An Overview of Implementation Strategies on Cyber Security

Akshat Goel

School Of computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Akashay Kumar

School Of computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Akshay Nigam

School Of computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Abstract:

In modern society, cyber security has become increasingly critical due to the widespread use of technology and internet. This research paper consist of a comprehensive overview of current state of cyber security, highlighting the need for effective practices and regulations to prevent cyber-attacks in the future. A comprehensive analysis of cyber security, focusing on its importance, types of threats, practices and techniques, regulations and standards, challenges, and future directions will also be presented. Various types of cyber security threats, including malware, phishing, ransom ware, and more, are discussed in detail, explaining how each type of threat works and the potential harm they can cause. Common cyber security practices and techniques, such as firewalls, antivirus software, and encryption, are also presented, along with a discussion of their effectiveness in preventing cyber-attacks. The paper also covers regulatory frameworks and standards, like the General Data Protection Regulation (GDPR) and the ISO 27001, and their limitations and vulnerabilities. Furthermore, emerging cyber security challenges, such as the Internet of Things (IOT) and Artificial Intelligence (AI), are discussed, and the need for continuous monitoring and updates to cyber security practices and regulations is highlighted. Finally, the paper presents suggestions for future improvements and developments in the field of cyber security.

Introduction:

The Internet has become crucial to international communication and has permeated more and more aspects of people's daily life. It has built up a sizable global network that contributes billions of dollars every year to the world economy. The majority of international economic, commercial, cultural, social, and governmental exchanges currently take place online. A large worldwide network made possible by cyberspace has helped the world economy to grow by many billions of dollars each year. Governments now face new security concerns as a result of cyberspace's low barrier to entry, anonymity, lack of public transparency, unclear threat geography, and dramatic impact. This has resulted in both powerful and weak actors, such as governments, terrorist organisations, and even individuals, as well as threats like cyber warfare, cyber terrorism, and cyber espionage. Cyber risks are different from traditional national security concerns, which are more open and whose perpetrators are recognised governments and countries in a particular region. Analysts have been considering the potential effects of cyber-attacks, which can result in serious and occasionally widespread physical or economic damage, for more than ten years. It will be challenging for specialists to handle the complex and many dimensions and features of the issue and offer legal guidance and analysis, though, until governments come up with a precise definition of a cyber-attack that is accepted and favoured by the international community. What constitutes a cyber-attack, what are its features, and can just about any attack that occurs in cyberspace be considered one? The infrastructure of modern living that is rising the fastest is the internet. The face of humanity is evolving as a result of numerous new technologies in today's technological environment. However, because of these new technology, we are unable to effectively protect our private information, which is why cybercrime is on the rise right now.

Cybercrime:

Cybercrimes will rise in tandem with technological advancements as they are made. Criminal action that targets or makes use of a computer or networked device that are known as cybercrime. However, it can also be done to harm computers or networks for political or personal reasons. It is typically carried out by hackers who wish to earn money. It can be carried out by both people and groups, and some cybercriminals are well-organized, employ cutting-edge methods, and have sophisticated technical skills. Cybercrime is a criminal activity that primarily perpetrates and commits theft via computers. It encompasses computer-based versions of pre-existing crimes like identity theft, stalking, bullying, and terrorism as well as crimes made feasible by computers, such network intrusions and the spread of computer viruses. A computer and the internet are used in cybercrime to steal someone's identity, sell illegal goods, stalk people, and disrupt operations via malicious software.

