MAINCRAFTS TECHNOLOGY INTERSHIP

Threat Report

(Awareness & Research Project)

Cybersecurity Task – 1

Submitted by
Thakor Kirankumar Kirtiji

Internship Project Report

January 2026

Table of Contents

1.INTRODUCTION TO CYBERSECURITY

1.1 What is Cybersecurity

- ➢Cybersecurity is important because most personal and organizational activities are now done online.
- ➢The increasing use of the internet has also increased cyber threats such as phishing, data theft, and ransomware attacks.
- ➢Cybersecurity refers to protecting systems, networks, and data from unauthorized access.
- ➢Weak security practices can lead to financial loss and data breaches.
- ➢Proper cybersecurity helps ensure safe and secure use of digital technologies.

1.2 Importance of Cybersecurity

- ➢Cybersecurity protects personal and sensitive information such as passwords, bank details, and identity data.

- ➢It helps prevent financial losses caused by online fraud, hacking, and ransomware attacks.
- ➢Cybersecurity ensures smooth and uninterrupted operation of organizations and businesses.
- ➢It helps maintain trust between users, customers, and organizations.
- ➢Strong cybersecurity reduces the risk of data breaches and cybercrime.
- ➢It supports legal and regulatory compliance for data protection.

1.3 Current Cybersecurity Trends

- Rise of AI-driven cyberattacks
- Increased use of cloud services
- Expansion of Internet of Things (IoT) devices
- Remote work and digital transformation

2. MAJOR MODERN CYBER THREATS

2.1 AI-Powered Phishing Attacks

AI-powered phishing attacks use artificial intelligence to create realistic fake emails, messages, and voice deepfakes. These attacks trick users into sharing sensitive information such as login credentials and bank details.

Risks:

- Identity theft
- Account compromise
- Financial fraud

2.2 Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service allows cybercriminals to rent ransomware tools, making attacks easier and more frequent. Attackers encrypt data and demand ransom payments to restore access.

Risks:

- Data loss
- Business downtime
- Financial damage

2.3 Cloud Security Misconfigurations

Cloud security misconfigurations occur when cloud services are not properly secured. This exposes sensitive data to unauthorized users.

Risks:

- Data breaches
- Loss of customer trust
- Compliance violations

2.4 Internet of Things (IoT) Vulnerabilities

IoT devices such as smart cameras and home automation systems often lack strong security controls, making them easy targets for hackers.

Risks:

- Unauthorized access
- Botnet attacks
- Privacy invasion

2.5 Zero-Day Exploits

Zero-day exploits target unknown software vulnerabilities for which no patch is available. These attacks are highly dangerous.

Risks:

- System compromise
- Advanced persistent threats
- High-impact cyberattacks

3. IMPACT ANALYSIS

Impact on Individuals

- Identity theft
- Financial loss
- Loss of privacy
- Emotional stress

Impact on Organizations

- Operational downtime
- Data loss
- Reputation damage
- Legal and regulatory penalties

4. REAL-WORLD CASE STUDIES

4.1 Change Healthcare Ransomware Attack (2024)

In 2024, Change Healthcare, a major U.S. healthcare technology provider, suffered a large-scale ransomware attack. The attack disrupted healthcare payment systems across hospitals and pharmacies.

Impact:

- Nationwide healthcare service disruption

- Financial losses running into billions
- Highlighted poor segmentation and credential security

Lesson Learned:

Strong identity protection, network segmentation, and ransomware preparedness are critical.

4.2 Microsoft Cloud Email Breach (2024)

In early 2024, a state-sponsored threat actor exploited a cloud security weakness, gaining access to corporate email accounts.

Impact:

- Exposure of sensitive email communications
- Raised concerns about cloud identity security
- Impacted government and enterprise users

Lesson Learned:

Cloud identity protection and monitoring are essential to prevent advanced attacks.

4.3 Snowflake Data Breach Campaign (2024)

In 2024, multiple organizations experienced data breaches due to compromised Snowflake cloud accounts using stolen credentials.

Impact:

- Large-scale data theft
- Financial and reputational damage
- Exposed weak MFA adoption

Lesson Learned:

Mandatory MFA and credential hygiene are crucial for cloud platforms.

4.4 AI-Driven Phishing Campaigns (2025)

In 2025, cybercriminals increasingly used generative AI to create deepfake voice and email phishing attacks targeting executives.

Impact:

- High-value financial fraud
- Increased difficulty in detecting phishing attempts

Lesson Learned:

Advanced email security and user awareness training are essential.

5. PREVENTIVE MEASURES

To protect individuals and organizations from modern cybersecurity threats, a combination of technical controls, organizational policies, and user awareness is required.

5.1 Technical Security Measures

1. Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring more than one form of verification. It helps prevent unauthorized access even if passwords are compromised.
Especially effective against cloud account breaches and phishing attacks.

2. Regular Patch Management

Keeping operating systems, applications, and devices up to date helps prevent exploitation of known vulnerabilities and zero-day related attacks.

3. Advanced Email Security Solutions

AI-based email filtering systems can detect phishing,spoofed emails, and malicious attachments before they reach users.

4. Network Security Controls (Firewalls, IDS/IPS)

Firewalls and Intrusion Detection/Prevention Systems monitor and block suspicious network activities, reducing the risk of ransomware and malware attacks.

5. Secure Cloud Configuration

Proper access control, encryption, logging, and continuous monitoring must be applied to cloud services to prevent misconfiguration-related data breaches.

5.2 Organizational Security Measures

1. Security Awareness and Training

Regular training programs help employees identify phishing emails, social engineering attacks, and suspicious activities.

2. Zero Trust Security Model

Zero Trust assumes no user or device is trusted by default. Continuous verification helps reduce insider threats and unauthorized access.

3. Incident Response and Backup Strategy

Organizations must maintain an incident response plan and secure offline backups to recover quickly from ransomware attacks.

4. Regular Security Audits and Risk Assessments

Periodic audits help identify vulnerabilities and improve the organization's overall security posture.

5.3 Best Practices for Individuals

- Use strong and unique passwords
- Enable MFA on all accounts
- Avoid clicking unknown links or attachments
- Keep devices and apps updated

6. CONCLUSION & FUTURE SCOPE

Conclusion

- ➢Cybersecurity is very important in today's digital world where most activities depend on the internet.
- ➢Modern cyber threats such as phishing, ransomware, and data breaches can cause serious damage.
- ➢Understanding cyber risks and following basic security practices can reduce cyberattacks.
- ➢Both individuals and organizations must take cybersecurity seriously.

Future Scope

- ➢Use of artificial intelligence for cyber defense will increase.
- ➢Demand for skilled cybersecurity professionals will continue to grow.
- ➢Cloud security and identity protection will become more important.
- ➢Regular training and awareness programs will be necessary to handle future threats.

7. REFERENCES

1. CISA – Cybersecurity and Infrastructure Security Agency

- https://www.cisa.gov

2. OWASP Top 10 Web Application Security Risks

- https://owasp.org/
- https://owasp.org/www-project-top-ten/

3. IBM Security – Threat Intelligence Reports

- https://www.ibm.com/security
- https://www.ibm.com/security/data-breach

4. ENISA Threat Landscape Report

- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

5. Krebs on Security – Cybercrime Analysis
- https://krebsonsecurity.com/

6. Microsoft Security Blog
- https://www.microsoft.com/security/blog/