IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 7, January 2023

Role of Cyber Security in Office Management Systems

[1]Ritu Arya, [2]Vandana Sinha, [3]Ritu arya[4], Ashish Verma

Department of Physics, Dr. Harisingh Gour Vishwavidyalaya, Sagar, M.P.[1,3,4]

Shri G.P.M. Degree College of Science and Commerce, Andheri, Mumbai, Maharashtra[2]

Abstract*: In today's world, technology and network connections are integral to our daily lives. It is therefore crucial to understand what cyber security is and to use it effectively. Systems, important files, data, and other virtual assets are at risk if they are not adequately protected. Every company, regardless of whether it is an IT firm or not, must be equally protected. However, as new cyber security technologies are developed, attackers are also continually improving their hacking techniques and targeting the vulnerabilities of many businesses. Cyber security is essential because military, government, financial, medical, and corporate organizations accumulate, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, including financial data, intellectual property, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. In the future a lot of work can be done in the field of quantum computing and its applications in cyber security.*

Keywords: IT firm, Cyber security, Intellectual property.

I. INTRODUCTION

Cyber security is essential for protecting sensitive information, maintaining data integrity, and ensuring system functionality in office management systems. Cyber security is the process of protecting your company's data against attacks that might come from both internal and external sources. It can consist of an assortment of instruments, protocols, structures, and techniques for blocking unauthorized entry or damage to computers, networks, software, and information.[Figure 1] The goal of any cyber security plan should be to ensure data confidentiality, availability, and integrity.[1]

Cybercriminals frequently rely on human error, such as neglecting to update software patches, clicking on malicious links, and creating simple passwords that are easy to guess, to obtain access to systems and information, as demonstrated by recent significant cyber security events. Everyone in our firm, from the top executives to the entry-level workers, is accountable for maintaining the security of its systems and data. Strong cyber security procedures are crucial for this reason.

Not only is cyber security the responsibility of the IT department. The Internet is necessary for many of our tasks, and anyone who has access to our network could be a security risk. Because cybercriminals are always improving their skills, we need to be on guard to keep our systems and data safe from online attacks.

Cyber security problems have multiple main ways to impact, if not completely ruin, an organization's reputation. Hackers might potentially gain access to private data, including credit card or bank account numbers. On the "dark web," there are open markets for this kind of information. Should unauthorized individuals obtain such confidential data, the company may be in violation of privacy regulations or risk having its credit card or banking privileges revoked. High-profile security breaches affecting personal information are announced worldwide each month.[1,2]

Another related concern is that an organization's reputation could be severely damaged if a hacker manages to access confidential information about it. Few small businesses can withstand the harm that such deleted data could do to their reputation. It's possible that the harm to goodwill and reputation will be more devastating than the data loss itself. If consumer data is lost, the company could face legal or regulatory repercussions. A third party may sue an organization because they have suffered a loss of their own. In many jurisdictions, violations of privacy regulations can also result in serious penalties and/or legal action for organizations.Another related concern is that an organization's reputation could be severely damaged if a hacker manages to access confidential information about it. Few small businesses can withstand the harm that such deleted data could do to their reputation. It's possible that the harm to goodwill and reputation will be more devastating than the data loss itself. If consumer data is lost, the company could face legal or regulatory repercussions. A third party may sue an organization because they have suffered a loss of their own. In many jurisdictions, violations of privacy regulations can also result in serious penalties and/or legal action for organizations.

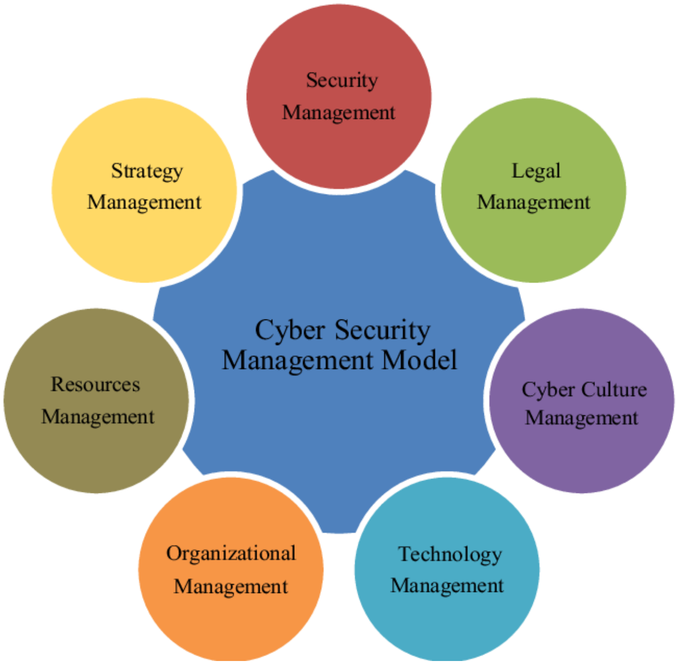

Figure 1: Applications of Cyber security in management

Once all accessible data—including, frequently, backup data and systems—is encrypted, an adversary will either remove the encryption key and the data is lost, or the organization will be told how to pay a ransom within days. The adversary who is essentially holding the data hostage gives rise to the name ransomware. It would be economically impossible to crack the encryption key without paying the ransom because it is so strong; estimates suggest that it would take an ordinary desktop computer five quadrillion years to decrypt the data without the key. In extremely rare cases, the target organization might hold out hope that some researchers have discovered a way to decrypt the data by using a design flaw.

