e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

EMERGING THREATS IN CYBERSECURITY SPACE

Dr. Damingo, Levi A.S*1, Dr. Elliot, Kizzy N*2, Dr. Ojekudo, Nathaniel A*3

*1,3Department Of Computer Science, Ignatius Ajuru University Of Education Port-Harcourt, Nigeria.
*2Department Of Computer Science And Informatics And Cybersecurity, Federal University Otuoke, Nigeria.

DOI : https://www.doi.org/10.56726/IRJMETS58296

ABSTRACT

Cyber security is concerned with preventing illegal usage, invasions, sabotage, and natural catastrophes from affecting information, hardware, and software on the internet. Because of the myriad ways in which computer systems and data may be exploited, cyber security is a burgeoning discipline. Online banking information, medical or financial information, and intimate images are examples of data that may require cyber protection. However, as there are challenges to cyber security, it is not always straightforward to apply. Any criminal act that aims to destroy or steal data, as well as disrupt digital life in general, is considered a cyber-security threat. This paper discussed the emerging threats in the cyber security space, analysed and identified some associated cyber security risks and proffered possible solutions that could mitigate the activities of cybercriminals on the internet and evoke vigilance on those that use the internet daily for business and personal activities.

Keywords: Cyber space, cybercrime, cyber security, espionage.

I. INTRODUCTION

The advent of the computers, Internet, as well as the increased usage of information technologies, has resulted in significant changes in the way people live, play and work globally. It is revolutionizing many growths of nations, removing obstacles to business, and allowing individuals all over the world to interact, cooperate, and exchange ideas regardless of class, geographical location, or time. This convergence of the internet, information systems, and people is known as the cyberspace, which has resulted in the creation of a worldwide virtual environment for competitive advantage. Governments, corporations, organizations, and individuals all across the world are progressively embracing cyberspace technology to boost productivity and profitability. It is, in fact, changing socioeconomic activity, security postures, and opening up prospects for innovation and wealth increasing the resources available for better global governance and people's well-being thereby unleashing their individual and national creativity and productivity seamlessly on a global scale (Mbanaso & Dandaura, 2015).

II. LITERATURE REVIEW

Understanding the Cyberspace

Cyberspace is a phrase that has yet to be fully defined and has no geographical boundaries. It is a word linked with the use of the Internet on a global scale. It is sometimes referred to as a virtual space since the physical existence of cyberspace cannot be detected. Cyberspace is defined as "the absolute interconnectivity of human beings through computers and telecommunications regardless of physical geography." William Gibson, a science fiction novelist, created the word "cyberspace" to characterize the entire spectrum of information resources accessible via computer networks. For our purposes, cyberspace is a place in which digital data sent through computer networks facilitates communication and interaction between two people or between a person and a machine. This engagement or conversation can be employed for a variety of reasons. Madahar (2013) posit that the cyberspace is pervasive and unconstrained by boundaries or geography; it pervades most, if not all, civil and military sectors and is difficult, if not impossible, to govern and impose national authority on. It is ethereal and complicated, with many potentials to do good as well as bad.

According to the UK Cabinet Office (2011), the rush of innovations resulting from the convergence of information and communication technology (ICT), as well as shifting mobility and social media environments, is undoubtedly constructing a new world. Similarly, the rapid progress and sophistication of mobile technology has resulted in a quick transition in the presentation and interaction with cyberspace resources. Similarly, advancements in core technologies have resulted in decreasing technology expenses, making worldwide access to cyberspace more inexpensive and stress-free. As a result, cyberspace's population will continue to rise, making it more enticing to all actors and stakeholders. As a result, there is a transition from the physical to the virtual world, which is aided by the rapid improvement of computers, telecommunications, people's responsiveness, and auxiliary technologies such as core electronics.

Furthermore, according to the 2022 UK Cyber Security Strategy study, exponential technological discoveries combined with decreasing pricing have made the world more intimately linked than ever before, offering outstanding potential, innovation, and development. The coronavirus (COVID-19) pandemic has accelerated this trend, but it is most likely only the beginning of a long-term structural shift. The global expansion of cyberspace is changing how people live, work, and communicate, as well as reinventing critical institutions that people rely on, such as banking, electricity, food delivery, healthcare, and transportation. To recapitulate, cyberspace is now vital to the future security and prosperity of the planet (UK Cabinet Office, 2022).

