Organization Feedback

Cyber Hygiene Self-Assessment Feedback

Score: 50.00%

Needs Improvement: You've made some progress, but key areas need attention to enhance your organization's security posture.

What You're Doing Well

Currently, no standout strengths have been identified from your assessment. Addressing the areas below will help in developing robust cybersecurity measures.

Areas to Improve

Access Control

- **Multi-Factor Authentication (MFA):**

Implement MFA fully across all critical systems to strengthen login security.

- **Password Policies:**

Ensure strong password policies are enforced. Focus on enhancing length, complexity, expiration, and reuse restrictions.

- **Password Managers:**

Provide and mandate the use of password managers for better password security and management.

Awareness

- **Cybersecurity Training:**

Regularly schedule and conduct comprehensive cybersecurity awareness training for all employees.

- **Phishing Simulations:**

Implement simulated phishing attacks to test and heighten employee awareness.

- **Role-Specific Training:**

Offer cybersecurity training tailored to the specific roles of employees to improve overall security knowledge.

Backup and Recovery

- **Data Backup Process:**

Develop a reliable data backup and recovery process and ensure it is fully implemented.

- **Backup Frequency:**

Increase the frequency of data backups to minimize data loss risks.

General Security

- **User Access Privileges:**

Regularly review and adjust user access privileges to align with the principle of least privilege.

- **Account Deactivation:**

Ensure inactive or terminated employee accounts are deactivated immediately to prevent unauthorized access.

- **Software Updates:**

Centralize and manage software updates to keep systems secure.

- **Vulnerability Scans & Protection:**

Conduct regular vulnerability scans and keep antivirus and endpoint protection solutions updated.

- **Data Encryption:**

Ensure sensitive files and communications are encrypted both at rest and in transit for data protection.

- **Incident Reporting:**

Educate employees on how to report security incidents and suspicious activity effectively.

Potential Risks

- **Credential Theft:** Weak access controls could lead to unauthorized access.
- **Data Loss:** Unreliable backups pose a risk of data loss.
- **Phishing Attacks:** Insufficient training leaves employees vulnerable to phishing scams.
- **System Compromise:** Unpatched vulnerabilities can result in system failures and data breaches.

Action Plan

Immediate (0–30 Days)

- **Implement MFA:** Secure all critical systems with multi-factor authentication.
- **Begin Training:** Initiate regular cybersecurity awareness training sessions.
- **Enforce Password Policies:** Adopt and enforce strong password policies.

Short-Term (60–90 Days)

- **Automate Backups:** Set up reliable, automated backups and test the recovery process.
- **Patch Systems:** Address and update any outdated systems and software.

Medium-Term (3–6 Months)

- **Review Access Privileges:** Regularly review user access to ensure compliance with the least privilege principle.
- **Encrypt Data:** Implement encryption for sensitive data in rest and transit.

By taking action on these recommendations, you will significantly enhance your cybersecurity defenses and mitigate potential risks. Please reach out if you need further guidance or assistance.
