CYBERSECURITY THREAT INTELLIGENCE REPORT 2024-2025

Strategic Analysis of Modern Threats and Defensive Frameworks

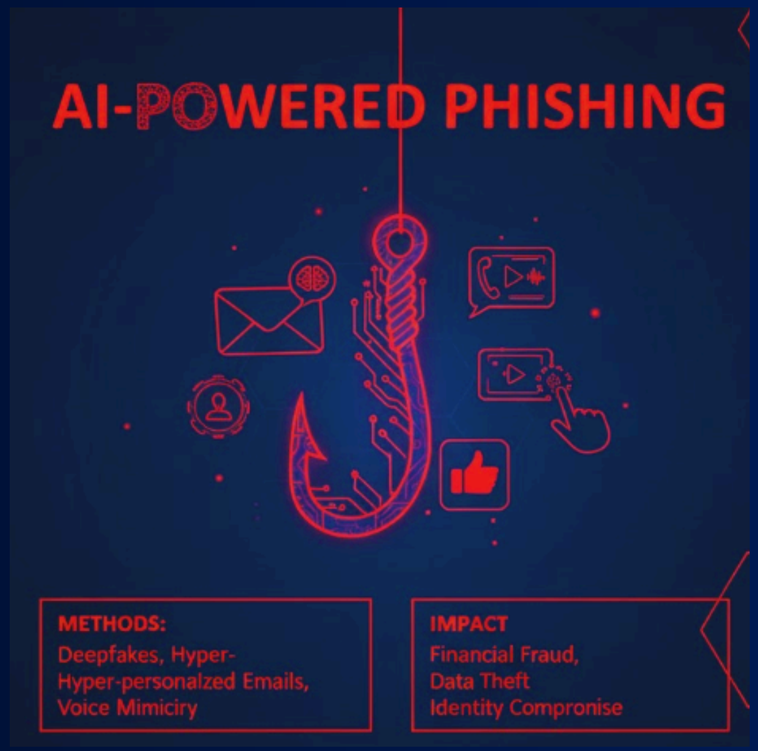
PREPARED BY: ANJITA NEGI
ROLE: CYBERSECURITY ANALYST INTERN
TASK: TASK-1: MODERN THREAT LANDSCAPE

Introduction to Cybersecurity

- *What is it?* The practice of protecting systems, networks, and data from digital attacks.
- **Importance (Individuals):** Prevents identity theft and financial loss.
- **Importance (Businesses):** Protects intellectual property and maintains customer trust.
- **Current Relevance:** AI-driven threats automate and scale attacks.
- **Digital Dependency:** Banking, health, and work are online.
- **Increasing Crime:** Cybercrime costs projected to hit trillions annually by 2025.

Threat 1 – AI-Powered Phishing

- **Overview:** Attackers use LLMs to craft error-free emails and deepfakes.
- **Impact (Individuals):** Convincing scams leading to credential theft.
- **Impact(Organizations):**Business Email Compromise (BEC) and unauthorized wire transfers.
- **Case Study (2024):** Arup Deepfake Scam — $25M lost via AI-generated video call.
- **Defense:** AI email security filters and out-of-band verification.



Threat 2 – Ransomware-as-a-Service (RaaS)

- **Overview:** Developers rent ransomware to affiliates for a share of ransom.
- **Impact(Individuals):** Permanent loss of personal data.
- **Impact(Organizations):** Operational shutdown and double extortion.
- **Case Study(2025):** Qilin group targeting healthcare providers; data leaks and downtime.
- **Defense:** Immutable backups and network segmentation.