With the increased use of cyberspace by individuals and organizations for high-impact service delivery, as well as the ever-increasing traffic and business activities online, there is a growing need to secure data transmission processes from malicious users in order to ensure data integrity, as the threat inherent in cyberspace is also increasing. Despite the enormous benefits of the cyberspace's expansion, there have been constant attacks on information management systems with the purpose to either steal or corrupt information important to the enterprise. Attacks against websites and databases (both personal and corporate) occur at an alarming rate, and these attacks and their modes of operation have changed and continue to grow as time passes.

Overview of Cyber Security

Attacks on information management systems are becoming more sophisticated daily with features involving very high skilled attackers with knowledge about their targets, there is therefore the need for some system to be put in place that could detect those attacks on the databases as they impact heavily on individual, small organization and Multinational Corporation (Shukla & Verma, 2015). With the global nature of web application servers in the sense that they are remotely accessible, it becomes much more vulnerable and easier for malevolent users to launch attacks on the network at different protocol level which include the transport and network layer of the TCP/IP, with additional vulnerability induced by custom web applications designed with little or no consideration to security and privacy concerns which can be utilized by the attackers to invade and infiltrate network systems security leading to loss of data and disruption of web servers which adversely affects impacts the organizations and their customers (Sher, 2016).

Creating a safer and more secure cyberspace have become one of the critical needs of the industries and individuals in the twenty-first century as cyber criminals have devised novel approach to infiltrating network infrastructures to steal and plunder vital business and personal information. Cyber security therefore is the process of safeguarding an internet-connected systems, which include hardware, software, and data from possible threats. In the computing environment, security includes both cyber security and physical security, both of which are employed by businesses for protection against unwanted access to data centres and other computerized systems. A subset of cyber security is data security, which is aimed to ensure the confidentiality, integrity, and availability of data (Seemma et al., 2018).

Kalakuntla et al., (2019) refers to cyber security as both the insecurity created by and through the use of the internet and the cyber space, as well as the techniques or processes used to make it progressively safe and secured. It refers to a variety of exercises and procedures, both specialized and non-specialized, that are anticipated to protect the bioelectrical state as well as the information it carries and conveys from all potential risks. It is essentially the security of systems, networks, and data in cyberspace, and it is becoming increasingly important as more people across the world connect to the internet. It addresses not just confidentiality and privacy, but also data availability and integrity, both of which are critical for the quality-of-service delivery.

With the recent trend of attacks on the internet and the speed at which these attacks are transmitted it is clear that the defence mechanism deployed by organization to protect host computers connected to the internet can easily be compromised and defied. In order to realize an efficient intrusion prevention from this malevolent attacker, there is need for a relative knowledge to be acquired on the pattern of potential attack or threat to the system (Diebold et al., 2005). As networks assets becomes increasingly vulnerable to the speedy growth of the internet, the impacts of automated attacks on computer networks have gone beyond the scope of individual host and enterprise, not only infecting these hosts with malicious codes but also denying legitimate users access to network services and resources. Internet worm is one threat that can operate on a network undetected as it blurs the conventional threat detection and makes quarantining very difficult (Bailey et al, 2006).

Researchers and network security professionals have expressed rising worry about how to control, simplify, and possibly eradicate the activities of harmful assaults and attackers on individual and organizational network infrastructures. To thwart these hostile assaults, network assets must be monitored and protected (Joseph, 2015).

Cyber Security Attacks

According to Farhat (2021), a cyber-attack is an attack launched from a computer against a website, computer system, or individual computer collectively or a single computer that jeopardizes the computer or information stored on it to disrupt its confidentiality, integrity, or availability. The cyber-attacks and threats on an organization information security architecture may take the following form;

- Unauthorized access to a computer system or its data;
- Unwanted disruption or denial of service attacks, including the complete shutdown of websites;
- Virus or harmful code (malware) installation on a computer system;
- Unauthorized access to a computer system for the purpose of processing or storing data;
- Changes to the hardware, firmware, or software of a computer system without the owner's knowledge, instruction, or agreement;
- Workers of former employees making inappropriate use of computer systems.

