Journal of Management and Service Science, 2024,
Vol. 04, Iss. 01, S. No. 049, pp. 1-13
ISSN (Online): 2583-1798

Cybersecurity: An In-Depth Analytical Review

Kushagra Srivastava[1]*, P. Singh[2]

[1,2]Amity School of Engineering & Technology, Amity University Uttar Pradesh, Lucknow, India
[1]skushagra645@gmail.com, [2]pawansingh51279@gmail.com

How to cite this paper: K. Srivastava and P. Singh, "Cybersecurity: An In-Depth Analytical Review," *Journal of Management and Service Science (JMSS),* Vol. 04, Iss. 01, S. No. 049, pp. 1-13, 2024.

https://doi.org/10.54060/a2zjournals.jmss.49

Received: 07/06/2023
Accepted: 01/03/2024
Online First: 09/04/2024
Published: 25/04/2024

Abstract

This study highlights cybersecurity's core elements and their function in protecting digital systems and data while also providing an overview of the technology's fun-da-mental operation. The research places a focus on the necessity of a proactive and layered approach to defense as well as the significance of cybersecurity in defending organizations from cyber threats. Various security measures are covered, such as network security and access controls. In order to foster a security-conscious culture, the research also looks at the importance of user awareness and training. Organizations can build a strong foundation for risk management, preventing unauthorized access, and guaranteeing the honesty, reliability, and accessibility of their critical in increasingly interconnected and threat-prone digital landscape by understanding the fundamental functionality of cybersecurity.

Keywords

Cybersecurity, Security Frameworks, Cyber Threats, Incident Response, Data Protection, Technical Aspects, Security Controls.

1. Introduction

Cybersecurity, usually referred to as security, is the process of guaranteeing the privacy, availability, and accuracy of data by defending systems, devices, users, and data from unauthorized access or malicious use.

1.1. History and Evolution of Cybersecurity

The evolution of cybersecurity has been driven by technology and emerging threats. It started with physical security measures and progressed to protect digital information. The rise of malware and viruses led to essential antivirus software. The internet brought new vulnerabilities, requiring firewalls, IDS, and VPNs. Encryption and secure communication became vital for e-commerce. A paradigm shifts towards proactive approaches emphasized risk management frameworks. Mobile and cloud technologies introduced new challenges, addressed through MDM and cloud security measures. Advanced threats like APTs and ransomware posed significant challenges. Collaboration and awareness among stakeholders are emphasized. Contributions from cryptographers like Claude Shannon and Whitfield Diffie, security re-searchers, ethical hackers, cybersecurity experts like Bruce Schneir, government agencies like the NSA and FBI, technology companies like IBM and Microsoft, academic institutions, and international organizations play crucial roles in advancing cybersecurity. Ongoing innovation, collaboration, and awareness are essential to protect digital systems and data [1].

1.2. Importance

In the current digital era, cybersecurity is of utmost importance, particularly for protecting sensitive and personally identifiable information (SPII) and personally identifiable information (PII). SPII includes extremely private data such as medical records and biometrics, whereas PII includes information like names, addresses, and financial information. Identity theft, A few of the negative outcomes that can occur include money losses and reputational damage from PII and SPII breaches [2]. The confidentiality, integrity, and availability of such data are ensured by placing a high priority on cybersecurity, shielding people, businesses, and governments from harm. We can reduce risks, stop breaches, safeguard the privacy and security of PII and SPII, and promote confidence in online interactions by putting strong cybersecurity measures in place.

1.3. Current state of cybersecurity threats and challenges

The current state of cybersecurity is marked by an ever-evolving landscape of threats and challenges. As technology advances and becomes increasingly integrated into our daily lives, new vulnerabilities emerge, and cybercriminals continuously devise sophisticated tactics to exploit them. Here are some key aspects of the current cybersecurity landscape:

i. **Advanced Persistent Threats (APTs):** APTs are persistent and targeted attacks often sponsored by nation-states or organized cybercriminal groups. These threats employ sophisticated techniques to infiltrate networks, exfiltrate data, and remain undetected for extended periods. As of 2021, APTs were responsible for a significant portion of data breaches. For example, according to a report by Mandiant, APT groups were responsible for 41% of all cyber incidents in 2020 [4].

