Cyber Security in Focus: From Core Principles to Global Strategies

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

CONTENTS

Introduction

In a world increasingly reliant on digital technology, cybersecurity has become crucial. Cyber attacks, from data breaches to ransomware, are escalating in frequency and sophistication, impacting individuals, businesses, and governments alike. As the digital landscape evolves, so do the threats, requiring constant adaptation and innovation in security measures.

This paper explores the fundamentals of cybersecurity, examines emerging threats such as AI-driven attacks and quantum computing challenges, and highlights the importance of global cooperation in safeguarding our digital future. Understanding these elements is essential for navigating and protecting the increasingly complex digital world.

Cyber Security

According to the Cybersecurity and Infrastructure Security Agency (CISA): "Cyber Security is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring CIA triad.

CIA Triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

1) **C**onfidentiality: Ensures that information is accessible only to those authorized to view it. This involves protecting data from unauthorized access and breaches.

2) **I**ntegrity: Guarantees that information is accurate and unaltered. This means safeguarding data from unauthorized modification and ensuring that it remains reliable and trustworthy.

3) **A**vailability: Ensures that information and resources are accessible to authorized users when needed. This involves maintaining the operational performance of systems and preventing disruptions or downtime.

Why is Cyber Security Important?

1) Protecting Privacy – a fundemental right. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7).

2) Protecting sensitive data: Digitization of data has highlighted the need to protect sensitive information. A cyber attack that results in a data breach can expose trade secrets, intellectual property, and other sensitive information.

3) Safeguard critical infrastructure: Power grids, healthcare facilities, transportation systems, and communication networks have one thing in common. They all rely on interconnected computer systems. An attack on these systems can disrupt essential services and impact the safety of individuals. Malicious actors may intentionally exploit vulnerabilities in systems. This can cause disruption to vital operations.

4) Prevent financial loss: Cybercrime Magazine predicts that cybercrime will cost businesses across the world $10.5 trillion annually by 2025. Cybersecurity in the financial sector is vital as fraud and extortion are common. The costs of recovering from a cyber breach can be substantial. This can involve incident response, system repairs, and forensic investigations.

Why is Cyber Security Getting More Crucial?

1) Cyberspace grows faster than Cyber Security.

    a. Cyberspace is a word that was firstly used by William Gibson in his book Neuromancer in 1984. The word itself means “environment in which communication over computer network occurs” Cyberspace is defined as the dynamic and virtual space that connects the different computer systems. An analogy can be drawn between cyberspace and the human brain. Like there are innumerable neurons present in the brain, cyberspace has countless connections and networks that exist between the computer systems.

2) With the developments of AI cybercriminals are getting more sophisticated. Cyberattacks are taking new forms everyday.

3) With the more data becoming digitized with IoF (Internet of Things) the more data needs protection.

