Volume 3, Issue , 2024
PP 423-430

International Journal of Futuristic Innovation in Arts, Humanities and Management (IJFIAHM)

# CYBER SECURITY AND THREATS

1st **Mr. Saurabh Bobade**
22saurabhbobade22@gmail.com
Student
Dept. of CSE
Shri Sai College of Engineering and Technology
Chandrapur, India

2nd **Mr. Lowlesh Yadav**
Lowlesh.yadav@gmail.com
Assistant Professor
Dept. of CSE
Shri Sai College of Engineering and Technology
Chandrapur, India

3rd **Mr. Neehal Jiwane**
neehaljiwane@gmail.com
Assistant Professor
Dept. of CSE
Shri Sai College of Engineering and Technology
Chandrapur, India

## ABSTRACT

The rapid developments of technology have provided huge areas of new opportunity and potential sources of efficiency for organizations of all sizes, these new technologies have also brought unprecedented threats with them. However, multimedia editing tools can be used to efficiently and seamlessly alter the content of digital data, thus compromising the credibility of information. Cyber security defined as the protection of systems, networks and data in cyberspace to preserve the original data and to remove all doubt about genuineness. In business this is a critical and challenging issue in the cyber world. Cyber security will only become more important as more devices the internet of things become connected to the internet. This paper focus on types of cyber security, types of vulnerabilities and cyber threats techniques, techniques to avoid threats. Finally ends up with advantages of cyber world.

**Keywords:** cyber security, cyber threats, data mining, cybercrime, cyber terrorism.

## INTRODUCTION:

Today's era the government and organizations are having more vulnerable on security of their data over network and computers. Cyber security is the process to protect the information and system from unauthorized access. This is become more vulnerable because of cyber-attacks and threats. Cyber threats refer to the person who encroaching unapproved access using various techniques to a control network and system. The evidences show that the magnitude of threats are increasing beyond from our expectations. Weblogs and mobile apps like WhatApp, hike, messengers are rapidly gained to attack our information infrastructure.

Cyber threats can be disaggregated, based on the criminals and their aims into four baskets, cyber terrorism, and cybercrime, cyber espionage cyber warfare. In cyberspace there are numerous vulnerabilities are used by cyber attackers to commit these acts. They exploit the weaknesses in hardware and software design through the use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defence of protected computer systems and interfering with their functioning. Identity theft is also common. The nature with every passing day. New method of attack are launching continuous.

## CYBER SECURITY

There are three core principles of cyber security. It involves Integrity, Confidentiality and Availability. Integrity means information unaltered from its original state withoutauthorization. Informationnot to be shared with inappropriate users. Availability refers to system and information available and accessible to who need it essentially.

### a) Types of Cyber Security

1. Physical Computer Security

It is the easiest and most basic type of computer security. In this anyone who has physical access to the computer controls it. Hidden files, Passwords and other protections not to save out a determined attacker seriously by computer hosting companies. They are hire guards, use secure doors, and even put computers on military bases or deserted islands just to keep them safe. But the average people can't protect their private files on office computers and other places. Either the computer repair technician not aware about the important files.

2. Network Security

It is a branch of computer security specifically related to the Internet. The goal of network security is measures and establish rules to protect against attacks over the Internet and internet accessible resources. It is controlled by the network administrator. It is useful for private and public. It includes wired and wireless networks of Network Protocols, IP security, Email security, Web security, Intruders, Viruses and Firewalls. In firewall is a critical part of computer security. The main functionality of firewall is blocking unapproved

network access attempts from computer. Home computers can be easily protecting by firewalls.

**b) Cyber Security Standards**

When identifying the most useful best-practice standards and guidance for implementing effective cyber security, it is important to establish the role that each fulfils, its scope and how it interacts with other standards and guidance.

## CYBER THREATS

Cyber threats mean the possibility of a malicious attempt to disrupt or damage a system or a computer networks . The goal of attacks is depending on the requirements of cyber criminals. The attacks are affected many important areas like military, financial institutions, governments, corporations, business and hospitals to collect, store and process a sensitive information of computers and sharing the data to other computers through networks.

**a) Types of Cyber Threats and Techniques**

Information and Data security is of high concern for almost all organization. The attackers are creating a new technique to detect the patterns, signature and information in the cyber space. Here we are explaining some of the threats and techniques for cyber land.

