GKU Journal of Multidisciplinary Research (GKUJMR)
ISSN: 3049 – 298X, Volume – II, Issue – I, April – 2026

Cybersecurity Threats and Prevention Techniques: A Comprehensive Review

[1] Ms. Asifa Akhter, [2] Dr. Shalu Gupta, [3] Ms. Jaspreet Kaur

[1]Student, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Bathinda.

[2]Associate Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Bathinda

[3]Assistant Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Bathinda

Email ID: [1] paswanveeru914@gmail.com

Accepted: 10.04.2026 Published: 30.04.2026 Page No. 22 – 26 DOI: 10.5281/zenodo.19908876

Abstract

The rapid expansion of cloud services, digital platforms, and online communication has significantly amplified cybersecurity risks. Cyberattacks, including ransomware, phishing, malware, and unauthorized access, persistently threaten the confidentiality, integrity, and availability of data. This review paper examines prevalent cybersecurity threats impacting modern information systems and explores effective prevention techniques to mitigate these risks. Key security measures such as firewalls, encryption, intrusion detection systems (IDS), access controls, and user awareness training are analysed. Recent data indicates that global cybercrime costs are projected to reach $10.5 trillion annually by 2025, underscoring the urgency of robust defences. The paper emphasizes the importance of a layered (defence-in-depth) security approach, incorporating risk assessment models, to protect systems and ensure secure digital operations. Emerging threats like AI-driven attacks and supply chain vulnerabilities are also discussed.

Keywords: Cybersecurity, Cyber Attacks, Malware, Phishing, Ransomware, Data Protection, Network Security, Prevention Techniques, Risk Assessment

1. Introduction

Cybersecurity plays a crucial role in protecting digital systems and sensitive information against more advanced cyberattacks. Since organizations are becoming more dependent on internet-based technologies, attackers use the loopholes to amass wealth, steal information, or interfere with the services [1-3]. These attacks impact both individuals and businesses as well as critical infrastructure. Recent news indicates that cyberattacks take place about every few seconds, ransomware, and phishing are the most popular vectors. The paper will recognize the typical cybersecurity threats and the prevention measures as well as integrating quantitative risk assessment to offer a complete review.

2. Overview of Cybersecurity

Cybersecurity refers to technologies, processes and practices that are aimed at securing networks, devices, programs and data against attack, damage, or unauthorized access [4, 5]. It encompasses areas like network security, application security, information security and operational security. Cybersecurity is defined as the set of technologies, policies and practices that aim at securing information systems against cyberattacks [6, 7]. It covers several areas such as:

- Network Security
- Information Security
- Application Security
- IoT Security.

One of the key goals of cybersecurity is to uphold the CIA triad:

"Security"= {Confidentiality, Integrity, Availability}

The defense-in-depth strategy is one of the key principles and entails the use of various layers of security controls to reduce the risks.

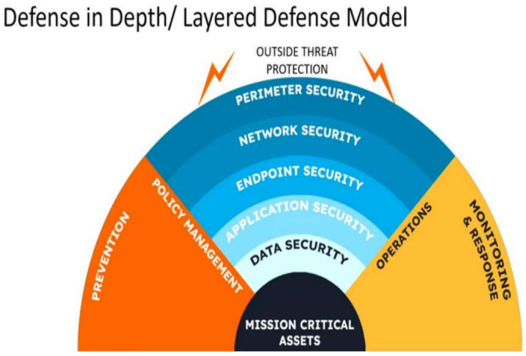

Figure 1: Layered Defence-in-Depth Model in Cybersecurity (Illustrating multiple security layers: physical, network, endpoint, application, and data) [11].

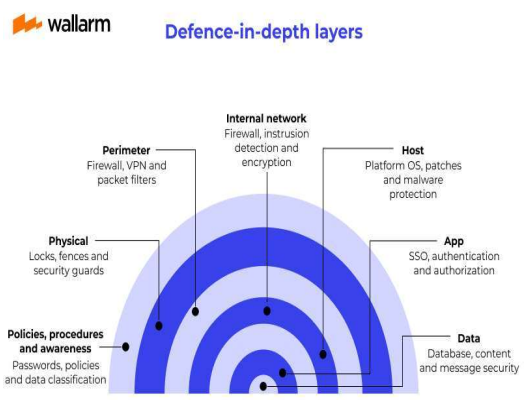

Figure 2: Alternative Representation of Defence-in-Depth Layers [12].