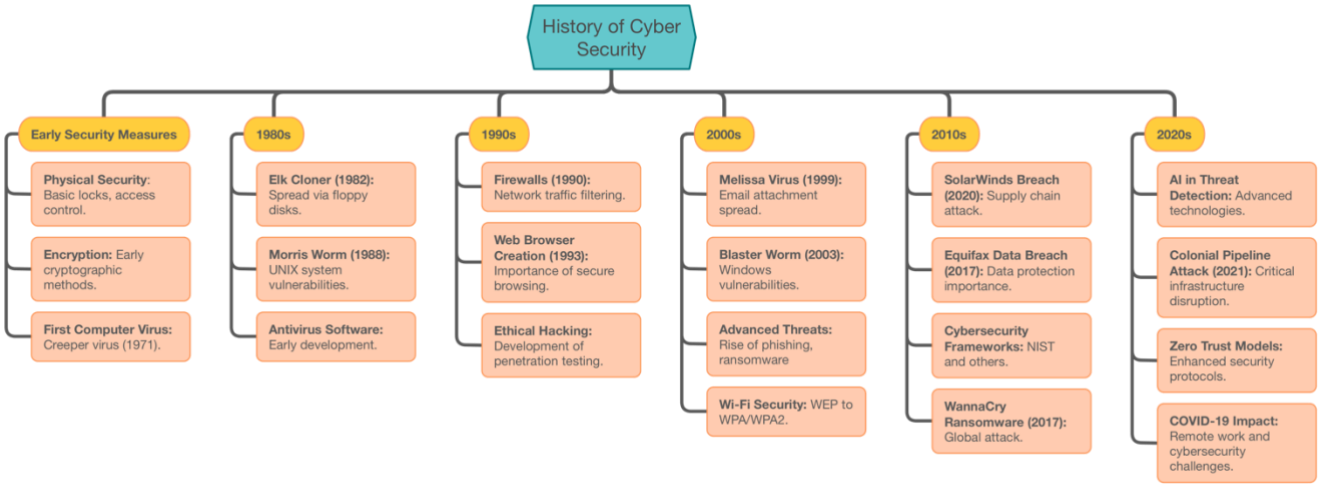
History of Cyber Security

1) Cybersecurity started with basic physical security for early mainframes and evolved with passwords, encryption, and access controls as networking emerged. The first computer security incident was the “Creeper” virus (1971), which marked the beginning of digital threats.
2) In the 1980s, the rise of personal computers and the internet introduced early viruses like “Elk Cloner” and the “Morris Worm”, leading to antivirus software and better practices. The 1990s brought firewalls and ethical hacking to address vulnerabilities.

3) The 2000s saw a rise in threats like worms, Trojans, and phishing, prompting the adoption of multi-factor authentication, VPNs, and intrusion detection systems. Advanced encryption was introduced to secure wireless networks.

4) By the 2010s, attacks like WannaCry ransomware and Stuxnet highlighted the need for comprehensive frameworks such as NIST's and emphasized cybersecurity education.

5) In 2020, the shift to remote work due to COVID-19 increased focus on securing remote environments, leading to the use of VPNs, secure collaboration tools, and advanced endpoint security. The SolarWinds breach underscored the importance of supply chain security and accelerated the adoption of zero-trust models.



Major Cyber Security Disciplines

1) Network Security: This involves protecting the entire network infrastructure from attacks and unauthorized access.
2) Application Security: Focuses on securing applications from vulnerabilities and threats. AppSec can be and should be applied during all phases of development, including design, development, and deployment.

3) Information Security: It is a set of security procedures and tools that broadly protect information from unauthorized access. InfoSec covers a range of IT domains, including infrastructure and network security, auditing, and testing.
4) Cloud Security: It procedures and technology designed to address external and internal threats to business security. Cloud infrastructure supports nearly all aspects of modern computing in all industries and across multiple verticals.
5) IoT (Internet of Things) Security: Internet of Things (IoT) devices are connected objects like security cameras and smart appliances. IoT security involves protecting these devices from network threats.
6) Endpoint Security: Endpoint security involves protecting devices like desktops, laptops, and mobile devices from cybersecurity threats. These endpoints can be potential entry points for cybercriminals to access organizational networks.

Cyber Security Threats

Cyber Security threats are malicious activities aimed at compromising CIA of data. These threats can cause data breaches, financial loses and reputational damages. These threats can come from individual hackers or organized crime groups.

1) Malware: A sofware that is designed to harm or exploit any programmable device, service network.

    - Viruses, Trojans,Worms, Botnets
    - Example: Wannacry Ransomware attack in 2017. Wannacry caused lots of computer getting damaged and also impacted medical services like UK or NHS greatly.
    - How to defend: Antivirus programs and conducting regular scan. Keeping devices updated so the vulnebalarities in them can be patched regularly. Some network security measures like Firewalls and IDS's can also prevent malicious softwares.