Figure 2: Security for data protection

Today's organizations possess information. Organizations use this data to conduct business. They keep this data on file. The information frequently belongs to third parties rather than the company (such as customers, business partners, suppliers, etc).Because of negligence, hackers can access confidential information through even the most basic techniques, demonstrating that there are threats both inside and outside of a workplace.

Many businesses overlook the fact that outside criminals typically do not target an organization's technology. They use sophisticated phishing emails that mimic correspondence from the company that is intended for employees. There are far too many of these attacks. According to the RSA Anti-Fraud Command Center, a fresh phishing attack occurs every thirty seconds! The management and leadership of the organization are realizing that the only way to secure their environment is to prioritize cyber security[Figure 2]. As a result, the board has mandated cyber security. It is part of the mandate for CEOs. CIOs have specific security objectives in mind.

Work space culture of cyber security:

A workplace where security is embedded and permeates every facet is one that prioritizes cyber security. It is a part of planning and thought processes. It is a part of the processes, systems, and application. It is an inherent aspect of the work process, reducing the likelihood of a cyberattack in the process. An organization's culture has a significant impact on its cyber security posture. Creating a cyber security-focused workplace culture will help to defend your company from cyber attacks by highlighting and reinforcing security practices among employees.Despite being widely seen as a difficult task, creating a cyber security workplace culture is not as difficult as you may think.

Think about a few components, attitude being the first. Establishing a cyber security workplace culture successfully depends on a variety of factors, including the management's approach to cyber security and how it is implemented while making sure that plans for education and communication are in place.

Important measures to attain cyber security at a workplace:

First things first: make sure your workspace and digital devices are tidy and safe. Minimize or eliminate stray files, changing information ends, and clutter on your desktop should be the first step. A tight, secure workspace must be maintained by keeping mobile devices and desktops tidy. Emptying the recycling bin, minimizing the amount of deleted files, and frequently updating should all be part of your desktop and mobile hygiene routine.Installing software updates and enabling automatic updates on all devices linked to the internet can prove to be effective.

Spoofing email display names is a common practice that has caused internal brand destruction for hundreds of large companies. A fraudster will use a phony display name that is similar to the real one in order to impersonate a brand. The header address of each email should be examined rather than relying solely on the display name. The email should either be delete or provided to the ITS department.

Reporting any indication of malware, adware, or viruses should be done immediately, in addition to email security, online judgment, and reporting dubious links. The PCs in the place of business probably have antivirus software installed, but when strange activity happens, it will still raise an alarm.

II. CONCLUSION AND FUTURE WORK

The social aspect of cyber security entails fostering open communication among staff members and being aware of how your actions may affect other people within the company. It is impossible to exaggerate the significance of cyber security. Whether an organization is located offline or on the internet, it is imperative that it take precautions against possible attacks and data leaks. To become certified as a cyber security professional, one must possess a strong grasp of computer operation and online threat prevention. Furthermore, one must be skilled in the use of a range of software tools designed to prevent hackers from breaking into computer networks. Anyone with the capacity to help others protect their data should consider a career in cyber security.

Emerging technology called quantum computing has the potential to significantly improve cyber security. Compared to conventional computers, quantum computers can perform calculations far more quickly and effectively because of the special qualities of quantum physics. A fantastic academic resource that offers the most recent findings and advancements in cryptography and cyber security through quantum applications is Quantum Cryptography and the Future of Cyber Security.[3]

ISSN
2581-9429
IJARSCT

The capacity of quantum computers to solve intricate puzzles that conventional computers would be unable to compute is one of their main advantages. Quantum computing might be used, for instance, to break very strong encryption schemes. They might also be used to get around antivirus software and other sophisticated cybersecurity defences. Hackers would be able to enter networks and take advantage of important data. A successful cyber attack could have disastrous effects, such as severe economic disruption and even international conflict.

There may be significant effects of quantum computing on artificial intelligence (AI). Large data sets are necessary for AI to learn from and forecast the world around it. These enormous volumes of data can now be processed in new ways thanks to quantum computing, which could lead to major advancements in AI technology. Although it will take a long time and a lot of work to develop quantum computing, it seems like the technology is getting closer to becoming a reality. Establishing a cybersecurity governance and risk management program that is suitable for the organization's size is necessary. The owners and directors should view cybersecurity risk as a major business risk. Along with appropriate measurement criteria, results should be tracked and managed, and it should be on par with risks related to compliance, operations, finances, and reputation.[4]

The demand for qualified workers in the field and the emergence of new opportunities make the future of cybersecurity jobs extremely bright. Its high time IT professionals gave cybersecurity more consideration. [5]

REFERENCES

[1]. Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). Implementing enterprise cybersecurity. Enterprise Cybersecurity Study Guide, 135–171. https://doi.org/10.1007/978-1-4842-3258-3_4

[2]. Moallem, A. (2021). Cybersecurity Technologies Classification. Understanding Cybersecurity Technologies, 1–4. https://doi.org/10.1201/9781003038429-1

[3]. Taulli, T. (2023). Goals of cybersecurity. Cybersecurity for Small Business. https://doi.org/10.1007/978-1-4842-9478-9_1

[4]. Jarjoui, S., & Murimi, R. (2021). A framework for Enterprise Cybersecurity Risk Management. Advances in Cybersecurity Management, 139–161. https://doi.org/10.1007/978-3-030-71381-2_8

[5]. Mounir, S., & Maleh, Y. (2023). Cybersecurity management in cyber-physical systems using blockchain. Computational Intelligence for Cybersecurity Management and Applications, 209–234. https://doi.org/10.1201/9781003319917-14