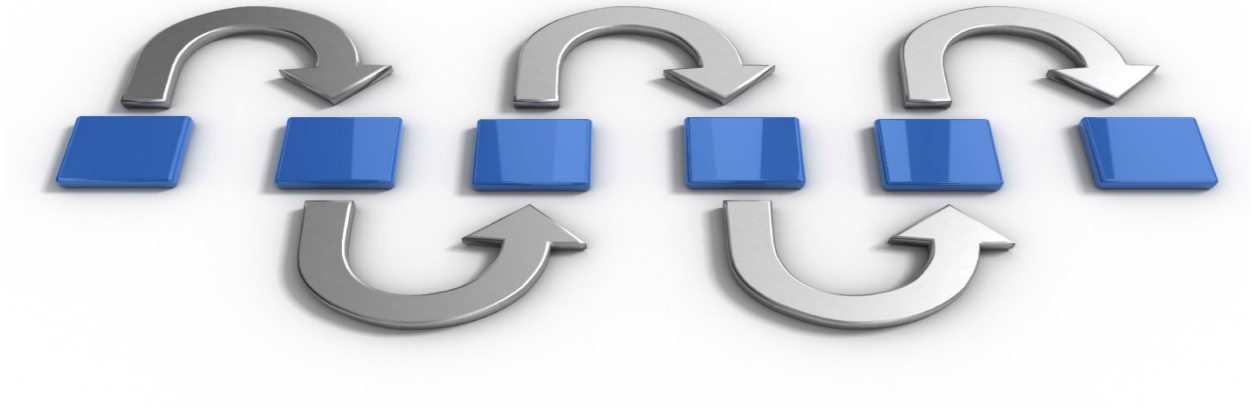
What is Security?

Security according to a child of 10 years old

Security According to Junior High School ICT teacher

Security is a process, not an end state.

Security is the process of maintaining an acceptable level of perceived risk.



No organization can be considered "secure" for any time beyond the last verification of adherence to its security policy.
If your manager asks, "Are we secure?"
you should answer, "Let me check."
If he or she asks, "Will we be secure tomorrow?
" you should answer, "I don't know."
Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

Meaning of the Word CYBER

It is a combining form relating to information technology, the Internet, and virtual reality.

Cybersecurity Fundamentals – Introduction to Cybersecurity

Adoption of Internet by businesses and enterprises has made mobile-banking, online shopping, and social networking possible. Whilst it has opened up a lot of opportunities for us, its not altogether a safe place because its anonymity also harbors cybercriminals.

What is cybersecurity?

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. It may also be referred to as **information technology security**.

The term cybersecurity refers to techniques and practices designed

to protect digital data. The data that is stored, transmitted or used on an information system. After all, that is what criminal wants, *data*. The network, servers, computers are just mechanisms to get to the data. Effective cybersecurity reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies.

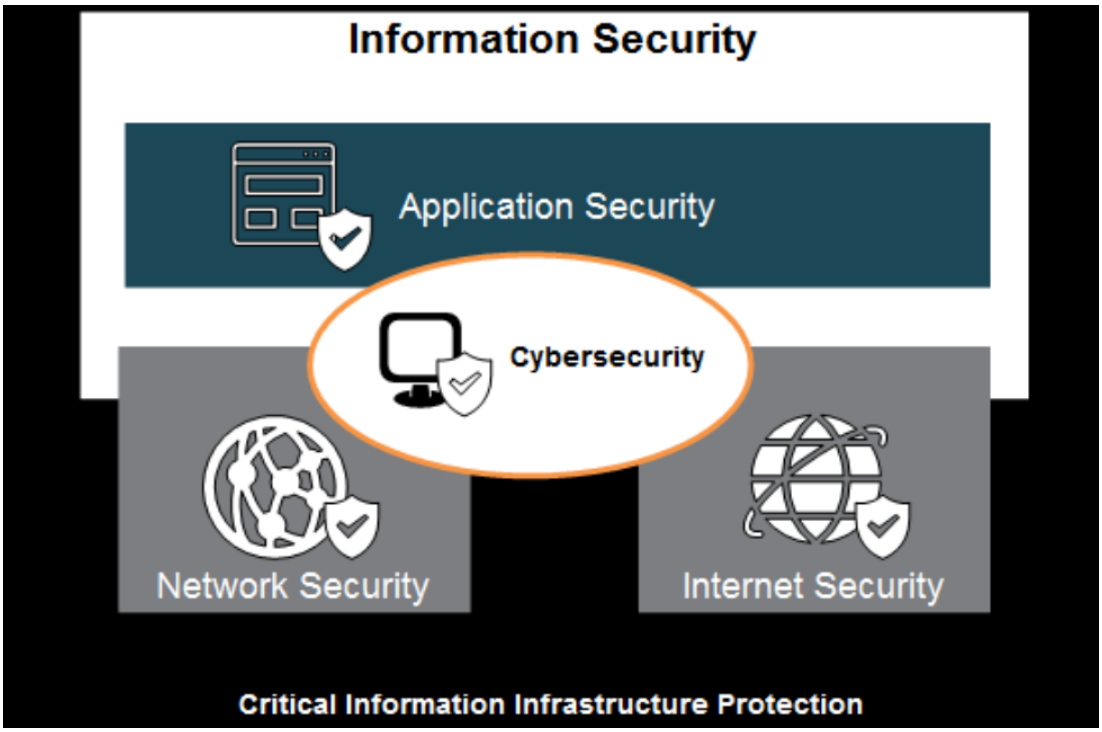
Robust cybersecurity implementation is roughly based around three key terms: *people, processes, and technology*. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error.

The attacks evolve every day as attackers become more inventive, it is critical to properly define cybersecurity and understand cybersecurity fundamentals.

Cyber security encompasses all aspects of security viz., Physical, Technical, Environmental, Regulations and Compliance including Third Parties involved in delivering an objective

With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also

Major areas covered in cyber security are:



1) Application Security: Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: a) Input parameter validation, b) User/Role Authentication & Authorization, c) Session management, parameter manipulation & exception management, and d) Auditing and logging.

2) Information Security: Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: a) Identification, authentication & authorization of user, b) Cryptography.

3) Disaster recovery: Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

4) Network Security: Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include: **a)** Anti-virus and anti-spyware, **b)** Firewall, to block unauthorized access to your network, **c)** Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks, and **d)** Virtual Private Networks (VPNs), to provide secure remote access.

5) Internet Security - measures to protect data during their transmission over a collection of interconnected networks

The history of Cybersecurity

About forty years ago words like *worms, viruses, trojan-horse, spyware, malware* weren't even a part of conventional information technology (IT) vocabulary. Cybersecurity only came into existence because of the development of viruses. But how did we get here?

In 1969, **Leonard Kleinrock**, professor of UCLA and student, **Charley Kline**, sent the first electronic message from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer, at the Stanford Research Institute. This is a well-known story and a moment in the history of a digital world. The sent message from the UCLA was the word "login." The system crashed after they typed the first two letters "lo." Since then, this story has been a belief that the programmers typed the beginning message **"lo and behold."** While factually believed that **"login"** was the intended message. Those two letters of messages were changed the way we communicate with one another.

The history of cybersecurity began as a research project. In the 1970's, Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts, created the first computer "worm". It was called ***The Creeper***. The Creeper, infected computers by hopping from system to system with the message *"I'M THE CREEPER: CATCH ME IF YOU CAN."* Ray Tomlinson, the inventor of email, created a replicating program called ***The***

Reaper, the first antivirus software, which would chase Creeper and delete it.

