

Building a Cybersecurity Foundation for AI Readiness



As organizations explore the transformative potential of artificial intelligence (AI), it's critical to prioritize cybersecurity. AI systems rely on sensitive data, complex integrations, and interconnected systems — all of which can become prime targets for cyber threats if not properly secured.

For small and midsize businesses (SMBs), cybersecurity isn't just a technical concern — it's a business imperative. This checklist will guide you through the essential steps to establish a strong cybersecurity foundation, ensuring your AI initiatives can scale securely and sustainably.

ANTICIPATE

Recognize Cybersecurity as a Business Priority: Treat cybersecurity as a core business responsibility; not just an IT issue. Ensure executive-level ownership and oversight of your cybersecurity strategy.

Assess Your Current Security Posture: Conduct a thorough review of your existing cybersecurity practices, tools, and vulnerabilities. Identify gaps that could expose your AI systems to risk.

Understand AI-Specific Risks: Evaluate how AI will increase the number of systems, data flows, and integrations in your organization. Identify potential attack surfaces and prioritize securing them.

Develop a Cybersecurity Roadmap: Create a plan that aligns with your AI goals, outlining immediate actions, long-term strategies, and key milestones for improving security.

RESPOND

Designate a Cybersecurity Leader: Assign an internal team member or external partner to oversee cybersecurity efforts. This ensures accountability and timely decision-making.

Develop an Incident Response Plan: Create a clear, actionable plan for responding to cyber incidents. Include steps for containment, communication, and recovery.

Monitor for Threats: Use tools or managed service providers to continuously monitor your systems for suspicious activity and potential breaches.

WITHSTAND

Implement Basic Cybersecurity Measures: Start with proven, cost-effective safeguards:

- Use strong, unique passwords for all accounts.
- Enable multi-factor authentication (MFA) wherever possible.
- Regularly update software and systems to patch vulnerabilities.
- Perform consistent data backups to protect against ransomware and data loss.

Leverage Affordable Security Tools: Use tools like Microsoft 365's built-in security features, cloud-based backup solutions, and endpoint protection software to secure your systems without straining your budget.

Secure Data Flows and Integrations: Ensure that all data used by AI systems is encrypted in transit and at rest. Review third-party integrations for potential vulnerabilities.

RECOVER

Test Your Recovery Plan: Regularly test your disaster recovery and business continuity plans to ensure they work as intended. Simulate scenarios to identify gaps and improve response times.

Review and Update Security Practices: Conduct biannual reviews of your cybersecurity posture to account for evolving threats, business changes, and technology updates.

Invest in Scalable Solutions: Choose security tools and services that can grow with your organization and adapt to new AI-driven demands.

Your Takeaway: No matter how much — or little — your organization has incorporated AI tools into its operations, Rehmann's AI experts can ensure your AI foundation is solid and safe, internally and externally. To learn more about Rehmann's AI Consulting services, visit: www.rehmann.com/solutions/ai-consulting/.