Threat 3 – Cloud Security Misconfigurations

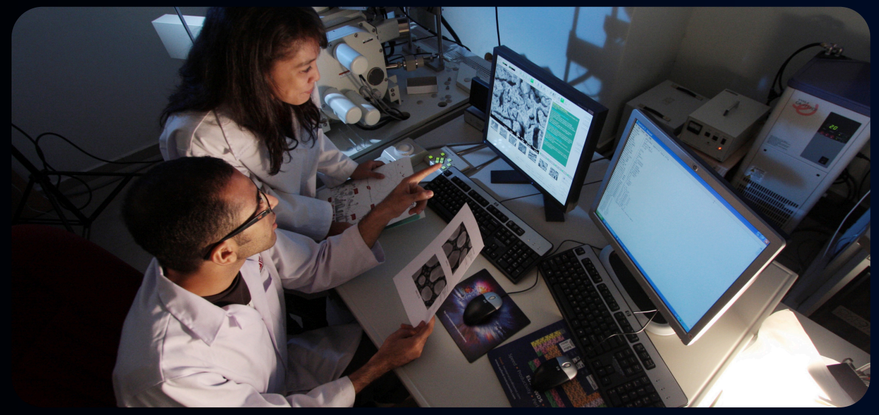
- **Overview:** Errors in cloud setup expose data to the public internet.
- **Impact (Individuals):** Mass exposure of PII.
- **Impact (Organizations):** Regulatory fines and brand damage.
- **Case Study (2024):** Microsoft AI Research leak — 38 TB exposed due to misconfiguration.
- **Defense:** CSPM tools and Principle of Least Privilege (PoLP).

Threat 4 – IoT Vulnerabilities

- **Overview:** Smart devices often lack basic security controls.
- **Impact (Individuals):** Privacy invasion and identity theft.
- **Impact (Organizations):** Devices used in botnets for DDoS attacks.
- **Case Study (2025):** Mozi botnet evolution targeting thousands of devices.
- **Defense:** Change default passwords and isolate devices on separate VLAN.

Threat 5 – Zero-Day Exploits

- **Overview:** Attacks on unknown vulnerabilities (0 days to fix).
- **Impact (Individuals):** Remote code execution on personal devices.
- **Impact (Organizations):** Espionage and lateral movement.
- **Case Study (2025):** Ivanti VPN zero-day exploited to bypass authentication.
- **Defense:** Rapid patch management and Zero Trust Architecture.



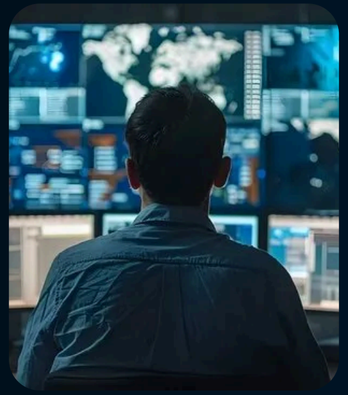
Impact Analysis Summary

- Financial Impact: Revenue loss, ransom payments, and legal penalties.
- Operational Impact: Weeks of downtime halting business activity.
- Reputational Impact: Loss of trust drives customers to competitors.
- Compliance Impact: Audits and lawsuits due to data protection failures.

Preventive Measures (Strategic Defense)

Measure	Description
Multi-Factor Authentication (MFA)	Adds a second layer beyond just a password.
Zero Trust Model	Assumes breach and verifies every request.
Security Awareness Training	Teaches employees to spot phishing and social engineering.
EDR/XDR Systems	Detect and respond to threats in real-time.

Role of the Cybersecurity Analyst



- Monitoring: Analyze logs for suspicious activity.
- Threat Hunting: Proactively look for vulnerabilities.
- Incident Response: Lead cleanup and recovery after breaches.
- Compliance: Ensure standards like ISO 27001 or NIST are met.

Conclusion & Future Scope

SUMMARY:

Threat actors are more professional and AI-driven; proactive defense is essential.

FUTURE TREND:

Growth of quantum-resistant cryptography.

FUTURE TREND:

Increased use of AI for defense and automated threat hunting.

FINAL WORD:

Continuous learning is the only way to stay ahead.

References

- IBM Security: Cost of a Data Breach Report 2024.
- CISA: Known Exploited Vulnerabilities (KEV) Catalog.
- OWASP Top 10 (2024–2025 Update).
- Verizon 2025 Data Breach Investigations Report (DBIR).

THANK YOU

FOR YOUR ATTENTION