Organization Feedback

Cybersecurity Feedback for Your Organization

Cyber Hygiene Score: 46.32%

Your current score indicates notable gaps that require swift attention to ensure your organization remains resilient against potential threats.

What You're Doing Well

- **Password Management:** Enforcing strong password policies contributes significantly to security.
- **Access Control:** Implementing the least privilege principle minimizes unnecessary access and limits potential security breaches.
- **Patching & Updates:** Automated patching ensures systems are consistently up-to-date, reducing vulnerabilities.
- **Data Security:** Encrypting all sensitive data protects it from unauthorized access.
- **Data Recovery:** Regular testing of backups guarantees data can be restored swiftly in case of loss.
- **Phishing Defense:** Conducting regular phishing simulations improves employee recognition of cyber threats.
- **Incident Handling:** Clear procedures for incident reporting and 24/7 emergency support provide a solid foundation for addressing issues promptly.
- **Endpoint Protection:** Implementing advanced measures prevents unauthorized access to company devices.
- **Insurance & Compliance:** Comprehensive cyber insurance and full compliance with industry standards strengthen your overall security posture.
- **Vendor Management:** Continuous monitoring of vendor security ensures aligned standards.

Areas to Improve

Identity & Access Management

- **Multi-Factor Authentication (MFA):** Ensure MFA is fully implemented to enhance security significantly.
- **Access Review:** Regular review of access privileges can prevent outdated or excessive permissions.
- **Account Termination:** Implement swift deactivation of terminated accounts to prevent unauthorized access.
- **Password Managers:** Offer and require the use of password managers to enhance secure credential management.

Software & Patch Management

- **Centralized Patch System:** Establish a centralized system for patch management to streamline and ensure thorough updates.
- **Vulnerability Scans:** Regular scans are essential to identify and address potential security weaknesses.
- **Endpoint Security:** Strengthen endpoint protection measures to safeguard against threats.

Data Classification & Protection

- Develop a formal data classification policy to ensure sensitive data is appropriately handled and protected.

Backup & Recovery

- Ensure back-up processes are in place, regularly conducted, and securely stored offsite to prevent data loss and ensure recovery.

Security Awareness & Training

- Increase the frequency and role-specific tailoring of security training to cultivate a robust security culture within the organization.

Network & Endpoint Security

- Improve Wi-Fi and remote access security measures to prevent unauthorized network access.

Incident Response & Business Continuity

- Formulate an incident response plan, log and analyze incidents, and establish a timeline for reporting incidents to minimize damage.

Compliance & Regulatory Alignment

- Implement formal security requirements for vendors to ensure alignment with your standards.

Physical Security

- Enhance physical security measures to control access and prevent unauthorized breaches.

Remote Work Security

- Establish and enforce security protocols specifically for remote access to safeguard the organization's assets.

Potential Risks

- While no major risks have been identified, maintaining current efforts is crucial to continue this positive trajectory.

Action Plan

Immediate (0–30 Days)

- Maintain existing strong practices to reinforce your current security posture.

Short-Term (60–90 Days)

- Focus on the implementation of MFA across all accounts and initiate regular vulnerability scans.

Medium-Term (3–6 Months)

- Plan for and conduct regular cybersecurity reassessments to identify further areas for improvement and ensure continued compliance with evolving best practices.

Your dedication to improving your cybersecurity measures is commendable, and focusing on these key areas will substantially enhance your resiliency against cyber threats.