International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 02 | February - 2023 Impact Factor: 7.185 ISSN: 2582-3930

CYBER SECURITY

Vinisha Bhagwani, Sakina Balasinorwala

KJ Somaiya Polytechnic VidyaVihar Mumbai..

Abstract:

"Cyber security has become a critical concern for individuals, businesses, and governments around the world. With the increasing reliance on technology and the internet, cyber attacks and data breaches have become more frequent and sophisticated. In this article, we examine the current state of cyber security and the most common types of cyber threats, including malware, phishing, and ransomware. We also explore best practices for individuals and organizations to protect themselves from cyber attacks, such as regularly updating software and using strong passwords. The results of our research highlight the importance of staying vigilant and proactive in the face of growing cyber threats. In conclusion, we discuss the need for continued investment in cyber security research and development to help keep pace with the evolving threat landscape".

Keywords: Cyber security, cyber attacks, technology, internet, data breaches, malware, phishing, ransomware, best practices, protection, investment, research and development.

Introduction:

"The rapid development of technology and the internet has brought many benefits to our lives, but it has also created new challenges, particularly in the realm of cyber security. With the increasing reliance on technology and the internet, cyber attacks and data breaches have become more frequent and sophisticated, posing a significant threat to individuals, businesses, and governments. In light of this growing concern, it is crucial to understand the current state of cyber security and the most common types of cyber threats, including malware, phishing, and ransomware.

In this article, we aim to provide a comprehensive overview of the current state of cyber security, examining the most common types of cyber threats and exploring best practices for individuals and organizations to protect themselves from cyber attacks. Our research highlights the importance of staying vigilant and proactive in the face of growing cyber threats, and the need for continued investment in cyber security research and development to help keep pace with the evolving threat landscape."

Purpose:

To examine the current state of cyber security and the most common types of cyber threats, such as malware, phishing, and ransomware..To explore best practices for individuals and organizations to protect themselves from cyber attacks, such as regularly updating software and using strong passwords. To present the results of research on cyber security, highlighting the importance of staying vigilant and proactive in the face of growing cyber threats.To discuss the need for continued investment in cyber security research and development to help keep pace with the evolving threat landscape.

History of Cyber Security [1]

Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks. It is also known as Information Security (INFOSEC) or Information Assurance (IA), System Security. The first cyber malware virus developed was pure of innocent mistakes. But cybersecurity has evolved rapidly because of the impeccable increase in the cybercrime law field on the Web. In this article, we will see the history of cyber security.

The Cybersecurity checking began in the 1970s when researcher Bob Thomas created a computer program called Creeper that could move across ARPANET's network. Ray Tomlinson, the innovator of email, wrote the program Reaper, which chased and deleted Creepers. Reaper was the very first example of checking a malware antivirus software and the first self-replicating program i.e. Viruses, as it made first-ever computer worms and trojans.

In 1971s, Programmer Bob Thomas made history by innovating a program that is widely accepted as the first incident ever computer trojan as the worm and trojan bounced between computers pc, which has groundbreaker at the time. The trojan was not at all malicious. Threats diversify and multiply in the 2000s:

In the early 2000s criminal organizations started to heavily fund professional cyberattacks and governments began to clamp down on the criminality of hackings, giving much money serious sentences to those culpable hackers and Information security continues to advance as the internet grows as well but, unfortunately so having the viruses**.[1]**

Timeline Of Cyber Security:

1970s: ARAPNET and the Creeper[2]

Cybersecurity began in the 1970s when researcher Bob Thomas created a computer programme called Creeper that could move across ARPANET's network, leaving a breadcrumb trail wherever it went. Ray Tomlinson, the inventor of email, wrote the programme Reaper, which chased and deleted Creeper. Reaper was the very first example of antivirus software and the first self-replicating programme, making it the first-ever computer worm.

1980s: Birth of the commercial antivirus

1987 was the birth year of commercial antivirus although there were competing claims for the innovator of the first antivirus product. Andreas Lüning and Kai Figge released their first antivirus product for the Atari ST – which also saw the release of Ultimate Virus Killer in 1987. Three Czechoslovakians created the first version of the NOD antivirus in the same year and in the US, John McAfee founded McAfee and released VirusScan.

1990s: The world goes online

With the internet becoming available to the public, more people began putting their personal information online. Organised crime entities saw this as a potential source of revenue and started to steal data from people and governments via the web. By the middle of the 1990s, network security threats had increased exponentially and firewalls and antivirus programmes had to be produced on a mass basis to protect the public.