There are two distinct categories of cyber-attack on a computer network, they include

- Active and
- Passive attack,

Passive and Active Attack

In a passive attack, an intruder observes a system and network traffic and looks for open ports and other weaknesses. For example, they may exploit an unpatched system or take advantage of an expired certificate on a security device (Saxena et al., 2012). Immediately the intruder has gained access to the network, they can gather information in a variety of methods. In a passive foot printing attack, the intruder will strive to gather as much intelligence as possible in order to utilize it later to attack the target system or network. An example is when an intruder captures network traffic for subsequent study using a packet analyzer program such as Wireshark (Hassan, 2020).

Installing a keylogger is another type of passive attack in which an intruder waits for the user to submit their credentials before recording them for later use. The following are the two most popular applications for passive attacks:

- Traffic analysis: In this kind, an attacker watches communication channels to acquire a variety of information, such as human and machine identities, locations of these identities, and, if relevant, the type of encryption employed.
- Message content disclosure: In this case, an attacker will monitor an unsecured communication channel, such as an unencrypt

Other sorts of passive assaults include "passive reconnaissance," in which an attacker attempts to get critical information about a target organization connected to the internet without delivering any traffic (packets) to the target server or network. An example of this sort of attack is reading the contents of a website for important information (such as employee contact information) that may be utilized in active assaults or discovering files that have been left unprotected on a target server, such as meeting documents or intellectual property.

An "active" attack aims to alter system resources or affect their operation. This form of cyber-attack includes compromising a person or network using information obtained during a passive assault. Active attacks come in a variety of forms. In a masquerade attack, an attacker impersonates another user in order to gain access to a restricted part of the system. In a replay attack, the intruder takes a packet from the network and sends it to a service or application as if the intruder were the user who provided the packet in the first place. Hassan (2020) further states that active attacks include denial-of-service (DoS) and distributed denial-of-service (DDoS), both of which function by stopping authorized users from accessing a specific resource on a network or the internet (for example, flooding a web server with more traffic than it can handle). An active assault, as opposed to a passive attack, is more likely to be detected by the target shortly after it is launched. The following are various countermeasures to this sort of attack:

- A random session key that is only valid for one transaction at a time can be produced; this should successfully prevent a malicious user from re-transmitting the original message after the original session has ended.
- The use of one-time passwords assists in the authentication of transactions and sessions between communication parties. This ensures that even if an attacker is successful in capturing and retransmitting the intercepted message, the associated password will have expired by that time.
- Using the Kerberos authentication system (often found in Microsoft Windows Active Directory), which provides several safeguards against various forms of replay attacks.

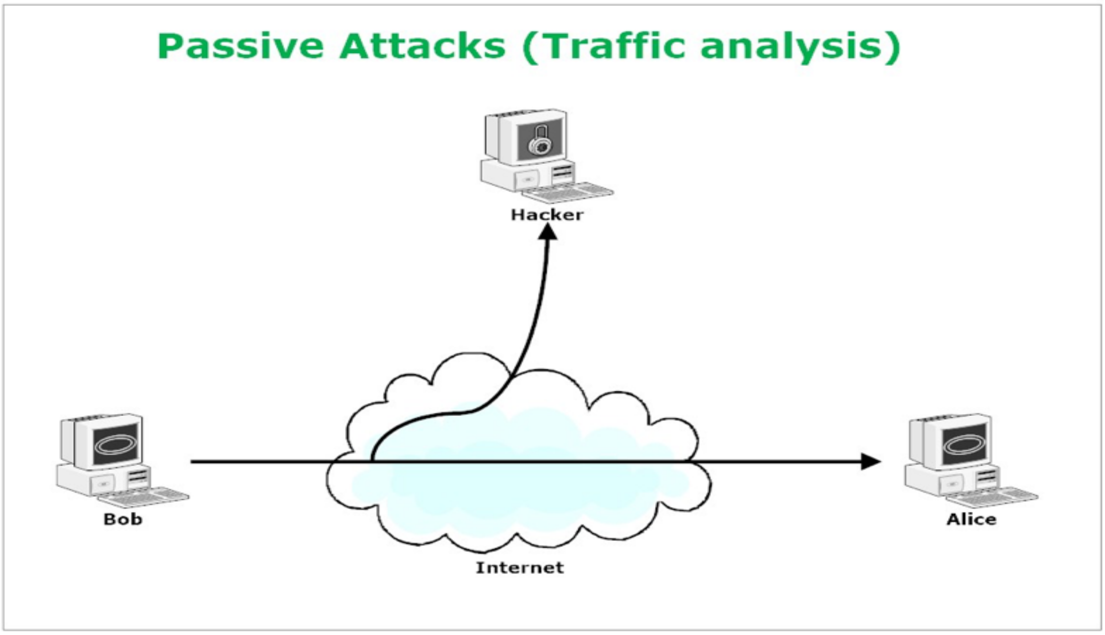

Figure 1: Passive attack-Traffic analysis (Source: Hassan, 2020)

