Cyber Security Services - Cyber Security Framework

Alok Tuli , Assistant Professor
SRPA Adarsh Bhartiya College Pathankot

Abstract

Cyber security protects computers, devices, systems, and networks against digital dangers by constructing many levels of security and protection. Information security is a subset of which cyber security is a considerably broader discipline. In the event of a cyberattack, whether successful or not, companies usually have a system and a structure in place to deal with the situation acceptably. In the event of a successful attack, a reliable framework can help with threat detection and identification, network and system defense, and data restoration. Cybersecurity is an increasingly pressing issue as more and more of our daily conveniences are realized via networks of linked devices and systems. The Internet of Things (IoT) is changing how the world works, making deploying cybersecurity in all vulnerable systems more critical than ever. This is essential to forestall cyberstalking, attempts at extortion, identity theft, the loss of important data, and the inappropriate use of sensitive information, among other behaviors of a similar kind. Not only do vital infrastructures such as hospitals, financial service organizations, power plants, and other such establishments have private information about their clients, but they also have private information about themselves. In light of this fact, significant consideration must be given to deploying cybersecurity measures to ensure that our society continues functioning normally.

Keywords:*Security,Protection, Mobile Security, Network Security, Cloud Security*

Introduction

Cyber-security practices focus on protecting computers and other electronic devices against purposeful and inadvertent forms of malware (including viruses, trojans, and bugs). The scale and severity of cyber threats are rapidly growing in every region of the globe. Due to the political and economic value of having access to vast volumes of data, there are persistent attempts to breach data and sensitive, private, or classified information. Robust cyber security measures are, thus, essential. You'll find people from all walks of life and income levels in India. Due to their affordability, a wide range of electronic devices are in use, from high-end, password-protected electronics to low-end mobile phones. This makes it harder for authorities to establish uniform regulations and technical standards for protecting personal information. The average person also needs to understand computers and the web better. Young people under 25 comprise a significant share of Internet and online service users in today's globally linked world. Around one-third of all internet users are children and teenagers under eighteen. Among young people, Internet usage is closely related to searching for educational information and material, developing digital skills for expanding opportunities, and maintaining online/digital personae and networks of social connections. Unfortunately, along with this wealth of information, there is also a rise in the number of risks and unsuitable materials children encounter while using the internet. Immature and rapidly developing cognitive and emotional capabilities make children and teens particularly vulnerable to cyber-predators and -perpetrators.

Every company's assets are the product of the coordination of many different systems. It will need a deliberate effort on everyone's part to ensure the security of these systems. Therefore, we may classify cyber security as one of the following:

- **Network Security:**It requires guarding data while it is stored and when it is being transferred.
- **Application Security:**Securing the hardware and software against malicious attacks. The programs may be kept safe from malicious use by regularly receiving security patches. Before a piece of software or hardware is released into the wild, security measures such as source code authoring, validation, threat modeling, etc. must be implemented.
- **Information or Data Security:**Protecting information while it is in transit or stored requires a reliable data storage technique.
- **Identity management:**Data asset management analyses and decides how to treat and protect data.
- **Operational Security:**Handling and protecting digital assets requires processing and decision-making.
- **Mobile Security:**Mobile device security protects sensitive business and personal information held on smartphones, tablets, and other portable electronic devices from cybercriminal.. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:**Information in the company's digital environment or infrastructures must be protected. It uses a plethora of cloud services, like AWS, Azure, Google, etc., to ward against various threats.
- **Disaster Recovery and Business Continuity Planning:**If malicious activity is causing a loss of operations or data, it discusses the procedures, monitoring, alarms, and strategies that will be put into place to cope with the situation. After a catastrophe, operations must be restored to pre-disaster levels under company policy.
- **User Education:**It addresses the procedures, monitoring, alarms, and contingency plans put in place by an organization to cope with the loss of operations or data due to hostile behavior. Its regulations require that any interrupted operations be restored to pre-disaster levels immediately.

