting phishing scams, data theft, and other online vulnerabilities–demand that we remain vigilant about securing our systems and information. [5] The today's user is computer and especially internet dependent. The data which is especially posted on the social media sites is the key source for the hackers to pose a threat to user's safety, which gives rise to cyber criminals.

There will be new attacks on Android operating system-based devices, but it will not be on a massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. Small and medium-sized businesses face critical challenges due to limited resources and information, as well as competing priorities. The speed at which technology is evolving makes it difficult to stay current with security. However, better security awareness and planning can help these businesses protect their intellectual property and trade secrets, and reduce loss of productivity due to downtime. [6]

Greater organizational and public awareness is essential to inform and shape an effective national cyber security culture. Incorporating cyber risk into existing risk cultures will mean considering it together with wider organizational risks. It needs to be a standard item on the agenda rather than being seen as distinct, inscrutably complex and 'someone else's problem'. A robust cyber security culture should be responsive to the rapid pace of change in technology and innovation. [7]

III. LATEST ISSUES ON CYBER SECURITY IN INDIA

A) Cyber Terrorism:

There is one more term associated with this topic "Cyber Security", i.e., "cyber terrorism". Now what this exact means is very important to know. This term is associated with the safety of our nation's strategy because this is a way to invade the privacy of any nation's infrastructure.

Cyber terrorism is a way or a path or a mechanism through which an enemy is trying to know all the secrets of any nation and posing the threat to nation's policy.

'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at reast cause enough harm to generate fear, Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not' [8]

B) Use of internet in cyber terrorism:

The use of internet was found to be beneficial since late 1980s. It is found to be useful for the means of communication and the source of information. It must also be recognized, however, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism. The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism. [9]

C) Threat to ICT infrastructure:

Means to exploit, distort, disrupt, and destroy information resources range from hacker tools to devices such as electromagnetic weapons; directed energy weapons; HPM (High Power Microwave) or HERF (High Energy Radio Frequency) guns; and electromagnetic pulse (EMP) cannons. The attack against an information infrastructure can be carried out with both physical implements (hammer, backhoe, bomb, HERF, HPM) and cyber-based hacking tools. The same is true for the target: It can be cyber, consisting for example of information or applications on a network, or physical, such as computers or a telecommunications cable. [10]

D) National cyber security :

There is no way to underestimate the hacker, because the method by which the information is stolen by illegal means is totally out of imagination, as we are ignorant about the ways of stealing information. The changing phase of cyber attacks as well as ever-increasing sophistication of attack methods have complicated the efforts of collecting valuable intelligence information for effective proactive, preventive and protective measures. [11]

IV. CYBER SECURITY MANAGEMENT

In order to ensure safety from the incidences due to the lack of cyber security, there is need to implement cyber security management.

The goal of a cyber security management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, a robust risk management program includes ongoing evaluation and assessment of cyber security risks and controls throughout the life cycle of smart grid component software. [12] The user can ensure his safety by taking the following precautions:

1. First, update your computer, laptop, mobiles, smartphone, etc. with the anti-virus software. Now, it is also packaged with anti-malware, anti-spyware, anti-phishing, etc.
2. Access the internet carefully. While doing online shopping, online banking transactions, it is the user's responsibility to verify the trueness of the website and to check the information by the helpline number.
3. Keep the passwords secured. Choose those passwords which cannot be easily guessed or accessed by anyone.
4. Handle your personal information with care so that user will not be frustrated and be a cyber victim.

Once a nation has set its cyber security priorities, a national strategy should focus on the risks that must be identified, managed, mitigated, or accepted. National cyber risks are typically thought of as risks to information systems, that, if exploited, could negatively impact national security, economic well-being, or public safety to a significant degree. [13]

Ensure that timely and effective planning, communication, and training are prioritized. Jurisdictions handling special events on a routine basis should consider building events security training into basic and in-service training. [14] Security risk and threat assessments will change over time. If a company suffers an attack or an incident is reported in another comparable organization then this may reveal new threats that were not considered during an initial analysis. Similarly, the detection or response to a threat may provide new insights into the consequences of an attack. It is for this reason that risk assessments must be linked to incident reporting within a security management system. The Government's approach to cyber security must be consistent with the overarching principles of the National Security Strategy: Our approach to national security is clearly grounded in a set of core values, including: human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all. [15]