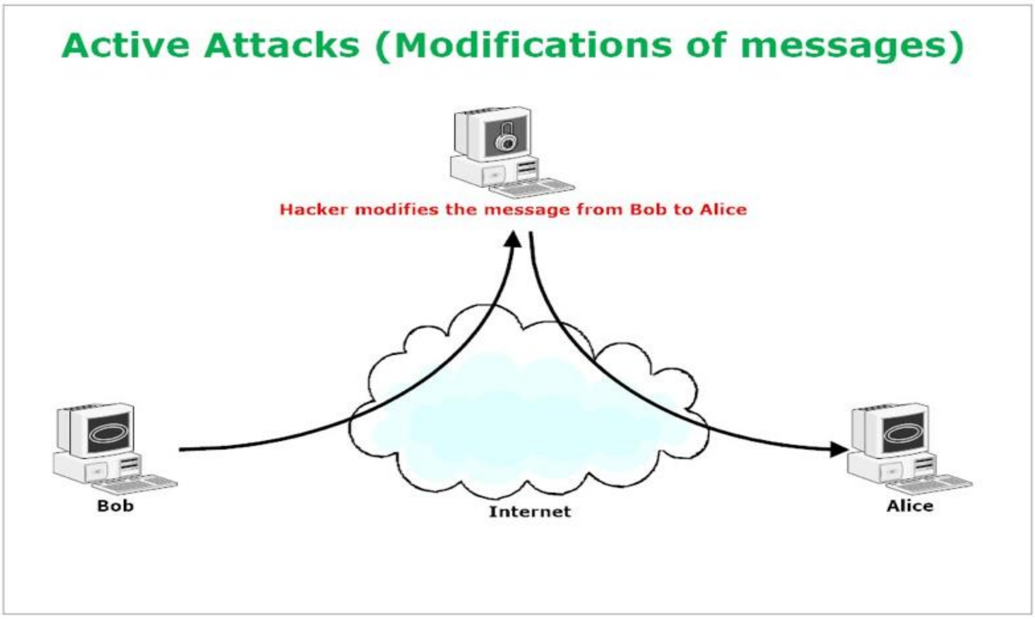
Active Attacks (Modifications of messages)
Hacker modifies the message from Bob to Alice
Bob
Internet
Alice

Figure 2: Illustration of an Active Attack (Source: Hassan, 2020)

Cyber Security Threats

The massive number of connected devices, objected and individual on the cyber space and the large volume of data and other activities conducted per second calls for the need to review the cyber security architecture at regular interval. The world of the internet has evolved drastically as people from across the globe carryout huge business transactions virtually with little or no previous knowledge of the person of the other side of the bargain, the risk factor is unimaginable. Irrespective of the level of security deployed in these online transactions, malevolent users and cybercriminal still find their way to swindle unsuspecting members of the society via the cyber space on daily basis. The threat is growing at an alarming rate with more innovation deployed by these cybercriminals to beat the best of cyber security technologies deployed.

A threat is a hostile act committed with the intent of corrupting or stealing data or disrupting an organization's system or the entire company. Humans and nature are the two principal sources of threats. Human threats are those that are created by humans, such as malevolent threats that include both internal and external threats that seek to harm and disrupt a system. While natural disasters such as earthquakes, hurricanes, floods, and fires can inflict serious damage to computer systems, no one can stop those (Obotivere & Nwaezeigwe, 2020). Moreover, Abi (2020) defined cyber security threat as a malevolent act that aims to harm, steal, or disrupt digital life in general.