ii. **Ransomware Attacks:** Ransomware attacks have become a prevalent and lucrative form of cyber-crime. Malicious actors use ransomware to encrypt data, rendering it inaccessible until a ransom is paid. Recent attacks have targeted organizations of all sizes, including hospitals, government agencies, and businesses, causing significant disruptions and financial losses. In 2020 and 2021, there was a notable increase in the frequency and severity of ransomware attacks. One of the most prominent ransomware incidents during this period was the Colonial Pipeline attack, which resulted in a $4.4 million ransom payment.

iii. **Supply Chain Attacks:** Supply chain attacks involve compromising trusted software or hardware providers to infiltrate target organizations. This method exploits the trust placed in third-party suppliers, allowing cybercriminals to gain unauthorized access to networks and systems. Notable examples include the SolarWinds and Kaseya incidents, which impacted numerous organizations worldwide.

iv. **Social Engineering and Phishing:** Cybercriminals continue to rely on social engineering techniques and phishing attacks to deceive individuals and gain unauthorized access to sensitive information. Phishing emails, smishing (SMS

phishing), and vishing (voice phishing) attempts have become increasingly sophisticated. In 2020, the FBI's Internet Crime Complaint Center (IC3) received over 28,000 complaints related to phishing attacks, with reported losses exceeding $57 million [5].

v. **Cloud Security Risks:** With the widespread adoption of cloud computing, securing cloud environments has become paramount. Misconfigurations, unauthorized access, and data breaches in cloud ser-vices can lead to significant data exposure. Additionally, shared responsibility models require organizations to understand their respective security responsibilities when using cloud platforms. Misconfigurations in cloud environments were a prevalent issue. In 2020, a Gartner report predicted that 99% of cloud security failures would be the customer's fault due to misconfiguration.

Overall, the current state of cybersecurity presents a complex and dynamic landscape that requires constant vigilance, collaboration, and innovation to mitigate risks and protect critical systems and data.

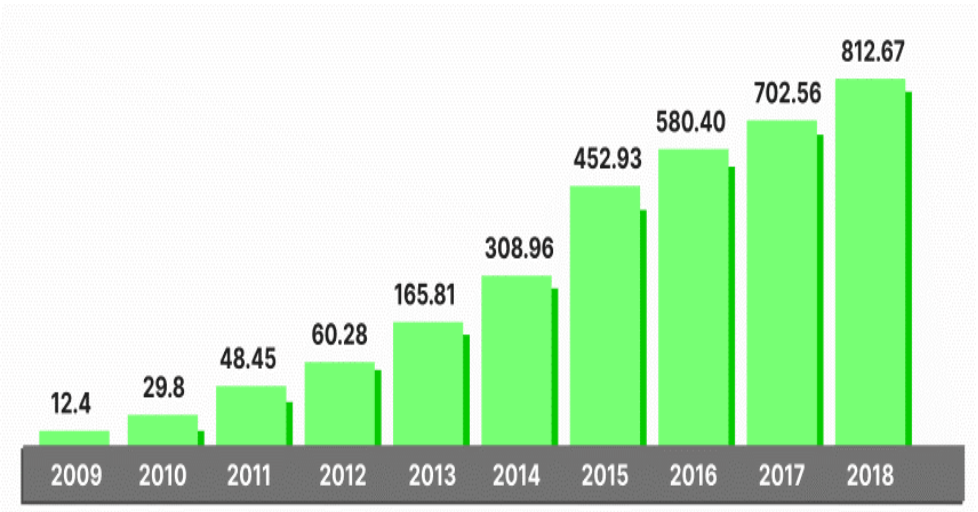

Figure 1. Total Malware Infection Growth Rate (in millions)

2. Types of Cyber Threats

Cyber threats encompass a wide range of malicious activities that aim to exploit vulnerabilities in digital systems, networks, and data [6]. Here are various types of cyber threats along with explanations and examples for each category:

A. Malware

Malware refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples include:

a. Viruses: Self-replicating programs that attach themselves to legitimate files and spread when those files are executed.

b. Trojans: Disguised as legitimate software, Trojans trick users into installing them, allowing attackers to gain unauthorized access or control over the infected system.

c. Ransomware: Encrypts a victim's data and demands a ransom in exchange for its release. Examples include WannaCry and NotPetya. In 2020, ransomware attacks increased by a staggering 485%, with the global cost estimated at over $20 billion.