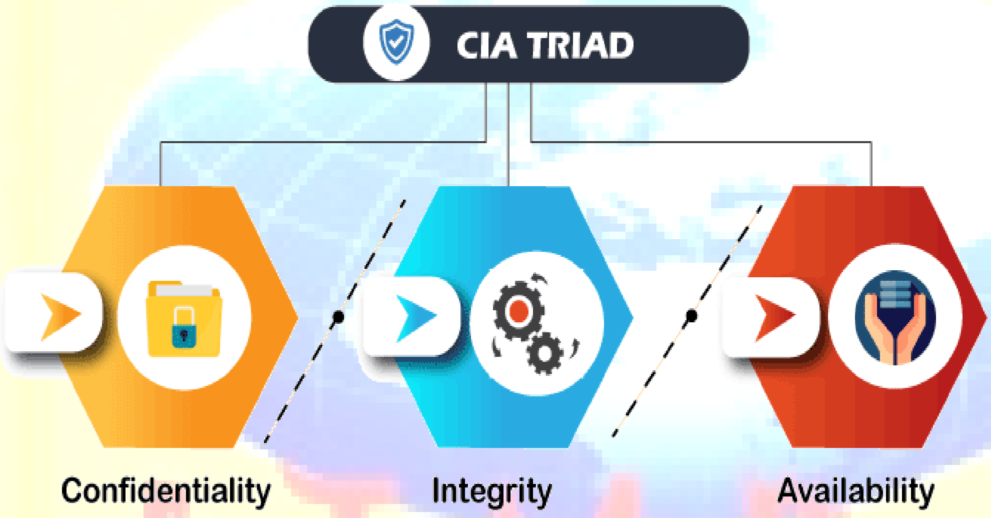
Importance of Cyber Security

The internet, computers, and other electronic devices and software are increasingly fundamental to all facets of contemporary life. All financial, healthcare, monetary, governmental, and industrial infrastructure relies heavily on Internet-connected gadgets. Information that slipped into the wrong hands might gravely damage them, including their intellectual property, financial information, and personal data. This creates an opportunity for spies and other threat actors to gain in and conduct crimes such as vandalism, theft, espionage, etc.

The worldwide rise in hacking and other forms of cybercrime is a serious danger to economic stability. Therefore, it is essential to have a robust cybersecurity strategy in place to prevent widely publicized data breaches. The need to implementrobust cybersecurity rules and practices to protect sensitive commercial and personal data is growing as the frequency of cyberattacks rises.

Cyber Security Goals

Protecting private data is the top priority in the realm of cyber security. The security industry has developed a triangle of three related concepts to protect data from attackers. The CIA's dynamic trio elaborates on this idea. The CIA model may be used to guide a company's approach to data protection. Every time a security hole is found, it indicates violating one or more of these guidelines.The CIA paradigm has three distinct components: privacy/security, trustworthiness, and accessibility. It’s a security approach that facilitates introspection throughout information technology protection. Let's break this out, section by component..



Confidentiality

Confidentiality refers to the state of having information shielded from public view. It requires restricting access to the data to thoseauthorized to use it. It ensures that no unintended parties may access sensitive information. Encryption is a method used to safeguard sensitive data.

Integrity

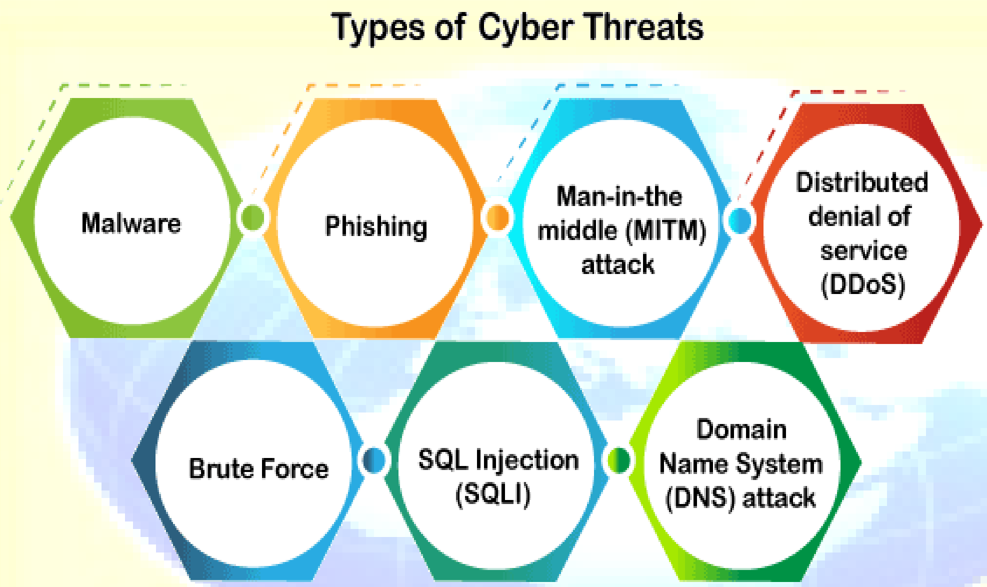
By adhering to this concept, data will always be accessible to the appropriate parties. It ensures that neither a malfunctioning system nor a cyberattack impedes such access.Information can always be accessible and valuable to authorized people thanks to this principle. This prevents any disruption to these connections due to bugs in the system or malicious hacking attempts.

