MAINCRAFTS PROFESSIONAL INTERNSHIP

Domain:

Cyber security

Task 1: Threat Report

(Awareness & Research Project)

MAINCRAFTS TECHNOLOGY

Submitted By:

ASODIYA ROHAN DINESHBHAI

Project Intern, JAN (2026)

TABLE OF CONTENTS

1. INTRODUCTION TO CYBERSECURITY

❖ What is cyber security?

Cybersecurity is the practice of protecting computer systems, networks, and data from cyber threats such as hacking, malware, phishing, and ransomware. It ensures data confidentiality, integrity, and availability. With increasing reliance on digital technologies and the internet, cybersecurity is essential to prevent data breaches, financial losses, and attacks on critical infrastructure.

❖Why is it important for individuals and businesses?

Cybersecurity is the practice of protecting computers, networks, and digital data from threats like hacking, malware, phishing, and ransomware. It uses security technologies and best practices to ensure data confidentiality, integrity, and authorized access. As digital systems and online services continue to grow, cybersecurity is essential to prevent data breaches, financial losses, and attacks on critical infrastructure.

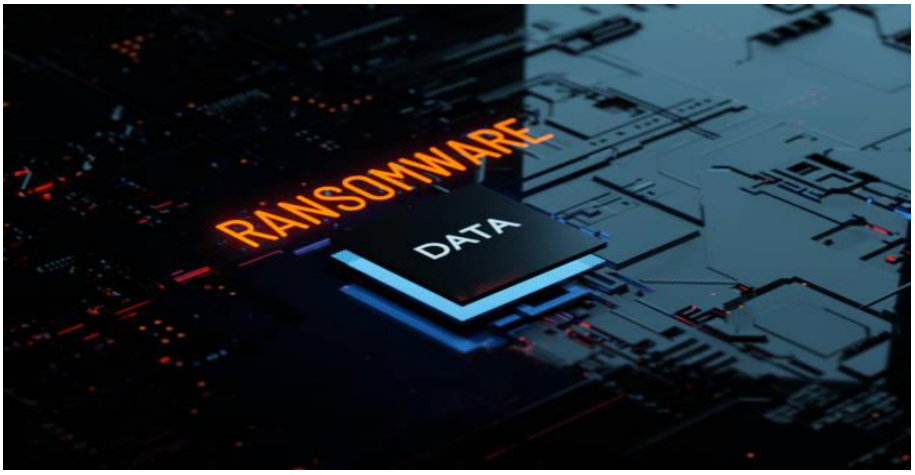
❖ Current relevance (cybercrimes increasing, digital dependency, AI-driven threats).

Cybersecurity is highly important today due to the rise in cybercrimes and increased reliance on digital technologies. Online systems used for communication, banking, and data storage are frequent targets of cyberattacks. With advanced threats like AI-driven phishing and automated hacking, strong cybersecurity measures are essential to protect digital assets and maintain trust in online systems.

2. 5 Major Modern Cyber Threats

❖ Ransomware Attack

Ransomware is a type of cyberattack where hackers encrypt a victim's files and demand money to restore access. These attacks can lock entire systems, causing work to stop completely. Ransomware mainly spreads through malicious emails, fake downloads, or insecure websites. It affects both individuals and businesses by causing data loss and financial damage.



❖ Zero-Day Exploits

Zero-day exploits occur when attackers take advantage of a software vulnerability before developers are aware of it or release a fix. Since no security patch exists, these attacks are difficult to detect and prevent. Cyber criminals use zero-day vulnerabilities to gain unauthorized access or steal sensitive data. Such attacks can cause serious damage before they are discovered.