Late in 1988, a man named Robert Morris had an idea: he wanted to test the size of the internet. To do this, he wrote a program that went through networks, invaded Unix terminals, and copied itself. The Morris worm was so aggressive that it slowed down computers to the point of being unusable. He subsequently became the first person to be convicted under Computer Fraud and Abuse Act.

From that point forward, viruses became deadlier, more invasive, and harder to control. With it came the advent of cyber security.

Objectives of cyber security.

Our world today is ruled by technology and we can't do without it at all. From booking our flight tickets, to catching up with an old friend, technology plays an important role in it.

However, the same technology may expose you when it's vulnerable and could lead to loss of essential data.

Cyber security, alongside physical commercial security has thus, slowly and steadily, become one of the most important topics in the business industry to be talked about.

Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

Cyber security becomes important as Business are being carried now on Network of Networks.

Computer networks have always been the target of criminals, and it is likely that the danger of cyber security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations can take to minimize losses from those who seek to do harm.

Why is cyber security important?

We live in a digital era which understands that our private information is more vulnerable than ever before. We all live in a world which is

networked together, from internet banking to government infrastructure, where data is stored on computers and other devices. A portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cybersecurity describes to protect that information and the systems used to process or store it.

As the volume of cyber-attacks grows, companies and organizations, especially those that deal information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

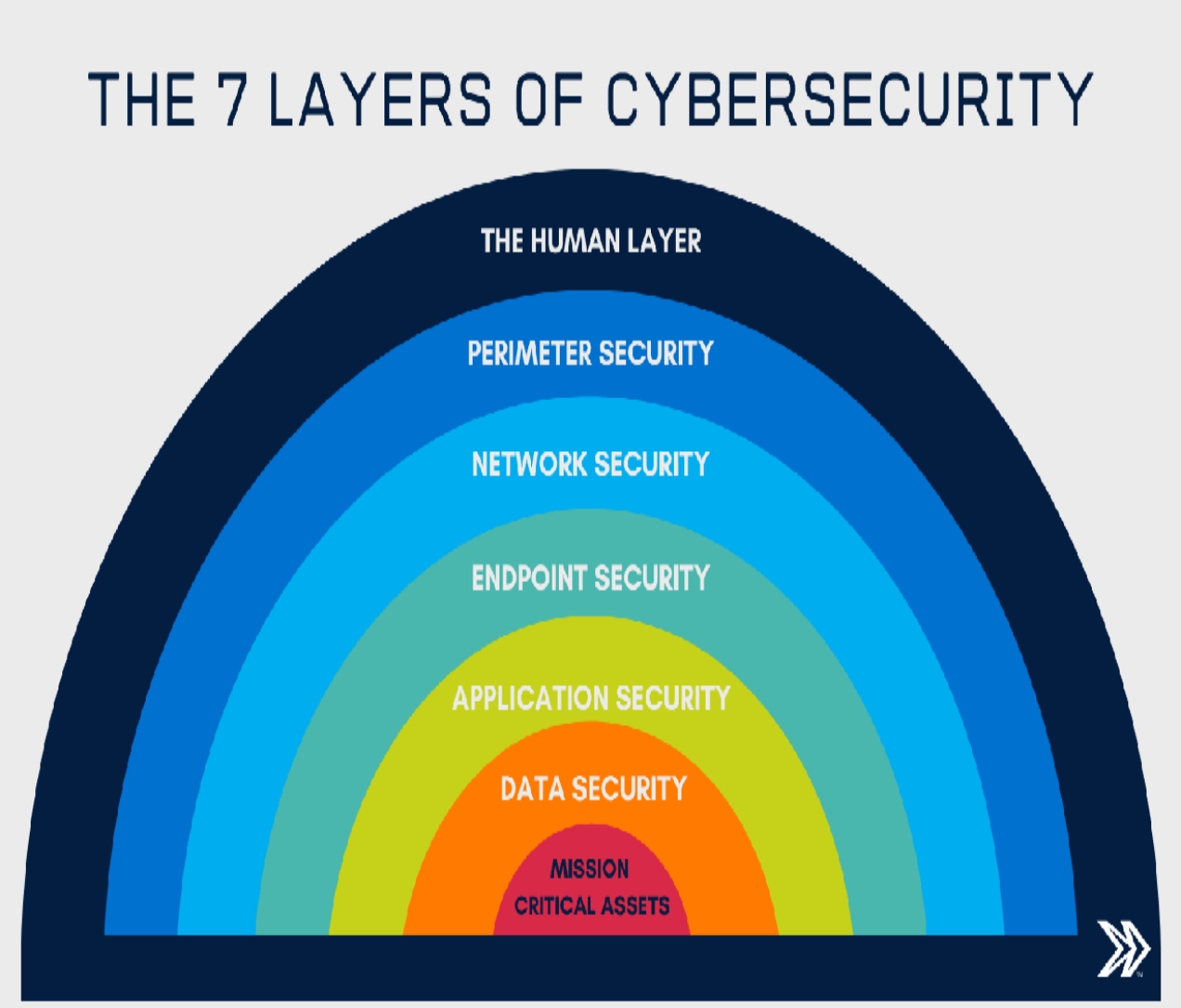
- With each passing year, the sheer volume of threats is increasing rapidly. *According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.*
- Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

The golden age of Hackers – What is Cybersecurity – Edureka

It can be rightfully said that today's generation lives on the internet, and we general users are almost ignorant as to how those random bits of 1's and 0's reach securely to our computer. For a hacker, it's a golden age. With so many access points, public IP's and constant traffic and tons of data to exploit, black hat hackers are having one hell of a time exploiting vulnerabilities and creating malicious software for the same. Above that, cyber attacks are evolving by the day. Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffles many people.

Therefore there has to be some sort of protocol that protects us against all these cyber attacks and make sure our data doesn't fall into the wrong hands. This is exactly why we need cybersecurity.

The 7 Layers of Cyber security



The 7 layers of cybersecurity should center on the mission critical assets you are seeking to protect.

1. **Mission Critical Assets** – This is the data you need to protect
2. **Data Security** – Data security controls protect the storage and transfer of data.
3. **Application Security** – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
4. **Endpoint Security** – Endpoint security controls protect the connection between devices and the network.

5. **Network Security** – Network security controls protect an organization's network and prevent unauthorized access of the network.
6. **Perimeter Security** – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
7. **The Human Layer** – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

Vulnerability is the intersection of three elements:

1. A system susceptibility or flaw,
2. Attacker access to the flaw, and
3. Attacker capability to exploit the flaw.

To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

What is the source of a vulnerability?

– Bad software (or hardware)
– Bad design, requirements
– Bad policy/configuration
– System Misuse
  • unintended purpose or environment
  • E.g., student IDs for liquor store

Vulnerabilities:

They make threat outcomes possible and potentially even more

dangerous. A system could be exploited through a single vulnerability, for example, a single SQL Injection attack could give an attacker full control over sensitive data. An attacker could also *chain* several exploits together, taking advantage of more than one vulnerability to gain more control.

Examples of common vulnerabilities are SQL Injections, Cross-site Scripting, server misconfigurations, sensitive data transmitted in plain text, and more.

SQL Injection: SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database. An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their OWASP Top 10 2017 document as the number one threat to web application security.

Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation.

This attack type is considered a major problem in web security. It is listed as the number one web application security risk in the OWASP Top

10 – and for a good reason.