B. Phishing

Phishing attacks involve the use of deceptive tactics to trick individuals into revealing sensitive information. Examples include:

a. Email Phishing: Cybercriminals send fraudulent emails posing as reputable entities, tricking users into clicking on malicious links or providing personal information. In the first quarter of 2021 alone, the number of phishing websites detected increased by 47%.

b. Spear Phishing: Targeted phishing attacks tailored to specific individuals or organizations. Attackers research their targets to increase the chances of success.

c. Whaling: Phishing attacks targeting high-profile individuals such as executives or CEOs to gain access to sensitive corporate data.

C. Distributed Denial of Service (DDoS)

DDoS attacks overwhelm a targeted system or network with an overwhelming volume of traffic, rendering it inaccessible to legitimate users. Examples include:

a. Botnet Attacks: A network of compromised computers (botnets) is used to flood a target with traffic. Notable botnet-based attacks include the Mirai botnet.

b. Application Layer Attacks: Exploit vulnerabilities in specific applications or services to over-whelm targeted servers.

In the first half of 2020, DDoS attacks increased by 20%, with the largest attack reaching a peak of 2.3 terabits per second.

D. Man-in-the-Middle (MitM) Attacks

MitM attacks intercept and manipulate communication between two parties without their knowledge. Examples include:

a. Wi-Fi Eavesdropping: Attackers intercept Wi-Fi communications to capture sensitive information transmitted over unsecured networks.

b. Session Hijacking: Unauthorized interception and control of an ongoing session between a user and a system.

E. Insider Threats

Insider threats involve individuals within an organization who misuse their access privileges to cause harm or gain unauthorized access. Examples include:

a. Malicious Insiders: Employees or contractors with authorized access who deliberately steal or leak sensitive information or sabotage systems.

b. Negligent Insiders: Employees who unintentionally cause harm or compromise security through negligence or lack of awareness.

F. Social Engineering

Social engineering attacks exploit human psychology and manipulate individuals into revealing sensitive information or performing actions. Examples include:

a. Pretexting: Attackers impersonate someone else to deceive individuals into disclosing information or performing actions.

b. Baiting: Lures individuals with enticing offers or rewards to trick them into taking malicious actions.

Understanding these various types of cyber threats is crucial for implementing appropriate security measures and staying vigilant to protect against potential attacks.

Table 1. Types of Cyber Threats

Threat	Description	Examples	Potential Impact
Malware	Malicious software designed to harm or gain access.	Viruses, Trojans, Ransomware	Data loss, system damage
Phishing	Deceptive tactics to trick individuals.	Email phishing, Spear phishing	Identity theft, data breach
Distributed Denial of Service (DDoS)	Overwhelming a system with traffic.	Botnet attacks, Application layer attacks	Service disruption, data loss
Man-in-the-Middle (MitM) Attacks	Intercepting and manipulating communication.	Wi-Fi eavesdropping, Session hijacking	Data interception, fraud
Insider Threats	Misuse of access privileges within an organization.	Malicious insiders, Negligent insiders	Data theft, sabotage
Social Engineering	Exploiting human psychology to deceive.	Pretexting, Baiting, Whaling	Data disclosure, unauthorized access

2.1. Consequence of cyber threats

Cyber threats have significant impacts on individuals, businesses, and society, resulting in financial, reputational, and operational consequences [7-10].

A. **Financial Consequences:** Cyber-attacks lead to financial losses through fraud, ransom payments, and business disruptions.
B. **Reputational Damage:** Breaches damage trust, erode customer confidence, and result in legal and regulatory repercussions.
C. **Operational Disruptions:** Attacks cause service interruptions, data loss, destruction, and damage to critical infrastructure.
D. **Societal Impact:** Cyber threats affect economies, national security, and privacy, leading to broader societal implications.

Understanding these impacts highlights the need for robust cybersecurity measures and awareness to mitigate risks and protect against the consequences of cyberattacks.

3. Security Frameworks and Control

i. Security controls are specific safeguards that reduce risks, while a security framework provides management guidelines for security measures.
ii. A security framework is a methodical approach that outlines how security controls should be implemented within a company to establish a strong security posture.
iii. Security controls are procedures that safeguard assets and mitigate risks.
iv. Both the security framework and controls guarantee the privacy and accessibility of data and systems.
v. They support policy development, risk identification, and the implementation of security measures.
vi. Organizations can protect themselves, secure sensitive information, and foster trust by implementing a thorough framework and strong controls.
vii. Regular evaluations consider new risks and technology to ensure ongoing effectiveness.