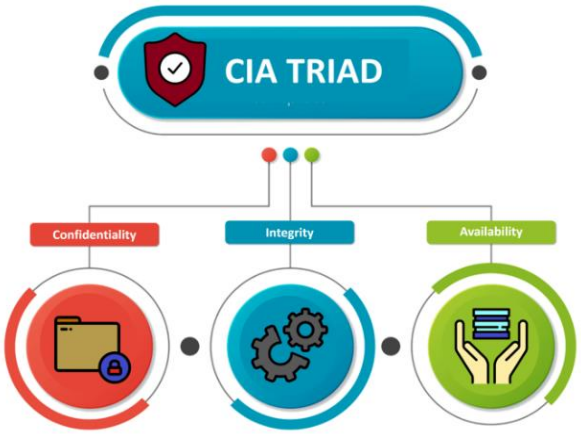
Classification of Cyber Crime:

1. Email and internet fraud.
2. Identity fraud
3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyber extortion
6. Cyber espionage
7. Interfering with systems in a way that compromises a network.
8. Infringing copyright.
9. Illegal gambling.
10. Selling illegal items online.

Cybercriminals who target your computer can infect your device with malware to damage it, stop it from working, or use malware to erase or steal your data. You can also ban users from using her website or network, or ban companies from providing software services. Using computers to commit other crimes Cybercrime may include using computers or networks to distribute malware, illegal information, or illegal images. Some jurisdictions recognize his third category of cybercrime. This is where computers are used as aids in crime, for example, computers are used to store stolen data.

Malware:

When a computer system or network is infected with malware, such as a computer virus, an attack takes place. Cybercriminals may use it to destroy your data, steal your sensitive information, or utilise your computer in other illegal ways. The WannaCry ransom ware outbreak is a well-known instance of malware, and it spread globally in May 2017. 230,000 systems in 150 countries were impacted by the WannaCry ransom ware assault, which targeted weaknesses in computers running Microsoft Windows. Users received messages requesting them to pay a bit coin ransom to regain access after being locked out of their data. An estimated $4 billion in economic losses have been attributed to the



WannaCry cyber-attack worldwide.

Phishing:

Sending phoney messages to people in an effort to get sensitive information, such as login credentials or credit card information, is known as phishing. Ransom ware is a type of malicious software that blocks access to files and computer systems until a ransom is paid. Social engineering is a tactic used by adversaries to compel you into disclosing private information. It is not guaranteed that your system will be returned to its initial form or that your records will be recovered if you pay the ransom.

Goals:

Cyber security is a practise with the goal of preventing intrusion, erasure, and unauthorised access to complicated data stored on the Internet and other devices. The main goal of cyber security is too avoid the sharing of the important details and credentials to the third person so that no one else can access to your personal details. The objective is to guarantee a good environment for safeguarding data, networks, and equipment from cyber terrorism. Estimating the cost of reconstruction and doing a risk assessment are both crucial for loss prevention.

Goals of Cyber Security:

There are three main goals of cyber security are there that are important for Cyber security. The objective of this cyber security is that the data should not be stolen.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only to approved users

A safety model used to direct internal corporate or societal data security policies is the CIA triad model. It

reflects the three most important safety mechanisms and is used to gauge risk and select the best safety measures. It is the most widely accepted practise to assess, choose, and implement the appropriate safety measures to reduce risk. Similar to how the AIC (Availability, Integrity, and Confidentiality) triad was substituted for this paradigm to avoid the Central Intelligence Agency error. The three most important critical mechanisms of safety are mirrored in the basic elements of the triad.

Confidentiality:

The capacity to keep information from being disclosed to unauthorised people, programmes, or processes is known as confidentiality. Because it necessitates having control over who has access to protected information, it relates to information security. It indicates that something is confidential and shouldn't be disclosed to unauthorised people or organisations. Confidential information may be revealed to the public or other people if confidentiality is compromised, which could result in loss of privacy. Numerous pieces of information, including sensitive ones like financial and medical data, could be deemed confidential. Certain information needs a higher level of confidentiality than other types because it is more sensitive.

Methods to Safeguard Confidentially:

1. Information encryption
2. Multi- or two-factor authentication
3. Validating biometrics

Integrity:

Information is protected from improper modification and destruction by integrity, which also ensures that changes to the data cannot be made covertly. To offer the strongest defence against online dangers and attacks, including cyber espionage, it is based on encryption and hashing. Data must be precise and trustworthy, and it cannot be switched in the programme from the fact to fact.

