Journal of Management and Service Science, 2022,
Vol. 02, Iss. 01, S. No. 002, pp. 1-10
ISSN (Online): 2583-1798

Managing Cyber Security

Ujjwal Singh[1], Pawan Singh[2]

[1]Amity School of Engineering & Technology, [2]Amity University Uttar Pradesh, Lucknow, India
singhujjwal161@gmail.com[1], pawansingh51279@gmail.com[2]

How to cite this paper: U. Singh and P. Singh (2021) Managing Cyber Security. Journal of Management and Service Science, 2(1), **2**, pp. 1-10.

http://doi.org/10.54060/JMSS/002.01.002

Received: 24/05/2021
Accepted: 15/02/2022
Published: 25/02/2022

Abstract

In the area of information technology, cyber security plays a critical role. In today's world, protecting information has become challenging tasks. When we think of cyber security, the first thing that comes to mind is "cyber-crimes," which are on the rise at an alarming rate. Various governments and organizations are taking a variety of steps to combat cybercrime. Despite many steps, cyber security remains a major issue for many people. This paper focuses on the issues that cyber security faces in the modern era. It also covers the most up-to-date information on cyber security tactics, ethics, and trends that are transforming the face of cyber security.

Keywords

Cyber Security, Cyber Attacks, Cyber Security Trends, Cyber Security Tools

1. Introduction

Today, Internet is the quickest developing foundation in consistently life. In the present specialized climate, numerous most recent advancements are changing the substance of humankind. Be that as it may, because of these emerging innovations, we can't protect our private data in an effective way, and henceforth these days cybercrime is expanding step by step. More than 80% of online transactions are done on the web, so this field requires a great deal of safety for straightforward and best transaction. Henceforth, digital protection has turned into a most recent issue.

The most current innovations, such as cloud computing, e-commerce, and online banking, all need a high level of security. Since these innovations hold some significant data with respect to an individual, their security has turned into an unquestionable requirement. Improving network safety and ensuring basic data frameworks are crucial for every country's security and monetary prosperity. The battle against digital cybercrime needs an exhaustive and more secure methodology. Considering that specialized measures alone can't forestall any cybercrime, it is important that law implementation offices are permitted to research and arraign digital crimes adequately. Currently, several countries and governments are enforcing strict rules on digital security in order to avoid the loss of critical data. Everyone should likewise be prepared on this digital protection and save themselves from these expanding digital crimes.

2. Purpose

The objective of the paper is to provide data about cyber-security and its elements. It also gives information about cyber-attacks and its types. The paper gives some essential data about cybercrime and gives a few strategies for forestalling cyber-attacks.

Cyber-crime has become a major threat to everyone in modern society. Hackers are stealing huge sensitive information from government and some enterprise firms. There are many different types of cyber-crimes evolving, and everyone should be aware of them. To avoid cyber-crime, a variety of measures and technology can be used. Every company wants to keep their sensitive information safe from a hacker; that's way the knowledge of cyber-security in necessary.

3. Cyber Security

Cyber security is the practice of protecting networks and IT (Information Technology) systems against digital attacks. In the context of IT systems, security includes cyber security and physical security; both are used to protect data centers and other IT systems from illegal access. A component of cyber security is data security, which is aimed at maintaining privacy protection, integrity, and reliability.

Information security and protection will always be at the forefront of every organization's safety measures. Social networking sites provide a space where clients have a sense of security as they connect with loved ones. Cyber attackers will continue to target social networking sites to steal personal data. Individuals should use all required caution while using social media and when doing financial transactions.

4. Elements of Cyber-Security

The following are examples of strong cyber security based on a systematic approach.

4.1. Network Security

The goal of network security is to keep the network and data usable and reliable. A network penetration test is used to evaluate a system's vulnerabilities as well as other security issues that may arise on servers, network hosts, devices, and network services.

