Cybersecurity

A short guide

2024

Waleed ahmed

SP 23873

Jahanzaib

SP 23870

Sibgha zameer

SP 23863

Fiza tahir

SP 23865

Table of contents

INTRODUCTION:

- Cybersecurity is the practice of protecting internet connected systems such as hardware, software, and data from cyberthreats. It's used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems.
- An effective cybersecurity strategy can provide a strong security posture against malicious attacks designed to access, alter, delete, destroy, or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks designed to disable or disrupt a system's or device's operations.
- Cybersecurity protects digital systems, networks and data from unauthorized access, theft, or damage. It involves implementing various measures and technologies to ensure the confidentiality, integrity and availability of information stored and processed on computer systems. In other words, it refers to the practice of keeping computers, networks, and digital information safe from unauthorized access, attacks, or damage.

Figure 1

- The word cybersecurity is made up of two parts: "**Cyber**" and "**Security**".
  - Cyber: This refers to anything related to computers, networks, and the digital world.
  - Security: This means the protection of something from harm, loss or authorized access.
  - It is vast field that constantly evolves, and it encompasses a wide range of practices to protect computers, networks and data from unauthorized access, theft, or damage.

Three critical aspects of cybersecurity are:

- **Prevention:** It involves implementing security measures to prevent unauthorized access or breaches in the system.
- **Detection:** It involves identifying potential threats and vulnerabilities in a system.

- **Response:** It involves taking necessary actions to mitigate the impact of a security breach.

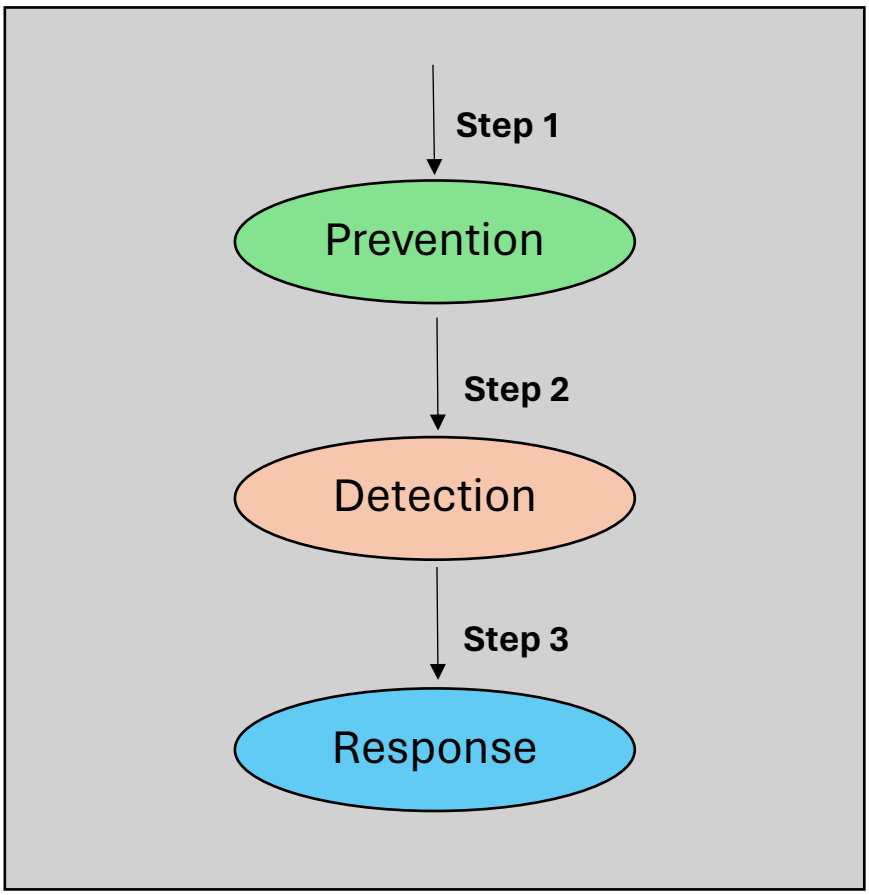

Figure 2

❖ HISTORY OF CYBER SECURITY:

- It is thought to have started in 1971 when Bob Thomas, a computer programmer with BBN, created and deployed a virus that served as a security test.
- The first cybercrime was recorded in the year 1980.
- The first spam email took place in 1987 when it was sent over the Arpanet.
- The first virus was installed in an apple computer in 1982.