Types of Injection Attacks

SQL injection (SQLi) and Cross-site Scripting (XSS) are the most common injection attacks but they are not the only ones. The following is a list of common injection attack types.

Injection attack	Description	Potential impact
Code injection	The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full web server compromise.	Full system compromise
CRLF injection	The attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence. This sequence is used to split an HTTP response header and write arbitrary contents to the response body. This attack may be combined with Cross-site Scripting (XSS).	Cross-site Scripting (XSS)
Cross-site Scripting (XSS)	The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application. This script is then executed inside the victim's browser.	• Account impersonation • Defacement • Run arbitrary JavaScript in the victim's browser
Email Header Injection	This attack is very similar to CRLF injections. The attacker sends IMAP/SMTP commands to a mail server that is not directly available via a web application.	• Spam relay • Information disclosure
Host	The attacker abuses the implicit trust of the	• Password-reset

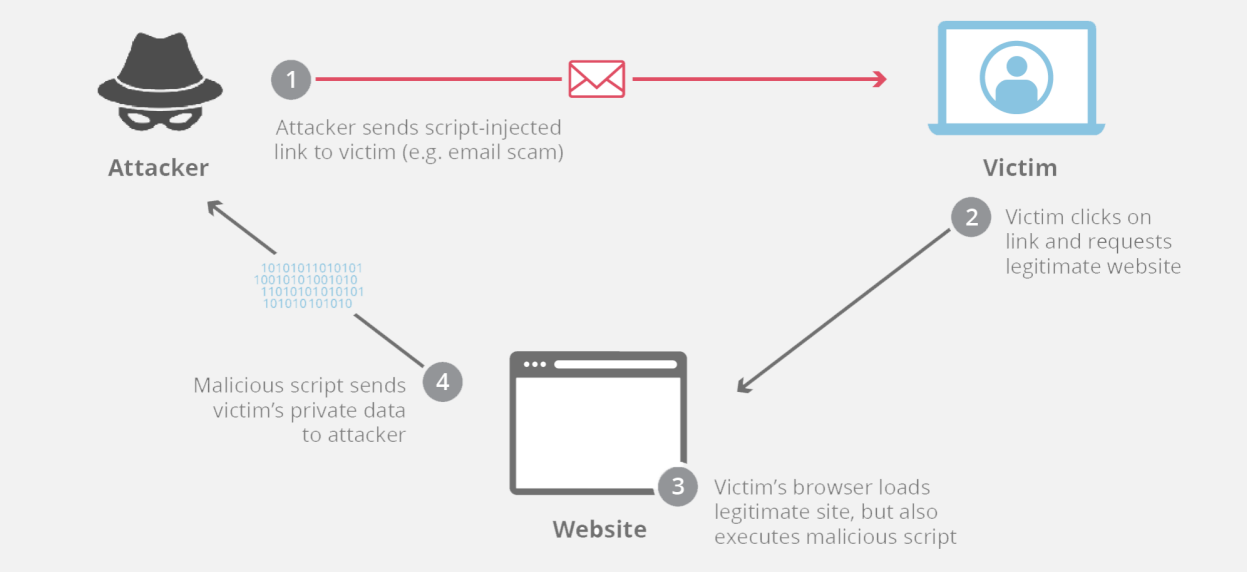
Injection attack	Description	Potential impact
Header Injection	HTTP Host header to poison password-reset functionality and web caches.	poisoning • Cache poisoning
LDAP Injection	The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands. They can gain permissions and modify the contents of the LDAP tree.	• Authentication bypass • Privilege escalation • Information disclosure
OS Command Injection	The attacker injects operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full system compromise.	Full system compromise
SQL Injection (SQLi)	The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.	• Authentication bypass • Information disclosure • Data loss • Sensitive data theft • Loss of data integrity • Denial of service • Full system compromise.
XPath injection	The attacker injects data into an application to execute crafted XPath queries. They can use them to access unauthorized data and bypass authentication.	• Information disclosure • Authentication bypass

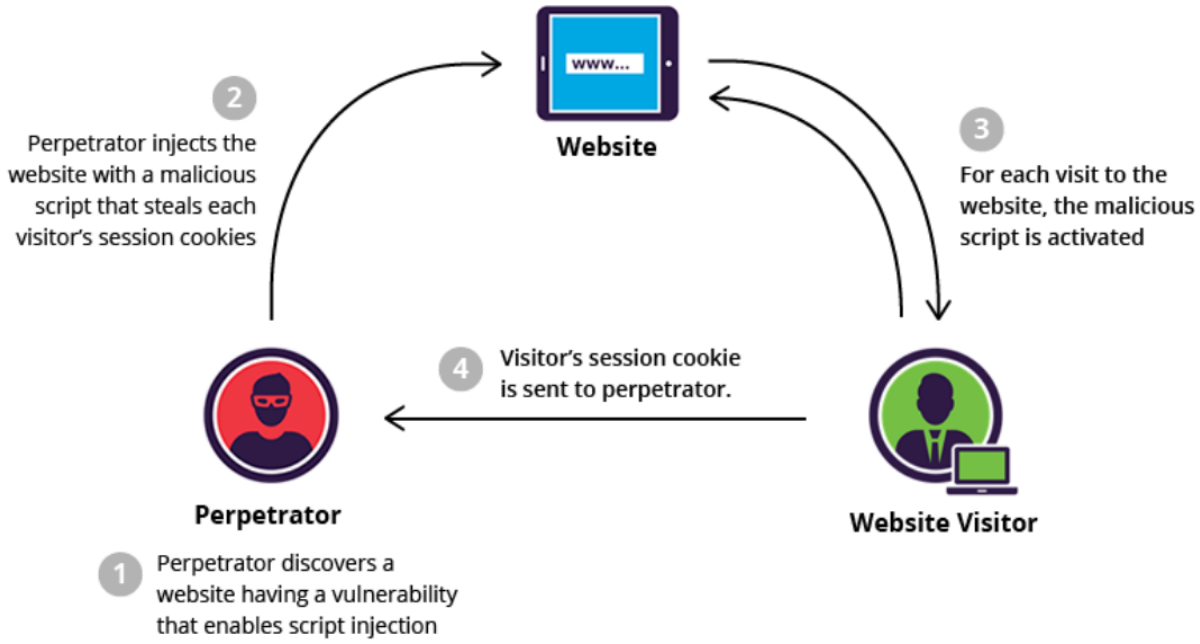
Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users.