Integrity ensure methods:

1. No illegal access should be allowed to delete records, as this violates privacy.
2. Operators contact control.
3. Appropriate backups must be in place to return quickly.
4. Version supervisory must be present to monitor changes in the log.

Availability:

Regardless of the moment, place, or circumstance, availability guarantees prompt and dependable access to information.

Other elements. Operators must make sure that all available evidence is available before requesting a section of statistics because Denial of Service (DOS) attacks can prevent this. The ability to get the data may be hampered, for instance, if an attacker controls a website.

Trends Changing Cyber Security:

There are some of the trends that have their results on the cyber security.

Web Servers: There is still a risk of attack on web applications for data extraction and malicious code distribution. Cybercriminals spread malicious code through compromised legitimate web servers. But data theft attacks, many of which have received a lot of media attention, are also a big threat, so we need to focus more on protecting web servers and web applications. Web servers, in particular, are the platform

of choice for cybercriminals to steal data. Therefore, to avoid becoming a victim of these crimes, you should always use a safer browser, especially for important transactions.

Cloud Computing: This and Its Services at present, all small and medium enterprises and large enterprises are gradually adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend poses major challenges to cyber security as traffic can bypass traditional checkpoints. Additionally, as the number of applications available in the cloud increases, policy controls for web applications and cloud services must also evolve to prevent loss of valuable information. Cloud services have developed their own model, but many questions remain about their security. The cloud offers tremendous opportunities, but we must always keep in mind that as the cloud evolves, so do security concerns.

APTs and Targeted Attacks: APT are Advanced Persistent Threats (APTs) are an entirely new breed of cybercriminal ware. Over the years, network security features such as web filtering and IPS have played an important role in detecting such targeted attacks, usually after the initial compromise. As attackers become more daring and use more obscure techniques, network security must integrate with other security services to detect attacks. Therefore, security techniques need to be improved to prevent further threats from emerging in the future.

Cellular Networks: Today we can connect with anyone anywhere in the world. However, security is a very big concern for these cellular networks. Today, as people use devices like tablets, phones, and PCs, firewalls and other security measures are becoming more prevalent, requiring additional protection beyond what exists in the applications we use. We should always think about these mobile network security issues. Additionally, mobile phone networks are highly vulnerable to this cybercrime, so you should be very careful when it comes to security issues.

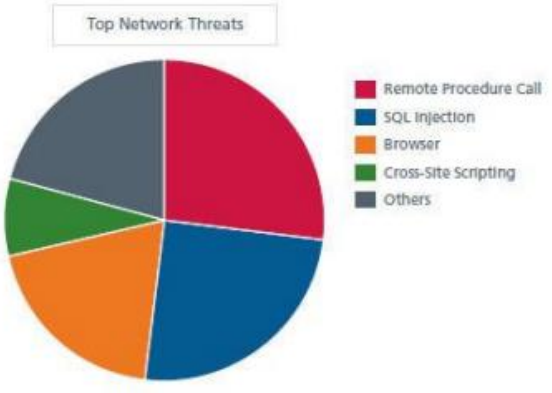


Fig -1

The above pie chart shows about the major threats for networks and cyber security.

Cyber Ethics:

Cyber ethics is the computer technology which is used to define the practices that are used by user and when using the computer system. It is the ethics and etiquette that are followed when using a computer system. It mainly aims on the moral, social behaviour and financial behaviour and used to protect them. This empathizes the behaviour that must be adopted when the cyber technology is using.

Cyber bullying:

Cyberbullying is a form of bullying carried out via internet technology such as social media, where individuals are mocked on their physical appearance, lifestyle, preferences, etc. It affects the emotional ethics of individuals and can cause mental disturbance. Teenagers are the major victims.

Hacking:

The leaking of data is a risky thing that involves the passing of the secret information like password and other important items for which the third person can access to your personal accounts. It is not considered a good practice.