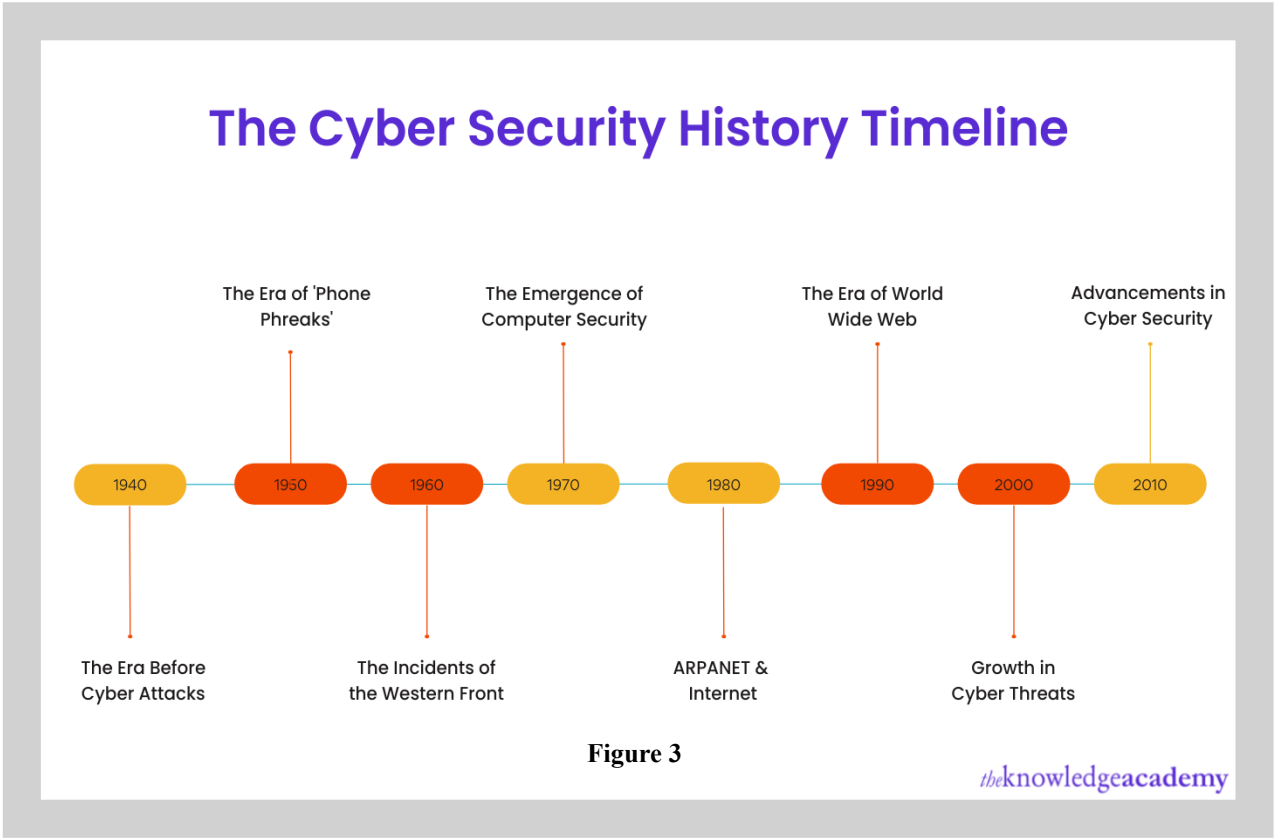

Figure 3

❖ CYBERSECURITY PRINCIPLES:

- Effective cybersecurity plans are built on fundamental rules and best practices known as **cybersecurity principles**. Protecting computer systems, networks and data from cyberattacks is crucial in the digital age where data and information are vital assets.
- These guidelines are intended to protect against unauthorized access, data breaches and other nefarious online actions.