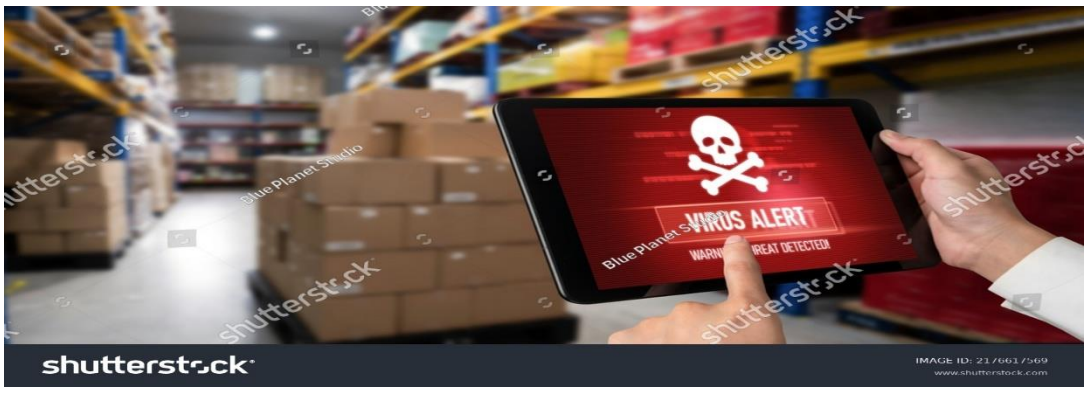
❖ AI-Driven Phishing and Social Engineering Attacks

AI-driven phishing attacks use artificial intelligence to create realistic fake emails, messages, or voice calls. These attacks trick users into sharing passwords, bank details, or personal

information. Because AI can imitate human behaviour, these phishing attempts are harder to identify. This makes individuals and organizations more vulnerable to fraud and data theft.

❖ Supply Chain Cyber Attacks

Supply chain attacks target trusted software vendors or service providers to reach larger organizations. Instead of attacking a company directly, hackers compromise a third-party system used by many businesses. This allows attackers to spread malware widely without being noticed. Supply chain attacks are dangerous because they affect multiple organizations at once.



❖ Cloud Security Misconfigurations

Cloud security misconfigurations occur when cloud services are set up incorrectly, such as leaving data storage publicly accessible or using weak access controls. These mistakes expose sensitive information to hackers without the need for complex attacks. Many organizations adopt cloud platforms quickly, often overlooking proper security settings. As a result, attackers can easily access confidential data, leading to data breaches and compliance issues.

3.IMPACT ANALYSIS

1. Ransomware Attacks

Impact on Individuals:

Ransomware attacks can cause serious harm to individuals by encrypting personal files such as documents, photos, and financial records. Victims may lose access to important data and may be forced to pay a ransom to regain it. Even after payment, there is no guarantee that data will be restored, leading to permanent data loss. Ransomware can also expose sensitive personal information, resulting in financial fraud and identity theft.

Impact on Organizations:

For organizations, ransomware attacks can completely shut down business operations and cause long periods of downtime. Critical business data may be lost or leaked, affecting productivity and customer services. Organizations often face financial losses due to ransom payments, recovery costs, and system repairs. In addition, ransomware incidents can damage the organization's reputation and lead to compliance and legal issues if customer data is compromised.

2. Zero-Day Exploits

Impact on Individuals

Zero-day exploits can silently compromise personal devices without the user's knowledge. Attackers may steal sensitive information such as passwords, emails, and banking details. Since no security patch is available at the time of attack, individuals remain vulnerable until the issue is discovered. This can lead to financial fraud, data theft, and loss of privacy.

Impact on Organizations

Organizations are highly vulnerable to zero-day attacks because these exploits bypass traditional security controls. Such attacks can lead to unauthorized access to critical systems and confidential business data. The lack of immediate fixes increases the risk of large-scale data breaches. Organizations may face severe compliance violations, financial penalties, and long-term damage to customer trust.

3. AI-Driven Phishing and Social Engineering Attacks

Impact on Individuals

AI-driven phishing attacks are more convincing and harder to detect, making individuals easy targets. Attackers use fake emails, messages, or voice calls to trick users into sharing personal and financial information. This can result in identity theft, financial fraud, and misuse of personal accounts. Many victims realize the attack only after significant damage has occurred.

Impact on Organizations

Organizations may suffer major security incidents when employees fall victim to AI-driven phishing attacks. Compromised employee credentials can give attackers access to internal systems and sensitive data. These attacks can cause data breaches, financial losses, and disruption of business operations. Repeated phishing incidents also harm an organization’s reputation and customer confidence.

4. Supply Chain Cyber Attacks

Impact on Individuals

In supply chain attacks, individuals may unknowingly use infected software or applications from trusted vendors. This can lead to malware infections, data theft, or unauthorized access to personal systems. Since the software appears legitimate, users are less likely to detect the threat early.

Impact on Organizations

Supply chain attacks can impact multiple organizations at once by targeting a common vendor or service provider. Organizations may experience widespread system compromise, data leaks, and extended downtime. These attacks are difficult to detect and can cause severe financial and reputational damage. Loss of trust in third-party vendors also creates long-term security challenges

5. Cloud Security Misconfigurations

Impact on Individuals

Cloud security misconfigurations can expose personal data stored online, such as emails, documents, and account details. This increases the risk of identity theft and misuse of private information. Individuals may not even be aware that their data has been publicly exposed.

Impact on Organizations

For organizations, cloud misconfigurations are a major cause of data breaches. Sensitive business and customer data may be publicly accessible due to improper security settings. This can lead to regulatory penalties, legal action, and loss of customer trust. Cloud-related breaches also harm the organization’s reputation and highlight weaknesses in security management.

4. REAL-WORLD CASE STUDIES

Ransomware Attack – WannaCry Ransomware (2017)

The WannaCry ransomware attack was one of the largest cyber attacks in history and affected over 150 countries worldwide. It exploited a vulnerability in Microsoft Windows systems to spread rapidly across networks. Once infected, users lost access to their files, and a ransom was demanded in cryptocurrency to restore them. Many organizations, including hospitals, government offices, and businesses, were forced to shut down their systems temporarily.

Impact:

- Large-scale system shutdowns across hospitals and public services
- Encrypted files leading to permanent data loss in many cases
- High recovery costs and interruption of essential operations
- Long-term trust and reputation damage for affected organizations

Zero-Day Exploit – Google Chrome Zero-Day Vulnerability (2021)

In 2021, Google disclosed a zero-day vulnerability in its Chrome web browser that was actively exploited by attackers before a fix was available. Cybercriminals used this flaw to run malicious code on users' systems simply by visiting compromised websites. Since no patch existed at the time, millions of users were unknowingly exposed to the attack.

Impact:

- Silent execution of malicious code on user devices
- Increased exposure of sensitive browsing and login data

- Security risks due to absence of immediate patches
- Pressure on organizations to deploy emergency security responses

AI-Driven Phishing and Social Engineering – Twitter Bitcoin Scam (2020)

In 2020, A major social engineering attack targeted Twitter's internal systems, leading to the compromise of several high-profile accounts. Attackers used advanced phishing techniques to trick employees into revealing credentials. Fake cryptocurrency messages were posted from verified accounts, convincing users to send money to the attackers.

Impact:

- Direct financial fraud through fake cryptocurrency messages
- Unauthorized control of verified social media accounts
- Loss of platform credibility and user confidence
- Need for stronger internal access controls and monitoring

Supply Chain Attack – SolarWinds Supply Chain Attack (2020)

The SolarWinds cyberattack was one of the most significant supply chain attacks in history. Hackers compromised a software update of SolarWinds, which was used by many government agencies and large organizations. This allowed attackers to secretly access sensitive systems for months without detection. The incident highlighted the risks associated with third-party vendors and supply chain security.

Impact:

- Stealthy infiltration of multiple organizations through trusted software
- Prolonged unauthorized access to sensitive systems
- Exposure of confidential government and corporate data
- Increased scrutiny of third-party vendor security practices

Cloud Security Misconfiguration – Capital One Data Breach (2019)

The Capital One data breach occurred due to a misconfigured cloud server hosted on Amazon Web Services (AWS). An attacker exploited this misconfiguration to access sensitive data, including credit card application details of millions of customers. The breach went unnoticed for a significant period before being detected.