Table 2. Comparison of Security Frameworks

Framework	Key Control Categories	Description
NIST CSF	Identify, Protect, Detect, Respond, Recover	A flexible framework emphasizing risk management and cybersecurity practices.
ISO 27001	Risk assessment, Security policies, Asset management	An international standard for information security management systems.
CIS Controls	Inventory and control of hardware, Continuous vulnerability management	A set of prioritized actions for improving an organization's cybersecurity posture.

3.1. CIA Triad

"The Confidentiality, Integrity, and Availability (CIA) triangle" is a fundamental idea in information security. Sensitive data is shielded from unauthorized access thanks to confidentiality. Integrity prevents unauthorized modifications, ensuring the reliability and correctness of information. Availability guarantees that data and systems are usable when required. A compromise in any of these three principles could have an effect on the others because they are linked. Organizations may safeguard data, uphold trust, adhere to legislation, and respond to security issues efficiently by following the CIA triangle.

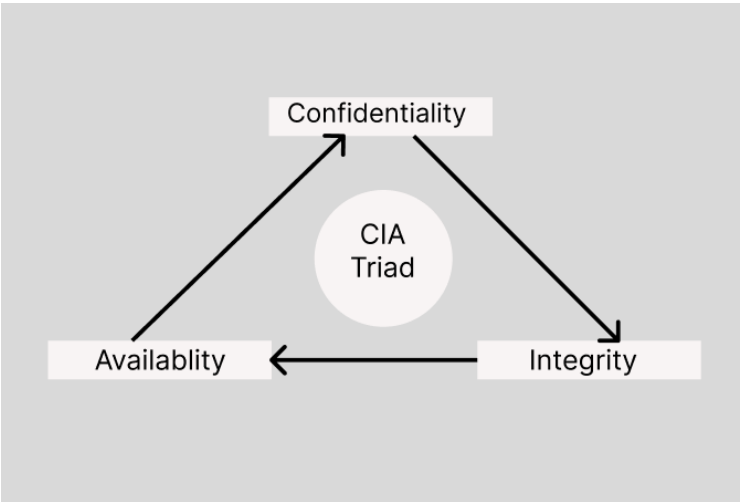

Figure 2. CIA TRIAD

3.2. NIST CSF

A thorough set of standards and best practices called the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is created to assist organizations in enhancing their cybersecurity capabilities. By concentrating on five fundamental functions—Identify, Protect, Detect, Respond, and Recover—it offers a disciplined method for addressing cybersecurity threats. The framework gives businesses the ability to evaluate their existing cybersecurity posture, set cybersecurity objectives, and put policies in place to efficiently identify, guard against, and recover from cybersecurity incidents. It is a flexible and adaptable framework that can be customized to meet the unique requirements and needs of numerous businesses in different industries.