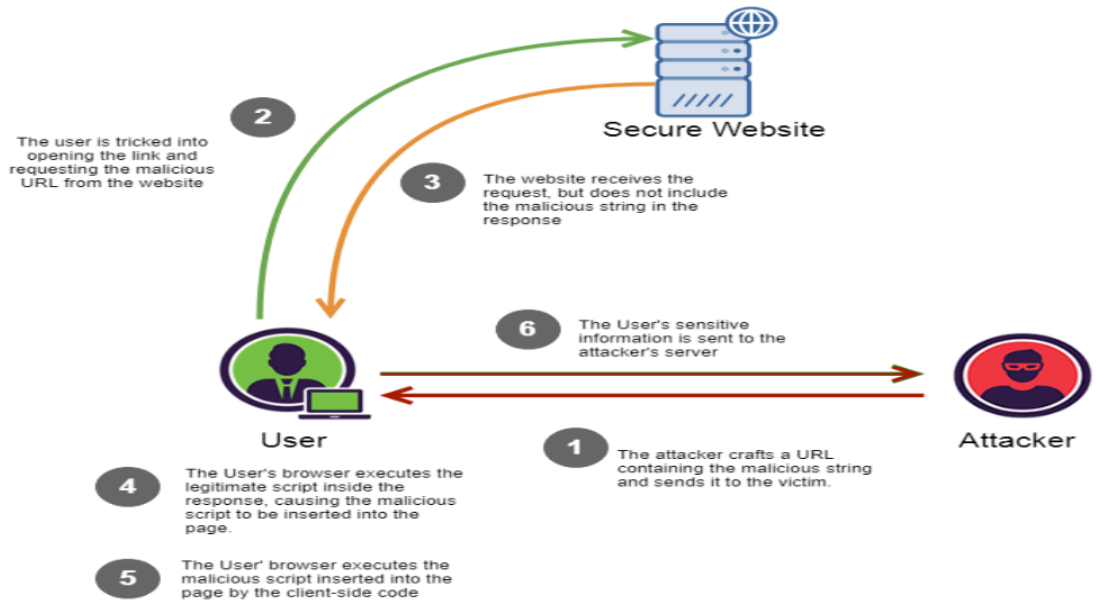
•XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

•Three types: Reflected XSS,





Stored XSS



DOM Based XSS

TOOLS:

GOOGLE DORKS

BURPSUITE

SCRIPT: <script>alert(123)</script>

WEB: http://brodyaga.ru/pages/search.php
WEB: https://www.fontel.com/

How to prevent XSS attacks

- Filter/Validating input on arrival.
- Encode data on output.
- Use appropriate response headers
- Content Security Policy.

Threats

A cyber threat is a potential for violation of cyber security that exists when there is a circumstance, capability, action, or event that could cause a data breach or any other type of unauthorized access.

Any vulnerability that can be exploited is a cyber threat. Cyber threats can come in both intentional and accidental ways:

- **Intentional cyber threat:** An example is a cybercriminal installing the WannaCry ransomware attack, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
- **WannaCry**

  The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, targeting only the Microsoft Windows operating systems.

  The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. However, email phishing was the main method of spreading the WannaCry ransomware.

  The WannaCry ransomware attack had exploited a vulnerability in Windows OS called EternalBlue.

Impact

•This attack impacted a number of businesses, institutions and

hospitals all over the world.

•Businesses like Nissan and Renault had to pause their activities after some of their computers were affected.

•In hospitals, computer systems used for various purposes were affected, like MRI scanners and computers.

•Many critics said that this attack could have been prevented if people took steps, to solve the flaws on which the attacks were based, earlier.

•Some even blame the governments for their inability to secure vulnerabilities.

•Estimates state that around 200,000 to 300,000 computer systems were affected in this attack in approximately 150 countries.

- **Accidental cyber threats:** Poorly configured S3 bucket security leading to a big data breach. Check your Amazon S3 security or someone else will.

This is why understanding the difference between cybersecurity and information security, as well as how to perform a cybersecurity risk assessment is more important than ever. Your organization needs to have a set of policies and procedures to manage your information security in accordance with risk management principles and have countermeasures to protect financial, legal, regulatory, and reputational concerns.

Should a cyber attack lead to a security incident, your organization should have steps to detect, classify, manage, and communicate it to customers where applicable. The first logical step is to develop an incident response plan and eventually a cybersecurity team.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome to your network or other data management systems. Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that causes a data breach or even a tornado that takes down your company's data headquarters, disrupting access.

When threat probability is multiplied by the potential loss that may result, cybersecurity experts refer to this as risk.

An object, person, or other entity that represents a constant danger to an asset

• Management must be informed of the different threats facing the organization

• By examining each threat category, management effectively protects information through policy, education, training, and technology controls

• 2004 Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI) survey found: – 79% of organizations reported cyber security breaches within the last 12 months – 54% of those orgs. reported financial losses over $141 million

• A threat is a specific means by which a risk can be realized by an adversary – Context specific (a fact of the environment) – An attack vector is a specific threat (e.g., key logger)

• A threat model is a collection of threats that deemed important for a particular environment – E.g., should be addressed – A set of "security requirements" for a system

• Take the survey with a grain of salt – Underreporting, fear of bad publicity – Cybercrime: easy $$ at perceived low risk to attacker

Threats to Info. Security

Threat Category	Examples
Acts of human error or failure	Accidents, employee mistakes
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. Disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
Deliberate software attacks	**Viruses, worms, denial of service**
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure

Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

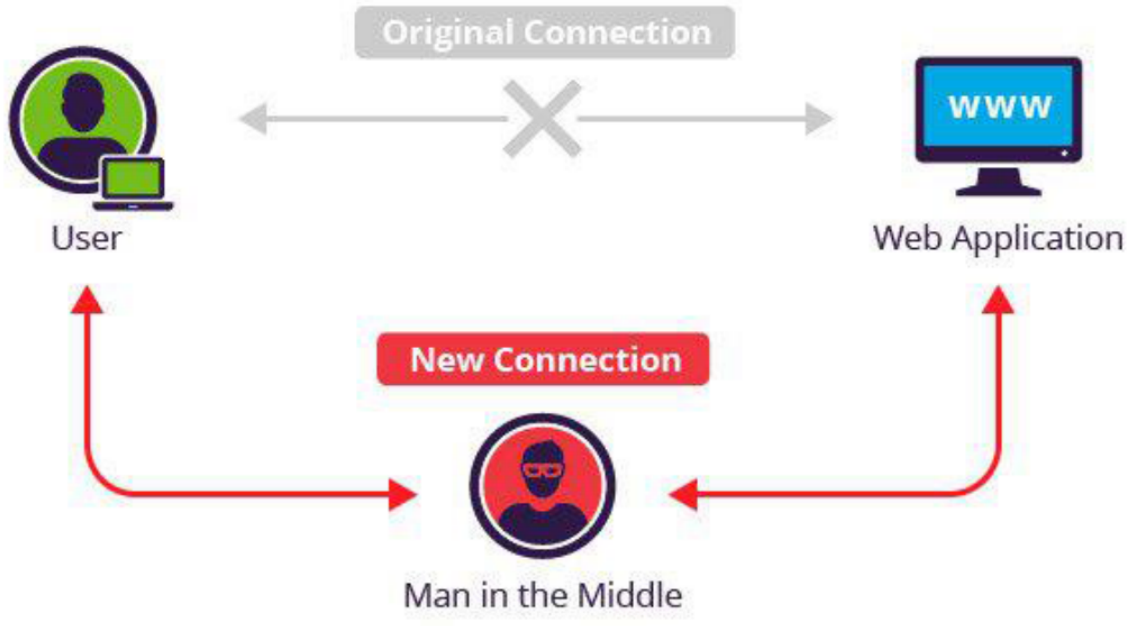
TYPES OF CYBER SECURITY THREATS

Just as there is a plethora of various germs and diseases that can attack the human body, there are numerous threats that can affect hardware, software and the information you store. Some of the major ones include the following:

- **Viruses**: similar to the way the common cold replicates itself repeatedly in one person's body and is then spread, a software virus is designed in such a way that can be easily transmitted from one computer or system to another. Often sent as email attachments, viruses corrupt and co-opt data, interfere with your security settings, generate spam and may even delete content.
- **Computer worms** are similar; they spread from one computer to the next by sending itself to all of the user's contacts and subsequently to all of the contacts' contacts.
- **Trojans**: these malicious pieces of software insert themselves into a legitimate program. Often, people voluntarily let trojans into their systems in the form of email messages from a person or an advertiser they trust. As soon as the accompanying attachment is open, your system becomes vulnerable to the malware within.
- **Bogus security software** that tricks users into believing that their system has been infected with a virus. The accompanying security software that the threat actor provides to fix the problem actually causes it.
- **Adware** that tracks your browsing habits and causes particular advertisements to pop up. Although this is common and often something you may even agree to, adware is sometimes foisted upon you without your consent. Similarly, spyware is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
- **Denial of service (DOS) attack**: this occurs when hackers deluge a website with traffic, making it impossible for users to access its content. A distributed denial of service (DDOS) attack is more forceful and aggressive

since it is initiated from several servers simultaneously. As a result, a DDOS attack is harder to mount defenses against.