1. Trojan Horses – Trojan Horses are a harmful codes or a malicious program are hidden behind genuine programs which can cause damage to the system or allow complete access to the system for data corruption and stolen the data, log your key strokes and watch through webcam. It is not easily detectable and acts as a backdoor.
2. Rootkits –ARootkit is a malicious software developed to hides certain programs or a process to a privilege to access a system and from regular anti-virus scan detection. Whenever booting a system that software which runs and gets activated each time and are difficult to install and detect various process and files in the system.
3. Spyware – Spyware refers to a hidden component of a freeware program which naturally gather and spy information from the system without the knowledge of users through an internet connection.Suchspyware inundates with uncontrollable pop-up ads.

4. Scareware – Scareware is a type of threat whichacts as an honest system message and guides to purchase and download potentially dangerous and useless. But actually they are harmful and take control of all software's running on certain computers control of all the software's running on certain computers.
5. Spoofing – It is a cyber-attack where a program or a person impersonate another by creating false data in order to gain illegal access to a system. This type of threats is generally found in emailswhere the sender's address is spoofed.
6. Malware – Malware is a malicious software that are designed to do unwanted actions into the system or to damage the system. Malware is of many types like Trojans, viruses, etc., which can behalf and Take control of your computer and all the software running on it.
7. Adware – Adware is a software will collect allyour data without our consent. That would come in the form of installed automatically or a free download and send your passwords, usernames, surfing habits, settings, downloaded applications to third parties. Take you to unwanted sites or inundate you with uncontrollable pop-up ads. These are difficult to remove and can infect your computer with viruses.

**b) Techniques to Avoid Cyber Threats**

The innovation of technology tosses up new online risks. To identify and eradicate the security holes from system that makes vulnerable to cyber threats. There are some of the steps to help our systems and information's.

1. Properly configure and patch operating systems, browsers, and other software programs.
2. Use and regularly update firewalls, anti-virus, and anti-spyware programs.
3. Use strong passwords (combination of upper and lower case letters, numbers and special characters) and do not share passwords.
4. Be cautious about all communications; think before you click. Use common sense when communicating with users you do and do not know
5. Do not open e-mail or related attachments from un-trusted sources and don't access questionable web locations

**METHODOLOGY:**

Today's era the government and organizations arehaving more vulnerable on securityof their data over network and computers. Reconnaissance refers to gathering information about the target for the ex-Domain name, IP, Target personal information, Email, Sub-domains, Job information, etc. Reconnaissance is also known as Foot-Printing. We have many tools to gather information about target tools are Net craft , who is, HTT track-used to mirror the website, Firebug-data extractor, Recognizing-recon-naissance of the network, sublist3r-for sub-domains, etc. Scanning refers to identifying hosts, IP addresses, running service in the target system, open ports, and services in the target network. Usually in this phase, hacker tries to prepare a blueprint of the target. we have so many tools to know about the target tools are- N map-complete network scanner this is one of my favorite Network scanning tool, Angry IP scanner-pings each IP address and resolves and port, Hping3/2-used for packet crafting for TCP/IP, Net scan pro-it helps to troubleshoot the network, ID serve-for Banner grabbing/OS Fingerprinting, Nessus /Open VAS/Q-for vulnerability scanning .

There are some security measures, and these will give you a basic level security against the most common IT risks, by Use strong passwords, Control access, put up a firewall, use security software, Update programs and systems regularly, Monitor for intrusion. Strong passwords are vital to good online security. Make your password difficult to guess. Make sure that individuals can only access data and services for which they are authorized. Firewalls are effectively gatekeepers between your computer and the internet, and one of the major barriers to prevent the spread of cyber threats such as viruses and malware. You should use security software, such as anti-spyware, anti-malware, and anti-virus programs, to help detect and remove malicious code if it slips into your network. Updates contain vital security upgrades that help protect against known bugs and vulnerabilities. You can use intrusion detectors to monitor system and unusual network activity.