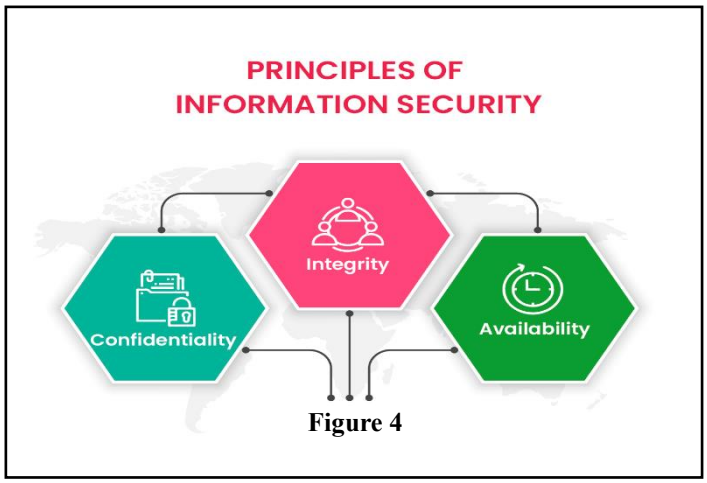

Figure 4

❖ Confidentiality:

This principle emphasizes the necessity to preserve secret and only allow authorized people to access to sensitive information. By guaranteeing that data remains encrypted throughout storage and transmission and allocating access rights in accordance with the principle of least privilege, encryption and access control play a critical role in upholding secrecy.

Maintaining the confidentiality of sensitive information is crucial in protecting an organization's competitive advantages, safeguarding customer and employee privacy and ensuring compliance with relevant laws and regulations.

❖ Some key concepts of confidentiality in cybersecurity are:

1. **Access control:** Restricting access to sensitive information based on the principle of least privilege.
2. **Encryption and Cryptography:** Applying strong encryption to protect data confidentiality.
3. **Physical security:** Implementing physical access controls and secure disposal of data.
4. **Security awareness and training:** Educating users on the importance of confidentiality.
5. **Incident response and breach management:** Promptly identifying, containing and mitigating confidentiality breaches.

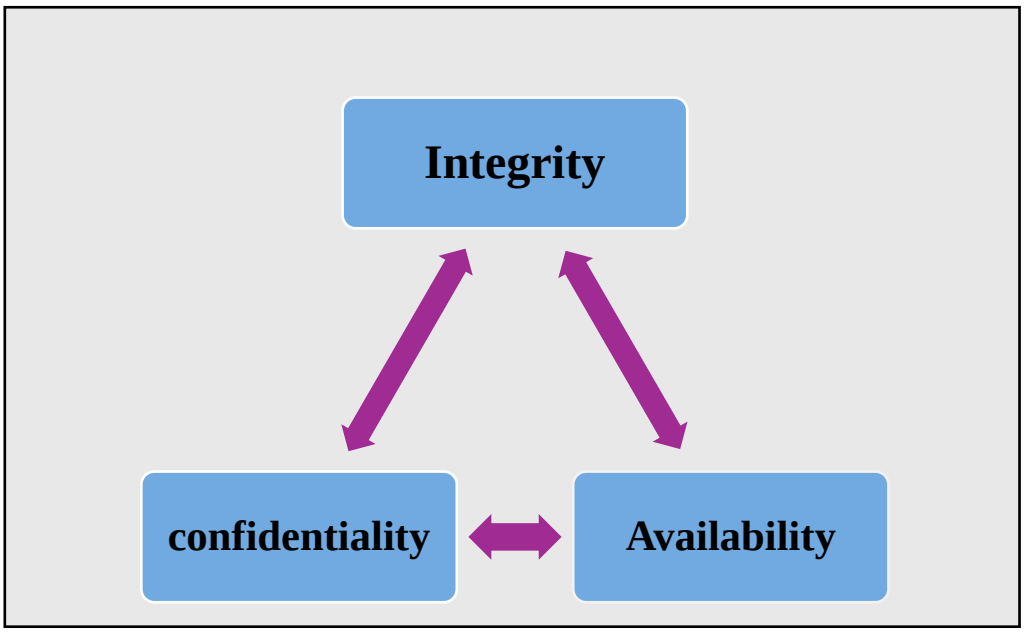

Figure 5

❖ Integrity:

Data integrity refers to the accuracy, consistency, and reliability of data over its entire lifecycle. It guarantees accurate and unaffected information. Data integrity is checked using cybersecurity tools like checksums, hashing and digital signatures, which enable the identification of any unauthorized changes or manipulation.

