Data Security Strategies and Threat Management Techniques
Hassan Saad Fadhil

IT Engineer, Department of Computer Engineering, Mosul University, IRAQ

Email: computer.eng.hassan@gmail.com

**Abstract:** *Today's businesses have a difficult time finding the personnel they need to defend their systems against cyber security threats. Even if there are shortages everywhere, the largest demand is for experts with extensive technical knowledge who can fill highly valuable positions like secure system design, tool creation, and penetration testing. In this paper, we have looked at the most important information security technologies and* *discussed the challenges they face.*

**Keywords:** *information security, Threats Management, Cybercrime,* *Data protection*

1. **INTRODUCTION**

The information revolution is reshaping the world. Networked connections have connected those billions through nearly instantaneous and global communications, and microscopic semiconductors have given billions of people information processing power that were unimaginable a century ago. However, concurrently with the expansion of that networked computing power has come to a startling increase in vulnerability. Cyber theft and disruption can affect anyone, even those who do not own a computer. By using an automated and remote control, malicious actors can inflict personal harm or obfuscated harm on an anonymous basis [1]. Since the Internet is now a part of everyone's life, it's vulnerable to a variety of threats because of its widespread interconnectedness. Cyber security threats range from jail breaking to two-faced malware, network intrusions, and more. A security arms race has developed as a result of these threats. There are a lot of security companies working on new technologies to protect computers, networks, and software applications from malware infections and network intrusions [2].

The need for safe computer systems becomes increasingly apparent as more and more business operations are automated and more computers are used to store sensitive data. As systems and applications are distributed and accessed via an unsecured network like the Internet, this requirement becomes even more apparent. Governments, businesses, financial institutions, and millions of everyday users all depend on the Internet. Organizations of PCs support a huge number of exercises whose misfortune would do everything except cripple these associations. As a result, concerns regarding national security have evolved into cybersecurity concerns. It's hard to keep the Internet safe [3]. Cost, function, convenience, and societal values like openness, privacy, freedom of expression, and innovation can all be at risk when information security levels rise. Evaluation of suggestions for improvement is difficult without a widely accepted doctrine, and debate regarding their adoption cannot be persuasive or conclusive [4]. From low-level Internet-facilitated criminality to military cyber operations and strategic computer network interventions in world powers' domestic affairs, a cursory glance at the headlines will reveal a wide range of cyber security issues affecting contemporary societies. Our increased reliance on and imbrication with transnational assemblages of information technologies enables and worsens these, which are functions of economic and political motives [5].

Realize that, despite its significance, cyber-security only accounts for a sizable portion of computer science research. Security experts rightly point out that a single security breach can occur with a single flaw in virtually any program [6].

1. THREATS AND CHALLENGES

Threats to information security include a wide range of online activities that could be illegal. It can generally be broken down into one of two categories: crimes that are facilitated by computer networks or devices and whose primary target is independent of the computer network or devices, such as identity theft, phishing scams, information warfare, or cyber stalking, as well as crimes that directly target or harm computer networks or devices, such as malware, viruses, or denial of service attacks[7]. Associations are turning out to be more mindful of data and related advancements in pretty much every capability, especially in driving development and creating the upper hand. In today's information environment, corporate information and technology services are susceptible to a variety of security risks, such as the leakage of sensitive data and prolonged interruptions in email and internet access, both of which have a significant impact on business continuity [8].

2.1 Security Analytics for Threat Detection

Threat monitoring and incident investigations are the most common uses of security analytics, and both financial and defense institutions are particularly concerned about this. The focus is on identifying and learning both known and unknown patterns of cyberattacks. This is expected to significantly improve the speed with which hidden threats can be identified, the ability to locate attackers, and the accuracy with which future attacks can be predicted (minimum false positive rate) [9].