Cyber security threats are designed by those who seek to gain unauthorized access to a control system device and network through a data communications channel. This access can be directed from within an organization by trusted people or from remote areas over the Internet by unknown individuals. Control system threats can arise from a variety of sources, including hostile governments, terrorist organizations, disgruntled personnel, and criminal intruders. Cyber security threats can be categorized based on their character, impact, origin, and actor as follows:

1. Accidental or Intentional Threats
2. Active or Passive Threats
3. Origin of Threat
4. Threat Actor
5. Vulnerability

Accidental or Intentional Threats

Accidental threats arise when there is no intentional aim. For example, system or software failures, as well as physical failures. Intentional threats, on the other hand, are the outcome of purposeful activities against an asset's security. Intentional threats vary from casual network investigation using readily available monitoring tools to complex assaults requiring particular system expertise. Intentional threats that manifest as attack (Bendovsch, 2015).

Active or Passive Threat

Active threats are those that cause a change in the status or functioning of a system, such as data alteration or physical equipment destruction. Passive threats, on the other hand, do not involve a change in the status of the equipment. Passive threats seek information from a system while causing no harm to the system's resources. Eavesdropping, wiretapping, and deep packet analysis or inspections are examples of common passive threat approaches. Passive threats that are successful become passive attacks.

Origin of Threat

The origin of threat might be defined as an entity that seeks to break the security controls of information or physical assets. The main goal of the origin or originator of the cyber security threat is to make financial gain from the cyber security breach that is initiated.

Threat Actors

A cyber security threat actor is a person or entity that carries out the attack or, in the case of an accident, exploits the mishap. For example, if an organized criminal gang corrupts an employee, the organization is the Threat Source, and the employee is the threat actor. They could be states, groups, or individuals with malicious intent who seek to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks by exploiting vulnerabilities, low cyber security awareness, or technological developments.

Vulnerability

The origin of threat and the actors' intents frequently manifest as attacks, owing to gaps in security mechanisms. A vulnerability might be a lack of software patching or a faulty setup. Even good technological protections may fail if social engineering assaults trick employees with limited expertise into violating security.

Cyber Security Threat

Some notable cyber security threats include;

a. Ransomware

Ransomware is a type of malware that encrypts a victim's data. The attacker then demands a ransom from the victim in order to regain access to the data upon payment. Users are shown how to pay a charge in order to obtain the decryption key. The charges can range from a few hundred dollars to thousands of dollars, and they are paid in Bitcoin to hackers. Ransomware is growing more prevalent: In 2013, Symantec saw a 500% month-on-month spike in ransomware (Fruhlinger, 2020; Hassan, 2020).

According to Alaba and Jegede (2021). this attack is one of the riskier risks that can allow the system to escape with no losses. Once the victim has been locked, they are unable to view their data or results. Ransomware also targets sensitive items such as bank details, company databases, and personal files. The attackers then demand payment to decrypt the data and files. The primary goal of such attacks is usually money. According to Kerner (2023), the rate of ransomware assaults increased in 2022, accounting for more than 25% of all breaches globally. As more individuals utilize the Internet and rely on cloud-based services, ransomware becomes an undesirable possibility that can penetrate and compromise sensitive data and key assets. To lessen these difficulties, ransomware must be addressed, and mitigating techniques must be deployed. A proactive security posture is also required to protect against ransomware assaults. A corporation can defend itself against ransomware attacks by adopting a security posture that includes careful monitoring of potential risks.

b. Malware

Malware, sometimes known as "malicious software” or scumware is any file or program that is injected onto the computer of a target with the intent of inflicting damage or gaining unauthorized access. Malware can take many forms, such as viruses, spyware, worms, ransomware, Trojan horses, and keyloggers, to name a few (Obotivere & Nwaezeigwe, 2020). According to Edgar and Manz (2017), it is a technique by which people are exposed to worms or viruses and have their devices infected. This type of program can be developed in practically any programming or scripting language and distributed in a variety of file formats. Malware can collect information and spy for an extended period of time without alerting the compromised computer system. Furthermore, it can be used to harm or sabotage the system into which it is introduced like in Stuxnet, or it can be used to extort money or payments (Kramer & Bradfield, 2010).

This attack is set up so that a user or victim who is weak to it is tricked into clicking on the malware source which is typically presented as a script or executable code and unintentionally downloads the malware onto the victim's machine. Some malware strains are designed to monitor users in order to access and collect credentials or other useful information, while others are only designed to disrupt the smooth running of the target machine and some are designed to get persistent access into the target network (Perwej et al., 2021).

c. Social Engineering

Cybercriminals and attackers use social networks to gather personal information about persons of interest, which they then use to strengthen the persuasiveness of their targeted emails. This approach is known as social engineering, and it is a significant area where cyber security threats are on the increase. According to Breda et al (2017), social engineering is one of the simplest strategies for gathering knowledge about a subject by exploiting human weaknesses that are inherent in every business. In essence, social engineering is the deliberate invention and deployment of deceptive strategies to manipulate human targets (Conteh & Schmi, 2016). In the domain of cyber security, it is generally used to persuade victims to provide confidential data or to perform acts that violate security regulations, such as accidentally infecting systems or leaking classified information.