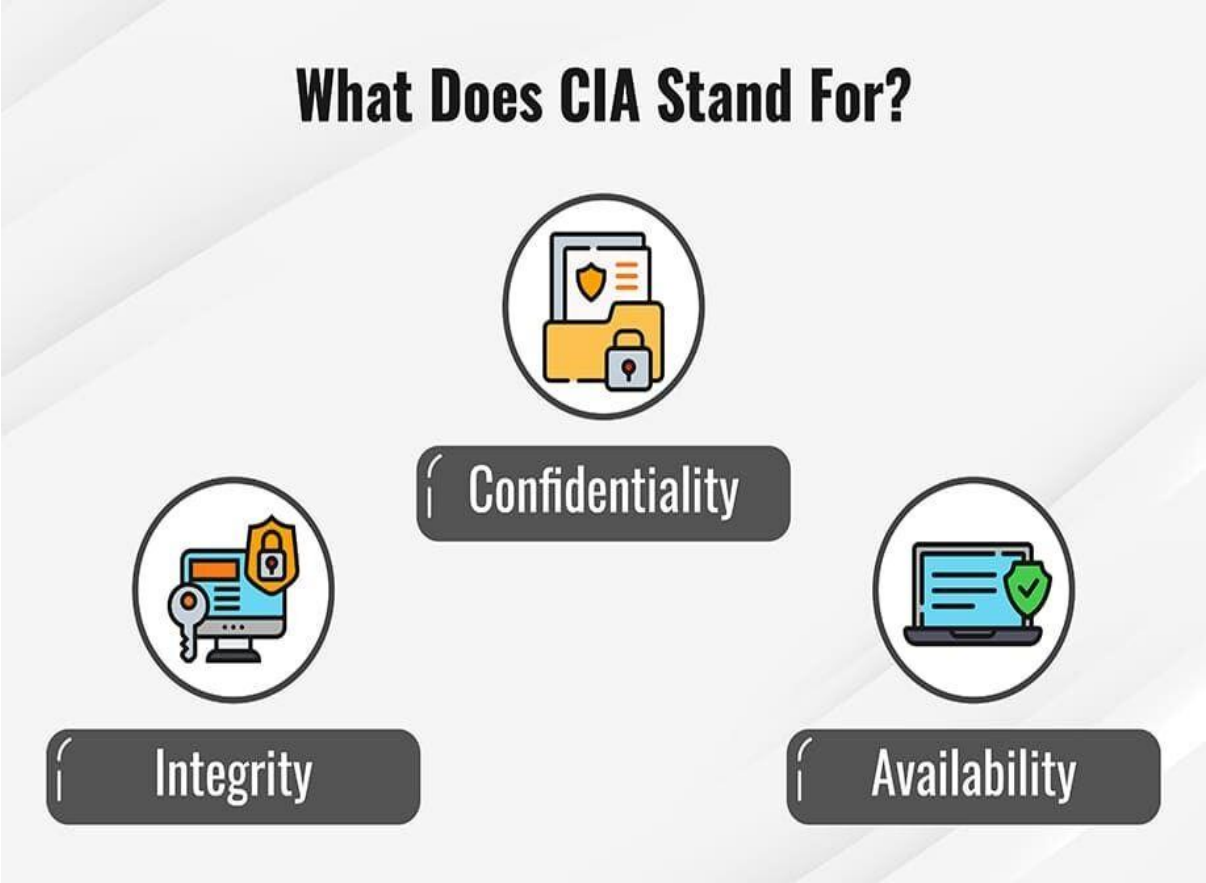
2000s: Threats diversify and multiply

In the early 2000s crime organisations started to heavily fund professional cyberattacks and governments began to clamp down on the criminality of hacking, giving much more serious sentences to those culpable. Information security continued to advance as the internet grew as well but, unfortunately, so did viruses.

2021: The next generation

The cybersecurity industry is continuing to grow at the speed of light. The global cybersecurity market size is forecast to grow to $345.4bn by 2026 according to Statista. Ransomware is one of the most common threats to any organisation's data security and is forecast to continue to increase**.[2]**

CIA Traid [3]



Important components of triad of information security are:

Confidentiality

The first part of the CIA triad is Confidentiality. This component focuses on who has access to what information and what they're able to do with it. Confidentiality usually involves segmenting data into specific groups and authenticating users' identities before they can gain access.

Integrity

The second part of the CIA triad is Integrity. This component seeks to protect data from modification or other forms of tampering by unauthorized sources. Integrity usually involves activity logging and data backup/recovery.

Availability

The third part of the CIA triad is Availability. This component ensures that the appropriate data is available to authorized users whenever they need it. Availability usually involves maintaining software updates, monitoring network bandwidth, and creating/updating business continuity plans**.[3]**

Examples of the CIA Triad in Practice [4]

1. Putting Confidentiality into Practice

Data encryption is one method to assure confidentiality so that unauthorized users cannot retrieve or access the data to which they do not have permission access. Access control is also an essential part of preserving confidentiality by governing which users have permission for accessing data. Healthcare organizations that collect and operate patient data must maintain confidentiality and comply with HIPAA.