❖ There are several aspects to data integrity:

1. **Accuracy:** Data should be correct and free from errors.
2. **Consistency:** Data should be consistent across all instances and systems. In other words, if data is updated in one place, it should be updated everywhere it is stored or maintained.
3. **Reliability:** Data should be reliable and trustworthy.

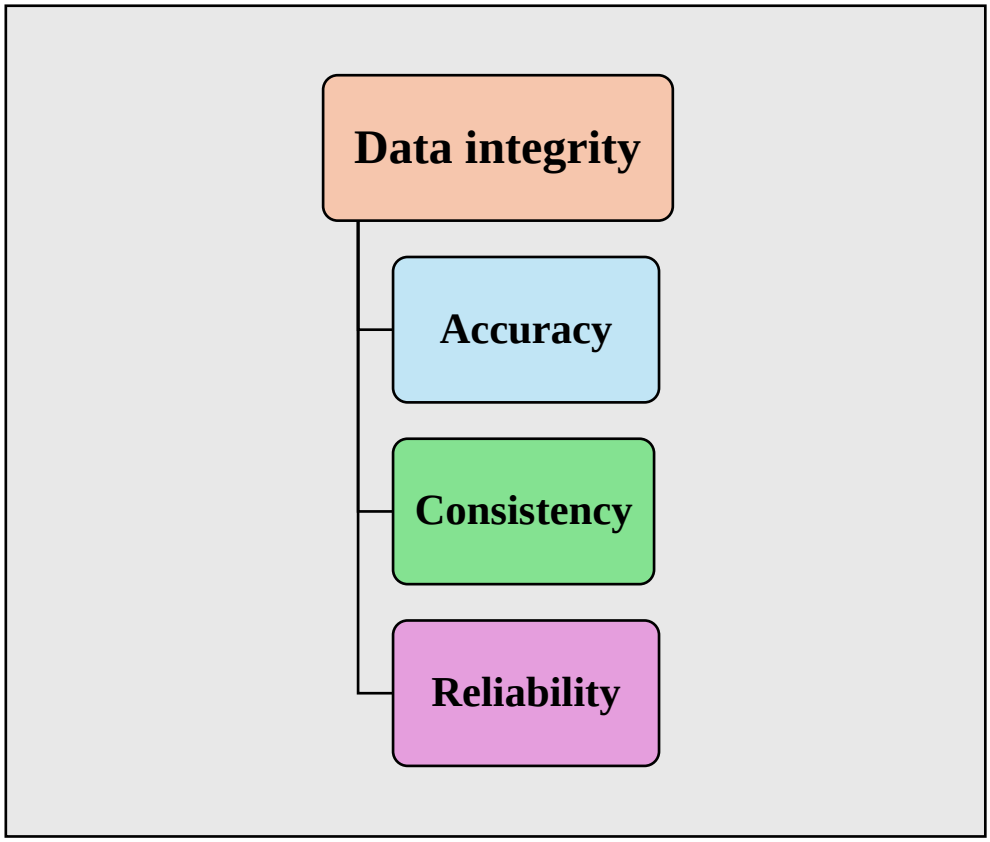

Figure 6

❖ Availability:

The availability principle guarantees that data, services, and systems are readily available and usable when required by authorized users or systems. Even in the face of cyberattacks or system failures, procedures including redundancy, load balancing and disaster recovery plans assist preserve ongoing access to crucial resources.

❖ Key components of data availability include:

1. Redundancy
2. Fault tolerance
3. Scalability
4. Monitoring and management
5. Disaster recovery

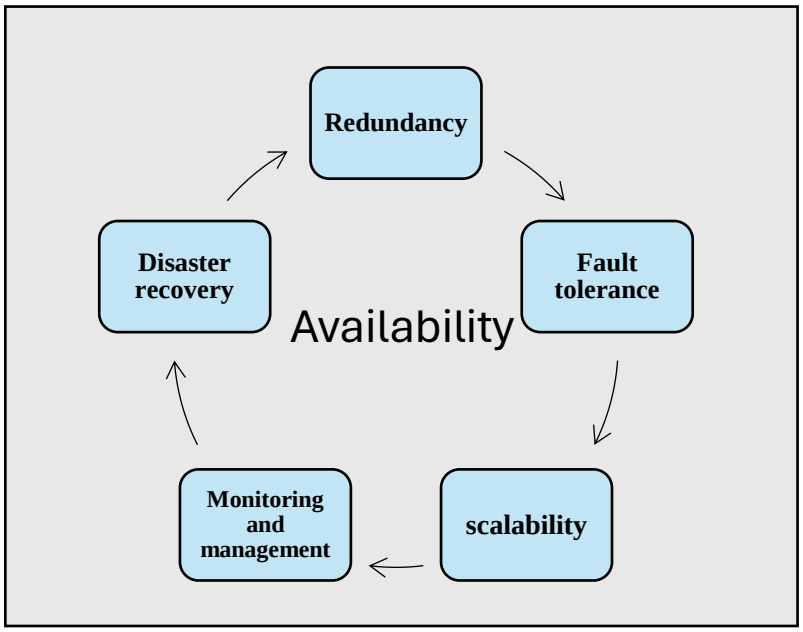

Figure 7

❖ COMMON TYPES OF CYBER ATTACKS:

- ❖ Cyberattacks are malicious and deliberate attempts to breach the security of a computer, system, network, or technology infrastructure with the intention of causing harm, stealing sensitive information, or disrupting operations.
- ❖ These attacks can take many forms, including hacking, malware, phishing, ransomware, denial of service and other types of cyberattacks.
- ❖ Cyberattacks can be launched by individuals, groups or nation-states, and ca be motivated by a variety of factors including financial gain, political ideology or simply to cause chaos and disruption.
- ❖ Cyberattacks can have serious consequences, including financial loss, reputational damage, and disruption of operations.

Attack types	Description
Malware	Software designed to harm or gain unauthorized access.
Phishing	Deceptive techniques to trick users into revealing info.
DoS and DDoS Attacks	Overwhelm systems with excessive traffic.
Data breaches	Unauthorized access to sensitive data.
Insider threats	Threats from within an organization.
Spyware	Software that Secretly gathers information about a person or organization without their consent or knowledge.
Ransomeware	Software that encrypts files or locks a device, demanding payment for their release.

❖ SOME COMMON CYBERCRIMES:

1. Cyber Bullying:

It is also known as online or internet bullying. It includes sending or sharing harmful and humiliating content about someone else which causes embarrassment and can be a reason for the occurrence of psychological problems. It has become very common lately, especially among teenagers.

2. Cyber Stalking:

Cyberstalking can be defined as unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating like unwanted continued calls and messages.

3. Software Piracy:

Software piracy is the illegal use or copy of paid software with violation of copyrights or license restrictions.

4. Social Media Frauds:

The use of social media fake accounts to perform any kind of harmful activities like impersonating other users or sending intimidating or threatening messages. And one of the easiest and most common social media frauds is Email spam.

5. Online Drug Trafficking:

With the big rise of cryptocurrency technology, it became easy to transfer money in a secure private way and complete drug deals without drawing the attention of law enforcement. This led to a rise in drug marketing on the internet.

❖ PROTECTION AGAINST CYBERCRIMES:

1. Keep software and operating system updated
2. Use anti-virus software and keep it updated
3. Use strong passwords
4. Never open attachments in spam emails
5. Do not click on links in spam emails or untrusted websites

6. Do not give out personal information unless secure
7. Contact companies directly about suspicious requests
8. Be mindful of which website URLs you visit
9. Keep an eye on your bank statements

❖ CONCLUSION:

Cyberspace offers immense benefits and opportunities as well as considerable threats and hazards. It is routinely exploited by a variety of adversaries, aggressors, and predators: hostile states; political extremists and terrorists; businesses practicing commercial espionage and theft; individuals and criminal organizations undertaking financial fraud and trafficking in people, armaments, and narcotics; and individual so-called 'nuisance' hackers. The efficient and effective response to these threats and hazards is what cybersecurity is all about. The idea that cybersecurity could also have a larger, more comprehensive, and progressive goal might seem to some to be fanciful: an unrealistic and other-worldly response to the very real possibility of encountering substantial harm in and from cyberspace.

THE END