- **Phishing attacks** are social engineering infiltrations whose goal is to wrongfully obtain sensitive data such as passwords and credit card numbers. Via emails or links, the hacker causes malware to be downloaded and installed. Many phishing attacks appear to come from trusted companies and financial institutions and ask users to verify their identity, thus leaving them open to hacking.
- **SQL injections** are network threats that involve using malicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed or destroyed. This type of attack is quickly becoming the most serious network security issue.
- **Man-in-the-middle attacks** involve a third party intercepting and exploiting communications between two entities that should remain private. Not only does eavesdropping occur but also information can be changed or misrepresented by the intruder, causing inaccuracy and even security breaches.



- **Rootkit tools** gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

Harmful Acts

- Harmful Acts committed form or against a computer or network
- Illegal computer-mediated activities that can be conducted through global electronic networks
- Unlawful acts wherein the computer is either a tool or target or both
- Online or internet-based illegal acts

Cyber Criminals:

Cybercrime involves such activities as child pornography ,credit card fraud, cyber stalking, defaming another online, gaining un authorized access to computer systems, ignoring copyright, software licensing and trade mark protection, overriding encryption to make illegal copies, software piracy and stealing another's identity to perform criminal acts.

They can be categorized into 3 groups.

1. Type I: Cybercriminals- hungry for recognition

- hobby hackers
- IT professionals
- Terrorist organizations

2. Type II: Cybercriminals-not interested in recognition

- psychological perverts
- financially motivated hackers
- organized criminals

3. Type III: Cybercriminals- The insiders

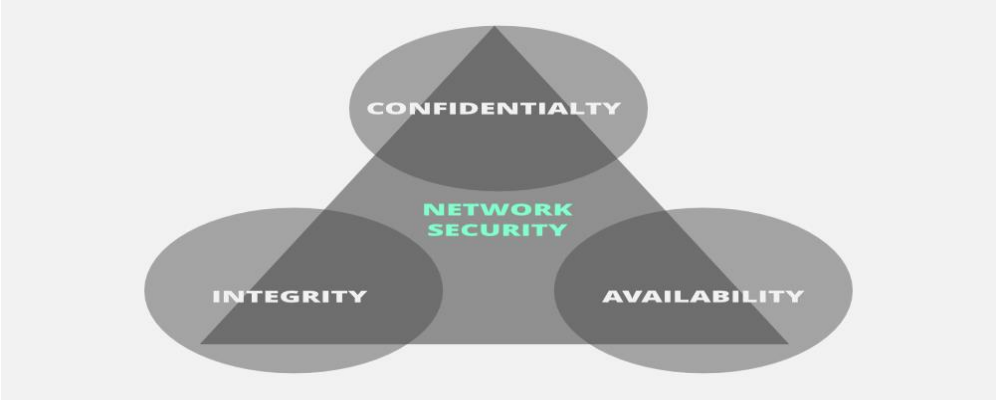
- disgruntled or former employees seeking revenge
- competing companies using employees to gain economic advantage through damage and/or theft.

The CIA triad :

The **CIA** triad is one of the most important model which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

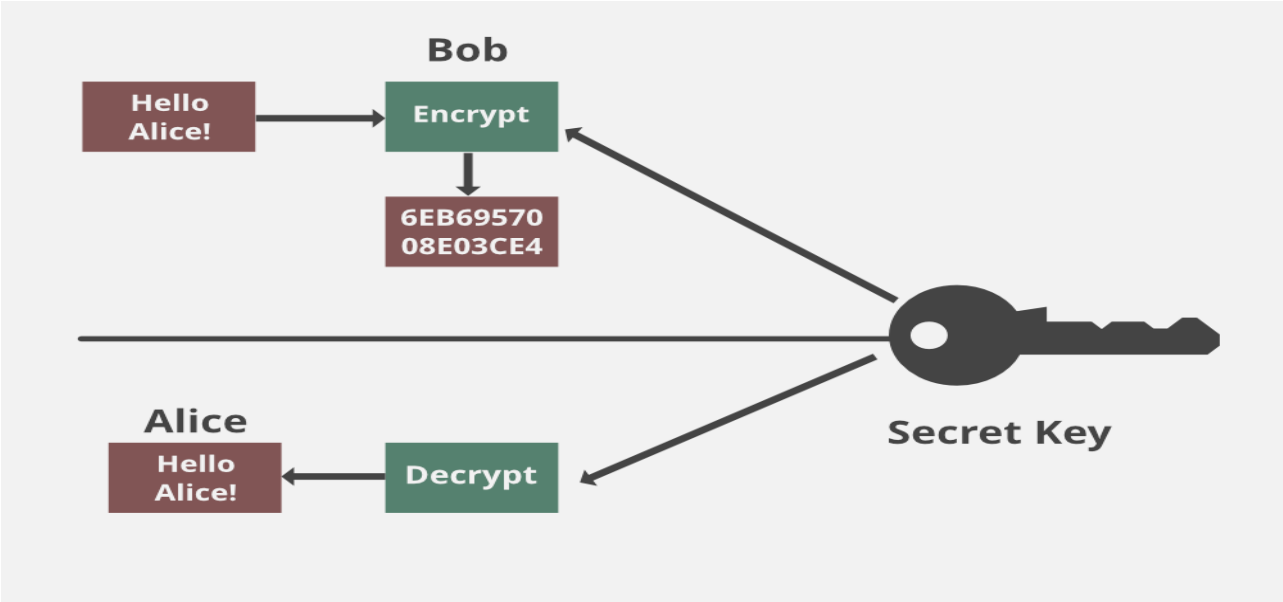


These are the objectives which should be kept in mind while securing a network.

Confidentiality:

Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to our information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.

VPN stands for Virtual Private Network and helps the data to move securely over the network.



Integrity :
The next thing to talk about is integrity. Well, the idea here is making sure that data has not been modified. Corruption of data is a failure to maintain data integrity.

Availability :
This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over and prevent bottleneck in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network gets exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

Motive of attacks:

The most common types of cyber-crime affecting small businesses are phishing emails, malware attacks and ransom ware, which analysts estimate costs on average £3,000 per business.

Cash
A primary motivation for hackers is the money they can obtain by stealing your passwords, bank details, holding your customer information for ransom or selling your data to competitors or on the dark web.

Challenge
A large portion of hackers are driven by the opportunity to break the unbreakable system and gaining the recognition from their peers. This competitive behaviour drives groups of hackers to challenge each other to cause disruption at the expense of another business.

Hacktivism
Infamous hacker groups use their skills to target large organisations and embarrass their IT teams, break their sophisticated security systems and humiliate the upper management.

