Rehmann Recommends: 15 Security Moves to Make Before Your Org Incorporates AI

In today's rapidly evolving digital landscape, integrating artificial intelligence (AI) into small and medium-sized enterprises (SMEs) offers unprecedented opportunities for innovation, efficiency, and competitive advantage. However, this technological leap forward also introduces complex cybersecurity challenges that require proactive and robust measures to ensure the safety and integrity of your organization's digital assets.

That's where Rehmann comes in. Our expertise in AI and cybersecurity positions us uniquely to guide and support your organization through every step of implementing AI securely and effectively. From conducting comprehensive cybersecurity assessments to developing tailored incident-response plans, we ensure your AI initiatives are built on solid data governance, secure data storage, and a strong culture of cybersecurity awareness.

Because security is at the forefront of our strategy, we enable your team to confidently navigate the complexities of AI integration leveraging its full potential, while safeguarding your organization against the evolving threats of the digital age.

As you look to implement AI within your organization, consider addressing the following:

1. **Cybersecurity Assessment:** Start with a comprehensive cybersecurity assessment of the organization's existing infrastructure and practices. Identify vulnerabilities, potential risks, and data protection requirements specific to AI initiatives.
2. **Data Governance:** Establish strong data governance policies and practices, including data classification, encryption, and access controls. Ensure that any sensitive data used in AI applications is adequately protected.
3. **Secure Data Storage and Processing:** Implement secure storage solutions for AI datasets and models. Apply encryption —both at rest and in transit — to safeguard data integrity.
4. **User Access Controls:** Enforce strict access controls for AI systems and data. Ensure that only authorized personnel can access and manipulate AI models and data.
5. **Security by Design:** Incorporate security into the AI development process from the beginning. Perform security testing and code reviews during AI model development to identify and mitigate vulnerabilities.
6. **AI Model Security:** Monitor AI models in production for anomalies and potential attacks. Implement measures to protect against adversarial attacks and ensure model fairness and accountability.
7. **Incident Response Plan:** Develop a robust incident-response plan specifically tailored to AI-related threats and breaches. Ensure that your organization has clear protocols in place detailing how to react and recover in case of a security incident.
8. **Training and Awareness:** Educate (and continue to re-educate) employees about the cybersecurity risks associated with AI. Provide regular training on safe practices, phishing awareness, and the importance of data protection.
9. **Third-Party Vendors:** If using third-party AI services or solutions, vet their security measures thoroughly. Ensure that their practices align with your organization's cybersecurity standards.
10. **Regulatory Compliance:** Stay informed about relevant data privacy and AI regulations in your industry or region (e.g., GDPR, HIPAA). Ensure that AI initiatives comply with these regulations.
11. **Continuous Monitoring:** Implement continuous monitoring and auditing of AI systems to ensure prompt detection of any unusual behavior or security breaches.
12. **Cybersecurity Team:** Ensure that your organization has a skilled cybersecurity team that specializes in AI security, thoroughly understands your organization's systems and processes, and is vigilant about the latest threats and mitigation techniques in the cyber space.
13. **Documentation and Reporting:** Maintain detailed records of AI system configurations, access logs, and security incidents. Report any breaches or incidents to relevant authorities as required by law.
14. **Cybersecurity Awareness Culture:** Foster a culture of cybersecurity awareness throughout your organization. Encourage employees to report security concerns promptly.
15. **Cybersecurity Partnerships:** Consider collaborating with cybersecurity experts and organizations that specialize in AI security. Leverage their expertise to strengthen your cybersecurity strategy.