1. CYBERCRIME

 Cybercrime can be defined as any type of criminal activity that uses a laptop as its primary platform for commission and larceny. An increasing number of these crimes include computer-enabled crimes like network espionage and the spread of laptop viruses, as well as computer-enabled crimes like stalking and bullying and some frauds that have become a big problem for the public and the government. A simple definition of the term "cybercrime" would be any crime committed using a computer. Additionally, by using the internet to sell illegal goods and steal people's identities. As innovations and technologies emerge, so do the number of crimes[10]. The United States Department of Justice has broadened the definition of cybercrime to include any offense that makes use of a device for the storage of evidence [11]. Combating cybercrime is essential if this technology is to be used by the general public in a way that is both beneficial and dependable [12].

1. CONCLUSION

Academic and professional literature is replete with advice on information security. The majority of study focuses on how to stop security threats through technological countermeasures; however other strategies like deterrence, deception, detection and reaction are feasible. In today's cyberspace, every business is getting online to stay afloat and has put important resources on web servers that are openly accessible through the HTTP interface. Every organization is required to adhere to a set of security standards or guidelines to protect these resources. Unfortunately, the majority of security solutions are static and based on signatures (i.e., if a signature is present, it can detect malicious activity; otherwise, it cannot). As a result, a dynamic solution is required to address the ever-present vulnerabilities. Besides, there is a need for a semantic arrangement that can grasp the setting of weaknesses before fixing them.

**REFERENCES**

[1] M. Warner, “Cybersecurity: A pre-history,” *Intell. Natl. Secur.*, vol. 27, no. 5, pp. 781–799, 2012, doi: 10.1080/02684527.2012.708530.

[2] S. Mahdavifar and A. A. Ghorbani, “Application of deep learning to cybersecurity: A survey,” *Neurocomputing*, vol. 347, pp. 149–176, 2019, doi: 10.1016/j.neucom.2019.02.056.

[3] Suparyanto dan Rosad (2015, “済無No Title No Title No Title,” *Suparyanto dan Rosad (2015*, vol. 5, no. 3, pp. 248–253, 2020.

[4] B. Von Solms and R. von Solms, “Information & Computer Security Article information : Cyber Security and Information Security – What goes where ?,” *Inf. Comput. Secur.*, 2018.

[5] T. Stevens, “Global cybersecurity: New directions in theory and methods,” *Polit. Gov.*, vol. 6, no. 2, pp. 1–4, 2018, doi: 10.17645/pag.v6i2.1569.

[6] S. L. Garfinkel, “Inside risks the cybersecurity risk,” *Commun. ACM*, vol. 55, no. 6, pp. 29–32, 2012, doi: 10.1145/2184319.2184330.

[7] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, “Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications,” *Proc. - 2013 11th Int. Symp. Auton. Decentralized Syst. ISADS 2013*, 2013, doi: 10.1109/ISADS.2013.6513420.

[8] D. Ghelani, “Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review,” *Authorea Prepr.*, vol. 8345, no. X, 2022, doi: 10.11648/j.XXXX.2022XXXX.XX.

[9] T. Mahmood and U. Afzal, “Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools,” *Conf. Proc. - 2013 2nd Natl. Conf. Inf. Assur. NCIA 2013*, pp. 129–134, 2013, doi: 10.1109/NCIA.2013.6725337.

[10] M. L. Ali, K. Thakur, and B. Atobatele, “Challenges of cyber security and the emerging trends,” *BSCI 2019 - Proc. 2019 ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, co-located with AsiaCCS 2019*, pp. 107–111, 2019, doi: 10.1145/3327960.3332393.

[11] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, “Cyber Security Challenges and its Emerging Trends on Latest Technologies,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022062.

[12] R. Khatoun and S. Zeadally, “Cybersecurity and privacy solutions in smart cities,” *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 51–59, 2017, doi: 10.1109/MCOM.2017.1600297CM.

**Author's Biography (Mandatory)**

**Hassan S. Fadhil,** is a student of Computer Engineering at the College of the Engineering/ University of Mosul. He completed his M.Sc. in the department of Electrical and Computer Engineering/ ECE at Istanbul Altinbas University. His research interests are Cybersecurity, Smart Cities, Data Security, Data Hiding, and Social Engineering.



**Cite this paper:**

Hassan S. Fadhil, “Data Security Strategies and Threat Management Techniques”, Vol. xx, No. xx, pp. xx-xx, Dec 2022.