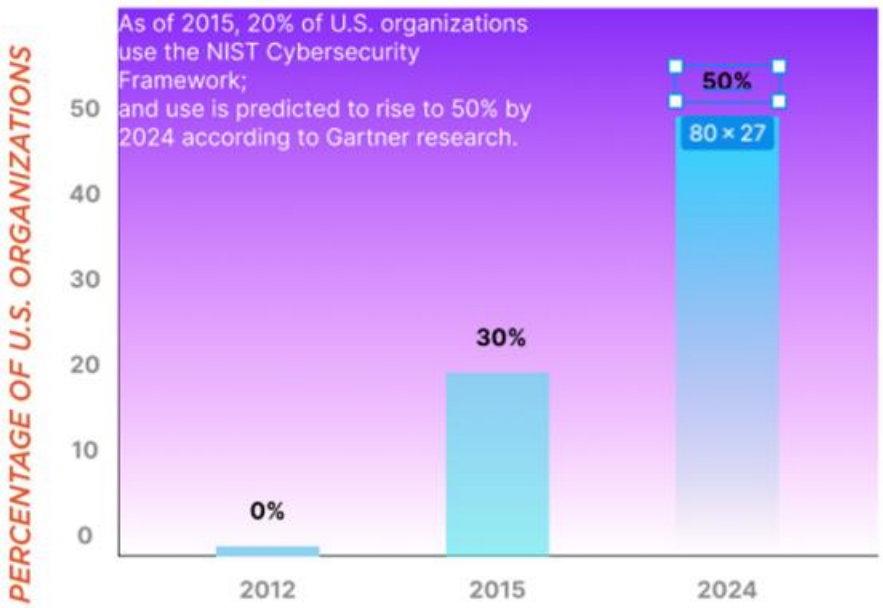

Figure 3. NIST Framework usage as of 2015

4. Technical Aspects of Cybersecurity

Technical aspects play a crucial role in the implementation of effective cybersecurity measures. Here are various technical aspects and commonly used tools and technologies in cybersecurity:

A. Network Security Mechanisms

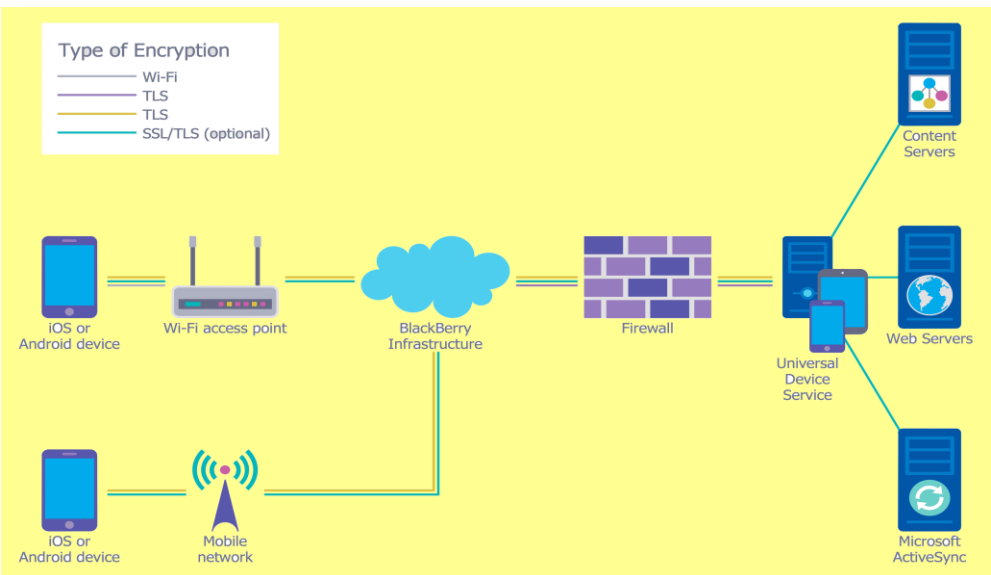

Figure 4. Network Security Topology

a) **Firewalls:** Firewalls control incoming and outgoing network traffic based on predetermined security rules, helping to protect against unauthorized access.
b) **Intrusion Detection Systems (IDS):** IDS monitors network traffic and identify potential security breaches or suspicious activities.
c) **Intrusion Prevention Systems (IPS):** IPS go beyond IDS by actively blocking or mitigating identified threats.
d) **Virtual Private Networks (VPNs):** VPNs establish secure encrypted connections over public networks, ensuring secure data transmission.

B. Vulnerability Assessment Tools

a) **Nessus:** Nessus is a popular vulnerability scanning tool that identifies vulnerabilities in systems, networks, and applications.
b) **OpenVAS:** OpenVAS is an open-source vulnerability scanner that helps identify and manage security vulnerabilities.
c) **Qualys:** Qualys provides cloud-based vulnerability management solutions for organizations to assess and prioritize vulnerabilities.

Table 3. Vulnerability Assessment Tools

Tool	Features	Scanning Speed	Ease of Use	Cost
Nessus	In-depth scanning, extensive plugin library	Fast	Moderate	Paid
OpenVAS	Open-source, vulnerability management	Moderate	Moderate	Free
Qualys	Cloud-based, scalable, continuous scanning	Fast	Easy	Paid

C. Security Information and Event Management (SIEM) Tools

a) **Splunk:** Splunk is a SIEM tool that collects and analyses security event data from various sources, providing real-time monitoring and alerting.
b) **ArcSight:** ArcSight offers a comprehensive SIEM platform for security monitoring, threat detection, and compliance management.
c) **LogRhythm:** LogRhythm combines SIEM functionality with security analytics to detect and respond to security threats.