Availability

This method guarantees that users can always get to the information they need. It ensures that issues like system crashes or hacking do not hinder these sorts of access.

Types of Cyber Security Threats

Cybersecurity threats include those that destroy or steal data, gain access to networks, or impair digital life. The cyber community has recently identified the following threats:


Types of Cyber Threats
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

Malware

It's harmful software that can go from one gadget to another. It may remove infections, spread over a whole system, and compromise security.

- **Virus**: It's harmful software designed to infect other computers. Infects files, steal information or corrupts devices as it moves across a network.
- **Spyware**: It's a program that covertly logs everything you do on your computer. Hackers may use spyware for fraudulent purposes such as online purchases, cash withdrawals, etc.
- **Trojans**: It's a kind of malicious software that masquerades as a safe file or program so that it may be downloaded and executed. Its primary goal is to cause damage to our device or network by corrupting or stealing data.
- **Ransomware**: It's a program that locks down a user's device by encrypting all of the user's files and data so they can't be accessed or deleted. Then the bad guys want money in exchange for decryption.
- **Worms**: This program replicates itself and then spreads to other computers without any help from a human. They need not infiltrate any particular software to steal or corrupt the information.

- **Adware**: It's malicious advertising software designed to infect our device with ads. Without the user's knowledge or consent, it installs potentially unwanted software on their computer. The primary goal of this application is to display advertisements inside the user's browser to earn money for the program's creator.
- **Botnets**: A network of infected computers and other devices remotely controlled through the internet. It's a backdoor that hackers may employ to steal sensitive information and impersonate users.

Phishing

Phishing occurs when hackers pose as legitimate businesses or individuals to trick their targets into handing over sensitive information through email. They contact their prospective victim(s) by email, phone, or text message and include a link in the message in the hopes that the recipient(s) would click on the news. Users who click this link will be sent to malicious websites that steal personal data, financial data, social security numbers, and other sensitive information. If the victim clicks the link, malware will be installed on their device, giving the attackers remote access.

Man-in-the-middle (MITM) attack

A man-in-the-middle attack is a method used by cybercriminals to eavesdrop on a conversation or spy on a data transfer between two targets. A cybercriminal might inject oneself into a conversation and pose as either participant to get access to private information or influence the other's reaction. The targets of such attacks are often companies' or their customers' confidential information. For instance, in the case of an unsecured Wi-Fi network, a hacker may capture data as it travels from the target device to the network.

Distributed denial of service (DDoS)

A denial-of-service attack (DoS) is a kind of cyber threat or malicious attempt in which the attacker floods the target with Internet traffic to disrupt the regular operation of the target's servers, services, or network. Here, requests originate from several IP addresses, which might render the system inoperable, slow down or even knock down a company's servers, or prohibit it from performing its essential responsibilities.

Brute Force

An example of a cryptographic assault is the brute force attack, in which the hacker repeatedly attempts every possible input combination until success is obtained. Cybercriminals often use this attack to get private information, including login credentials, encryption keys, and social security numbers (PINS).

SQL Injection (SQLI)

Injection of malicious SQL scripts into a database's backend is a frequent sort of attack known as SQL injection. Following a successful attack, the hostile actor may access, modify, or destroy any SQL database-stored sensitive corporate data, user lists, or private customer information.

Domain Name System (DNS) attack

Domain Name System (DNS) attacks occur when cybercriminals use weaknesses in the system to hijack users' browsers and steal sensitive data (DNS hijacking). This is a huge cybersecurity issue since the DNS system is essential to the internet's underlying architecture.

Latest Cyber Threats

The governments of the United Kingdom, the United States, and Australia have recently reported the following cyber threats:

Romance Scams

The U.S. government first learned about this cyber threat in February 2013. Cybercriminals took advantage of this vulnerability by using it in online dating, chat rooms, and mobile apps. To collect personal information, they prey on lonely people on dating websites.

Dridex Malware

A new strain of financial Trojan malware was discovered in the United States in December 2014, posing a danger to businesses, governments, and individuals worldwide. It spreads to PCs by phishing emails or previous malware and takes sensitive data to perform financial and identity theft. The National Cyber Security Centre of the United Kingdom suggests that people protect their information by permanentlyinstalling the most recent updates, having the most recent anti-virus software, and performing frequent data backups.

