

Cybersecurity Threat Intelligence Report (2024–2025)

Cybersecurity Analyst Internship – Task 1

Prepared by: [Gnaneshwar L]

Date: [19/02/2026]

Table of Contents

1. Introduction
 2. Modern Cyber Threat Landscape
 3. AI-Powered Phishing
 4. Ransomware-as-a-Service
 5. Cloud Security Misconfigurations
 6. IoT Vulnerabilities
 7. Zero-Day Exploits
 8. Impact Analysis
 9. Preventive Security Framework
 10. Conclusion
 11. References
-

1. Introduction

Cybersecurity refers to the protection of systems, networks, and digital assets from cyber threats. With rapid digital transformation, organizations increasingly rely on cloud platforms, AI systems, and remote connectivity.

In 2024–2025, cyber threats have become more sophisticated due to artificial intelligence, automation, and dark web marketplaces.

Cybersecurity is critical for:

- Protecting personal data
 - Preventing financial fraud
 - Ensuring business continuity
 - Maintaining regulatory compliance
-

2. AI-Powered Phishing Attacks

AI-powered phishing leverages artificial intelligence to generate convincing emails, deepfake voices, and impersonation scams.

In 2024, a Hong Kong-based company lost approximately \$25 million due to a deepfake video impersonation scam.

Impact:

- Identity theft
- Financial fraud
- Corporate data breaches

Preventive Measures:

- Multi-Factor Authentication (MFA)
 - Email filtering systems
 - Security awareness training
-

3. Ransomware-as-a-Service (RaaS)

RaaS allows cybercriminals to rent ransomware kits, increasing the number of attacks globally.

Example: Colonial Pipeline ransomware attack disrupted fuel supply operations.

Impact:

- Operational downtime
- Financial losses
- Reputation damage

Preventive Measures:

- Regular offline backups
 - Endpoint Detection & Response (EDR)
 - Network segmentation
-

4. Cloud Security Misconfigurations

Cloud misconfigurations occur when storage or databases are exposed due to poor security settings.

Example: Capital One data breach caused by AWS misconfiguration.

Impact:

- Exposure of sensitive customer data
- Regulatory fines
- Legal consequences

Preventive Measures:

- Cloud Security Posture Management
 - Role-Based Access Control
 - Regular audits
-

5. IoT Vulnerabilities

IoT devices often lack strong security controls.

Example: Mirai botnet compromised IoT devices to launch DDoS attacks.

Impact:

- Privacy invasion
- Service disruption
- Botnet-based attacks

Preventive Measures:

- Change default credentials
 - Firmware updates
 - Network isolation
-

6. Zero-Day Exploits

Zero-day exploits target unknown vulnerabilities before patches are available.

Example: SolarWinds supply chain attack.

Impact:

- Espionage
- Intellectual property theft
- National security risks

Preventive Measures:

- Zero Trust Architecture
 - IDS/IPS systems
 - Continuous patching
-

7. Impact Analysis

Modern cyber threats affect both individuals and organizations by causing:

- Financial losses

- Data breaches
- Operational disruption
- Reputational damage

Organizations must implement proactive cybersecurity measures to reduce risk exposure.

8. Preventive Security Framework

Key defense mechanisms include:

- Multi-Factor Authentication
 - Zero Trust Security Model
 - Security Awareness Training
 - Threat Intelligence Monitoring
 - Patch and Vulnerability Management
-

9. Conclusion

Cyber threats in 2024–2025 continue to evolve rapidly. AI-driven attacks and ransomware ecosystems pose significant risks.

Organizations must adopt proactive cybersecurity strategies and continuously update security practices to mitigate risks effectively.

Cybersecurity is an ongoing process that requires vigilance, learning, and adaptation.

10. References

- OWASP Top 10
- NIST Cybersecurity Framework
- CISA Cybersecurity Advisories
- IBM Security Reports
- KrebsOnSecurity