This multi-layered approach ensures that if one layer fails, others remain effective.

3. Common Cybersecurity Threats

The threats of cyber-attacks are also dynamic, and hackers' resort to sophisticated methods, such as AI [8-10]. Key threats include:

- **Malware**: Virus software that can harm or to be installed without authorization.
- **Phishing**: Fraudulent attempts to gain access to sensitive data through phishing messages.
- **Ransomware**: Scramble data and requires money to be decrypted.
- **Denial-of-Service (DoS/DDoS):** Floods systems to affect availability.
- **Unauthorized Access**: Weak credentials or vulnerabilities exploitation.
- **Third-party vendors** (emerging in 2025) are a threat to the supply chain.
- **Artificial Intelligence Threats**: Deepfakes and attacks by machines.

Table 1: Common Cybersecurity Threats and Their Impact

Threat Type	Description	Possible Impact
Malware	Malicious software	Data loss, system damage
Phishing	Fake emails or links	Credential theft
Ransomware	Data encryption attacks	Financial loss
DoS	Service overload	System downtime
Unauthorized Access	Illegal system entry	Data breach

Figure 3: Infographic of Common Cyber Threats [13].

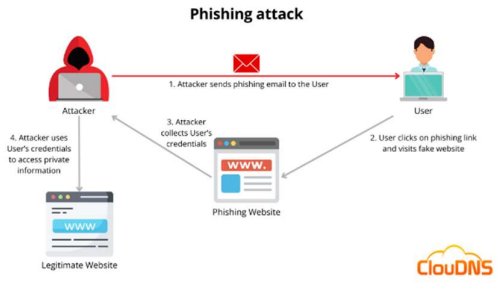

Figure 4: Illustration of a Phishing Attack Process [14].

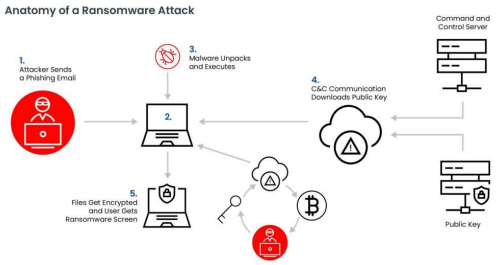

Figure 5: Diagram of a Ransomware Attack Lifecycle.

Table 2: Common Cybersecurity Threats, Impacts, and 2025 Statistics

Threat Type	Description	Possible Impact	2025 Insights/Statistics
Malware	Malicious software	Data loss, system damage	Part of rising malware-free attacks
Phishing	Fake communications	Credential theft	Leading breach cause (~16% of breaches)
Ransomware	Data encryption for ransom	Financial loss, downtime	Attacks every 11 seconds; $10.5T global cost projection
DoS/DDoS	Service overload	System downtime	25% rise in multi-vector attacks (2024-2025)
Unauthorized Access	Illegal entry	Data breach	Often via weak credentials
Supply Chain	Third-party compromise	Widespread infiltration	45% of organizations affected

4. Risk Assessment in Cybersecurity

Prioritization of threats requires the use of quantitative risk assessment. One of the fundamental equations is:

$$\textbf{Risk} = \textbf{Likelihood} \times \textbf{Impact}$$

Where Likelihood is the likelihood of happening (0-1), and Impact is the possible loss (e.g. in dollars).

An enhanced formula incorporates vulnerabilities and controls:

$$\textbf{Risk} = \frac{\textbf{Threat} \times \textbf{Vulnerability} \times \textbf{Impact}}{\textbf{Controls in Place}}$$

Single Loss Expectancy (SLE) = Asset Value × Exposure Factor

Annualized Loss Expectancy (ALE) = SLE × Annual Rate of Occurrence (ARO)

These equations enable organizations to quantify risks and justify investments.

Cybersecurity Prevention Techniques

To be effective in prevention, a multi-layered approach is needed:

1. **Firewalls**: sieve network traffic.
2. **Encryption**: Safeguard data privacy.
3. **Intrusion Detection/Prevention Systems (IDS/IPS):** Detect and block malicious activity.
4. **Access Control & Multi-Factor Authentication (MFA):** Restrict access.

