Obtainium.ai

ENGINEERED INTELLIGENCE. REAL IMPACT.

AI Security for Small Business: Build It In

Obtainium.ai LLC

Engineered Intelligence. Real Impact.

Why AI Automation Creates New Security Risks

KPMG research shows cybersecurity is now the top investment priority inside AI budgets. AI agents don't just store data — they act on it.

More system access. Automated workflows need permissions across email, databases, CRM, and third-party platforms.

Fewer human checkpoints. The whole point of automation is removing manual steps — which were also informal security reviews.

Faster failure. A compromised workflow can execute hundreds of bad actions before anyone notices.

What 'Secure by Design' Means

- **Least privilege access** — only what the automation needs
- **Human-in-the-loop** for high-stakes actions
- **Audit trails** — log every significant action
- **Separation of environments** — test before touching real data
- **Vendor security review** — SOC 2, data retention policies

A Pre-Deployment Checklist

Access: What systems does this connect to? More access than needed?

Data: What customer data does it touch? Where is it stored?

Failure: What happens if it runs incorrectly? How quickly would you know?

Oversight: Human review points for high-stakes actions? Activity logs?

Vendor: Documented security practices? Breach notification policy?

Key Takeaways

- AI automation expands your attack surface
- Security should be designed in before deployment
- Least privilege, human checkpoints, and audit logs are basics any business can implement
-

Run through the checklist before any automation goes live