2. Putting Integrity into Practice

Event log management whenever the Security Incident happens and an Event Management system are important for ensuring data integrity.Enforcing version control and audit trails to organizations IT structure will let your organization assure that its data is accurate and original.Integrity in cyber security is a crucial component for organizations with compliance necessities. For example, a condition of SEC compliance conditions for financial services institutions requires providing correct and complete data to federal regulators**. [4]**

What is Virus and Types?[5]

Computer viruses have the "virus" name because they resemble illnesses in the way they infect a system. Doctors can usually diagnose a virus based on symptoms exhibited by the body. IT professionals can do the same with computers. Typical signs of computer virus infections include:

- Ongoing crashes and blue screen errors
- Slow performance
- Missing files
- Low storage
- Unexpected behavior
- Constant browser pop-ups

- Unidentifiable programs
- Increased network activity
- Disabled security software

1. Resident Virus
Resident viruses set up shop in your RAM and meddle with your system operations. They're so sneaky that they can even attach themselves to your anti-virus software files.

2. Multipartite Virus
This virus infects the entire system – multipartite viruses spread by performing unauthorized actions on your operating system, folders, and programs.

3. Direct Action
This virus targets a specific file type, most commonly executable files (.exe), by replicating and infecting files. Due to its targeted nature, this virus type is one of the easier ones to detect and remove.

4. Browser Hijacker
Easily detected, this virus type infects your browser and redirects you to malicious websites.

5. Overwrite Virus
As the name implies, overwrite viruses overwrite file content to infect entire folders, files, and programs.

6. Web Scripting Virus
This sneaky virus disguises itself in the coding of links, ads, images, videos, and site code. It can infect systems when users download malicious files or visit malicious websites.**[5]**

Types Of Cyber Security:[6]

Cybersecurity can be categorized into five distinct types:

- Critical infrastructure security
- Application security
- Network security
- Cloud security
- Internet of Things (IoT) security

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

· **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization**.**

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:**Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

Phishing : Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information**.[6]**

WHAT IS CADM?[7]

Centralized Administration and Dynamic Monitoring framework (CADM) based on virtualization for network intrusion detection. CADM is able to centrally administrate, and monitor network behaviour in the virtual computing environment by automatically deploying and updating intrusion detection processes and rules. In the aspect of monitoring capability, CADM allows the monitoring locations in intrusion detection to be automatically adjusted in real time, thus adapting to the dynamic changes (such as migration) of virtual machines (VMs). Moreover, the monitoring processes involved in intrusion detection could also be automatically updated by dynamically updating security strategies. In the aspect of monitoring granularity, CADM is able to monitor network interfaces of each virtual machine (VM) for fine-grained network intrusion detection and network traffic acquisition. **[7]**

1. What are the five benefits of using cyber security? [8]

The five benefits of using cyber security are:

1. Increased protection of sensitive data
2. Reduced risks of data breaches
3. Enhanced detection and response to attacks
4. Improved overall security posture
5. Greater peace of mind

2. What are cyber security and its advantages?

Cyber security is the practice of protecting computer networks and user data from unauthorized access or theft. The advantages of cyber security include:

- The prevention of data breaches.
- Deterring cyber-attacks.
- Protecting the privacy of users.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure Wi-fi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks**.[8]**

Cybersecurity in the future After 2022:[9]

The cybersecurity industries are continuing to grow. The most global cybersecurity market size is forecast to grow to $345.4bn by 2026 according to Statista. Ransomware is one of the most common threats to any organization of data security and is forecast to continue to increase applications.

We live in a digital world where cyber security and cyber crimes are buzzwords. Everyone using the cyberspace should consider cyber security as a vital part of a well- ordered and well- preserved digital world. Let's first look into what cyber security actually means.

Cyber Security : Cyber security also known as "Information Technology Security" or "Computer Security" means safeguarding information, equipment, devices, computer, computer resources, communication devices and information stored therein from unauthorized access, use, disclosure, disruption, modification or revelation; according to IT Act, 2000**. [9]**

References:

1. https://www.geeksforgeeks.org/history-of-cyber-security/
2 .https://cybermagazine.com/cyber-security/history-cybersecurity

3.https://www.webopedia.com/definitions/cyber-security/

4.https://www.knowledgehut.com/blog/security/cia-in-cyber-security

5. https://hightouchtechnologies.com/9-common-types-of-computer-viruses/

6 - https://youtu.be/88-FENio9Yw
https://www.comptia.org/content/articles/what-is-cybersecurity

7.https://ieeexplore.ieee.org/document/6904241

8**. https://www.knowledgehut.com/blog/security/importance-of-cyber-security**

9**. Various Search Engines..**