5. **Frequent Software Updates and Patching**: patch vulnerabilities.
6. **User Awareness Training:** Fight social engineering.
7. **Endpoint Detection and Response (EDR):** Real time threat hunting.

5. Encryption Model

Data encryption can be represented as:

$$C = E(P, K)$$

where

P= Plaintext,

K= Encryption key,

C= Ciphertext.

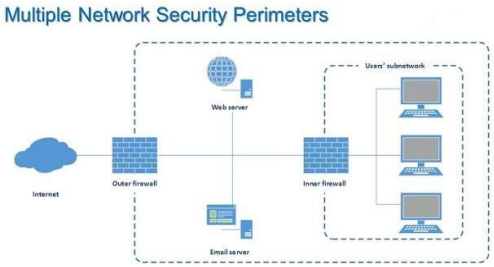

Figure 6: Diagram Showing Firewall in Network Security.

Table 3: Prevention Techniques and Purpose

Technique	Purpose	Effectiveness Insight
Firewalls	Block unauthorized traffic	Core network defence
Encryption	Protect sensitive data	Essential for data in transit/rest
IDS/IPS	Detect/block suspicious behaviour	Real-time monitoring
Access Control/MFA	Restrict system access	Reduces unauthorized entry
Software Updates	Patch known vulnerabilities	Prevents exploitation
User Training	Reduce human errors	Addresses ~34% insider threats
Zero-Trust Architecture	Verify every access request	Adoption rising to 60% in enterprises

6. Challenges in Cybersecurity

Among the challenges are the changing threats (e.g. AI-enhanced attacks), skills gaps (3.5 million unfulfilled jobs worldwide in 2025), supply chain complexity, and regulatory fragmentation. One of the main causes of breach is human error. Even with technological changes, cybersecurity has several challenges:

- Quickly developing attack methods.
- A shortage of qualified cybersecurity specialists.
- Low level of security awareness among users.
- Complexity of IT infrastructures.
- Human error has been the most common cause of security breaches, and hence the importance of conducting training and awareness programs.

7. Conclusion

This review indicates the importance of cybersecurity as a critical component in the protection of contemporary digital ecosystem. Detection of cyber threats and application of effective prevention methods will greatly minimize security threats. Multi-layered defence strategy, coupled with encryption, monitoring, frequent updates and user awareness is critical in ensuring secure computing environments. Artificial intelligence, automation, and sophisticated threat detection mechanisms will become more and more powerful in cybersecurity development in the future. Risk mitigation through awareness of cybersecurity threats and layered prevention methods go a long

way in minimizing risks. Cybercrime expenses have now become trillions of dollars; therefore, quantitative risk models, frequent updates and awareness training are crucial. The future will use AI to detect threats and automate to increase resilience in a more complex landscape.

References

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson Education, 2018.

[2] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, 2003.

A. Singh and R. Kumar, "Cybersecurity threats and defense techniques," *Int. J. Computer Science*, vol. 15, no. 2, pp. 45–52, 2019.

[3] P. Mell and T. Grance, "The NIST definition of cybersecurity," NIST Special Publication 800-53, 2011.

[4] S. Behl and K. Behl, *Cyberwar: The Next Threat to National Security*. Oxford University Press, 2017.

[5] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th ed. Pearson, 2018.

A. K. Jain and S. Gupta, "Machine learning based intrusion detection systems: A review," *IEEE Access*, vol. 9, pp. 132–150, 2021.

[6] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *IEEE Symp. Security and Privacy*, pp. 305–316, 2010.

[7] N. Kshetri, "Cybersecurity and cloud computing," *IEEE Computer*, vol. 53, no. 2, pp. 15–18, 2020.

[8] Kumar, R. (2025, April). Adaptive cybersecurity with AI: Enhancing threat detection and response in intrusion detection systems. Indian Journal of Modern Research and Reviews. https://doi.org/10.5281/zenodo.15319429

[9] ENISA, "Threat Landscape Report," European Union Agency for Cybersecurity, 2023.

[10] https://aws.plainenglish.io/the-power-of-defense-in-depth-a-layered-security-approach-22bd468e93b1

[11] https://www.wallarm.com/what/defense-in-depth-concept

[12] https://blog.totalprosource.com/6-common-types-of-cyber-attacks

[13] https://www.cloudns.net/blog/understanding-phishing-attack-and-how-to-stay-protected/