Revenge
Certain types of hackers are motivated by anger and use their skills to directly affect a person, group or company without any fear of repercussion.

Subversion
Hackers have been accused of meddling in current and corporate affairs - a modern-day version of espionage.

Infamy
Hackers are motivated by a sense of achievement, working independently or in groups they want to be recognised. Social media has given them a platform to boast about their exploits on a global scale.

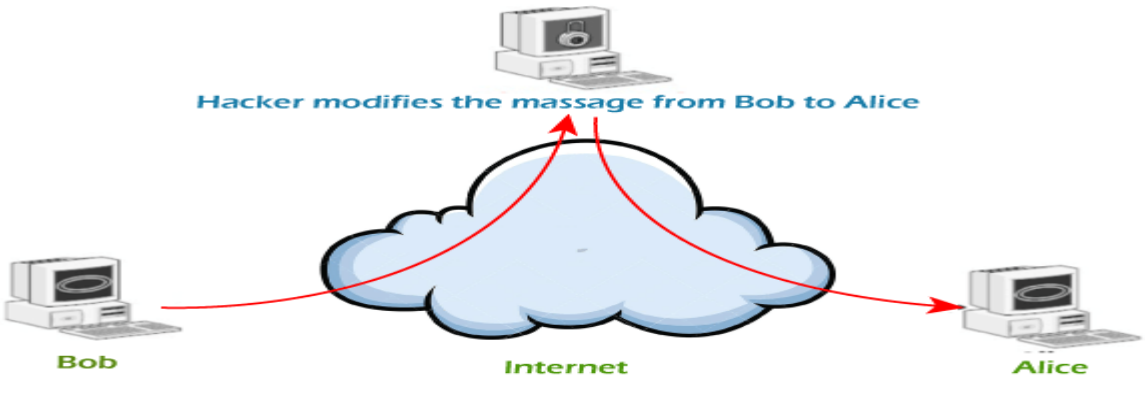
What is a Security attack?

These are the unauthorized or illegal actions that are taken against the government, corporate, or private IT assets in order to destroy, modify, or steal the sensitive data. They are further classified into active and passive attacks, in which the attacker gets unlawful access to the system's resources.

Active attacks

In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for integrity and availability of the message. Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. The system resources can be changed due to active attacks. So, the damage done with active attacks can be harmful to the system and its resources.

In the below image, we can see the process of active attacks.



Active Attacks (Modifications of messages)

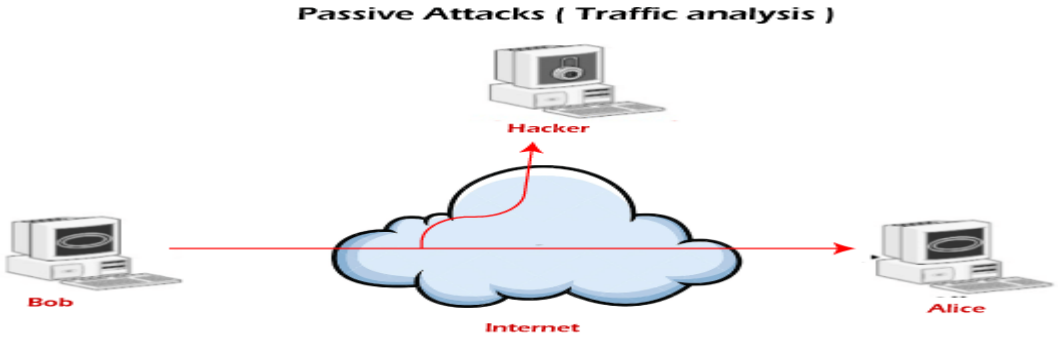
In active attacks, the victim gets notified about the attack. The implication of an active attack is typically difficult and requires more effort. Active attacks can be

prevented by using some techniques. We can try the below-listed measures to prevent these attacks -

- Use of one-time password help in the authentication of the transactions between two parties.
- There could be a generation of the random session key that will be valid for a single transaction. It should prevent the malicious user from retransmitting the actual information once the session ends.

Passive attacks

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.



Unlike active attacks, in passive attacks, victims do not get informed about the attack. It is difficult to detect as there is no alteration in the message. Passive attacks can be prevented by using some encryption techniques. We can try the below-listed measures to prevent these attacks -

- We should avoid posting sensitive information or personal information online. Attackers can use this information to hack your network.
- We should use the encryption method for the messages and make the messages unreadable for any unintended intruder.

Active attack v/s Passive attack

Now, let's see the comparison chart between Active attack and Passive attack. We are comparing both security attacks on the basis of some characteristics.

On the basis of	Active attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
Modification	In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
Victim	In active attacks, the victim gets notified about the attack.	Unlike active attacks, in passive attacks, victims do not get informed about the attack.
System's impact	The damage done with active attacks can be harmful to the system and its resources.	The passive attacks do not harm the system.
System resources	In active attacks, the system resources can be changed.	In passive attacks, the system resources remain unchanged.
Dangerous for	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Emphasis on	In active attacks, attention is on detection.	In active attacks, attention is on prevention.
Types	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.

Prevention	Active attacks are tough to restrict from entering systems or networks.	Unlike active attacks, passive attacks are easy to prohibit.

Software attacks:

The software attack surface is **the complete profile of all functions in any code running in a given system that are available to an unauthenticated user**. ... The software attack surface is particularly at risk in the case of Web applications, which expose the coding to the Internet.

Ex: **Malware**, in which malicious software is used to attack information systems. Ransomware, spyware and Trojans are examples of malware.

Hardware attacks:

It is a **process of protecting hardware against vulnerabilities** that ae targeting these devices. It is a process of protecting software against malicious attack and other hacker's risks. ... Hardware cannot modify features just like software.

Hardware attacks are not as well-known as these software attacks, but they are just as dangerous. They **involve directly exploiting interaction with a system's electronic components**. These sneak attacks are particularly effective against connected objects.

Ex: Directory traversal, Bad USB, PCB tampering etc

IP Spoofing:

Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.

What does IP spoofing do?

IP spoofing enables an attacker to replace a packet header's source IP address with a fake, or spoofed IP address. The attacker does this by intercepting an IP packet and modifying it, before sending it on to its destination. ... As you can see, IP spoofing facilitates anonymity by concealing source identities.

Every packet comprises an IP address header that possesses data about the IP address of the sender and the receiver and other relevant information about the packet under consideration.

Cyber Crime:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cybercrime

Here are some specific examples of the different types of cybercrime:

Email and internet fraud.

Identity fraud (where personal information is stolen and used).

Theft of financial or card payment data.

Theft and sale of corporate data.

Cyberextortion (demanding money to prevent a threatened attack).

Ransomware attacks (a type of cyberextortion).

Cryptojacking (where hackers mine cryptocurrency using resources they do not own).

Cyberespionage (where hackers access government or company data).

Cyber Terrorism:

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

What are the methods of cyber terrorism?

Typical practices of cyberterrorists may include: Denial of Service (Dos) attacks and Distributed Denial of Service attacks (DDos) Web defacement which may include negative or derogatory comments against the government, political parties or other religious organizations. Misinformation campaigns.

Cyber Espionage:

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

There are 2 types of espionage.

The first of which defines the two types of espionage: covert operations and covert intelligence, distinguishing between the human and cyber variants of both.

Cyber Threats:

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.

Top 10 Computer Security Threats to Prepare for in 2021.