4.2. Web Application Security

Web application security is a set of protocols and tools that work together to keep all mobile, website, and desktop apps safe against malicious attacks as well as unintentional breaches and failures. It's the process of identifying, repairing, and removing flaws in software that allow hackers to attack them.

4.3. Information Security

Information security safeguards sensitive data against illegal access, modification, or recording, as well as any disturbance or destruction. The purpose is to protect vital data such as customer account information, financial information, and intellectual property.

4.4. Mobile Security

Mobile security alludes to shielding both hierarchical and individual information hung on cell phones, for example, cells, workstations, tablets, and other comparable gadgets, from risks like unapproved access, gadget misfortune, malware, etc.

4.5. Cloud Security

Data stored online via cloud computing platforms is protected from theft, leakage, and destruction by cloud security.

4.6. Operational Security

Operational security (OPSEC), otherwise called procedural security, is a danger, the executive’s cycle that urges supervisors to see tasks according to the viewpoint of an enemy to shield sensitive data from falling into some unacceptable hands.

4.7. End User Education

Human mistake is one of the most common causes of data breaches. It is critical for a company to provide cyber security training to its staff. Every employee should be aware of phishing assaults via emails, and links, as well as the ability to deal with any cyber dangers they may encounter. Employees should not utilize an insecure network.

5. Cyber Attack

Any attempt to obtain unauthorized access to a computer, computing system, or computer network with the intent to cause harm is referred to as a cyber-attack. To harm the IT system and steal data, cyber-attackers use illegal methods, tools, and approaches.
The following list illustrates some of the most common cyber-attacks used by attackers to target IT systems:

i. Malware

Malware is malicious software program created by a computer criminal or hacker to harm a genuine user's computer. It is one of the most frequent cyber dangers. Malware can be distributed by links in emails and email attachments, or by downloading and installing infected software. Malware may be utilized by computer criminals to gain money. Types of Malwares.
Virus: (Vital Information Resources under Siege): A virus is a program designed to infiltrate your computer and corrupt your files or data. Viruses can also multiply and spread across the computer system.
Worms: They are a type of virus that can multiply itself. They vary from viruses in that they do not require human interaction to travel over the network and propagate from one infected system to the whole network. Worms can propagate over a network, through operating system flaws, or by email. The worm's replication and spread throughout the network uses network resources such as space and bandwidth, causing the network to seize.
Trojan Horse: A Trojan horse is software that is downloaded and installed on a computer that looks to be innocent but is actually dangerous. Unexpected changes to computer settings and unexpected activity, even when the computer is supposed to be inactive, are significant indicators that a Trojan is present. The Trojan horse can be spread through emails or while downloading files from unsecure websites. When a user opens an email attachment or downloads free software, the virus contained inside is transmitted to the user's computer device. Once inside, the malicious code may carry out whatever task the attacker has programmed it to do.
Spyware: Software that surreptitiously records what a user performs in order for hackers to utilize this information. Spyware, for example, may record credit card information and ID's while entering on a web site or a software.
Ransomware: Ransomware is a program 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 instructed by the hacker how they can pay for a decryption key.
Adware: Adware is any software application that displays advertisements while a program is being used. Adware is mostly designed for desktops, although it may also be found on mobile devices. It collects the data from your browser history and

shows ads of your interest.

Scareware: Scareware is a malware technique that tricks users into believing they must download software. While browsing the Internet, a pop-up alert appears on the screen, warning of the existence of hazardous viruses, spywares, and so on, and then it offers phony antivirus or other software. Scareware, or software carrying dangerous malware, is downloaded onto the user's computer while the user continues to download. Some codes are so powerful that they cannot be removed.

ii. Web Attack

A web attack damages the device via the internet. These viruses may be acquired through the internet and end up causing extensive and permanent harm to your system.

iii. SQL Injections

SQL injection is a sort of cybercrime in which malicious code is used to modify backend databases in order to obtain information that is not intended to be displayed. These often involve private and sensitive data elements such as user lists and client information, among other things.