D. Penetration Testing Tools

a) **Metasploit:** Metasploit is a widely used framework for penetration testing and vulnerability assessment, offering a range of tools and exploits.
b) **Burp Suite:** Burp Suite is a web application testing tool that helps identify and exploit vulnerabilities in web applications.
c) **Nmap:** Nmap is a network scanning tool used for network mapping, identifying open ports, and detecting potential vulnerabilities.

E. Encryption Techniques

a) **Public Key Infrastructure (PKI):** PKI provides the framework for secure communication, authentication, and encryption through the use of public and private key pairs.

b) Secure Sockets Layer (SSL) / Transport Layer Security (TLS): SSL/TLS protocols encrypt data transmitted over the internet, ensuring confidentiality and integrity.

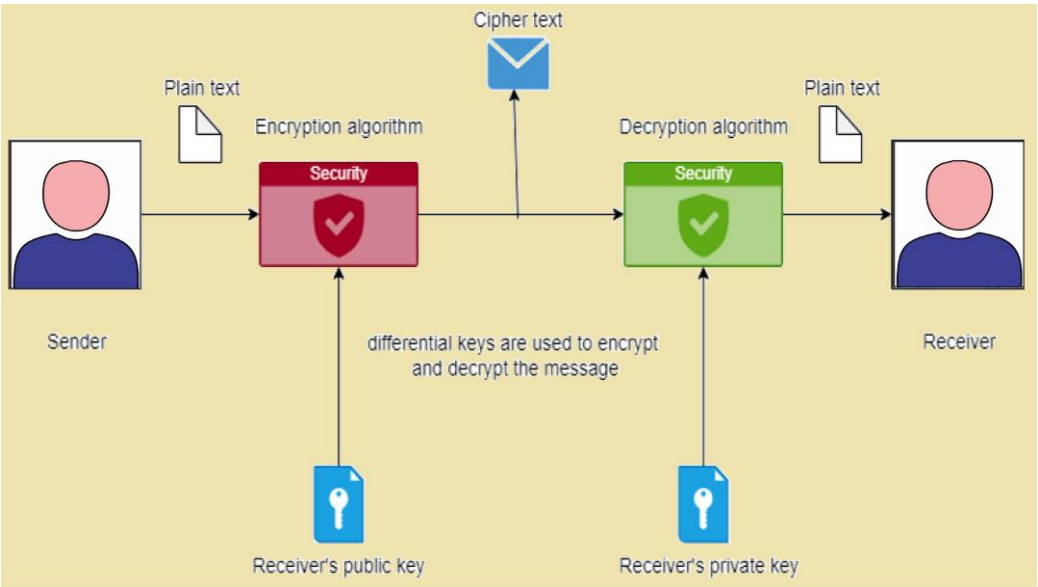

Figure 5. Encryption Procedure

F. Endpoint Protection Tools

a) Antivirus Software: Antivirus software detects, prevents, and removes malware from endpoint devices.

b) Anti-malware Software: Anti-malware tools provide broader protection against a range of malicious software beyond traditional viruses.

c) Host-Based Intrusion Detection Systems (HIDS): HIDS monitors and analyzes activities on individual endpoints, detecting potential intrusions or suspicious behavior.

G. Security Monitoring and Analytics Tools

a) Security Information and Event Management (SIEM) Solutions: SIEM solutions collect and analyze security event data from various sources for real-time threat detection and response.

b) Security Analytics Platforms: Security analytics platforms leverage advanced analytics techniques to detect patterns, anomalies, and indicators of compromise.

These tools and technologies serve as critical components in safeguarding digital systems, networks, and data, enabling organizations to detect, prevent, and respond to cyber threats effectively. Their proper implementation and utilization contribute to an enhanced cybersecurity posture.

