A guide to comprehending cybersecurity

Mrs. Manasi P. Shirurkar[1], Dr. Minakshi Tumsare[2]

[1,2]MCA Management
Institute of Management and Career Courses
Pune, India
msu.imcc@mespune.in , mst.imcc@mespune.in

Article Info
Page Number: ***231 - 236***
Publication Issue:
March-April 2019

Abstract:

Technology is emerging at a tremendously vigorous pace. Often common people are not acquainted with these new eccentric words ensuing from technological advancements and its communication with other branches of life. Therefore, paper will discuss cybersecurity as one of the most critical issues the society is facing today and its effects that will be seen in near future too! Firstly paper concentrate on the threats that are alive and emerging as a delinquent. Further it enlightens on the difference between cybercrime and cyber terrorism with some instances as pivotal factor in securing cyber space. The purpose of this paper is to make understand individuals the need of national cyber security which will yield support in global cyber security. Paper also educates on cyber warfare and cyber threats also. Finally paper will drive on cyber securing technological trends-cyber planning and cyber insurance.

Article History
Article Received: *02 March 2019*
Revised: *20 March 2019*
Accepted: *14 April 2019*
Publication: *29 April 2019*

INTRODUCTION:

Cyber security is the protection of systems, networks and data in cyberspace. The Internet allows users to gather, store, process, and transfer massive amounts of data, including proprietary and sensitive business, transactional, and personal data. At the same time that businesses and consumers rely more and more on such capabilities, Cybersecurity threats endure to plague the Internet economy. Cybersecurity extortions evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global. Cybercrime, Digital intrusion, Cyber terrorism are sides of same coin from which unintended individuals access resourceful data. These countless methods make us major to have rigorous techniques for guarding cyber space all over. Cyber Security complements major arenas from social networking, Ecommerce, Artificial Intelligence, Data warehouses etc. As a result, cyber security is becoming multifaceted issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses.

Cyber Terrorism Vs. Cyber Crime:

Cyber Terrorism is far way distinct from Cyber Crime. So far, the international community has not decided on an exact definition of “terrorism” that can be applied universally. But clearly, it is an emerging threat globally. Cyber terrorism is “a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal." To be more precise it is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies. Cyber terrorism is the convergence of terrorism and cyber space. Terrorist groups are increasingly computer savvy, and some probably are acquiring the ability to use cyber-attacks to cause isolated and brief disruptions of national infrastructure.

History and Instances:

a) The first cyber-attack by a terrorist was recorded in 1998 when the Black Tigers guerillas jammed Sri Lankan embassy email inboxes with hundreds of emails for a couple of weeks, generated by special software.
b) In the course of the Kosovo war in 1998, NATO computers were subjected to denial-of-service attacks and email bombs. Web defacement against US government websites was conducted by Chinese activists as retaliation for the accidental bombing of the Chinese embassy in Belgrade by NATO forces.
c) In 2007, Estonia's government and economy was struck by distributed denial-of-service attacks allegedly conducted by a Russian group.
d) Terrorist attacks on the World Trade Center U S in September 2001, is another example for Cyber terrorist attacks.

Cybercrimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. An increasing number of criminals are attracted by cybercrimes, because these types of crimes are convenient, anonymous, quick, diverse, and relatively low-risk. In the past, cybercrimes were committed by individuals or groups without decent organization, whilst nowadays organized crime structures and highly-trained professionals are deeply involved in this lucrative criminal activity.

Instances:

Now a days Cybercrime is done in many ways to numerous individuals .The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as Phishing, Hacking, Internet fraud or theft, Cyber stalking, Cyber intrusion through viruses or malware, money laundering, Cyber bulling, Copy right infringement etc.

We can review that Cyber terrorism is all about hindering cyber space security and attacking on any aspects of national or government domains; whereas cybercrime is illegally disturbing group of persons or individuals for information or data mugging for intentional/amusement or any sort of addictive reasons.

A way out should be developed so that an ethical way would be used to battle with cyber terrorism and cybercrime, which in result will benefit undue effects of cyber threats.