iv. Cross-Site Scripting Attacks

Another form of injection breach is cross-site, in which attackers transfer malicious scripts from websites. When a user visits an infected website, the malicious JavaScript code is run on the user's browser. This code may be used to steal sensitive information such as a username and password.

v. Dos Attacks

These are attacks aimed at shutting down services or networks and rendering them unreachable to their user requirements. These assaults flood the target with information and overwhelm it with visitors, causing the website to crash. Dos attacks are typically directed at strong organizations' web servers, such as governments or trade corporations.

vi. Password Attacks

These are merely designed to decode or even attempt to acquire a user's password. In such circumstances, attackers can use Password Sniffers or other cracking tools. These attacks are carried out by gaining access to credentials that have been exported or saved in a file.

vii. Eavesdropping Attacks

An eavesdropping attack, also known as a sniffing or spying attack, is the stealing of data while it is being transmitted across a network by a computer, smartphone, or other connected device. The attack uses unprotected network communications to get access to data as it is being delivered or received by the user.

Eavesdropping is a misleading phrase. Typically, attackers want valuable financial and commercial information that may be sold for illegal reasons.

viii. Brute-Force and Dictionary Network Attacks

These are network assaults in which the attacker attempts to directly log into the user's accounts by verifying and trying out many possible passwords until they locate the proper ones.

ix. Computer Hacking

It is the act of altering computer hardware and software to achieve a goal other than the creator's original intent. Hacking a computer system can be done for a variety of purposes, ranging from simple demonstrations of technical skill to sealing, altering, or deleting data for social, economic, or political objectives. Now, companies are employing hackers, or those who specialize in hacking computers, to purposefully break into a company's computer system in order to identify and repair security flaws.

x. Insider Threats

An insider threat is a security risk that originates within the company being targeted. It usually includes a current employee or business colleague who has access to sensitive information or privileged accounts on an organization's network and violates that access.

xi. Man-In-The-Middle Attacks

A man-in-the-middle attack is a sort of eavesdropping attack in which the attacker disrupts a data transmission. The attackers act as both legal parties after placing themselves in the "middle" of the transfer. This allows an attacker to intercept information and data from either side while also providing malicious links or other information to both legal parties in a manner that may go undetected until it is too late.

xii. AI-Powered Attacks

Computer systems may now be configured to learn and educate themselves, and AI-powered attacks represent a new form of cybercrime. AI is used in a variety of everyday applications through the use of computational processes known as Machine Learning. This program is designed to teach computers how to execute certain tasks on their own. They can also do these duties by educating themselves about potential roadblocks to their development. AI can also hack into numerous systems, like self-driving cars and drones, and turn them into potentially lethal weapons. Password cracking, identity theft, and other cybercrimes may be carried out via AI-powered programs.

xiii. Drive-By Attacks

Drive-by attacks are used to distribute malware via vulnerable websites. Hackers initially seek for websites with poor protection and then insert harmful scripts into PHP or HTTP code on one of the pages. The software may then instantly install malware onto any machine that accesses the site.

xiv. Phishing Attacks

Phishing is a sort of internet fraud in which thieves use email, text messages, advertisements, or other ways to mimic genuine businesses in order to obtain personal information. This is generally accomplished by providing a link that seems to take you to the company's website to fill out your information - but the website is a sophisticated forgery, and the information you submit gets directly to the scammers.

xv. Spear Phishing Attacks

Individuals seeking illegal access to certain companies' data are the targets of these assaults. These hacks aren't carried out by random attackers, but rather by those attempting to get access to particular information such as trade secrets, military intelligence, and so on.

xvi. Whale Phishing Attacks

A Whale Phishing Assault is a form of phishing attack that targets persons in leadership positions, such as Chief financial officers or CEOs. Its main goal is to steal information because these people usually have unrestricted access and work with sensitive data.