Table 4. Technical aspect of cybersecurity and respective tools

S.No.	Technical Aspects of Cybersecurity			
	Aspects	**Tools Used**		
1.	**Network Security Mechanisms**	Firewalls	Intrusion Detection System(IDS)	Virtual Private Network(VPN's)
2.	**Encryption Techniques**	Public Key Infrastructure (PKI)	Secure Sockets Layer (SSL)	Transport Layer Security (TLS)
3.	**Vulnerability Assessment Tools**	Nessus	OpenVas	Qualys
4.	**Security Information and Event Management (SIEM) Tools**	Splunk	ArcSight	LogRhythm
5.	**Penetration Testing Tools**	Metasploit	Burp Suite	Nmap
6.	**Endpoint Protection Tools**	Antivirus Software	Anti-Malware	Host-based Intrusion Detection Systems (HIDS)
7.	**Security Monitoring and Analytics Tools**	Security Analytics Platforms	Security Information and Event Management (SIEM) Solutions	

5. Human Factors in Cybersecurity

Human factors play a crucial role in maintaining a strong cybersecurity posture. Despite the presence of advanced technologies and security measures, humans remain susceptible to social engineering techniques, making user awareness and training essential in combating cyber threats. Here are key aspects related to human factors in cybersecurity:

A. User Awareness and Training:

User awareness is paramount in creating a security-conscious culture. Individuals should be educated about common cyber threats, best practices for secure behaviors, and the importance of maintaining strong passwords, avoiding phishing emails, and exercising caution while browsing or downloading files.

B. Social Engineering Techniques:

Social engineering exploits human behaviors and psychology to deceive individuals and gain unauthorized access to systems or sensitive information. Techniques include phishing, pretexting, baiting, and tailgating. Training users to recognize and report suspicious activities, and implementing robust authentication mechanisms, helps mitigate the risks associated with social engineering attacks.

C. Creating a Security-Conscious Culture:

Organizations should foster a security-conscious culture that prioritizes cybersecurity at all levels. This involves establishing clear security policies and procedures, conducting regular security training, and promoting open communication channels to report potential threats. Encouraging employees to actively participate in security initiatives and rewarding positive security behaviors reinforces a culture of security awareness.

D. Multi-Factor Authentication (MFA):

Implementing multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of authentication, such as a password and a unique code sent to their mobile device. This helps protect against unauthorized access even if passwords are compromised.

Table 5. Social Engineering Techniques

Technique	Description	Recognizing Signs	Mitigation Tips
Phishing	Deceptive emails or messages to steal data.	Check sender's email address, verify requests.	Educate users, use email filters, report suspicious emails.
Pretexting	Inventing a scenario to manipulate individuals.	Verify identities, question unusual requests.	Establish verification procedures, train employees.
Baiting	Luring victims with enticing offers or rewards.	Be cautious of offers, avoid downloading from untrusted sources.	Verify the source, use updated software.

6. Cybersecurity Incident Response

Incident response planning and preparedness are essential components of an effective cybersecurity strategy. They help organizations proactively address potential cybersecurity incidents, minimize damage, and quickly recover from attacks. Here are the reasons why incident response planning and preparedness are crucial:

A. **Timely Response:** Incident response planning ensures that organizations have a well-defined process in place to promptly detect, assess, and respond to cybersecurity incidents. By having a plan in advance, organizations can minimize the time between incident detection and response, reducing the potential impact and mitigating further damage.

B. **Minimize Impact:** Effective incident response planning aims to limit the impact of a cybersecurity incident on an organization's operations, reputation, and data. By quickly containing the incident and implementing appropriate mitigation measures, organizations can prevent the escalation of an attack, minimize data breaches, and reduce financial losses.

C. **Compliance and Legal Requirements:** Incident response planning helps organizations meet compliance and legal obligations related to cybersecurity. Many regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), require organizations to have incident response plans in place to protect sensitive data and respond to breaches effectively.

D. **Reputation Management:** A well-handled incident response can positively impact an organization's reputation. Demonstrating a swift and effective response to a cybersecurity incident can instill confidence in customers, partners, and stakeholders, showing that the organization takes cybersecurity seriously and is committed to protecting their data.

The stages of incident response are : detection, analysis, containment, and recovery.

A. **Detection:** Identifying and confirming a cybersecurity incident using tools like intrusion detection systems and log analysis to detect suspicious activities or indicators of compromise.

B. **Analysis:** Investigating the incident to understand its nature, scope, and potential impact. Gathering evidence, assessing affected systems, identifying vulnerabilities, and understanding the attacker's tactics, techniques, and motives.