V. CONCLUSION

1. It is important to remember that cyber security is not an end in itself. It should not discourage the use of new technologies. [16]

2. Protecting mobile users: Mobile and flexible working is on the rise. It helps growing business attract and retain great talent and reduce the cost of office space. [17] Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a “botnet”). Configure the device to be more secure. Many smartphones have a password feature that locks the device until the correct PIN or password is entered. Enable this feature, and choose a reasonably complex password. Enable encryption, remote wipe capabilities, and antivirus software if available. [18]

3. Protect wireless devices: Personal firewalls can protect individual devices from attacks launched via the “air connection” or from the internet. [19]

4. Everyone has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. [20]

REFERENCES

[1] G.Nikhita Reddy[1], G.J. Ugander Reddy[2], “A study of cyber security challenges and its emergning trends on latest technologies”, 1- 6.

[2] “Some perspectives on cyber security: 2012”, 16 November 2012, 2 – 22.

[3] ”Understanding cybercrime: phenomena, challenges and legal response”, September 2012, Telecommunication Development Sector, 2 – 366.

[4] Dr. Amos Nungu, “Cyber Security in Tanzania: Roles and Responsibilities”, CyberSecurity Mini-Conference, June 26, 2012, 1-3.

[5] “Why Cyber Security Is Important”, State of Wyoming, Office of the Chief Information Officer, 2001 Capitol Ave, Rm 237, Cheyenne, WY 82002, 2-2.

[6] Ravi Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society”, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518,1-4.

[7] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, “Cyber Security and the UK’s Critical National Infrastructure”, A Chatham House Report, 11-50.

[8] SS Raghav, “cyber security in india's counter terrorism strategy”, 2-5.

[9] “The use of the Internet for terrorist purposes, In collaboration with the united nations counter-terrorism implementation task force”.M M Chaturvedi1, MP Gupta1 and Jaijit Bhattacharya1, “Cyber Security Infrastructure in India: A Study”, 2-1.

[10] Dr Gulshan Rai, “National Cyber Security Policy”, draft volume 1.0, 6-21, 26 Mar 2011.

[11] Evgeny Lebanidze Cigital, “NRECA / Cooperative Research Network Smart Grid Demonstration Project Guide to Developing a Cyber Security and Risk Mitigation Plan”, 17-125.

[12] Cristin Flynn Goodwin[1], J. Paul Nicholas[2],” Developing a National Strategy for Cybersecurity foundations for security, growth, and innovation”, October 2013.

[13] Edward Connors, “Planning And Managing Security for Major Special Events: Guidelines for Law Enforcement”, March 2007, 30-128.

[14] Prof. Chris Johnson, “Trends in Information Security, Topic Description: The Economics of Threat Analysis for Cyber Security”, 3-4.

[15] “Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space”, June 2009, 13-32.

[16] “Meeting The Challenges of Endpoint Security”, volume 3.6, 2010, 5-10.

[17] Paul Ruggiero[1], Jon Foote[2], “Cyber Threats to Mobile Phones”, 3-6.

[18] “Wireless LAN Security, Enabling and Protecting the Enterprise”, 9-12.

[19] K Yadav, “Conclusions and Future Scope of the Work”, 2012, 3-4.

AUTHOR BIOGRAPHY

Vaishnavi J. Deshpande is student of Department of Computer Science and Engineering, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India-445001.

Dr. Rajeshkumar U. Sambhe is Associate Professor (Mechanical Engineering) in Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, India. He has completed his Doctoral studies from Government College of Engineering Amravati and awarded Ph.D. from Sant Gadge Baba Amravati University, Amravati. He holds his Bachelor Degree in Mechanical Engineering with University Merit and Master Degree in Production Technology with total 17 years experience. He has published 15 papers in international journals and conferences including paper International Journal of Productivity and Quality Management and International Journal of Business Excellence.