Organization Feedback

Cyber Hygiene Score

13.24%

Severe: Immediate and decisive cybersecurity action is required.

Introduction

Your current cybersecurity hygiene is weak. With a score of 13.24%, it's critical to take urgent action to address various cybersecurity vulnerabilities. Improving your cybersecurity posture is essential to protect your business from potential threats and to ensure the safety of your customer data and operations. Continuous improvement in cybersecurity practices is not only important but essential for the ongoing resilience and trustworthiness of your organization.

What You're Doing Well

- **Regular Software Updates:** If you are updating your operating systems, software, and applications consistently, this helps protect your systems from known vulnerabilities and provides better security features.
- **Frequent Data Backups:** Performing regular data backups ensures that your critical business information can be restored in case of data loss or cyber incidents, minimizing downtime and data loss.

Areas to Improve

Identity & Access Management

- **Enforce Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to your critical systems, making it more difficult for attackers to gain unauthorized access.
- **Regular Access Reviews:** Regularly review user access privileges to ensure that only authorized personnel have access to critical systems.
- **Strong Password Policies:** Implement strong password policies to safeguard access to your systems.
- **Inactive Account Management:** Immediately deactivate accounts for inactive or terminated employees to prevent misuse.
- **Least Privilege Principle:** Ensure employees only access the data and systems required for their job roles.

• **Password Managers:** Provide and require the use of password managers to securely store and manage credentials.

Software & Patch Management

• **Centralized Update System:** Implement a centralized system for managing software updates to ensure all systems are protected against vulnerabilities.

• **Regular Vulnerability Scans:** Perform regular vulnerability scans to identify security weaknesses promptly.

• **Endpoint Protection:** Update and maintain antivirus and endpoint protection solutions to guard against malware.

Data Classification & Protection

• **Formal Data Classification Policy:** Develop and implement a policy to categorize and restrict access to sensitive data.

• **Encryption of Sensitive Data:** Encrypt sensitive files and communications, both at rest and in transit, to protect against unauthorized access.

Backup & Recovery

• **Defined Backup Process:** Establish a data backup and recovery process to ensure data integrity and availability.

• **Secure Backup Storage:** Store backups securely in offsite or cloud locations to protect against physical and cyber threats.

• **Backup Testing:** Regularly test backups to ensure successful data restoration when needed.

Security Awareness & Training

• **Regular Employee Training:** Conduct frequent cybersecurity awareness training for staff to increase their security knowledge and vigilance against threats.

• **Simulated Phishing Attacks:** Perform simulated phishing exercises to test and improve employee awareness.

• **Role-Specific Training:** Provide role-specific cybersecurity training to enhance employee skills and response capabilities.

• **Incident Reporting:** Ensure employees know how to report security incidents and suspicious activities.

Network & Endpoint Security

• **Secure Wi-Fi Policies:** Enforce secure Wi-Fi policies, including WPA3 and separating guest networks, to protect against unauthorized access.

• **Comprehensive Endpoint Security:** Protect all devices with endpoint security solutions such as EDR, antivirus, and firewalls.

• **Secured Remote Access:** Implement measures to secure remote access to company systems.

Incident Response & Business Continuity

• **Documented Incident Response Plan:** Develop and document a comprehensive incident response plan.

• **Cybersecurity Expertise:** Engage a cybersecurity expert or service provider for support during emergencies.

• **Incident Logging and Analysis:** Log and analyze security incidents for patterns to prevent future occurrences.

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

Compliance & Regulatory Alignment

• **Follow Industry Standards:** Ensure compliance with industry-specific cybersecurity regulations or standards like ISO 27001.

• **Vendor Cybersecurity Requirements:** Require third-party vendors to meet cybersecurity standards before sharing data.

Physical Security

• **Device Security:** Ensure all devices are physically secured against unauthorized access to prevent theft or tampering.

Third-Party Risk

• **Vendor Risk Assessment:** Conduct assessments of vendors' cybersecurity practices before sharing data or system access.

Remote Work Security

• **Secure Remote Access:** Mandate the use of VPNs or secure networks for employees accessing company data remotely.

Potential Risks and Risk Scenarios

• **Email Account Takeover:** Without MFA, an attacker could take over email accounts and impersonate staff.

• **Data Breaches:** Weak password policies and failure to deactivate inactive accounts increase the risk of data breaches.

• **Malware Infection:** Lack of regular vulnerability scans and outdated antivirus solutions could lead to malware infections.

Action Plan

Immediate (0–30 Days)

• Implement MFA for all critical systems.

• Review and enforce strong password policies.

• Create an inventory of all current user access privileges.

• Document a basic incident response plan.

• Initiate regular data backups and test their restoration processes.

Short-Term (60–90 Days)

• Establish centralized system for software and patch management.

• Start conducting regular vulnerability scans.

• Conduct a full audit of data classification and protection policies.

• Begin consistent cybersecurity awareness training for employees.

• Develop secure Wi-Fi policies.

Medium-Term (3–6 Months)

• Finalize and implement a comprehensive data encryption strategy.

• Regularly engage vendors for cybersecurity assessments.

• Implement strategic updates based on regular audit findings.

• Implement role-specific training for employees.

• Secure and isolate any third-party access to sensitive systems.

Conclusion

Improving your cybersecurity posture requires immediate attention and sustained effort. By following this action plan, you'll significantly enhance your security defenses, reducing the risk of cyber threats. Reassess your cybersecurity measures in 6–12 months to adapt to new threats and ensure continued protection. Remember, even small steps can make a significant difference in securing your business.