Handhah, Sari M, 2023, 11:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Cyber Security

Handhah Sari M, Rashidi Humoud H
Area Information Technology Department, Saudi Arabia

Abstract-Cybersecurity encompasses a variety of measures to protect computer systems and networks from unauthorized access, damage, or theft. Cybersecurity is a pressing issue due to the rampant increase in cyber threats that can lead to significant losses and potential threats to privacy, data, and networks. This paper provides an overview of cybersecurity, explores the importance of cybersecurity, and presents some of the significant challenges in ensuring safe and secure cyberspace. Additionally, the paper provides suggestions to address challenges faced in implementing cybersecurity policies.

Keywords- cybersecurity, protection, vulnerability, threat

I. INTRODUCTION

Cyber security is the practice of protecting computer networks, devices, and programs from unauthorized access, damage, or theft. In today's digital age, cyber security has become increasingly crucial due to the exponential increase in cyber threats, cyber-attacks, and cybercriminal activities. With ever-increasing amounts of sensitive data being transferred through networks, cyber security has become a priority for individuals, businesses, and governments. In this paper, we discuss the importance of cyber security and provide an overview of the significant challenges and strategies employed to safeguard computer systems and networkers.

The Importance of Cyber security

Cyber security is essential for protecting sensitive information, intellectual property, and personal data. Cyber threats can lead to significant financial losses and reputational damages for organizations. Individuals' privacy also faces risks from data breaches, cyber blackmail, identity theft, and other online fraud. Furthermore, cybersecurity directly affects the national security of any country. Cybercriminals and hackers can steal sensitive military information or launch cyber-attacks on essential infrastructure, causing substantial damage. Hence, cybersecurity measures are critical to maintaining the integrity and security of computer systems and networks.

II.CHALLENGES IN THE IMPLEMENTATION OF CYBERSECURITY

Implementation of robust cybersecurity measures often faces several challenges, including the following.
1. Lack of cyber security awareness amongst individuals and organizations
2. Limited budget allocation for cybersecurity implementation
3. Rapidly evolving nature of cyber threats
4. Lack of skilled cybersecurity workforce
5. Integration issues with legacy systems
6. Conflicting regulations in different countries, making compliance challenging.

Strategies to Address Cybersecurity Challenges:
1. Cybersecurity awareness training for workers, including ethical hacking certifications, to improve knowledge and reduce risks.
2. Increase budget allocation for cybersecurity and encourage other firms to do the same.
3. Embrace multiple layers of cybersecurity measures,

including firewalls, antivirus software, and regular backups.
4. Develop a skilled cybersecurity workforce by promoting knowledge within the current workforce and trainingnew employees.
5. Encourage cost-effective and secure technology upgrades to reduce the use of legacy systems.
6. Encourage international cooperation to create a unified regulatory framework.

III.CONCLUSION

Cybersecurity is essential for safeguarding sensitive data, personal information, and national security. With the evolving nature of cyber threats, cybersecurity measures need to be constantly updated to remain effective. This paper has provided an overview of cybersecurity, the significance of protecting computer systems and networks, and the challenges faced in implementing cybersecurity policies. To overcome these challenges, organizations, governments, and individuals must promote cybersecurity awareness, allocate adequate resources, utilize effective cybersecurity measures, develop a skilled cybersecurity workforce, and encourage cost-effective and secure technology upgrades.

REFERENCES

1. Anderson, R. J. (2015). Security engineering: A guide to building dependable distributed systems. Wiley.
2. Cavelty, M. D. (2015). Cyber-security and threat politics: US leadership, policy entrepreneurship and the propagation of cyber-threats. International Studies Quarterly, 59(4), 706-721.
3. Cobb, M. (2016). The New Era of Cybersecurity. Financial Executive, 32(5), 37-39.
4. McAfee. (2018). McAfee Labs Threats Report. McAfee Corporation.
5. National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce.

Author’s details
1.Handhah Sari M, Area information technology, Saudi Aramco, Saudi Arabia, Abqaiq
2. Rashidi HumoudH , Area information technology, Saudi Aramco, Saudi Arabia, Abqaiq