



## Risk Readiness Quick Guide

# CYBER SAFETY & AI RISK

### Key Message

As cybercriminals increasingly leverage AI, organizations must strengthen cybersecurity controls, employee education and data protection strategies to reduce exposure.

### Key Takeaways

- AI is making phishing and social engineering attacks more convincing.
- Deepfake technology can be used to manipulate employees into sharing information or authorizing transactions.
- Weak passwords and delayed software updates remain common vulnerabilities.
- Employee awareness is a critical component of cyber risk management.
- Organizations should prioritize data protection and evaluate modern security frameworks.

### ACTION ITEMS

- Review employee cybersecurity awareness training.
- Evaluate password and multifactor authentication practices.
- Ensure software patching and update procedures are current.
- Assess incident response and business continuity plans.
- Conduct a cyber risk assessment focused on emerging AI threats.



#### Ready to prepare?

**Sean Majewski**

Risk Advisor - Casualty Loss Control

P 260-969-3975

E [sean.majewski@hylant.com](mailto:sean.majewski@hylant.com)