Cybersecurity Task-1

Threat Report (Awareness & Research Project)

Internship Program Name: Cyber Security & Ethical Hacking

Task-1

Name: Bharath Mourya S

Table of Contents

1.	Introduction toCybersecurity	**01**
2.	Major Modern Cyber Threats (2024–2025)	**02 - 05**
3.	Preventive Measures	**05**
4.	Conclusion & Future Scope	**05**
5.	References	**06**

1. Introduction to Cybersecurity

1.1 What is Cybersecurity?

Cybersecurity refers to the practice of protecting systems, networks, applications, and data from digital attacks. These attacks aim to access, alter, steal, or destroy sensitive information**,** disrupt business operations, or extort money from individuals and organizations.

Cybersecurity includes:

- Network Security
- Application Security
- Cloud Security
- Endpoint Security
- Identity & Access Management (IAM)

1.2 Why is Cybersecurity Important?

In today's digital era, individuals and businesses heavily rely on:

- Online banking and payments
- Cloud storage and SaaS platforms
- Remote work infrastructure
- IoT and smart devices

Without proper cybersecurity:

- Personal data can be stolen
- Financial fraud can occur
- Businesses can face legal penalties
- National infrastructure can be disrupted

Cybersecurity protects:

- **Confidentiality** – preventing unauthorized access
- **Integrity** – ensuring data is not altered
- **Availability** – ensuring systems remain operational

1.3 Current Relevance (2024–2025)

Cybersecurity is more critical than ever due to:

- Rapid **digital transformation**
- Increase in **AI-driven cyberattacks**
- Growth of **cloud and IoT ecosystems**
- Rising **cybercrime-as-a-service** models

Attackers are now using automation, artificial intelligence, and deepfake technology**,** making attacks more convincing and harder to detect.

2. Major Modern Cyber Threats (2024–2025)

2.1 AI-Powered Phishing Attacks

AI-powered phishing uses artificial intelligence to generate highly realistic emails, **voice calls, and videos** to deceive victims.

Key Characteristics:

- Personalized phishing emails
- Deepfake voice impersonation
- Fake video calls using CEO or HR identity
- Automated large-scale attacks

Impact

Individuals

- Credential theft
- Bank account fraud
- Identity theft

Organizations

- Business Email Compromise (BEC)
- Unauthorized fund transfers
- Data breaches

Case Study

- **Twilio (2022–2023)** – Employees were targeted using AI-generated phishing SMS, leading to internal system access.

Preventive Measures

- Multi-Factor Authentication (MFA)
- Email security gateways
- Security awareness training
- AI-based phishing detection tools

2.2 Ransomware-as-a-Service (RaaS)

RaaS allows criminals to **rent ransomware tools** without technical expertise. Developers take a share of the ransom.

Impact

Individuals

- Loss of personal files
- Financial extortion

Organizations

- Operational shutdown
- Data encryption and leakage
- Regulatory fines

Case Study

- **WannaCry** – Infected 230,000 systems globally, affecting healthcare, telecom, and transport sectors.

Preventive Measures

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

2.3 Cloud Security Misconfigurations

Cloud misconfigurations occur when **storage buckets, databases, or APIs are left publicly accessible**.

Impact

Individuals

- Exposure of personal records
- Credential leaks

Organizations

- Massive data leaks
- Compliance violations (GDPR, HIPAA)
- Reputation damage

Case Study

- **Capital One (2019)** – Data breach due to AWS misconfiguration exposed over 100 million customer records.

Preventive Measures

- Cloud Security Posture Management (CSPM)

- Least privilege IAM policies
- Regular cloud audits
- Encryption at rest and transit

2.4 IoT Vulnerabilities

IoT devices often lack:

- Strong authentication
- Regular updates
- Encryption

Impact

Individuals

- Home surveillance compromise
- Privacy invasion

Organizations

- Botnet-driven DDoS attacks
- Network infiltration

Case Study

- **Mirai Botnet** – Hijacked IoT devices to launch massive DDoS attacks.

Preventive Measures

- Change default passwords
- Firmware updates
- Network isolation for IoT devices
- Device inventory monitoring

2.5 Zero-Day Exploits

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

Impact

Individuals

- Malware infection
- Data theft

Organizations

- Advanced Persistent Threats (APT)

- Espionage
- Infrastructure compromise

Case Study

- **Microsoft Exchange Server Zero-Day (2021)** – Exploited by nation-state attackers.

Preventive Measures

- Intrusion Detection Systems (IDS/IPS)
- Behavior-based security tools
- Threat intelligence feeds
- Rapid incident response plans

3. Preventive Security Frameworks (Cross-Cutting)

Common defenses applicable across all threats:

- Zero Trust Architecture
- Regular vulnerability assessments
- Security Information & Event Management (SIEM)
- Incident response drills
- Continuous monitoring

4. Conclusion & Future Scope

Cybersecurity threats in **2024–2025 are more sophisticated, automated, and AI-driven** than ever before. Traditional defenses alone are no longer sufficient.

Organizations and individuals must:

- Adopt proactive security strategies
- Continuously update skills and knowledge
- Invest in threat intelligence and automation
- Build a strong cybersecurity culture

The future of cybersecurity lies in:

- AI-powered defense systems
- Zero Trust security models
- Continuous learning and adaptation

Cybersecurity is no longer optional — it is a business and personal necessity.

5. References

1. **OWASP** – https://owasp.org/www-project-top-ten/
2. **CISA** – https://www.cisa.gov/news-events/cybersecurity-advisories
3. **IBM Security** – https://www.ibm.com/security/data-breach
4. **KrebsOnSecurity** – https://krebsonsecurity.com
5. Verizon Data Breach Investigations Report – https://www.verizon.com/business/resources/reports/dbir/
6. ENISA Threat Landscape – https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends