MAINCRAFTS
TECHNOLOGY

Cyber Security Task-1 Threat Report (Awareness & Research Project)

- **Vanaparthi Vinay Kumar**

The goal of this task is to help you understand the current landscape of cybersecurity threats, analyze their impact, and learn how professionals present findings in the form of threat intelligence reports.

Task Description

You are working as a Cybersecurity Analyst Intern at a company (simulation). Your manager has asked you to prepare a Threat Intelligence Report highlighting the latest cybersecurity threats (2024–2025) and possible defence measures.

The report includes : 1. Introduction to cyber security

2. Identify 5 major modern cyber threats

3. Impact analysis

4. Real-World Case Studies

5. Preventive Measures

1. Introduction to cyber security

It is the practice of protecting systems, networks, devices, and data from unauthorized access, misuse, disruption, or destruction using technical, procedural, and human controls. It covers areas such as network security, application security, cloud security, identity and access management, and incident response to ensure confidentiality, integrity, and availability of information.

For individuals, cybersecurity is important to prevent identity theft, financial fraud, account takeover, and privacy violations as more personal activities move to online banking, e-commerce, and social media. For businesses, strong cybersecurity reduces the risk of data breaches, operational downtime, regulatory penalties, and reputational damage that can lead to revenue loss and legal exposure.

Cybersecurity has become even more critical in 2024–2025 as organizations depend heavily on cloud services, remote work, and digital supply chains while threat actors increasingly weaponize artificial intelligence for phishing, malware automation, and deepfake-based social engineering. At the same time, ransomware-as-a-service platforms and exploit marketplaces have lowered the barrier of entry for attackers, making sophisticated attacks accessible to less-skilled criminals.

2. Identify 5 major modern cyber threats

2.1 AI-powered phishing attacks

AI-powered phishing uses generative models to automatically craft highly personalized and grammatically correct emails, messages, and websites that convincingly impersonate trusted brands or colleagues.

Recent research shows that AI agents can now outperform human red-teamers in generating effective spear-phishing messages, and early studies indicate that a growing share of phishing emails that bypass filters are AI-written

2.2 Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service is a business model in which core ransomware developers sell or rent their malware, infrastructure, and branding to affiliates who conduct attacks in exchange for a share of the ransom Affiliates often combine double extortion (data encryption and theft) with threats to leak or auction stolen data, increasing pressure on victims to pay.

2.3 Cloud security misconfigurations

Cloud security misconfigurations occur when services such as storage buckets, virtual machines, databases, or identity policies are incorrectly set, exposing assets to the internet or granting excessive permissions Because cloud environments are elastic and complex, configuration drift and lack of visibility can quickly create exploitable gaps that attackers discover using automated scanning tools.[4][3]

2.4 IoT vulnerabilities

Internet of Things (IoT) vulnerabilities stem from insecure design, weak authentication, outdated firmware, and lack of monitoring in connected devices such as cameras, medical equipment, industrial controllers, and smart home gadgets. As organizations deploy more operational technology and smart infrastructure, the attack surface for IoT-driven incidents continues to grow.

2.5 Zero-day exploits

Zero-day exploits target previously unknown vulnerabilities for which no official patch or signature exists, giving attackers a window of opportunity to compromise systems before defenders can respond. Because defenders initially lack reliable indicators of compromise, zero-day campaigns can persist undetected until public disclosure or incident response investigations reveal them.

3. Impact analysis

3.1 Impact on individuals

-**AI-powered phishing:** Individuals may be tricked into entering credentials on convincing fake sites or sharing one-time passwords, leading to account takeover for email, banking, or social media

RaaS: When ransomware spreads to personal devices or small businesses, individuals can lose access to important documents, photos, and financial records, with limited ability to restore from backups.

Cloud misconfigurations: Misconfigured consumer cloud storage or SaaS accounts can expose personal files, IDs, or private messages to the public internet, sometimes indexed by search engines

IoT vulnerabilities: Compromised home cameras or voice assistants can lead to privacy invasion, stalking, or harassment, while hacked smart locks or alarms may facilitate physical burglary

Zero-day exploits: When zero-days impact widely used desktop, browser, or mobile platforms, individuals can be compromised simply by visiting malicious websites or opening crafted files, without visible signs

3.2 Impact on organizations

AI-powered phishing: Organizations face business email compromise, invoice fraud, unauthorized fund transfers, and credential theft for VPNs or admin portals when employees are deceived by tailored messages

RaaS: Ransomware incidents can cause days or weeks of downtime, disrupting operations, supply chains, and customer services, while recovery costs and ransom demands can reach millions of dollars

Cloud misconfigurations: For businesses, exposed cloud resources can leak intellectual property, customer databases, source code, and secrets such as API keys

IoT vulnerabilities: In enterprises and critical infrastructure, insecure IoT and OT devices can be abused to halt production lines, disrupt building management systems, or interfere with healthcare delivery

-**Zero-day exploits:** Zero-day attacks against edge devices, VPNs, or enterprise software can grant attackers privileged access to internal networks across many customers simultaneously

4. Real-World Case Studies

4.1 AI-powered phishing

Security research and industry reports describe campaigns where attackers used generative AI to mimic internal corporate communication and password-reset notifications with high success rates

4.2 RaaS – CDK Global ransomware attack (2024)

In 2024, the Black Suit ransomware group attacked CDK Global, a major software provider for car dealerships across North America

4.3 Cloud misconfiguration – major breach example

Recent analyses of cloud incidents show that misconfigured storage and databases exposed large volumes of customer records, including contact details and internal documentation, when access controls were left open to the internet

4.4 IoT attack incident

Case study collections on recent cyber incidents describe scenarios where insecure IoT devices in industrial or healthcare environments were compromised and used as entry points into wider networks

4.5 Zero-day exploitation in widely used software

Threat reports covering 2024–2025 highlight exploitation of zero-day vulnerabilities in popular file transfer and security products, allowing attackers to compromise multiple organizations through the same flaw

5. Preventive measures

5.1 Defending against AI-powered phishing

Implement multi-factor authentication (MFA) on critical accounts so that stolen passwords alone are insufficient for access

5.2 Mitigating RaaS

Maintain robust, tested backup and recovery strategies with offline or immutable backups to enable restoration without paying ransom.

5.3 Reducing cloud misconfigurations

Adopt infrastructure-as-code and automated security scanning tools to detect publicly exposed storage, insecure security groups, and overly permissive roles before deployment.

5.4 Securing IoT environments

Inventory all IoT and OT devices, change default credentials, and restrict management interfaces to dedicated, segmented networks

5.5 Managing zero-day risk

Implement a Zero Trust security model, verifying users and devices continuously and limiting implicit trust between network segments.

6. Conclusion and future scope

Modern cyber threats in 2024–2025 are characterized by increased automation, commoditization of attack tools, and expansion of the digital attack surface across cloud and IoT ecosystems. AI-powered phishing, RaaS, cloud misconfigurations, IoT weaknesses, and zero-day exploits together create a dynamic environment where both individuals and organizations face persistent risk.

Proactive cybersecurity—combining technical controls, process maturity, and user education—is essential to reduce the likelihood and impact of these threats. As adversaries continuously innovate, security professionals must commit to ongoing learning, threat hunting, and adaptation of defences to stay resilient against emerging attack techniques.