- Phishing Attacks. ...
- Cloud Jacking. ...
- Network Perimeter and Endpoint Security. ...
- Mobile Malware. ...
- 5G-to-Wi-Fi Security Vulnerabilities. ...
- Internet of Things (IoT) Devices. ...
- Deepfakes. ...
- Highly Developed Ransomware Attacks.

Cyber Warfare:

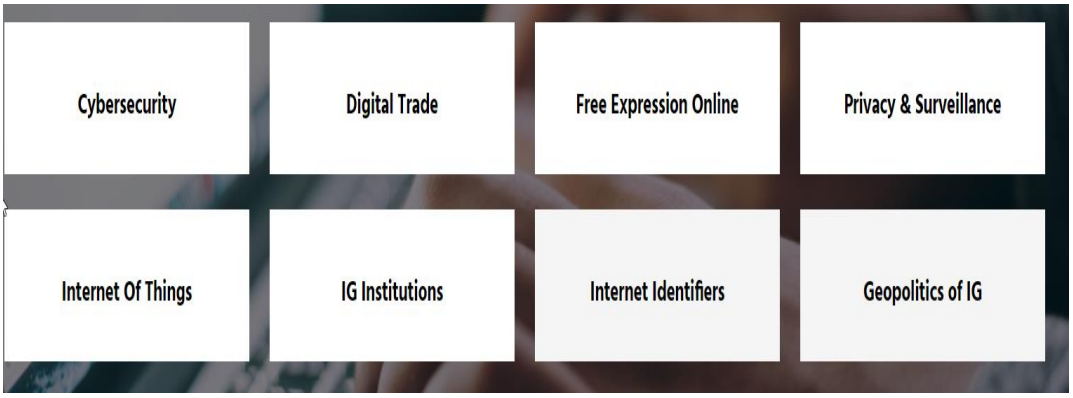
Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Internet governance

Internet governance refers to the rules, policies, standards and practices that coordinate and shape global cyberspace.

The Internet is a vast network of independently-managed networks, woven together by globally standardized data communication protocols (primarily, Internet Protocol, TCP, UDP & DNS). The common adoption and use of these protocols unified the world of information and communications like never before. Millions of digital devices and massive amounts of data, software applications, and electronic services became compatible and interoperable. The Internet created a new environment, a complex and dynamic “cyberspace.”

The term “Internet governance” first started to be used in connection with the governance of Internet identifiers such as domain names and IP addresses, which led to the formation of ICANN. Since then, the economic, political, social and military implications of Internet governance have expanded to embrace a number of other areas of policy:



The Internet impacts global interests and its governance "includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN); it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet". For these reasons, a single entity cannot and has not been designated as an international governance body. Instead, the Internet is primarily governed internationally by multiple stakeholders - government, the private sector, academia, and civil society - covering a range of technical and non-technical issues. Nevertheless, countries vary in terms of their views on which stakeholders should play a primary role in Internet governance. While some countries believe that multiple stakeholders should be responsible for Internet governance, other countries believe that Internet governance should be the exclusive domain of the state.

Methods of Defense

We investigate the legal and ethical restrictions on computer-based crime. But unfortunately, computer crime is certain to continue for the foreseeable future. For this reason, we must look carefully at controls for preserving confidentiality, integrity, and availability. Sometimes these controls can prevent or mitigate attacks; other, less powerful methods can only inform us that security has been compromised, by detecting a breach as it happens or after it occurs.

Harm occurs when a threat is realized against vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both. The possibility for harm to occur is called **risk**. We can deal with harm in several ways. We can seek to

- *prevent it*, by blocking the attack or closing the vulnerability
- *deter it*, by making the attack harder but not impossible
- *deflect it*, by making another target more attractive (or this one less so)
- *detect it*, either as it happens or sometime after the fact
- *recover* from its effects

Of course, more than one of these can be done at once. So, for example, we might try to prevent intrusions. But in case we do not prevent them all, we might install a detection device to warn of an imminent attack. And we should have in place incident response procedures to help in the recovery in case an intrusion does succeed.

Controls

To consider the controls or countermeasures that attempt to prevent exploiting a computing system's vulnerabilities, we begin by thinking about traditional ways to enhance physical security. In the Middle Ages, castles and fortresses were built to protect the people and valuable property inside. The fortress might have had one or more security characteristics, including

- a strong gate or door, to repel invaders
- heavy walls to withstand objects thrown or projected against them
- a surrounding moat, to control access
- arrow slits, to let archers shoot at approaching enemies
- crenellations to allow inhabitants to lean out from the roof and pour hot or vile liquids on attackers
- a drawbridge to limit access to authorized people
- gatekeepers to verify that only authorized people and goods could enter

Similarly, today we use a multipronged approach to protect our homes and offices. We may combine strong locks on the doors with a burglar alarm, reinforced windows, and even a nosy neighbor to keep an eye on our valuables. In each case, we select one or more ways to deter an intruder or attacker, and we base our selection not only on the value of what we protect but also on the effort we think an attacker or intruder will expand to get inside.

Computer security has the same characteristics. We have many controls at our disposal. Some are easier than others to use or implement. Some are cheaper than others to use or implement. And some are more difficult than others for intruders to override. We use one or more controls, according to what we are protecting, how the cost of protection compares with the risk of loss, and how hard we think intruders will work to get what they want.

Encryption is the formal name for the scrambling process. We take data in their normal, unscrambled state, called **cleartext**, and transform them so that they are unintelligible to the outside observer; the transformed data are called **enciphered text** or **ciphertext**. Using encryption, security professionals can virtually nullify the value of an interception and the possibility of effective modification or fabrication. In Chapters 2 and 12 we study many ways of devising and applying these transformations.

Encryption clearly addresses the need for confidentiality of data. Additionally, it can be used to ensure integrity; data that cannot be read generally cannot easily be changed in a meaningful manner. Furthermore, as we see throughout this book, encryption is the basis of **protocols** that enable us to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to a desired result. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security.

Although encryption is an important tool in any computer security tool kit, we should not overrate its importance. Encryption does not solve all computer security problems, and other tools must complement its use. Furthermore, if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system. Weak encryption can actually be worse than no encryption at all, because it gives users an unwarranted sense of

protection. Therefore, we must understand those situations in which encryption is most useful as well as ways to use it effectively.

Software Controls

If encryption is the primary way of protecting valuables, programs themselves are the second facet of computer security. Programs must be secure enough to prevent outside attack. They must also be developed and maintained so that we can be confident of the programs' dependability.

Program controls include the following:

- *internal program controls:* parts of the program that enforce security restrictions, such as access limitations in a database management program
- *operating system and network system controls:* limitations enforced by the operating system or network to protect each user from all other users
- *independent control programs:* application programs, such as password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities
- *development controls:* quality standards under which a program is designed, coded, tested, and maintained to prevent software faults from becoming exploitable vulnerabilities

We can implement software controls by using tools and techniques such as hardware components, encryption, or information gathering. Software controls frequently affect users directly, such as when the user is interrupted and asked for a password before being given access to a program or data. For this reason, we often think of software controls when we think of how systems have been made secure in the past. Because they influence the way users interact with a computing system, software controls must be carefully designed.

Hardware Controls

Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as

- hardware or smart card implementations of encryption
- locks or cables limiting access or deterring theft
- devices to verify users' identities
- firewalls
- intrusion detection systems
- circuit boards that control access to storage media

Policies and Procedures

Sometimes, we can rely on agreed-on procedures or policies among users rather than enforcing security through hardware or software means. In fact, some of the simplest controls, such as frequent changes of passwords, can be achieved at essentially no cost but with tremendous effect. Training and administration follow immediately after establishment of policies, to reinforce the importance of security *policy* and to ensure their proper use.

