CHAPTER 18: EVOLUTIONARY STEPS OF CYBERSECURITY THREATS AND THEIR SOLUTIONS

Siraj Nath Pyakurel
Student, MBA Integrated, Sharda School of Business Studies Sharda University, Greater Noida, India

Prof. Chavi Jain
Assistant Professor, Sharda School of Business Studies Sharda University, Greater Noida, India

INTRODUCTION

Cyber security is simple terms is the practice of defending network devices such as computers, mobile devices, servers, electronic systems that are network dependent.

- **Information security:** maintains security of data during transit and in storage. Privacy stands for data only being accessed by authorized personnel, Integrity means information can be altered, added or manipulated only by the authorized personnel and finally availability of system functions, information and data only to the authorized user. Cyber security systems achieve these by implementing authentication mechanisms, a simple example would be usernames and passwords where a username identifies a user and password acts as the authentication mechanism to prove that the user is who they claim to be.
  Air Force and several other organizations aimed at developing a security system for the Honeywell Multics Computer System. Continuous monitoring systems are threat detection strategy that enforces compliance, security and supports growth in businesses by monitoring data vulnerabilities within network systems and software's across devices. Continuous security monitoring (CSM) is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities, and other cyber threats to help organizations make risk-management decisions. In 2018 the US Department of Homeland Security introduced such guidelines, it focused on techniques to mitigate threats, fix vulnerabilities and recover from a cyber-attack.
- **Protect-** Through the use of tools such as firewalls and physical security systems such as locked data centers and server rooms. A cyber security threat is any malicious attack that tries to unlawfully access protected data, damage information systems and disturb network operations across devices be it personal or organizational.

LITERATURE REVIEW

As per an article published by James T Robert, Cyber-attacks are a serious threat; the article is based around the issues and evolution of cyber threats and possible solutions as presented by researchers.

According to Sudhakar Kumar, with rapid increase in cyber security software and preventive systems, the threats have also evolved accordingly. Malwares for example have gone from simple file-based malware to complex file less threats. The damages caused by file less malwares can be devastating and are spread with ease across systems. This article presents a robust model to counteract these threats.

The author of this literature, Kshetri N has underlined the exposure to cyber security threats faced by businesses and financial institutions across the globe. Damages caused by cyber-attacks on business amounted to over 5.2 billion dollars in 2020 alone. This includes sectors such as Healthcare, Education and Financial institutions. It is also important to learn why these threats persist and what a solution would look like

- With increasing dependency on cyber technology, Cyber-attacks and mal practices have become frequent and increasingly harmful.
- Threats are increasing as there seems to be a lack of knowledge among users and zero effort to prevent possible attacks.
- Cyber security will continue to evolve, and cybercriminals will be right on the trail of these new developments. Cybercriminals are anticipated to continue to use new technologies like artificial intelligence, blockchain, and machine learning in future attacks.

RESEARCH OBJECTIVES

The Key objectives of this research are stated below:

- Develop an understanding of how Cyber security frameworks functions.
- Provide an insight into the evolutionary steps of Cybersecurity Threats and solutions
- Provide statistical data showing damages caused by cyber-attacks worldwide and how to mitigate them.
- To identify what vulnerabilities modern network systems face.
- Examine the responsibilities of individuals against rising Cybercrime numbers
- Familiarize oneself with the key functions of antivirus systems and preventive programming.

RESEARCH METHODOLOGY

Sources of Secondary data

- Research papers, journals and articles
- Internet search engines i.e. Google Scholar, Wikipedia and websites
- Books and library literature

Secondary data: secondary data is information gathered by others. This Information is gathered by analyzing and studying primary data. It is a Readily available form of data gathered from various sources such as censuses, government publications, organizational internal records, books, websites, articles, journals, discussion papers, working papers, policy notes, and thesis, dissertations, project reports, newspapers, magazines, seminars, conferences, and workshops.

This research aims to provide a deep insight on:

- Evolution of Cybersecurity threats
- Evolution of Cybersecurity solutions
- Personal Responsibilities towards Cybersecurity
- Growth of Cyber-attacks in recent years

This research method supports the intent of filling a research gap in the field of cybersecurity and network systems protection. Although a fair amount of research has been conducted on this field, this research narrows down the evolutionary steps in the inception of cybersecurity threats and solutions.

The research data was processed with the help of statistical tools such as graphs, tables and average of numeric data.