A social engineering attack fundamental goal is to circumvent cyber security measures by lying, taking advantage of the individuals who are the weakest link in the chain. According to Prashant (2016), the victims do not realize how detrimental their behaviour is until after the conversation. Innocent inclinations are what the social engineer preys upon, not criminal behaviour. Social engineering does not include overt techniques like threats or bribery. A skilled practitioner of this profession is able to control the psychological features of the human mind by comprehending and perceiving social interaction patterns. Without spending money on technical security breaches, the attacker can carry out a quick and inexpensive security compromise using this technique. According to Wang et al (2020), social engineering has created a severe security danger to IT infrastructure, users, data, and the operations of personal and business activities on the cyberspace. This type of attack is costly, especially in large corporations. Between the years 2018 and 2020 in the developed countries like United State, Canada, United Kingdom, Australia, New Zealand and Germany, 48% of large organizations and 32% of all companies have had 25 or more social engineering attacks, with an estimated 30% per incident cost of over $100,000 stated in large corporations.

d. Phishing

Phishing is a sort of fraud in which false emails that appear to be from credible sources are sent; nonetheless, the goal of these emails is to obtain sensitive data, such as credit card or login information (Seemma et al., 2018). It is a deceptive attempt to get sensitive information from a victim in order to carry out some kind of activity. In these situations, cybercriminals and attackers attempt to obtain personal information or data, such as usernames, passwords, and credit card details, by pretending to be a reliable party. The majority of phishing attacks use technology, such as emails and phone calls. Attacks by phishers typically take the form of emails posing as coming from respected organizations like your bank, the tax department, or another reliable organization (Kim et al., 2016). There are different types of phishing attackes which includes; spear phishing, smishing, whaling, E-mail phishing, search engine phishing and vinshing.

Amongst the various types of phisihng attacks the most popular are the spear phishing and Email attacks respectively. According to Perwej et al (2021), the simplicity of use and astounding success makes spear phishing the most common kind of cyberattack. Spear phishing is a type of phishing attack that targets a particular group or kind of individual, like the system administrators at a business. On the other hand similar to spear phishing is the E-mail phishing which entails hackers sending emails to every single email address they can find. Typically, the email alerts the recipient that their account has been compromised and that they must act quickly by clicking on the "this" link. These attacks are generally simple to identify because the English is not always clear.

Emerging Cyber Security Threats and Possible Solutions

These new and emerging cybercriminals are essentially a hybrid between the once-esoteric, targeted attacker and the common supplier of off-the-shelf software, use manual hacking tactics not for espionage or sabotage, but to sustain their dishonourable money streams. Obotivere and Nwaezeigwe (2020) posited that the following are some of the emerging threats to cyber security;

- human nature,
- inadequate patch management and,
- man-in-the-middle attacks

Human Nature

Human nature or Characteristics has shown that individuals are the most serious hazards to cyber security. Employees, vendors, or anyone else with access to your network or IT-related systems are the source of these risks. A cyber-attack or data breach can also occur due to human error or a lack of cyber security knowledge, such as employing easy-to-guess passwords or falling for phishing emails. Hackers, for example, commonly utilize social engineering techniques such as "hacking without code" to persuade their victims to submit the information they want or to interact with dangerous material.

To manage the menace of human nature on cyber security architecture, having strong firewalls and antivirus solutions in place is insufficient; instead, businesses should use the services of an in-house or third-party cyber security operations centre (CSOC) to combat these types of cyber security threats for both their overall organizational cyber security and their webs.

Inadequate Patch Management

This is a procedure that causes gaps in an organization's information security system. Patching should ideally be implemented as soon as a vulnerability is discovered because it puts the organization at risk of cyber-attacks, necessitates remediation, which can cause downtime, harms the organizations' reputation, and renders her noncompliant with many industry and regulatory cyber security standards.