Copy writing:

The practise of producing text for marketing or other types of advertising is known as copywriting. The written material, often known as copy or sales copy, tries to raise brand recognition and eventually persuade an individual or group to perform a certain action.

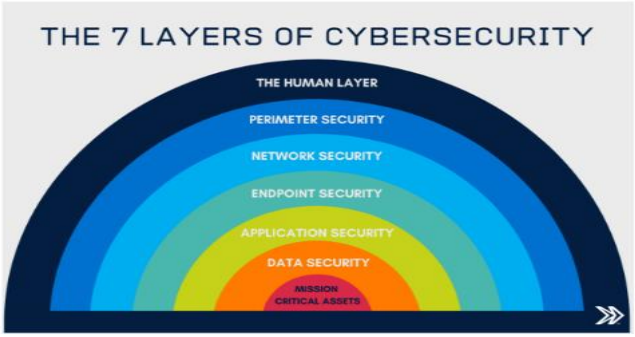
Layers of Cyber Security:

The mission-critical assets you are trying to protect should be the focal point of the seven levels of cyber security.

The information we need for the safeguard are the Mission Critical assets.

1. **Data Security** - It measures guard against unauthorised access to and storage of data.
2. **Application Security** - Applications security controls safeguard the internal security of an application as well as the application's ability to access your mission-critical assets.
3. **Endpoint Security** – The end point security used to measure the network connection between the two and more devices.
4. **Network Security** - The network security is the safe guard that a company used for the company's network so that no one can access to the authorization.
5. **Perimeter Security** - The physical and digital security approaches that safeguard the entire company are included in perimeter security controls.

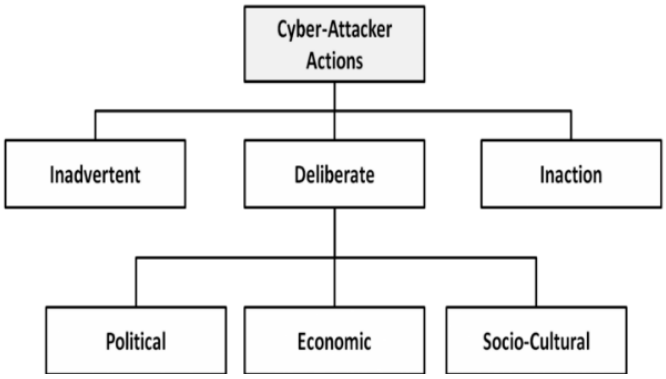
6. **The Human Layer** - In any cyber security system, people are the weakest link.



Motive of Attackers:

There are three types of cyber attackers: Without intending to cause harm, accidental acts are made, purposeful actions are taken with malevolent intent, and inactivity is the inability to act because one lacks the necessary abilities, information, direction, or access to the right people. Deliberate acts, for which there are three types of motivation, are of main interest.

1. **Political motivations:**
   These include making political declarations, or ganising protests, or taking punitive action. Ot her examples include damaging, interrupting, or seizing control of objectives.
2. **Economic motivations:**
   These attackers include the stealing of the money related and other economically things from the user. These include the frauds, and blackmails.
3. **Socio-cultural motivations:**
   These can include philosophical, theological, political, and humanitarian motives for an attack. Other socio-cultural drivers include enjoyment, curiosity, a desire for attention, or ego-gratification.



Conclusion:

The upcoming cyber security is a difficult concept to define in the words of digital skills and potentials because the cyber security will not be limited in upcoming days. Cyber security is difficult to define as digital skills interact with humanoid across all features of policies, society, and the family and outside. Cyber security has took a rapid boom after 2010 as the market was in a great need of cyber security. All the sectors are developing online so they all are in a great need of security for their servers and portals. We conclude that cyber security is going to be the "master problem" of the internet era and it will lead to major variation of mechanism of humanoid and digital machineries. We have left influences to military "cyber war" to the cross, which was a demonstrating select made to bind the difficulties. In future cyber wars and cyber battles will take place, so we need to strength our hands in the field of cyber security. It's necessary to focus on security of our severs and confidential details.