xvii. Teardrop Attack

A teardrop attack is a type of denial-of-service (Dos) attack that aims to knock down a target website or network. An attacker uses this method to transmit fragmented data packets to the target device. The packets' structure makes it difficult for the system to read the data. The work required to do so eventually exhausts the machine, leading it to crash

6. Computer Criminals

Computer criminals have access to massive amounts of hardware, software, and data, and they can disable most of the world's effective business and government systems. Cyber-security's objective is to prevent these criminals from harming others. Computer crime is defined as any crime involving or aided by the use of a computer. Although this definition is undoubtedly wide, it allows us to think about how we might safeguard ourselves, our businesses, and our communities against malevolent computer users.

Understanding who commits these acts and why one way to prevention or mitigation is. Much research has been done to figure out what makes computer criminals tick. We may be able to spot prospective criminals and prevent crimes in the future by researching those who have already used computers to commit crimes.

7. CIA Triad

The CIA Triad is a security paradigm that was created to assist people in thinking about several aspects of IT security. The CIA triad is divided into three parts:

i. **Confidentiality:** The term "confidentiality" means "privacy." Confidentiality safeguards are in place to guard sensitive data from illegal access. Data is frequently classified according to the amount and sort of harm it may cause if it falls into the wrong hands. Those classifications can then be used to implement more or less harsh actions.

ii. **Integrity:** Integrity refers to the consistency, accuracy, and reliability of data throughout its lifecycle. It must not be altered in transit, and precautions must be taken to ensure that unauthorized parties cannot alter data (for example, in a breach of confidentiality).

iii. **Availability:** The term "availability" refers to the capacity for authorized parties to access information on a consistent and timely basis. This is best accomplished by carefully maintaining all hardware, conducting hardware repairs as soon as they become necessary, and maintaining a stable operating system (OS) environment free of software conflicts. It's also critical to stay up to date on all necessary system upgrades.

8. Cyber Crime

Cybercrime is characterized as wrongdoing where an IT system is utilized as an instrument to carry out an offense. A cybercriminal may utilize a gadget to get to a client's very own data, classified business data, government data, or make device disable.

It is likewise a cybercrime to sell or evoke the above data on the web. The growing list of digital violations includes wrongdoings made possible by computers, such as network disruptions and the spread of computer viruses, as well as computer-based variants of existing violations, such as data fraud, stalking, tormenting, and psychological oppression, all of which have become serious issues for individuals and countries. Generally, in like common man's language cybercrime might be characterized as wrongdoing, perpetrated utilizing a computer and the web to steel an individual's identity or disturb activities with malignant projects. As technology continues to play an increasingly important role in people's lives, digital crimes will increase in tandem.

9. Cyber Terrorism

The intentional use of IT systems and networks to cause hurt for private gain is understood as cyber-terrorism. Experienced cyber-terrorists with advanced hacking skills will cause large harm to government networks, effort, a rustic prone to future attacks. Since this could be thought of as a kind of terror, the terrorists' goals could also be political or ideological.

10. Cyber Espionage

Cyber espionage, often known as cyber spying, is a sort of cyber-attack in which a malicious user tries to acquire access to highly sensitive or restricted data or IP (Intellectual Property) for commercial, competitive, or political gain.

Cyber espionage aims to steal confidential information from governments and organizations. These cyber-attacks could be motivated by a desire to know what is happening in the other government's backyard, or they could be a terrorist act.

11. Trends That Changing Cyber Security

Here are a few of the major trends that are affecting cyber security

11.1 Web Server

Attacks on web apps to extract data or transmit harmful code are still a problem. Malicious code is distributed by cyber thieves through legal web servers that have been hacked. However, data-stealing attacks, many of which garner public attention, are also a significant concern. We must now place a higher emphasis on the security of web servers and web applications. The ideal venue for these cyber crooks to steal data is through web servers. To avoid being a victim of these frauds, one should always use a safer browser, especially during critical transactions.