To mitigate and prevent cases of inadequate patch management organizations are to;

- Make patch management a priority rather than an afterthought.
- Implement effective patch management as it is critical to success of the organization and the protection of your customers' data.
- Develop and executing appropriate patch management rules and processes that will help in reducing the organizations' stolen data attack surface.
- Patching these vulnerabilities in real time via automation improves the effectiveness of your cyber defense.

Man-in-the-Middle Attacks

The majority of a business's everyday operations are conducted online because the Internet has gradually surpassed other factors in importance for modern life and business. The most popular internet activity for both personal and professional purposes is social media. Online banking and shopping have also become easier day by day, yet neither is viable without an internet connection. The requirement for the internet provided hackers with an opportunity to be readily targeted. Hackers primarily target various organizations in an effort to steal confidential data, which could result in financial loss (Abad & Bonilla, 2007).

In such a situation, the man in the middle attack is the most frequent attack, making it the main danger to network security. The most typical scenario for such an assault involves two victims (users) and a third party attacker. The attackers function as the intermediary between the two users, who are unaware that a third individual is truly standing between us. The attacker uses the communiqué channel to communicate with the other user, and it is capable of operating messages between the two users (Javeed et al., 2020). In this type of attack cyber criminals create some sorts of cyber security dangers by setting up bogus public Wi-Fi networks or installing malware on victims' computers or networks.

The objective of the attacker is also the definite data transmission among the endpoints in a network, and to infects the veracity and discretion of the data. The attacker has the capacity to compromise discretion through eavesdropping as well as veracity through message altering via communiqué interference. Attackers can also reroute, modify, or eliminate messages to trigger the end of communication for one of the users, compromising availability. The ultimate aim of this type of attack is to steal personal information such as login passwords, account information, and credit card numbers of the victim.

Some of the greatest strategies to defend your business, customers, and website from man-in-the-middle attacks include:

- HTTPS is truly required by major browsers such as Google Chrome, Firefox, and others.
- Installing an SSL/TLS certificate on your website allows you to use HTTPS.
- When using public Wi-Fi, using Virtual Private Networks (VPNs) can assist boost security and provide secure encrypted connections.

III. CONCLUSION

The place of security of personal or organization's information is critical to the development and growth of the organization therefore the need for vigilance in the use of the cyberspace. The most serious cyber security risks, like a sniper, are the ones you never see coming. As cyber security threats changes and become more complex, business information management professionals must maintain vigilance in securing their data and networks. To do so, there is the need to first understand the numerous cyber security risks and dangers they are expose to on the internet. After identifying and comprehending the numerous cyber threats to cyber security, care is the watchword for anybody who uses the internet as the malevolent user and hackers are on the watch for those who will let down their guard so they can plunder them and their information security infrastructure.

IV. REFERENCES

[1] Abad, C.I & Bonilla, R.I. (2007). An analysis on the schemes for detecting and preventing ARP

[2] cache poisoning attacks. Proceedings of the 27th International Conference of Distributed Computing Systems Workshops (ICDCSW'07), (p. 60).

[3] Abi, T. (2020). What is a Cyber Threat? Retrieved from Up Gaurd:
Http://www.upguard.com/blog/cyber threat

[4] Alaba, F.A & Jegede, A. (2021). Ransomware Attacks on Remote Learning Systems in 21st Century: A Survey. Biomedical Journal of Scientific & Technical Research, 35(1), 27322-27330.

[5] Bailey, M, Cooke, E, Watson, D, Jahanian, F and Provos, N. (2006). A Hybrid Honeypot Architecture for Scalable Network Monitoring. 20th Annual Network and Distributed System Security, (pp. 1-16).

[6] Bendovsch, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. 7th International Conference on Financial Criminology (pp. 24-31). Oxford, UK: Elsevier.

[7] Breda, F., Barbosa, H & Morais, T.S. (2017). Social Engineering and Cyber Security. International Technology, Education and Development Conference, (pp. 4204-4211).

[8] Conteh, N.Y & Schmi, P.J. (2016). Cybersecurity: risks, vulnerabilities and counter measures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(1), 23-31.

[9] Diebold, P; Hess, A and Schaefer, G. (2005). A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks. 14th Kommunikationin Verteinlten Systemen. , (pp. 1-26). Kaiserslautern.

[10] Edgar T.W & Manz D.O. (2017). Science and cyber security. In E. T. D.O, Research Methods for Cyber Security (pp. 33-62). Syngress.

