Organization Feedback

Cyber Hygiene Feedback

Cyber Hygiene Score: 23.61%

Critical: Significant weaknesses pose serious risks to the organization.

What You're Doing Well

- **Centralized Software Updates:** You have mostly implemented a system to manage software updates, which is a solid foundation for mitigating vulnerabilities.

Areas to Improve

Access Control

- **Multi-factor Authentication (MFA):** MFA is partially implemented. Complete the rollout to all critical systems to enhance security significantly.
- **Password Policies:** There is no enforcement of strong password policies. Implement guidelines on complexity, expiration, and reuse restrictions.
- **Password Manager Use:** Not currently utilized. Providing and requiring a password manager can help generate and store strong passwords securely.

Awareness

- **Cybersecurity Training:** Implementation is weak. Increase the frequency and depth of cybersecurity awareness training.
- **Phishing Simulations:** These are partially conducted. Regularly test and update training based on simulation results to improve employee resilience.
- **Role-specific Training:** Partially implemented. Tailor training to specific roles to boost relevant knowledge and application.

Backup and Recovery

- **Data Backup Process:** Weak implementation; establish a robust data backup system.

- **Backup Frequency:** Addressed weakly, leading to risk of data loss. Increase the frequency of backups and ensure processes are reliable.

Other Security Practices

- **User Access Privileges:** Partially reviewed; establish a regular review cycle for user access.
- **Deactivation of Accounts:** Inactive or terminated employee accounts are not promptly deactivated, posing security risks.
- **Principle of Least Privilege:** Ensure employees only have necessary access to systems and data.
- **Vulnerability Scans:** Currently not performed; regular scans are critical to identify and address vulnerabilities.
- **Antivirus Protection:** Install and update antivirus solutions to protect endpoints.
- **Software Updates:** Operating systems, software, and applications are not regularly updated, increasing vulnerability exposure.
- **Data Classification Policy:** Develop a formal policy to ensure data is managed and protected appropriately.
- **Encryption:** Weak implementation of encryption practices; strengthen the use of encryption for sensitive files and communications.
- **Incident Reporting:** Partially implemented. Establish clear procedures for reporting security incidents and suspicious activity.

Potential Risks

- **Unauthorized Access:** Lack of strong access controls increases risk of credential theft.
- **Phishing Vulnerability:** Limited awareness heightens risk of phishing attacks.
- **Data Loss:** Insufficient backup systems pose a significant threat of permanent data loss.
- **General Security Weaknesses:** Absence of several critical security measures exposes the organization to multiple threats.

Action Plan

Immediate (0–30 Days)

- **MFA Expansion:** Implement MFA for all critical accounts to reduce unauthorized access risk.

- **Password Policy:** Establish and enforce a strong password policy.

- **Awareness Training:** Launch comprehensive cybersecurity awareness training for all employees.

Short-Term (60–90 Days)

- **Backups:** Set up regular, automated backups and conduct tests of data recovery processes to ensure reliability.

Medium-Term (3–6 Months)

- **Cybersecurity Assessment:** Conduct a thorough assessment to identify and patch known vulnerabilities, strengthening overall security posture.