Task ‘Security Risk Assessment Report’ Unit 7

Security Risk Assessment Report: Security Measures to Mitigate Risks

Introduction

Due to the threat across the digital landscape today, Human vulnerability is very often exploited by threat actors. This report identifies three risks: phishing and social engineering, zero-day and malware, unauthorized access. To reduce the likelihood and impact of events and incidents, businesses must proactively manage risk.

(Kunreuther, Meyer, Van den Bulte and Chapman, 2004).

Phishing and Social Engineering

Threat: Using spear phishing attackers no longer randomly attack; they target individuals with precision. Personalized phishing emails now mimic internal requests, vendor messages, and login portals. These campaigns are designed to bypass filters, and even security-aware users are tricked into revealing credentials or downloading malware.

(Shaheen, A., 2023)

Vulnerability: User errors which can originate from sharing confidential information due to the lack of ongoing awareness training and weak endpoint and system security and outdated configuration.

Recommendation: Ongoing awareness training should be implemented on a regular basis, with a focus on training related to threats that are typical of specific roles, in addition to regular training, with these threats including spear phishing, strong endpoint security with browser isolation and effective processes and policies.

Zero-Day Malware and Fileless Attacks

Threat: Zero-day vulnerabilities are undiscovered vulnerabilities that can be leveraged by attackers. Malware is using payload to deliver and fileless attacks is using vulnerabilities to attack in-memory and become invisible to antivirus solutions. When persistence was achieved, attackers use legitimate administrative tools (So-called 'Living Off the Land Attack') to perform malicious actions. The attack surface has expanded due to the uncontrolled use of publicly available AI services and AI being used to leverage sophisticated automated attacks. Posing a threat to assets.

Vulnerability: The improper use of publicly available AI services by users. Outdated software and hardware. The absence of User Behavior Analysis (UBA). Inadequate patch and change management procedures.

Recommendation: Implement effective use case policies explicitly allowing limited software use including AI and other tools. Establish and enforce patch and change management procedures including vendor critical updates. Use anomaly-based detection, Endpoint Detection and Response (EDR) in active blocking mode, both signature-based Intrusion Detection and Prevention (IDS) and behavior-based detection, and disaster recovery. Set up a Security Operations Centre (SOC) with SIEM and centralized logging.

Multi-Factor Authentication (MFA) and User Behavior analysis (UBA)

Threat: Assets are under constant threat from unauthorized access using authentication-based attacks, such as social engineering, credential theft, brute-force attacks, replay attacks, credential dumping, and man-in-the-middle attacks. If attackers gain a user's credentials, they can cause significant damage, especially if the user is senior leader or high privileged expert.

Vulnerability: Type 1 authentication alone (a password or PIN code) is a weak and outdated authentication method that hackers can exploit easily, together with the absence of anomaly-based detection makes it vulnerable due to the inability to successfully identify attacks and persistence, which then remain undetected.

Recommendation: Implement Access Control with Multi-Factor Authentication (MFA) with FIDO based hardware keys or, Time-based One-time Password (TOTP),

combined with User Behavior Analysis (UBA), UBA uses context with factors like location, device, and login method to reduce risk drastically. is based on UBA and combines this with user behavior analytics. These approaches strike a balance between user convenience and strong security.

(Singh, 2025)

Conclusion

The number of threats and complexity of attacks on organizations are on the rise. A company's risk profile is affected by various factors, including its external relationships, internal defenses, and the behavior of its personnel. Organizations can stay ahead of attackers and foster a security-first culture, prepared for future threats, by improving practices of encryption, secure authentication, awareness and robust asset management.

References

Kunreuther, H., Meyer, R., Van den Bulte, C. and Chapman, R.E., (2004). *Risk analysis for extreme events: Economic incentives for reducing future losses*. Gaithersburg, MD, USA: US Department of Commerce, Technology Administration, National Institute of Standards and Technology. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=100961 [Accessed 09 September 2025]

Shaheen, (2023). Cybersecurity in the Modern Era: An Overview of Recent Trends. Journal of Engineering and Computational Intelligence Review, 1(1), pp.39-50.

Singh, H., (2025). Strengthening Endpoint Security to Reduce Attack Vectors in Distributed Work Environments. Available at: https://dx.doi.org/10.2139/ssrn.5267844 [Accessed 09 September 2025]