[11] Farhat, K. (2021). Explaining US Cybersecurity Policy Integration Through a National Regime Lens. Georgia Institute of Technology, School of Public Policy. Georgia: Georgia Institute of Technology.

[12] Fruhlinger, J. (2020). Ransomware explained: How it works and how to remove it. Retrieved from CSO online: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[13] Hassan, N. (2020). What Is an Active Attack vs Passive Attack Using Encryption? Retrieved from Venafi: https://www.venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption

[14] Jamal, M. (2017). Types of ML- Supervised, Unsupervised & Reinforcement Learning. Retrieved February 23, 2020, from LinkedIn:
https://www.linkedin.com/pulse/types-ml-supervised-unsupervised-reinforcement-learning-jamal

[15] Javeed, D., Badamasi, U.M., Ndubuisi, C.B., Soomro, F & Asif, M. (2020). Man in the Middle Attacks: Analysis, Motivation and Prevention. International Journal of Computer Networks and Communications Security, 8(7), 52-58.

[16] Joseph, S. (2015). Advanced Honeypot Architecture for Network Threats. International Journal of Scientific Engineering and Applied Science (IJSEAS), 1(5)., 5(1), 20-32.

[17] Kalakuntla, R., Vanamala, A.B & Kolipyaka, R.R. (2019). Cyber Security. HOLISTICA, 10(2), 115-128.

[18] Kerner, S. M. (2023). Ransomware trends, statistics and facts in 2023. Security. Retrieved from Tech target:https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#:~:text=According%20to%20the%202022%20%22Verizon,State%20of%20Ransomware%202022%22%20report

[19] Kim, L.K., Lee, H & Jun, M. (2016). A study on realtime detecting smishing on cloud computing environments. In L. L. Kim, Advanced Multimedia and Ubiquitous Engineering (pp. 495-501). Heidelberg:Springer.

[20] Kramer, S & Bradfield, J.C. (2010). A general definition of malware. Journal of Computer Virology, 6(1), 05–114.

[21] Madahar, B. (2013). Cyber Defence: Defence and Surveillance Section. Pan European Networks: Science & Technology, 1(4), 23-29.

[22] Mbanaso, U.M., & Dandaura, E.S. (2015). The Cyberspace: Redefining A New World. IOSR Journal of Computer Engineering (IOSR-JCE), 17(3), 17-24.

[23] Obotivere, B.A & Nwaezeigwe, A.O. (2020). Cyber Security Threats on the Internet and Possible Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 9(9), 92-97.

[24] Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N & Jaiswal, A.K. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 8(12), 669-710.

[25] Prashant, K. (2016). Prashant's algorithm for password management system. InternationalJournal of Engineering Science, 6(8), 2424-2426.

[26] Ray, S. (2017). Essentials of Machine Learning Algorithms (with Python and R Codes). Retrieved December 23, 2019, from Analytic Vidhya:

https://www.analyticsvidhya.com/blog/2017/09/common-machine-learning-algorithms/

[27] Salian, I. (2018). SuperVize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning? Retrieved February 20, 2020, from Nvidia:

https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/

[28] Saxena, P., Kotiyal, B & Goudar, RH. (2012). Cyber Era Approach for Building Awareness in Cyber security for Educational System in India . International Journal of Information and Education Technology, 2(2), 45-56.

[29] Seemma, P.S., Nandhini, S & Sowmiya, M. (2018). An Overview of Cyber Security. International Journal of Advanced Research in Computing and Communication Engineering, 7(11), 125-128.

[30] Sher, M. (2016). Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS). Retrieved from Semantic Scholar: https://www.semanticscholar.org/paper/Security-Threats-and-Solutions-for-Application-of-(-Sher/1db751da37420f25a2029204a5a34d683e7f421f

[31] Shukla, M & Verma, P. (2015). Honeypot: Concepts, Types and Working. International Journal of Engineering Development and Research, 3(4), 596-598.

[32] UK Cabinet Office. (2022). Policy paper on National Cyber Security Strategy 2022. Retrieved from UK:

https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[33] UK Cabinet Office. (2011). The UK Cyber Security Strategy 2011. Retrieved from UK Cabinet Office: httpswww.cabinetoffice.gov.uk

[34] Wang, Z., Sun, L & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. IEEE Access journal, 8(1), 85094-85115.