Organization Feedback

Cyber Hygiene Score

14.71%

Severe: Immediate and decisive cybersecurity action is required.

Introduction

Your organization's current cybersecurity hygiene is weak, scoring only 14.71% on our assessment. This indicates a high level of vulnerability to potential cyber threats. Continuous improvement is crucial to protect your business assets, data integrity, and customer trust. It's vital that we address these issues promptly to ensure your organization is better defended against cyber attacks.

What You're Doing Well

Despite the overall score, there are areas where your organization demonstrates good cybersecurity practices:

- **Least Privilege Principle:** You ensure that employees have access only to the data and systems necessary for their job roles. This reduces the risk of unauthorized access and potential data breaches.
- **Regular Data Backups:** You frequently perform data backups, ensuring that critical data can be restored in case of loss or corruption.

Areas to Improve

Identity & Access Management

- **Multi-Factor Authentication (MFA):** You are not enforcing MFA for critical systems, which can prevent unauthorized access.
- **User Access Reviews:** Conduct regular reviews of user access privileges to prevent unnecessary access or data breaches.
- **Password Policies:** Implement strong password policies, including length, complexity, expiration, and reuse restrictions.
- **Account Deactivation:** Ensure inactive or terminated employee accounts are deactivated immediately to prevent misuse.
- **Password Managers:** Provide and require the use of password managers to secure sensitive information.

Software & Patch Management

- **Centralized Updates System:** Implement a centralized system to manage software updates, ensuring all systems are up to date.
- **Vulnerability Scans:** Conduct regular vulnerability scans to identify and mitigate security weaknesses.
- **Antivirus Updates:** Ensure antivirus and endpoint protection solutions are installed and regularly updated.
- **Software Updates:** Keep all operating systems, software, and applications current.

Data Classification & Protection

- **Data Classification Policy:** Implement a formal policy for classifying and restricting access to sensitive data.
- **Data Encryption:** Encrypt sensitive files and communications both at rest and in transit.

Backup & Recovery

- **Backup Process:** Develop a comprehensive data backup and recovery process.
- **Secure Backup Storage:** Store backups securely offsite or in the cloud.
- **Backup Testing:** Regularly test backups for successful restoration.

Security Awareness & Training

- **Cybersecurity Training:** Regularly conduct cybersecurity awareness training for employees.
- **Phishing Simulations:** Use simulated phishing attacks to test and improve employee awareness.
- **Role-Specific Training:** Provide role-specific cybersecurity training.
- **Incident Reporting:** Ensure employees know how to report security incidents and suspicious activities.
- **Cybersecurity Participation:** Foster a culture where employees actively engage in cybersecurity practices.

Network & Endpoint Security

- **Secure Wi-Fi Policies:** Enforce secure Wi-Fi policies, including WPA3 protocol, no default credentials, and guest network separation.
- **Endpoint Protection:** Ensure all devices have endpoint security solutions.

• **Secure Remote Access:** Secure remote access to company systems through VPNs or similar solutions.

Incident Response & Business Continuity

• **Incident Response Plan:** Develop a documented incident response plan.

• **Emergency Support:** Have a cybersecurity expert or service provider available for emergencies.

• **Incident Logging:** Log and analyze security incidents to identify patterns.

• **Cyber Insurance:** Consider a cyber insurance policy to mitigate financial losses from cyber incidents.

• **Incident Reporting:** Establish quick internal reporting for cybersecurity incidents.

Compliance & Regulatory Alignment

• **Regulatory Compliance:** Adhere to industry-specific cybersecurity regulations or standards.

• **Vendor Standards:** Ensure third-party vendors meet your cybersecurity standards.

Physical Security

• **Device Security:** Physically secure laptops, servers, and other devices to prevent unauthorized access.

Third-Party Risk

• **Vendor Assessment:** Assess vendors' and partners' cybersecurity practices before sharing data or system access.

Remote Work Security

• **Secure Remote Access:** Require employees to use VPNs or secure networks when accessing company data remotely.

Potential Risks and Risk Scenarios

• Without MFA, an attacker could take over email accounts.

• Unpatched systems could be exploited by attackers to gain control.

• Sensitive data could be accessed by unauthorized personnel without proper data classification.

• Inadequately secured devices might lead to data breaches via physical access.

Action Plan

Immediate (0–30 Days)

- Implement MFA for at least critical systems like email and financial software.
- Review and deactivate unnecessary or inactive accounts.
- Initiate company-wide cybersecurity awareness training sessions.
- Draft a basic incident response plan and distribute it to the relevant team.

Short-Term (60–90 Days)

- Set up a centralized system for managing software updates.
- Conduct an organization-wide vulnerability scan and address high-risk issues.
- Enforce secure password policies and distribute password managers.
- Establish secure storage locations for data backups and test their effectiveness.

Medium-Term (3–6 Months)

- Formalize a data classification policy with restricted access protocols.
- Regularly conduct phishing simulations and tailor training sessions based on results.
- Develop comprehensive compliance documentation for regulatory alignment.
- Reassess third-party vendors’ cybersecurity practices and upgrade contracts if needed.

Conclusion

Improving your organization's cybersecurity posture is a step-by-step process. It’s crucial to integrate these recommended actions as part of your company culture. Reassess your cybersecurity status every 6–12 months to ensure continuous improvement. Small, consistent steps will significantly reduce risk and enhance the security integrity of your company.