We must not forget the value of community standards and expectations when we consider how to enforce security. There are many acts that most thoughtful people would consider harmful, and we can leverage this commonality of belief in our policies. For this reason, legal and ethical controls are an important part of computer security. However, the law is slow to evolve, and the technology involving computers has emerged relatively suddenly. Although legal protection is necessary and desirable, it may not be as dependable in this area as it would be when applied to more well-understood and long-standing crimes.

Society in general and the computing community in particular have not adopted formal standards of ethical behavior. As we see in Chapter 11, some organizations have devised codes of ethics for computer professionals. However, before codes of ethics can become widely accepted and effective, the computing community and the general public must discuss and make clear what kinds of behavior are inappropriate and why.

Physical Controls

Some of the easiest, most effective, and least expensive controls are *physical controls*. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters. Often the simple physical controls are overlooked while we seek more sophisticated approaches.

Cyber Risk management

Cyber threats are constantly evolving. The most effective way to protect your organisation against cyber attacks is to adopt a risk-based approach to cyber security, where you regularly review your risks and whether your current measures are appropriate.

IT Governance can help you develop a cyber threat management strategy, enabling you to take a systematic approach to managing your security challenges.

Cyber risk management:

Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation's cyber security threats.

The first part of any cyber risk management programme is a cyber risk assessment. This will give you a snapshot of the threats that might compromise your organisation's cyber security and how severe they are.

Based on your organisation's risk appetite, your cyber risk management programme then determines how to prioritise and respond to those risks.

The cyber risk management process

Although specific methodologies vary, a risk management programme typically follows these steps:

1. Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
2. Analyse the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
3. Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. Prioritise the risks.
5. Decide how to respond to each risk. There are generally four options:
    - Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.
    - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).
    - Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
    - Transfer – share the risk with another party, usually by outsourcing or taking out insurance.
6. Since cyber risk management is a continual process, monitor your risks to make sure they are still acceptable, review your controls to make sure they are still fit for purpose, and make changes as required. Remember that your risks are continually changing as the cyber threat landscape evolves, and your systems and activities change.

Standards and frameworks that mandate a cyber risk management approach

ISO 27001

ISO/IEC 27001:2013 – the international standard for information security management. Clause 6.1.2 of ISO 27001 states that an information security risk assessment must:

- Establish and maintain information security risk criteria;
- Ensure that repeated risk assessments produce "consistent, valid and comparable results";
- "identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system";
- Identify the owners of those risks; and
- Analyse and evaluate information security risks according to the criteria established earlier.

The NCSC's 10 steps to cyber security

The NCSC's (National Cyber Security Centre) 10 steps to cyber security - a set of ten practical steps that organisations can take to improve the security of their networks and the information carried on them. Defining and communicating your board's information risk management regime is central to your organisation's overall cyber security strategy and the first of the ten steps.

The CIS Controls

CIS (Center for Internet Security) Controls - the CIS Controls, formerly the 20 Critical Controls for Effective Cyber Defense, are a set of 20 actions, also known as CSC (critical security controls), for cyber defence, which provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

The PCI DSS

The PCI DSS (Payment Card Industry Data Security Standard) - applies to organisations of any size that accept card payments. Protecting digital cardholder data requires adherence to all the PCI DSS data security requirements. There are 12 PCI DSS requirements, which apply to "all system components included in or connected to the cardholder data environment". Requirements 5 and 6 deal with implementing and maintaining a vulnerability management programme – an essential part of risk management.

Security Models:

NIST Cyber Security Framework

National Institute of Standards and Technology (NIST) is a cybersecurity model commonly used by organizations in the US. Establishing and communicating your organization's tolerance for risk is key to increase program maturity, in accordance to this model. The NIST framework also accounts for the rapidly changing nature of cybersecurity threats, and advises its followers to continuously adjust their monitoring techniques and remediation strategies to match the ongoing threat environment.

The NIST cybersecurity model follows **five key phases** to reaching a mature security management program:

1. **Identify -** In the first phase, organizations establish a business-wide approach to cybersecurity management, including an understanding of the current risks to the network, what sensitive information lives throughout the organization, and what critical business operations exist that need to be protected from cybersecurity threats
2. **Protect** - The next step in building program maturity according to NIST's cybersecurity model is to organize and define the defenses necessary to protect the identified critical pieces of your security program.
3. **Detect** - This phase is probably what most organizations dive right into when it comes to cybersecurity program management, including establishing the most effective and encompassing monitoring tools to identify risks efficiently and effectively.
4. **Respond** - The fourth step to increase program maturity according to NISTs cybersecurity model is to tackle the threats to your organization. This is more than just patching your network, but means proper containment of the impact of malicious activity.
5. **Recover** - Just as detection and remediation are important to program maturity, having it in your management process to schedule time to recover and reflect on damages will allow for real program improvements and better protection of your network in the future.

The NIST cybersecurity model acknowledges the current practices most organizations use to protect their network. Instead of starting new, it guides organizations to better use what they're already doing and add in the right steps to reach program maturity.

ISO 27000

ISO 27000 is an international standard, created by the Internal Organization for Standardization (ISO) to highlight best practices for information security management systems. This cybersecurity model is more popular among organizations in the European Union, and focuses attention on the three main areas of a mature cybersecurity management program: people, processes, and technology. The recommendations of the ISO 27000 cybersecurity model is broken down into the following areas for security managers to use best practices to reach program maturity:

- Security risk assessment
- Security policy
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management

Similarly to the NIST framework, ISO 27000 guides organizations beyond the typical cyber security management practices to include greater security standards and protections. ISO 27000 includes management of critical physical and operational security measures, and is broken down into ISO 27000 Series to get more specific into the actual implementation and design of this cyber security model.

ISO 27000 Series	
ISO27001	ISMS Requirements
ISO27002	ISMS controls
ISO27003	ISMS implementation guidelines
ISO27004	ISMS Measurements
ISO27005	Risk management
ISO27006	Guidelines for ISO 27000 accreditation bodies

CIS 20

The final cyber security model many organizations follow to reach program maturity is the CIS 20. Designed by the center for Internet Security after the US defense industry experienced a data breach in 2008, the CIS 20 is a series of 20

controls deemed critical to protect an organization's network from expansive cyber attacks.

The CIS 20 is broken down into 3 main categories of controls:

1. Basic Controls (like inventory control, continuous vulnerability management, and controlled employee privileges)
2. Foundational Controls (like malware defenses, data protection, or wireless access controls)
3. Organizational Controls (like training programs and creation of incident response teams)

The CIS 20 cyber security model is designed to be all-encompassing, and require extreme attention and care to an organization's cyber security management process.

There are many cyber security models for organizations to both choose from, or to be required to follow. It's also important for a lot of businesses to become certified for following a specific framework to best represent themselves compared to their competition.

Comprehensive IT Security Policy:

A comprehensive IT security policy is essentially a battle plan that guides our organization, ensuring that your data and network is guarded from potential security threats. Think of it as a link between your people, processes, and technology.

Goals of a comprehensive security policy:

The CIA Triad refers to the 3 goals of cyber security Confidentiality, Integrity, and Availability of the organizations systems, network and data.

Confidentiality – Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when

they will occur. A security policy also considered being a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies-

1) It increases efficiency.

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.