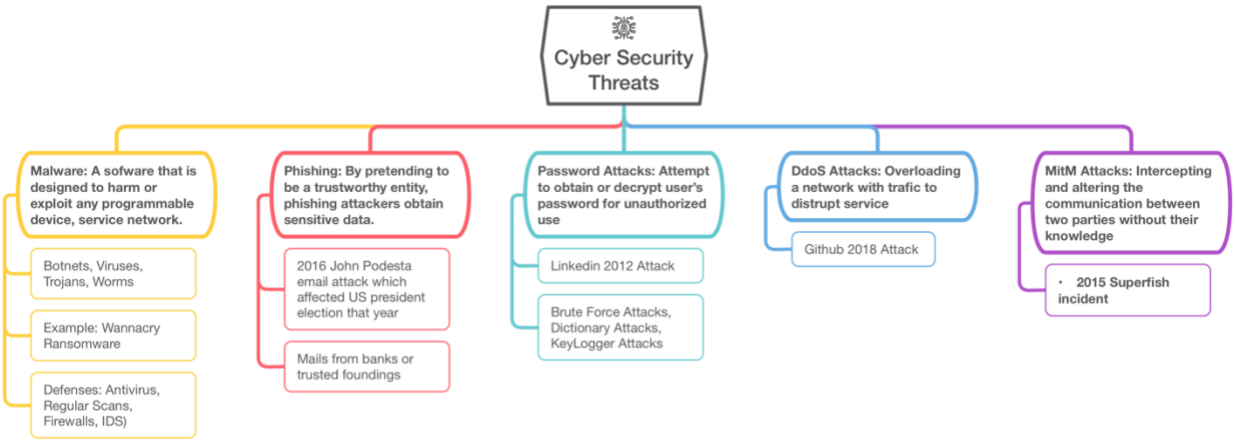
2) Phishing: They account more than %80 of reported security incidents.By pretending to be a trustworthy entity, phishing attackers obtain sensitive data.

    - Example: Mails from banks or trusted foundings. 2016 John Podesta email attack which affected US president election that year

3) Password Attacks: Attempt to obtain or decrypt user's password for unauthorized use

    - Example: Brute Force Attacks – Dictionary Attacks – KeyLogger Attacks. Linkedin 2012 Attack

4) DdoS Attacks (Distributed Denial of Service): Overloading a network with trafic to distrupt service.
    - Github 2018 Attack (Despite the attack being very large, github could mitigate it within a minute with usig DdoS protectin services
5) MitM Attack (Man in the Middle): Intercepting and altering the communication between two parties without their knowledge
    - 2015 Superfish incident



Cyber Security Frameworks

Frameworks are risk-based guidelines that help organizations assess their current cybersecurity practices and improve them. These frameworks provide a structured approach to managing cybersecurity risks. ISO and NIST Frameworks are two of the most referenced in cybersecurity. While both serve similar purposes, there are key differences.

1) **ISO 27001:** This is an international standard that specifies the requirements for an Information Security Management System (ISMS). It focuses on establishing, implementing, maintaining, and improving cybersecurity practices tailored to the organization's needs.
2) **NIST Cyber Security Framework (CSF):** Developed by the U.S. National Institute of Standards and Technology (NIST), this framework is aimed primarily at critical infrastructure sectors. It helps organizations identify, protect, detect, respond to, and recover from cybersecurity risks. NIST CSF is more flexible and less detailed compared to ISO 27001, making it easier for organizations to adapt.

3) **NIST 800-53:** This is a detailed regulatory document that provides security and privacy controls for federal information systems. It is more comprehensive than NIST CSF, covering a wide range of requirements, but it's more rigid and intended for government entities.

4) **Some Other Frameworks:**

- **COBIT**: A framework for the governance and management of enterprise IT. It helps organizations balance risk, resource use, and IT value.
- **ITIL**: Focuses on IT service management and includes best practices for providing quality IT services. ITIL Security Management is based on ISO 17799 and integrates security into IT service processes.
- **COSO**: Primarily a financial control framework that also influences risk management in IT security by requiring formal risk assessments.

