Assessment Review

{Company}

CyberMaxProtects conducted a general cybersecurity assessment of ***{Company}***, a *{Company Industry/Function}*.

Based on discussions with the organization and our review of publicly accessible online information, we observed the following opportunities to enhance the current cybersecurity posture:

Executive summary of observed strengths and weaknesses in Insured's security posture

Strengths

Endpoint & Network Security

- *{EDR tool}* provides real-time monitoring and automated threat detection
- Modern firewalls and advanced threat prevention features enhance network security.

Structured Vendor & Access Management

- Third-party vendors are vetted through *{process/policy}* with quarterly security audits.
- Role-based access control (RBAC) is enforced, ensuring least privilege access.

Proactive Security Awareness & Incident Response

- Quarterly phishing simulations help train employees against social engineering attacks.
- Bi-annual tabletop exercises prepare IT staff for incident response scenarios.

Areas for Improvement

Backup & Disaster Recovery Implementation

- Backup policy is still being implemented, meaning full coverage and reliability may not yet be established.
- Ensure testing and documentation of recovery time objectives (RTO) or recovery point objectives (RPO) for business continuity planning.

Patch & Vulnerability Management Refinements

- Monthly scanning is performed, but faster remediation for high-risk vulnerabilities could further reduce exposure.
- Patch compliance tracking is in place, but greater automation could help streamline deployments.

Formalization of Internal Security Testing

- Internal penetration testing *{at frequency}*, but adding structured remediation validation ensures identified risks are properly addressed.
- Security configuration audits should be expanded to verify firewall, endpoint, and cloud settings regularly.

Recommended and prioritized solutions for improvement

Solution Recommendations

Area for Improvement:

The company collects sensitive data in its web and mobile apps but has not conducted a dedicated security assessment. This may leave vulnerabilities unaddressed.

Solution: Conduct a Web & Mobile Application Penetration Test

A penetration test will evaluate how sensitive data is processed, stored, and protected in web and mobile applications. It will identify security gaps, misconfigurations, and risks of unauthorized access, ensuring alignment with OWASP and industry best practices. Simulating a real-world attack, testers will attempt to exploit vulnerabilities like injection flaws, weak authentication, and improper data handling to assess the system's resilience.

Improvement:

- Formalization of Internal Security Testing

Area for Improvement:

Without a clear understanding of data flows, the company may face risks related to improper storage, unauthorized access, or regulatory non-compliance.

Solution: Perform a Data Security & Privacy Risk Assessment

A risk assessment will map how sensitive data is collected, stored, and transmitted across systems, ensuring proper security controls are in place. It will identify gaps in encryption, access controls, and regulatory compliance. Simulating real-world data exposure risks, the assessment will evaluate potential misuse, unauthorized access, and insider threats to strengthen protections.

Improvement:

- Patch & Vulnerability Management Refinements