Human Factors of Securing Information to Reduce Cybercrime Activities

Walter. T. Mambodza
Department of IT, SRM University, Chennai, India

Abstract— *Threats and attacks are a way of trying to compromise the information asset that is stored in critical infrastructures. As the technology is advancing there are better and improved methods of acquiring information illegally or in an unorthodox way. Hackers are often active attackers who have the skill to gain unauthorized access and undermine the security goals within networks and systems. Humans play an important role in protecting data confidentiality, data integrity and availability. In cybercrime offences are done for various reasons and it is the responsibility of the human to ensure information security. There is a lot of risk associated with safeguarding the information asset that is technological risk, financial risk, operational risks, political risk, economic risk and human risk. The aim of this paper is to indicate the human factors of securing information in order to reduce cybercrime activities.*

Keywords—Attacks, Availability, Confidentiality, Cybercrime ,Integrity, Threats

I. INTRODUCTION

Cybercrime involves the issue of committing an incidence through the use of a computer or on the internet. It takes many forms such as cyber warfare, cyber espionage and software piracy. Though crime is presumed to be done by skilled personnel such as hackers, every human that can gain access to a computer or the internet is capable of cybercrime. Most developed countries have cyber law that help or assist in the governance and as a statutory instrument in fighting cybercrime. The most critical asset within an organization is information; it should be safeguarded against unauthorized access, modification and destruction. Mainly humans enforce physical security, computer security, network security and information security. The goal of Information security is to protect data confidentiality, data integrity and availability [1]. However there is a certain level of risk that is associated with safeguarding the information asset. Risk is when a threat agent compromises the information asset through the use of vulnerability within a system. Vulnerabilities are weaknesses in the system such as weak passwords, lack of patch management, lack of configuration management.

II. REVIEW OF LITERATURE

Information security is a way of protecting the information, critical elements, systems and hardware that store, use, transmit and safeguard the confidentiality, integrity and availability of information. Information System is a set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization [1]

E-commerce is now used to complete many very important transactions. However, due to the threat of cybercrime, these transactions are at risk and this can result in loss of critical data if not protected well. A range of possible threats exist that can compromise these transactions and this can be resolved by using known and trusted mechanisms (e.g. authentication) to secure them. Further research can be done on the tools used to discover and deal with the listed aspects of cybercrime as well as how the 2 entities interact and affect each other [3]

Today, the public enjoys shopping and banking from the comfort of their home while companies save money on processing transactions and hiring employees. However, with any innovation, there are obstacles to overcome before the venture is deemed successful. In e-business, encompassing any transaction via the internet, the information exchange can be simple. The law needs to adopt policies stating companies must report successful break-ins. It should be mandatory to report security breaches such as gaining access to databases or exposing financial information without regard to its reputation [4].

Cybercrime is a straightforward report on the major areas of criminal intrusions into computer networks, systems, and data bases. Hackers or crackers are individuals who illicitly access systems either though social or technological engineering. The authors introduce the basic set of actions they consider cybercrime, consistent with positive notions of damage to property and persons in or via cyberspace.

That set includes: Cracking or Hacking into systems inappropriately (and perhaps damaging that system); Pirating data or software without permission; Phreaking, or accessing the phone system to avoid payment for services, computer viruses, child pornography[5].

Many cybercrimes are now being committed from distant locations outside national borders. Through the strategic targeting of financial institutions such crimes can ultimately derail a nation's productivity. This was found to be true and in response, national security organizations in the EU and the USA put in place guidelines and policies to help avoid and handle such crimes as a united front. Increasing the scope to include industrial or national power-grid management institutions can be done in future. This is with the goal of dealing with homegrown threats which can cause the same problems from within the country's borders [6].

III. RESEARCH GAP

Information security is concerned with the confidentiality, integrity and availability of an information asset. Cybercrime takes many forms such as software piracy, online fraud and can take place from within or outside an organization. However humans play an important part of securing information in cybercrime

IV. OBJECTIVES OF STUDY

To perform a review of literature on related subjects

To highlight the human side of information security on cybercrime.

V. FINDINGS

Most organizations are now spending about 30 % of the budget on information security and many firms have set Information security departments to safeguard the confidentiality, integrity and availability of an information asset.