Broad research areas relevant to this research include

- Computer Network Security
- Application Security
- Web Services Securities
- Mobile Security
- Protective Security

ANALYSIS

With the threat landscape ever changing, it has become crucial to comprehend the evolution of cybersecurity threats. Below listed are some worrying data showing the increase in frequency of cyber-attacks?

- From March 2021 to February 2022, there were 153 million new malware samples (AV-Test), an almost 5% rise over the previous year's total of 145.8 million.
- According to a 2007 research, criminal hackers were previously targeting computers and networks at a pace of one every 39 seconds. According to the Internet Crime Complaint Center's 2020 report, there have been 465,177 recorded events that year, amounting to one successful assault every 1.12 seconds. Notably, this ignores attempted assaults and those that went unnoticed.
- Almost half of all corporate PCs and 53% of consumer PCs that were infected once were re-infected within the same year (2021 Webroot Threat Report)
- A successful cyberattack impacted 86.2 % of the firms investigated (Cyber Edge Group 2021 Cyber threat Defense Report)

In early 90s, Internet was basically a cesspool of malicious programs and viruses. Almost every system in existence was infected with a virus of some sort. All this has changed in recent years as the use of antiviral software's is on a rise, as more individuals become aware themselves of cybersecurity, the use of preventive programs are expected to grow further. Below is a compelling list of stats on the use of antivirus programs worldwide.

- The worldwide cybersecurity industry is expected to reach $40 billion by 2020.
- Antivirus software installed on 1.3 billion mobile devices worldwide.
- The most significant antivirus function is web surfing protection.
- Google searches for "best antivirus software" surged by 269% between 2018 and 2021.

CONCLUSION

This research has made an effort to trace the evolutionary steps of Cybersecurity solutions and threats. In doing so it has reviewed the history of the first cyber-attacks and the urgency it presented for the development of preventive frameworks and programs. One of the most critical parts of the rapidly evolving digital world is cyber security. Its threats are difficult to dismiss, therefore it is critical to understand how to guard against them and educate others how to do so as well. In today's networked domain, the opportunities for exploitation appear limitless - but cybersecurity specialists are also developing powerful defense measures to keep hackers at bay. Cybersecurity specialists use the most updated IT trade secrets to deter cyber criminals and mitigate data breaches.

The fact that practically everyone on the earth is ever more dependent on digitization implies that there is a thriving criminal potential for cybercriminals. Factors such as increased cloud storage and social media expansion have left people vulnerable to cyber assaults. As a result, cyber security is more vital than ever.

REFERENCES

1. *Cybersecurity Breaches per year*. (n.d.). [Graph]. Www.AuditAnalysis.Com. https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/
2. M., L. (2022, January 24). *What is Cyber Security: Learning About the Network Security*. BitDegree.Org Online Learning Platforms. https://www.bitdegree.org/tutorials/what-is-cyber-security/
3. *Managed cybersecutiry systems*. (n.d.). [Illustration]. Belltechlogix.Com. https://belltechlogix.com/wp-content/uploads/2015/06/SecurityWebpage1.png
4. *Managed cybersecutiry systems*. (n.d.). [Illustration]. Belltechlogix.Com. https://belltechlogix.com/wp-content/uploads/2015/06/SecurityWebpage1.png
5. *Number of Smartphone users*. (n.d.). [Graph]. Www.Internetadvisor.Com. https://www.internetadvisor.com/smartphone-statistics
6. SNITKIN, S. I. D. (n.d.). *Continuous monitoring systems*. Www.Arcweb.Com. Retrieved April 9, 2022, from https://www.arcweb.com/industry-best-practices/continuous-ics-security-monitoring-needed-critical-industries
7. *Use of Antivirus programs worldwide*. (n.d.). Https://Cybercrew.Uk. Retrieved April 11, 2022.
8. Kelley, K. (2022, March 17). *What is Cyber Security and Why It is Important?* Simplilearn.Com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security
9. Sienicka, M. (2021, April 7). *8 Reasons Cyber Security Is Important*. Hakin9 - IT Security Magazine. https://hakin9.org/8-reasons-cyber-security-is-important/
10. Upadhyay, I. (2020, October 23). *The Importance of Cyber Security In 3 Informative Points*. Jigsaw Academy. https://www.jigsawacademy.com/blogs/cyber-security/the-importance-of-cyber-security/