Impact:

- Massive exposure of customer financial and personal records
- Legal penalties and regulatory scrutiny
- Increased identity theft and fraud risks
- Highlighted weaknesses in cloud security management

5. PREVENTIVE MEASURES

❖ Ransomware Attacks

To prevent ransomware attacks, multiple cybersecurity techniques are used at different levels of the system.

- **Regular Patch Management:** Ensures that operating systems and applications are updated to remove known security flaws.
- **Offline and Cloud Backups:** Helps recover encrypted data without paying ransom.
- **Network Segmentation:** Limits the spread of ransomware by isolating critical systems from general networks.

❖ Zero-Day Exploits

Zero-day attacks require advanced detection and control techniques due to the absence of immediate fixes.

- **Intrusion Detection and Prevention Systems (IDS/IPS):** Monitors unusual activities and blocks suspicious behaviour.
- **Zero Trust Security Model:** Verifies every user and device before granting access.
- **Rapid Patch Deployment:** Reduces the window of exposure once a fix is released.

❖ AI-Driven Phishing and Social Engineering

Human-focused attacks can be reduced by combining technical controls with user awareness techniques.

- **Multi-Factor Authentication (MFA):** Adds an additional layer of security beyond passwords.
- **Email Security Gateways:** Filters phishing emails before they reach users.

- **Security Awareness Training:** Educates users to identify and avoid phishing attempts.

❖ Supply Chain Attacks

Supply chain security focuses on controlling risks introduced by third-party vendors.

- **Vendor Security Assessment:** Evaluates the security practices of suppliers and partners.
- **Least-Privilege Access Control:** Restricts vendor access to only necessary systems.
- **Software Integrity Checks:** Verifies authenticity of updates and software packages.

❖ Cloud Security Misconfiguration

Cloud security depends on proper configuration and continuous monitoring techniques.

- **Secure Cloud Configuration Policies:** Prevent unauthorized access to cloud resources.
- **Identity and Access Management (IAM):** Controls user permissions and authentication.
- **Regular Cloud Security Audits:** Identifies misconfigurations and vulnerabilities early.

6. CONCLUSION AND FUTURE SCOPE

❖Conclusion

Cybersecurity plays a vital role in protecting digital systems, data, and online services in an era where technology is deeply integrated into everyday life. With the increasing use of cloud computing, online transactions, and connected devices, cyber threats such as ransomware attacks, phishing, zero-day vulnerabilities, and data breaches have become more frequent and complex. Proactive cybersecurity focuses on prevention rather than reaction, helping organizations and individuals identify vulnerabilities early and reduce potential damage. Implementing strong security measures not only safeguards sensitive information but also ensures system reliability, business continuity, and user trust in digital platforms.

❖Future Scope

The future of cybersecurity will continue to evolve as cybercriminals adopt advanced techniques, including artificial intelligence–driven attacks, automated malware, and sophisticated social engineering methods. This constant evolution makes continuous learning and skill development essential for cybersecurity professionals and users alike. Regular training, research, and the adoption of emerging security technologies will be necessary to stay ahead of new threats. As digital dependency grows, the scope of cybersecurity will expand further, creating a strong need for innovation, awareness, and adaptive security strategies to protect future digital environments.

7. REFERRENCES

Cybersecurity Basics

- CISA – Cybersecurity Overview: https://www.cisa.gov/cybersecurity
- IBM Security – What is Cybersecurity?: https://www.ibm.com/topics/cybersecurity

Threat Reports & Preventions

- CISA Cybersecurity Advisories: https://www.cisa.gov/news-events/cybersecurity-advisories
- Verizon Data Breach Investigations Report (DBIR): https://www.verizon.com/business/resources/reports/dbir/

Major Cyber Threats

- WannaCry Ransomware Advisory (2017): https://www.cisa.gov/news-events/cybersecurity-advisories/aa17-132a
- SolarWinds Supply Chain Attack (2020): https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
- Capital One Data Breach Report (2019): https://www.capitalone.com/about/newsroom/capital-one-announdata-security-incident/