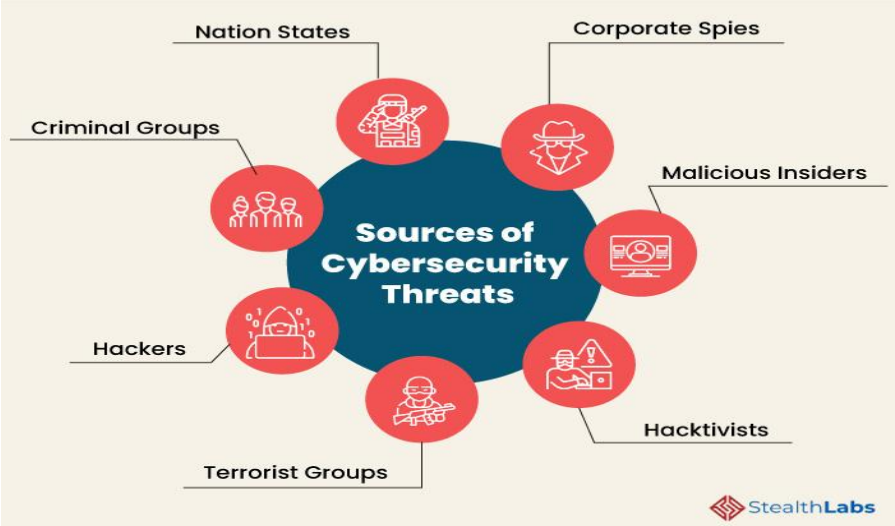


Figure 1: Cybersecurity Threats

**Here are some of the common sources of cyber threats:**

1. **Nation States**

Cyber attacks by a nation can inflict detrimental impact by disrupting communications, military activities, and everyday life.

2. **Criminal Groups**

Criminal groups aim to infiltrate systems or networks for financial gain. These groups use phishing, spam, spyware, and malware to conduct identity theft, online fraud, and system extortion.

3. **Hackers**

Hackers explore various cyber techniques to breach defenses and exploit vulnerabilities in a computer system or network. They are motivated by personal gain, revenge, stalking, financial gain, and political activism. Hackers develop new types of threats for the thrill of challenge or bragging rights in the hacker community.

4. **Terrorist Groups**

Terrorists conduct cyber attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties.

**5. Hacktivists**

Hacktivists carry out cyberattacks in support of political causes rather than for financial gain. They target industries, organizations, or individuals who don't align with their political ideas and agenda.

**6. Malicious Insiders**

97% of surveyed IT leaders expressed concerns about insider threats in cyber security. Insiders can include employees, third-party vendors, contractors, or other business associates who have legitimate access to enterprise assets but misuse that accesses to steal or destroy information for financial or personal gain.

**7. Corporate Spies**

Corporate spies conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

## CONCLUSION

In the event of a cyber security incident, such as an attack, studies show that the greatest defense is a PC-savvy customer .

To consider is by far the most vulnerable, who are identified in this investigation as new employees inside an organization, as specifically, with the adversary seeking for personally identifiable information from people involved. Mental issues that con-tribute to customer and organization vulnerability are also addressed in this investigation. This study finds that cyber security threats and approaches have a role to play in reducing the impact of digital attacks, risk, and vulnerability, while creativity has a role to play in reducing the influence of digital attacks, threat, and lack of strength. Cyber-attacks can be mitigated, but there does not appear to be an absolute solution for overcoming such network security threats at this time. Later, when the company implements the system security design, the operation of the cyberattack, threat, and vulnerability decreases.

**REFERENCES**

[ 1 ] H. Suryotrisongko and Y. Musashi, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspec-tive,"2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), Kaohsiung, Taiwan, 2019, pp. 162-167, doi: 10.1109/SOCA.2019.00031.

[2] Y. Liu, H. Qin, Z. Chen, C. Shi, R. Zhang and W. Chen, "Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant,"2019 IEEE International Conference on Energy Internet (ICEI), Nanjing, China, 2019, pp. 25-30, doi: 10.1109/ICEI.2019.00011

[3] F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, "Information Security:A Review of Information Security Issues and Tech-niques,"2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769504.

[4] Lowlesh Nandkishor Yadav, “Predictive Acknowledgement using TRE System to reduce cost and Bandwidth” IJRECE VOL. 7 ISSUE 1 ( JANUARY-MARCH 2019) pg no 275-278

[5] C. Ten, G. Manimaran and C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010, doi: 10.1109/TSMCA.2010.2048028.