C. **Containment:** Isolating the affected systems, preventing further damage, and stopping the attacker's access. Taking steps like disconnecting compromised systems, resetting passwords, or implementing firewall rules to limit the incident's impact.

D. **Recovery:** Restoring affected systems and data to their normal state. Removing malware, repairing or replacing compromised systems, and restoring backups. Documenting lessons learned to enhance future incident response efforts.

Digital forensics is essential for investigating cybersecurity incidents. It collects, analyzes, and preserves digital evidence to determine the cause, impact, and extent of an incident. It helps identify attackers, track their actions, and gather evidence for legal purposes. Digital forensics also helps understand the incident's root cause and implement preventive measures.

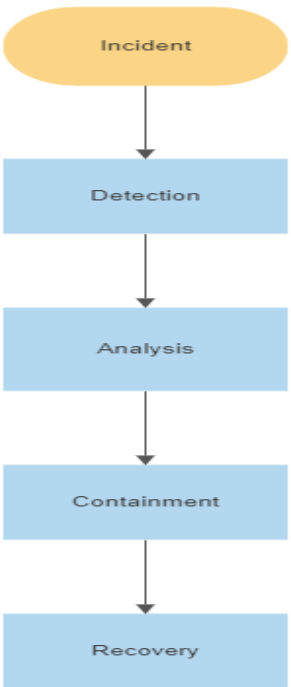

Figure 6. Stages in Incident Response

Conclusion

Cybersecurity is crucial for protecting systems, data, and individuals from unauthorized access and misuse. It has evolved alongside technology and emerging threats, with contributions from various stakeholders. In today's digital age, strong cybersecurity measures are essential for safeguarding data and preventing financial losses and reputational damage. Technical aspects like network security, encryption, and vulnerability assessment tools play key roles. However, the human factor is equally important. User awareness, recognizing social engineering techniques, and creating a security-conscious culture are vital for mitigating risks. Incident response planning is critical for minimizing the impact of cybersecurity incidents, ensuring timely detection, containment, and recovery. In conclusion, continuous efforts are needed to address the evolving cybersecurity landscape. By understanding its importance, adopting technical measures, and promoting user awareness, organizations can enhance their cybersecurity posture and protect against emerging threats.

Acknowledgement

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with

success. I would like to thank my faculty guide Asso. Prof. (Dr.) Pawan Singh who is the biggest driving force behind my successful completion of the project. He has been always there to solve any query of mine and also guided me in the right direction regarding the project. Without his help and inspiration, I would not have been able to complete the project. Also I would like to thank my batch mates who guided me, helped me and gave ideas and motivation at each step.

References

[1.] M. L. Gross, D. Canetti, and D. R. Vashdi, “Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes,” *Journal of Cybersecurity*, vol. 3, no. 1, pp. 49–58, 2017.

[2.] J. Hua and S. Bapna, “The economic impact of cyber terrorism,” *The Journal of Strategic Information Systems*, vol. 22, no. 2, pp. 175–186, 2013.

[3.] S. Kumar and V. Somani, “Social Media Security Risks, Cyber Threats andRisks Prevention and Mitigation Techniques,” *International Journal of Advance Research in Computer Science and Management*, vol. 4, no. 4, pp. 125–129, 2018.

[4.] K. O. Samuel and W. R. Osman, “Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea,” *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 5, pp. 1082–1090, 2014.

[5.] R. Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society,” *International Journal of Scientific & Engineering Research*, vol. 3, no. 6,pp. 1-4,2012.

[6.] M. Sreenu and D. V. Krishna, “A General Study on Cyber-Attacks on Social Networks,” *IOSR Journal of Computer Engineering (IOSR-JCE*, vol. 19, no. 5, pp. 01–04, 2017.

[7.] W. Trappe and J. Straub, “Journal of Cybersecurity and Privacy: A new open access journal,” *J. Cybersecur. Priv.*, vol. 1, no. 1, pp. 1–3, 2018.

[8.] L. A. D. Shen, “The nist cybersecurity framework: Overview and potential impacts,” vol. 10, no. 4, pp. 16–19, 2014.

[9.] E. A. Fischer, “Cybersecurity Issues and Challenges: In Brief,” *A51.nl.*

[10.] N. Clarke, "Cyber War: The Next Threat to National Security and What to Do About It," *HarperCollins*, 2012.