Cyber Threats-Existing and Emerging jeopardy:

Economy, Energy supply, Transportation, and Military defenses are dependent on vast, interconnected computer and telecommunications networks that are poorly defended and inherently vulnerable to theft, disruption by foreign states, criminal organizations, individual hackers and terrorists. The number of public and private cyber attackers, spies, and thieves is growing rapidly. Their weapons are hidden inside the billions of electronic communications that traverse the world each day. These weapons are becoming more powerful comparative to our defenses in a field where offense already naturally dominates. Cyber spies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. Cyber thieves are individuals who engage in illegal cyber-attacks for monetary gain. Examples include an organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a financial account.

Cyber attackers use numerous exposures in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware with the current state of technology, computer system defenders cannot easily determine when the systems are being attacked at least until the attack is underway or complete, and sometimes not even then. When defenders discover the attack or threat, the attacker's identity usually cannot quickly be ascertained. Even when the computer or geographical source of the threats is identified, it is hard to know whether some other computer in some other place launched the attack. Even if we have certain knowledge about which computer in which place was the ultimate source of the attack or threat, we usually do not know whether the agent behind the attack is a private party or a state actor. And even if we know the actor's geographical location and precise identity, he is usually located beyond our borders, where our law administration capacities are weak and where we cannot use our military power except in the most extreme circumstances. And even if we could use military force, it might not be effective in preventing the threat in any event.

The attacks or methods on the computer infrastructure can be classified into three different categories.

(a) Physical Attack. The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

(b) Syntactic Attack. The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.

(c) Semantic Attack. This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors.

Cyber Warfare- Evolving threat in Cyberspace Ecosystem:

Wars have been a part of human knowledge since the dawn of history. The term "cyber warfare" refers to warfare channeled in cyberspace through cyber means and methods. While "warfare" is commonly understood as referring to the conduct of military conflicts in situations of armed battle. In another words, Cyber warfare is internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official national websites and networks, disrupt or disable essential services, steal or alter classified data and cripple financial systems among many other possibilities. Cyber warriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyber-attacks in support of a country's strategic objectives. These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyber-attack and are often blamed by the host country when accusations are levied by the nation that has been attacked. There are many such examples which will enlighten on how cyber warfare may affect the cyberspace and hinder the objective of securing cyberspace:

In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.

In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.

Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.

In 2009, a cyber-spy network called "Ghost Net" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. Ghost Net was reported to originate in China, although that country denied responsibility.

The most effective protection against cyber warfare attacks is securing information and networks. Security updates should be applied to all systems -- including those that are not considered critical -- because any vulnerable system can be co-opted and used to carry out attacks. Measures to mitigate the potential damage of an attack include comprehensive disaster planning that includes provisions for extended outages.

National Cybersecurity: Security beyond Borders

National cyber security which is also known as Homeland security is at most important issue now a days in securing national cyberspace. Cybersecurity is not now, and never will be, a concern that one country can solve alone. The solution will require a concerted and ongoing collaboration between like-minded free nations. Treaties and global governance do not contain bad actors, and should thus not be the focus on international Cybersecurity efforts. Instead, nations must work with other friendly nations to alter bad cyber behavior by raising the costs of such behavior. Nations should work hard and implement different policies for domestic as well as different policies for international cyber security. They should collectively think about for cyber warfare, ethical attack policies and procedures, pacifism efforts for national cyber security. Nations must not cease collaborating with other bad cyber sector attackers on issues of national cyber security. Moreover, International internet information sharing ought to be dignified in accurate manner. There must be cyber information sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing. The Internet is a shared resource and securing it is a shared responsibility. Promotion and development of a viable cybersecurity liability and insurance system should be emerged. Nations should focus on cyber insurance and cyber planning for securing cyber space. On periodic basis cyber-supply-chain security assessments must be established. Most importantly boundaries and standards for cyber self-defense must be enlightened for smooth and efficient functioning of cyber space at par.

Cyber Planning and Cyber Insurance: Cyber securing technological trends

Cyber-insurance is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products. Coverage provided by cyber-insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks; liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds.

As cyber-insurance market in many countries is relatively small compared to other insurance products, its overall impact on emerging cyber threats is difficult to quantify. As the impact to people and businesses from cyber threats is also relatively broad when compared to the scope of protection provided by insurance products, insurance companies continue to develop their services.