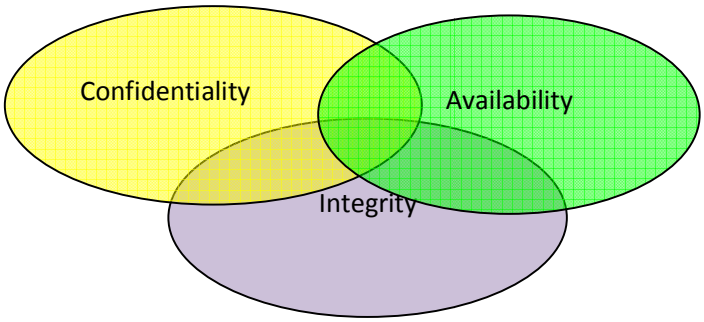

Fig. 1 Security Goals

Attackers of systems have been from within the organization that is internally or from outside the organization that is externally. An attacker can be a hacker or a cracker see figure 2 or 3 below.An attacker can also use various ways to gain unauthorized access to a system such as social engineering, password attacks, brute force approach, Denial of Service(DOS), Distributed Denial of Service(DDOS), eavesdropping, IP spoofing, ARP spoofing, phishing, packet sniffing, replay and man in the middle attacks. Cybercrime takes many forms such as

Software Piracy
Online fraud
Child pornography
Computer Virus
Identity theft
Unauthorized access
Downloading illegal stuff

In order to protect against attacks various mechanisms have been enforced such as Baseline controls, anti- virus, firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, access controls and biometric locks.

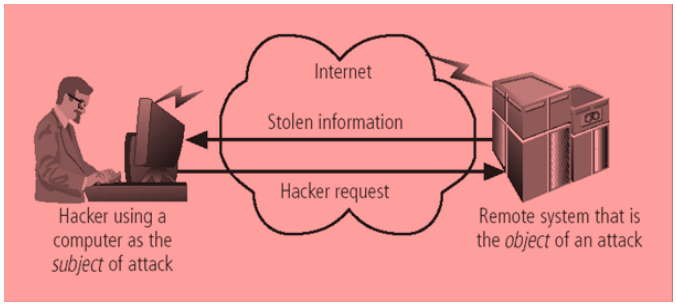

Fig. 2 - Hacker using a computer to attack [1]

The humans play a pivotal role in the implementation, monitoring, maintaining and management of information security. In order to reduce cybercrime that emanates from human error, mistakes, negligence and bad decisions there is need for

Careful planning of strategies
Implementation of sound security policies
Patch management
Configuration management
Good control measures
Good communication skills
Secure Education, Training and Awareness

VI. CONCLUSION

An attacker is a human being and most threats are developed by humans and an organization usually employees a system or network administrator, chief security officer, Information Security specialist to enforce security mechanisms within an organization. However humans play a vital role of information security against cybercrime. In conclusion organizations should invest more money on employees by providing security education, training and awareness (SETA), employ skilled manpower with qualifications and certifications and also motivate and keep abreast with the latest advances in technology.

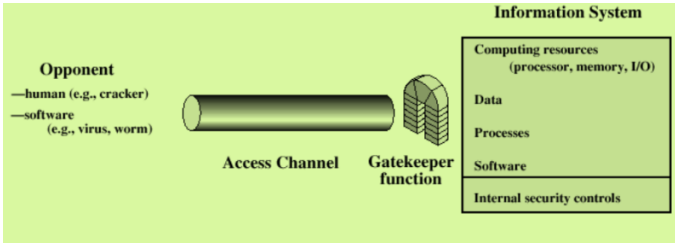

Fig. 3 - Network Access model by Human [2]

VII. SCOPE FOR FURTHER RESEARCH

The increase in cybercrime is being caused by the reason that the systems are dependent on the humans to a greater extent such that the attacks, threats and ways of implementing security revolve around humans. There is need for development of systems in Artificial Intelligent, machine learning, robotics and neural networks as an approach to reduce cybercrime

REFERENCES

[1] Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security", 4th edition
[2] William Stallings, "Cryptography and Network Security: Principles and Practice", 5th edition
[3] N. Leena, Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science & Technology Vol. 4(1), (2011)
[4] Changying Zhou, Chunru Zhang; A Trusted Smart Phone and Its Applications in Electronic Payment
[5] CYBERCRIME: A REFERENCE HANDBOOK, by Bernadette H. Schell and Clemens Martin. Santa Barbara, CA: ABC-CLIO, 2004. ISBN: 1-85109-683-3
[6] Raluca Georgiana, Borderless Crime: Computer Fraud, Database Systems Journal vol. III, no. 1/2012
[7] Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing
[8] Cyber Warfare And The Crime Of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. Law.duke.edu. Retrieved 2011-11-10.
[9] An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, October 1995
[10] Govil and J. Govil, "Ramifications of cybercrime and suggestive preventive measures," in 2007 IEEE International Conference on Electro/Information Technology, 2007, pp. 610–615.
[11] K. O. Shea, "Cyber Attack Investigative Tools and Technologies For more information :" no. May 2003.
[12] B. Sahu, N. Sahu, S. K. Sahu, and P. Sahu, "Identify Uncertainty of Cyber Crime and Cyber Laws," in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 450–452.
[13] Easttom C. (2010) Computer Crime Investigation and the Law
[14] Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[15] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "CRS Report for Congress the Economic Impact of Cyber-Attacks."
[16] R. Popa, "Borderless Crime-Computer Fraud," Database Syst. J., vol. III, no. 1, pp. 49–58, 2012.
[17] Jaishankar, K. (Ed.) (2011). Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.