Organization Feedback

Cyber Hygiene Score

13.24%

Severe: Immediate and decisive cybersecurity action is required.

Introduction

The current cybersecurity hygiene of your organization is weak. With a Cyber Hygiene Score of 13.24%, it is vital to recognize the need for urgent improvements. Cyber threats are evolving, and safeguarding your business's data and operations requires ongoing effort. Prioritizing cybersecurity enhancements will help protect your assets and maintain trust with your clients and partners.

What You're Doing Well

Here are some areas where your organization is doing well:

- **Operating Systems, Software, and Applications Updates**:

Regular updates help patch known vulnerabilities, preventing attacks exploiting outdated software.

- **Data Backups**:

Frequent data backups ensure that you can quickly recover important information in the event of data loss or a cybersecurity incident.

Areas to Improve

Below are areas that need improvement, categorized for clarity:

Identity & Access Management

- **Multi-Factor Authentication (MFA)**: Implement MFA to protect critical systems against unauthorized access.
- **User Access Privileges**: Regularly review access privileges to prevent unauthorized data access.
- **Password Policies**: Enforce strong password rules to strengthen account security.
- **Employee Account Deactivation**: Immediately deactivate accounts of inactive or terminated employees to prevent misuse.

• **Least Privilege Principle**: Limit data access based on employee roles to minimize potential breaches.

• **Password Managers**: Educate employees on using password managers to secure credentials efficiently.

Software & Patch Management

• **Centralized Software Updates**: Establish a centralized system to ensure timely software updates.

• **Vulnerability Scans**: Conduct regular scans to identify and address security vulnerabilities.

• **Antivirus Solutions**: Deploy and update comprehensive antivirus and endpoint solutions to prevent malware infections.

Data Classification & Protection

• **Data Classification Policy**: Implement a formal policy to manage sensitive data access.

• **Data Encryption**: Encrypt sensitive files in transit and at rest to protect against unauthorized access.

Backup & Recovery

• **Backup Process**: Develop a robust data backup and recovery process.

• **Secure Backup Storage**: Ensure backups are stored securely offsite or in the cloud.

• **Backup Testing**: Regularly test backups to ensure data can be restored successfully.

Security Awareness & Training

• **Cybersecurity Training**: Provide regular cybersecurity awareness training to all employees.

• **Simulated Phishing**: Conduct tests to improve employee vigilance against phishing attacks.

• **Role-Specific Training**: Offer training tailored to specific job responsibilities.

• **Incident Reporting**: Educate employees on reporting security incidents and suspicions.

Network & Endpoint Security

• **Wi-Fi Security**: Implement secure Wi-Fi policies, including guest network separation.

• **Endpoint Protection**: Ensure all devices have updated security solutions to detect threats.

• **Remote Access Security**: Secure how employees access company data remotely, such as by using VPNs.

Incident Response & Business Continuity

- **Incident Response Plan**: Create a documented plan for responding to cybersecurity incidents.
- **Cybersecurity Support**: Establish relationships with experts to assist during emergencies.
- **Incident Analysis**: Analyze logged incidents for patterns to prevent future occurrences.
- **Cyber Insurance**: Consider cyber insurance to reduce financial losses from incidents.

Compliance & Regulatory Alignment

- **Regulations & Standards**: Align your practices with industry-specific cybersecurity regulations.
- **Vendor Standards**: Require third-party vendors to follow your cybersecurity standards.

Physical Security

- **Device Security**: Ensure physical security measures are in place for critical equipment.

Third-Party Risk

- **Vendor Assessment**: Evaluate the cybersecurity of vendors before sharing data.

Remote Work Security

- **Secure Networks**: Mandate VPNs or secure networks for remote work access.

Potential Risks and Risk Scenarios

Without improvements, specific risks include:

- An attacker taking control of email accounts due to the lack of MFA.
- Data breaches from excessive user privileges remaining unreviewed.
- Malware infections from outdated software, risking operation disruptions.

Action Plan

Immediate (0–30 Days)

- Implement MFA for all critical systems.
- Enforce strong password policies, including the use of password managers.
- Set up centralized software update management.
- Conduct vulnerability scans and update antivirus solutions.
- Establish secure remote access protocols via VPNs for remote work.

Short-Term (60–90 Days)

- Review and adjust user access privileges following the least privilege principle.
- Train employees on cybersecurity awareness and incident reporting.
- Identify and encrypt sensitive files and communications.
- Initiate regular backup testing procedures.
- Develop a documented incident response plan.

Medium-Term (3–6 Months)

- Formalize a data classification policy and conduct an inventory of sensitive data.
- Align cybersecurity practices with industry regulations and standards.
- Conduct simulated phishing attacks to enhance employee awareness.
- Evaluate third-party vendors for their cybersecurity practices.
- Consider implementing a cyber insurance policy for risk mitigation.

Conclusion

Continuously improving your cybersecurity strategy is essential. I recommend reassessing your security posture in 6–12 months. Remember, even small steps can significantly lower your risks and protect your organization's valuable data and reputation.