11.2 Cloud Computing

All small, medium, and large businesses are gradually adopting cloud services these days. In other words, the world is gradually approaching the clouds. Because communications can bypass established ports of inspection, this latest trend poses a significant problem for cyber security. In order to prevent the loss of vital information, policy controls for web applications and cloud services will need to change as the number of applications available in the cloud rises. Despite the fact that cloud services are building their own models, security concerns continue to be raised. Although the cloud offers numerous advantages, it is important to remember that as the cloud evolves, so do its security issues.

11.3 APT's And Targeted Attacks

APT (Advanced Persistent Threat) is a new type of cybercrime software. For years, network security features like web filtering and intrusion prevention systems (IPS) have been critical in detecting such targeted attacks (mostly after the initial compromise). In order to detect attacks, network security must interact with other security services as attackers become more daring and use more ambiguous approaches. As a result, we must upgrade our security measures in order to prevent future threats.

11.4 Mobile Networks

We can now communicate with anyone in any area of the world. However, security is a major worry for these mobile networks. Firewalls and other security protections are getting weaker as people use more devices such as tablets, phones, computers, and other devices, all of which require additional security precautions in addition to those provided by the applications. We must always keep the security of these mobile networks in mind. Furthermore, because mobile networks are so vulnerable to cybercrime, extra caution must be exercised in the event of a security breach.

11.5 IPv6 (Internet Protocol Version 6)

IPv6 is a new Internet protocol that will replace IPv4 (the previous version), which has served as the backbone of our networks and the Internet in general. It's not merely a matter of moving IPv4 features to IPv6. While IPv6 is a complete replacement for IPv4 in terms of increasing the number of available IP addresses, there are certain basic modifications to the protocol that must be considered in security policy. As a result, it is always preferable to transition to IPv6 as soon as possible in order to avoid cybercrime risks.

11.6 Encryption of the Code

Encryption is the technique of encrypting communications (or information) in such a way that it cannot be accessed by hackers. An encryption technique converts a message or information into unreadable cypher text by encrypting it with an encryption algorithm. This is normally accomplished through the use of an encryption key, which determines the message's encoding method. At its most basic level, encryption safeguards data privacy and integrity. However, increasing encryption means more cyber security challenges. Encryption is additionally used to shield information on the way; for example, information sent across networks (e.g., the Internet, online business), cell phones, remote receivers, and remote radios, in addition to other things. Subsequently, by encoding the code, one might decide if data has been spilled.

12. Tools Used in Cyber Security

Here are some tools to prevent digital attacks and safeguard your business.

12.1 Firewalls

A firewall is a security device, either hardware or software, that helps safeguard your network by filtering traffic and preventing unauthorized access to your computer's sensitive data. A firewall can assist prevent dangerous malware from infecting your computer by blocking undesired traffic. All messages entering or leaving the web pass through the firewall, which examines each message and blocks those that do not comply with security requirements. Firewalls will now play a crucial role in identifying malware.

12.2 Malware Scanners

This is a tool that searches all of the files and documents on the computer for malicious code or viruses.

12.3 Penetration Testing

Penetration testing is an important method of evaluating your company's security systems. During a penetration test, cyber-security experts will apply the same tactics used by cyber attackers to look for potential flaws and vulnerabilities. A pen test seeks to simulate the kind of attacks that a company can encounter from criminal hackers.

12.4 Antivirus Software

Companies supply antivirus software as a security solution to ensure cyber-security. It's an application that runs on a variety of digital devices and looks for files that could harm your device. It can infect legal software on your computer and start spamming malicious advertisements or discreetly monitor your activities for sensitive information in many circumstances.

Some Tips to Forestall Cyber Attacks

Here are some basic tips to secure data from digital attacks.

i. Keep your operating system and system software up to date. Often, we ignore software updates, and this mistake opens the door for hackers to steal sensitive data-that's the reason we should keep our systems up to date.

ii. Always make strong password and avoid using personal information while making password.

iii. Try not to tap on links and attachments in emails from obscure senders or new sites. This is a typical way that malware is spread.

iv. Don’t use unsecure network. An unsecured network is one you can access without a secret key. Public network presented in places like bistros are regularly open. Although these give free remote Internet access, utilizing public Internet accompanies risks. Unsecured networks leave you vulnerable to man-in-the-middle attacks.

