

# Organization Feedback

## Cyber Hygiene Score

---

26.47%

**Critical:** Significant weaknesses pose serious risks to the organization.

## Introduction

---

The current cybersecurity hygiene of the organization is weak, with significant vulnerabilities that pose serious threats. It's crucial to prioritize improvements in your cybersecurity posture to protect your business and customer data from potential cyber attacks. Continuous improvement is essential to adapt to the evolving threat landscape and ensure your operations remain secure.

## What You're Doing Well

---

The organization has successfully implemented the following good security practices:

- **Deactivation of Employee Accounts:** Inactive or terminated employee accounts are deactivated immediately, minimizing the risk of unauthorized access by former employees.
- **Principle of Least Privilege:** Employees have access only to the data and systems necessary for their job roles, reducing the potential impact of a compromised account.

## Areas to Improve

---

### Identity & Access Management

- Implement multi-factor authentication (MFA) for all critical systems to mitigate unauthorized access.
- Regularly review user access privileges to ensure that employees only have access appropriate to their current role.
- Enforce strong password policies, including requirements for length, complexity, expiration, and restrictions on reuse.
- Provide and require the use of password managers to help employees manage strong, unique passwords for different systems.

### Software & Patch Management

- Establish a centralized system for managing software updates to ensure all systems are patched against known vulnerabilities.

- Conduct regular vulnerability scans to identify and address potential security weaknesses.
- Ensure antivirus and endpoint protection solutions are installed, active, and consistently updated.
- Implement a routine process for updating operating systems, software, and applications.

### **Data Classification & Protection**

- Develop a formal data classification policy to inventory and control access to sensitive data.
- Ensure that sensitive files and communications are encrypted both at rest and in transit, protecting them from unauthorized access.

### **Backup & Recovery**

- Establish a comprehensive data backup and recovery process to protect against data loss.
- Perform regular data backups and store copies securely in an offsite or cloud location.
- Regularly test backups to ensure successful data restoration in case of an incident.

### **Security Awareness & Training**

- Conduct regular cybersecurity awareness training for all employees to build a security-conscious culture.
- Implement simulated phishing attacks to test and improve employee awareness against social engineering threats.
- Provide role-specific cybersecurity training to ensure that employees understand specific risks associated with their responsibilities.
- Empower employees with knowledge on how to report security incidents and suspicious activity.

### **Network & Endpoint Security**

- Enforce secure Wi-Fi policies, ensuring networks use WPA3 encryption and separate guest networks.
- Protect all devices with endpoint security solutions such as EDR, antivirus, and firewalls.
- Secure remote access to company systems with VPNs or other secure connection protocols.

### **Incident Response & Business Continuity**

- Develop a documented incident response plan to efficiently handle potential cybersecurity threats.
- Establish relationships with cybersecurity experts or service providers for support during emergencies.

- Log and analyze security incidents to identify patterns and improve defenses.
- Secure a cyber insurance policy to mitigate financial losses from cyber incidents.

## Compliance & Regulatory Alignment

- Align with industry-specific cybersecurity regulations or standards like ISO 27001 to ensure compliance.
- Require third-party vendors to meet cybersecurity standards before accessing company data or systems.

## Physical Security

- Ensure devices such as laptops and servers are physically secured to prevent unauthorized physical access.

## Third-Party Risk

- Assess vendors and partners for cybersecurity practices before sharing data or system access to prevent third-party breaches.

## Remote Work Security

- Require employees to use VPNs or secure networks when accessing company data remotely to safeguard against cyber threats.

## Potential Risks and Risk Scenarios

---

Even with good practices in place, certain gaps introduce risks:

- **Unauthorized Access:** Without MFA, an attacker could easily exploit weak or stolen passwords to gain access to critical systems like email or financial databases.
- **Data Breach:** Ineffective data classification and protection processes can lead to exposure of sensitive information.

## Action Plan

---

### Immediate (0–30 Days)

- Implement multi-factor authentication (MFA) for all critical systems.
- Configure and activate centralized software patch management.
- Enforce and educate employees on strong password policies.
- Start conducting regular data backups and secure storage offsite.

## **Short-Term (60–90 Days)**

- Develop a comprehensive incident response plan and conduct a drill.
- Perform a security audit to ensure compliance with industry regulations.
- Provide training on security best practices and phishing awareness to employees.
- Establish a formal data classification and protection policy.

## **Medium-Term (3–6 Months)**

- Set up regular vulnerability scanning and remediation processes.
- Analyze security incident logs for patterns and adjust cybersecurity policies accordingly.
- Review and update vendor assessment processes for cybersecurity compliance.
- Develop a long-term cybersecurity strategy and budget for continuous improvement.

## **Conclusion**

---

The organization should continue to prioritize cybersecurity improvements to protect its operations and customer data. It's recommended to reassess the cybersecurity posture in 6–12 months to track progress and adjust strategies as necessary. Remember, even small improvements can significantly mitigate risks and enhance your organization's security resilience.