Current Trends and Challenges in Cyber Security

1) AI and Machine Learning: Artificial intelligence (AI) is increasingly becoming a key component in the evolution of cybersecurity, offering advanced, automated, and proactive defense mechanisms against the ever-growing threat of cyberattacks. Traditional cybersecurity methods, while still vital, often fall short in the face of sophisticated attacks. AI steps in to fill this gap by analyzing vast amounts of data, learning from patterns and behaviors, and making real-time decisions without the need for human intervention. AI can detect and respond to cyber threats as they happen, reducing the time it takes to mitigate potential damages. It also helps in identifying vulnerabilities and predicting potential future attacks. By automating these processes, AI significantly reduces the workload on cybersecurity teams, allowing them to focus on more complex issues. However, it’s important to note that AI in cybersecurity is not a panacea. The effectiveness of AI-driven systems depends heavily on the quality of data and algorithms used. As cybercriminals also begin to harness AI for malicious purposes, the cybersecurity field will need to continue advancing AI technologies to stay ahead.

2) Cloud Security: Cloud computing offers flexibility and cost savings but brings unique security challenges.

    a. Challenges

        i. Data Breaches: Cloud environments can be targeted by hackers looking to steal sensitive information.
        ii. Insider Threats: Employees or contractors with access can accidentally or deliberately cause security issues.

iii. Data Loss: Data might be lost due to accidental deletion or provider outages, despite backup efforts.
iv. Compliance: Meeting various regulations for data protection can be complex, especially with international data.
v. Shared Responsibility: Security is shared between the cloud provider (who secures the cloud infrastructure) and the customer (who secures their data and applications).
vi. Misconfigurations: Incorrect settings can expose data to unauthorized access.

b. Strategies

i. Data Encryption: Encrypt data in transit and at rest to protect it from unauthorized access
ii. Access Controls: Use strong authentication and role-based access to limit who can access sensitive information.
iii. Regular Security Checks: Perform regular assessments to find and fix potential security issues.
iv. Monitoring and Logging: Track cloud activity to spot and respond to suspicious behavior quickly.
v. Incident Response: Have a plan in place for responding to and recovering from security incidents.
vi. Compliance: Ensure your cloud services meet legal and regulatory requirements.
vii. Employee Training: Educate staff on best security practices to reduce human errors.

Role of Governments and International Cooperation for Cyber Security

1. International Frameworks: Develop global cybersecurity standards and best practices for consistent security measures.
2. Information Sharing: Threat Intelligence: Share information about threats and vulnerabilities to improve collective defense.
3. Cross-Border Law Enforcement: Collaborate internationally to respond to cybercrimes that cross borders.
4. Capacity Building: Assist less-secure regions in improving their cybersecurity capabilities.
5. Cybersecurity Diplomacy: Engage in global discussions to establish responsible behavior in cyberspace and prevent conflicts

References

1. Planet Compliance. (2022, November 30). *Financial cybersecurity: Third-party risk*. Planet Compliance. https://www.planetcompliance.com/financial-cybersecurity-third-party-risk/

2. Vedantu. (2024). *Introduction to cyberspace*. Vedantu. https://www.vedantu.com/commerce/introduction-to-cyberspace

3. IBM. (n.d.). *Cloud security*. IBM. https://www.ibm.com/topics/cloud-security

4. Kaspersky. (n.d.). *What is endpoint security?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security

5. Microsoft. (n.d.). *What is information security (Infosec)?* Microsoft. https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec

6. Institute Data. (2024, April 2). *What are the 7 types of cybersecurity?* Institute Data. https://www.institutedata.com/blog/what-are-the-7-types-of-cyber-security/

7. Tunggal, A. T. (2024, April 25). *Why cybersecurity is important*. UpGuard. https://www.upguard.com/blog/cybersecurity-important

8. Bayuk, J. [Jennifer Bayuk]. (2019, October 22). *The history of cybersecurity* [Video]. YouTube. https://www.youtube.com/watch?v=lvxFE-HO7oc

9. 51Sec. (2018, December). *Cyber security frameworks & resources*. 51Sec. https://blog.51sec.org/2018/12/cyber-security-frameworks-resources.html#point14