13. Discussion and Conclusion

Cyber security is a tremendous theme that is turning out to be more significant in light of the fact that the world is turning out to be exceptionally interconnected, with networks being utilized to do basic transactions. With each New Year that passes, cybercrime continues to divide into many forms, as does data security. Organizations are being challenged not just by how they safeguard their infrastructure, but also by how they require new platforms and intelligence to do so, as a result of the latest and disruptive technologies, as well as the new cyber tools and threats that emerge every day. There is no ideal answer for cybercrimes; however, we should attempt our level best to limit them to have a free from any danger future on the internet.

Acknowledgement

I have taken a lot of efforts in completion of this project report. It would have been impossible without the kind and generous support of some individuals and organizations. First of all, I would like to thank the organization, Amity University, Lucknow, Uttar Pradesh, for providing such a platform to complete this project. I would then like to express my sincere gratitude towards my NTCC Faculty Guide, Dr Pawan Singh, for providing all the necessary information and constantly guiding me till the commencement of my report. I would also like to thank my colleague for helping me and people who have willingly helped me out with their abilities.

Reference

[1] P. P. Ofori, E. A. Antwi, and A. Asante-Oduro, “The behavioral intention in accessing digital healthcare information on social media,” International Journal of Scientific Research in Science and Technology, pp. 510–521, 2021.

[2] V. Chhapre, K. Vartak, "Cyber Security: Issues, Challenges and Risks", VIVA-IJRI, Vol.1, no. 4, pp. 1-6, 2021.

[3] A. Bendovschi, “Cyber-Attacks – Trends, Patterns and Security Countermeasures,” *Procedia Economics and Finance*, pp. 24–31, 2015.

[4] K. Cabaj, Z. Kotulski, B. Księżopolski, and W. Mazurczyk, “Cybersecurity: trends, issues, and challenges,” EURASIP j. inf. secur., vol. 2018, no. 1, 2018.

[5] D. Y. Bhosale, “a study of cyber security challenges and its emerging Trends on latest technologies”, International Research Journal of Engineering and Technology, vol. 08, no. 05, pp. 2889- 2893, 2021.

[6] M. L. Gross, D. Canetti, and D. R. Vashdi, “Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes,” *Journal of Cybersecurity*, vol. 3, no. 1, pp. 49–58, 2017.

[7] J. Hua and S. Bapna, “The economic impact of cyber terrorism,” *The Journal of Strategic Information Systems*, vol. 22, no. 2, pp. 175–186, 2013.

[8] S. Kumar and V. Somani, “Social Media Security Risks, Cyber Threats and Risks Prevention and Mitigation Techniques,” *International Journal of Advance Research in Computer Science and Management*, vol. 4, no. 4, pp. 125–129, 2018.

[9] K. O. Samuel and W. R. Osman, “Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea,” *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 5, pp. 1082–1090, 2014.

[10] R. Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society,” *International Journal of Scientific & Engineering Research*, vol. 3, no. 6, pp. 1-4, 2012.

[11] M. Sreenu and D. V. Krishna, “A General Study on Cyber-Attacks on Social Networks,” *IOSR Journal of Computer Engineering (IOSR-JCE*, vol. 19, no. 5, pp. 01–04, 2017.

[12] D. Sutton, *Cyber Security: A Practitioner’s Guide*. Swindon, UK: BCS, the Chartered Institute for IT, 2017.

[13] O. Almutairi and N. Thomas, “Performance modelling of the impact of cyber- attacks on a web-based sales sytem,” *Electron. Notes Theor. Comput. Sci.*, vol. 353, pp. 5–20, 2020.