Emotet Malware

Emotet is a cyberattack that steals personal information and infects our device with other malicious software. In 2014, the Australian Cyber Security Centre highlighted this worldwide cyber danger.

The following are examples of systems that are vulnerable to assaults and security breaches:

- **Communication**: Phone calls, emails, texts, and messaging applications may all be used in cyberattacks..
- **Finance**: The security of sensitive financial data like bank and credit card information is addressed by this method. Cybercriminals naturally focus on this data first and foremost.

- **Governments**: When cybercriminals want to steal sensitive public data or private citizen information, they often go after government entities.
- **Transportation**: Connected vehicles, traffic management systems, and intelligent roadways are common targets for hackers in this system.
- **Healthcare**: A hacker aims to breach the healthcare system and get access to sensitive data housed at a regional clinic through national hospital IT networks.
- **Education**: Cybercriminals often target universities to steal sensitive student and faculty data used in research.

Cyber Safety

Let's go through some strategies for keeping oneself safe in a cyberattack. The following is a list of classic pieces of advice on online safety:

- **Conduct cybersecurity training and awareness:**For the policy to be successful, each employee will need to get training on cybersecurity, the regulations of the organization, and how to report incidents.Even the most cutting-edge technology safeguards risk failing due to human error or malicious intent, which might result in a devastating security breach. The frequency of security breaches may be reduced by educating employees on the importance of security via seminars, workshops, and online courses.
- **Update software and operating system**: The most common protection method is installing the most recent updates to the operating system and apps.
- **Use anti-virus software:**Anti-virus software that can identify and eliminate potential security risks is also recommended. This program's latest and greatest version is always used to ensure maximum security.
- **Perform periodic security reviews:**Additionally, it is recommended that you avoid using unsecured networks since they might make you susceptible to man-in-the-middle assaults.
- **Use strong passwords**: Users should be warned that man-in-the-middle attacks are possible on unsecured networks.
- **Do not open email attachments from unknown senders**: When receiving an email attachment from an unknown sender or on a website that is new to you, the cybersecurity expert will always advise against opening or clicking on the file since it may contain malware.
- **Avoid using unsecured Wi-Fi networks in public places**: Man-in-the-middle attacks may happen on unsecured networks. Thus, it's best to avoid them.
- **Backup data:**In a security breach, backups of all critical information must be kept. Data integrity with backups may be protected from threats like SQL injections, phishing, and ransomware.

Conclusion

You may feel comfortable relying only on password protection for your sensitive information. Even if strong passwords are required, hackers may eventually find a way to crack them. Effective cybersecurity measures, a tiered defense, are so essential. To remove the data from the computer: When you delete a file, it goes to the computer's Recycle Bin until you empty it. The information is stored on the hard disc in places like the temporary files folder, even after deletion.Services that provide encryption are unnecessary: Some businesses thinkinvesting in encryption software is unnecessary. It is mistakenly believed that using encryption would prevent data breaches. When protecting against fraudsters and ransomware attacks, encryption is crucial. Medium and small businesses are not the focus: It's a myth that only giant corporations are at risk or that hackers only bother with giant corporations. Since these businesses use less stringent security measures, this highlights the need to protect businesses against cyberattacks.

References

Branch, J. (2004). "What's in a Name? Metaphors and Cybersecurity". International Organization. Volume 75, Issue 1.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government, and Finance Division. Washington DC: The Library of Congress.

Costigan, Sean; Hennessy, Michael (2014). Cybersecurity: A Generic Reference Curriculum(PDF). *NATO.* ISBN 978-9284501960.

Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". ACM Transactions on Information and System Security. ***5*** *(4): 438–457.* doi*:*10.1145/581271.581274. S2CID 1500788

Kim, Peter (2014). The Hacker Playbook: Practical Guide To Penetration Testing. Seattle: CreateSpace Independent Publishing Platform. ISBN 978-1494932633.

Lee, Newton *(2012). Counterterrorism and Cybersecurity: Total Information Awareness (2nd ed.). Springer.* ISBN 978-3319172439.

Singer, P. W.; Friedman, Allan (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. ISBN 978-0199918119.

Wu, Chwan-Hwa (John); Irwin, J. David (2013). Introduction to Computer Networks and Cybersecurity. Boca Raton: CRC Press. ISBN 978-1466572133.