As insurers pay out on cyber-losses, and as cyber threats develop and change, insurance products are increasingly being purchased alongside existing IT security services. Indeed, the underwriting criteria for insurers to offer cyber-insurance products are also early in development, and underwriters are actively partnering with IT security companies to develop their products.

As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security breach. Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses to return to normal and reducing the need for government assistance.

Finally, insurance allows cyber-security risks to be distributed fairly, with cost of premiums commensurate with the size of expected loss from such risks. This avoids potentially dangerous concentrations of risk while also preventing free-riding. These all process is executed by a cyber-planner.

Mostly Cyber Insurance Covers:

- Besides legal fees and expenses, cyber insurance typically helps with:
- Notifying customers about a data breach
- Restoring personal identities of affected customers
- Recovering compromised data
- Repairing damaged computer systems

Conclusion:

As the global reach of the Internet keeps growing, its effect on all areas of online human endeavor becomes more pervasive. Individuals or groups can exploit the privacy afforded by cyberspace to engage in illegal activities that aim to intimidate, harm, threaten or cause fear to citizens, communities, organizations or countries. Governments, policy networks and the media around the globe have engaged in an effort to build defenses against Cyber-attacks, bring new regulations in effect while maintaining an almost mythological atmosphere over the threats and risks of potential Cybercrime and Cyber terrorist attacks. Cybercrime and Cyber terrorism are two issues that are likely to continue to exist for many years to come and they surely must be dealt with. But this process needs to be done in a way that will ensure the growth of the Internet in an inclusive and open way, maintaining the fundamental principles that it has been built upon. Cyber terrorism should be decoupled from Cybercrime and be specified in realistic terms, as to what are the probable threats of a Cyber terrorist act and to what extend society should go to face such effects. This will help alleviate unwarranted fears while at the same time enable individuals to make informed decisions when considering a new proposed policy by weighing its pros versus the cons and its effects on multiple levels, long and short term , instead of giving-in to fear and forfeiting their privacy and online freedom for better security.

References:

1. Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. “Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System”, Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
2. Tripathi S.P., Goyal R., Shukla P.K. (2014) Introduction to infor-mation security and cyber laws, KLSI
3. Santanam R. Sethumadhavan M. & Virendra M. (2011) Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, IGI Global.
4. A. Abur, Power System State Estimation: Theory and Implementation. Boca Raton, FL, USA: CRC Press, 2004.
5. J. M. Hendrickx, K. M. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, “Efficient computations of a security index for false data attacks in power networks,” IEEE Trans. Auto. Cont., vol. 59, no. 12, pp. 3194–3208, Aug. 2014
6. Integrated Defense Staff, “National Informatics Center”, Ministry of Defense, India
7. The most Important Instruments in fight against Cybercrime, Ch. 6.2
8. Booz Allen and Hamilton, Reports, “Top Ten Cyber Security Trends for Financial Services”, 2012
9. Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012
10. Nardin, T. (Ed.), (1998), "the ethics of war and peace", Princeton, NJ: Princeton University Press.
11. Nitzberg, S. (1998), "Conflict and the computer: Information warfare and related ethical

issues", In Proceed Ethics of Cyber War Attacking of the 21st National Information Systems Security Conference, Arlington, VA (p. D7)

12. Yibin Li, Wenyun Dai, Zhong Ming and Meikang Qiu, "Privacy protection for preventing data over-collection in smart city", *IEEE Transactions on Computers*, no. 99, pp. 1, 2015.

13. Nurjehan Mohamed. Malaysians are the most cyber-savvy among Asians. 2015. Retrieved Dec1, 2015 from http://www.therakyatpost.com/life/trends-life/2015/08/25/malaysiansare-the-most-cyber-savvy-among-asians/

14. Asia Pacific Cybersecurity Dashboard. 2015. Retrieved Dec 4, 2015 from http://cybersecurity.bsa.org/2015/apac/index.html

15. Zimmer, B. (2013). “Cyber” Dons A Uniform. Retrieved January 1, 2015, from http://www.wsj.com/articles/SB10001424127887323419604578569993261826614