AI, CYBER RISK, AND GOVERNANCE

The Board's Role in Overseeing Risk in a Machine-Driven World

AI-driven tools are transforming how organizations operate—but they can also create new vulnerabilities. Boards must ensure that innovation doesn't outpace internal safeguards.

WHY IT MATTERS

AI models can introduce risk in unexpected ways: **bias**, **hallucination**, **lack of explainability**, and **security gaps** from unvetted third-party tools. Many are being adopted without formal governance.

WHAT DIRECTORS SHOULD KNOW

- AI models learn from data—if that data is **sensitive**, **incomplete**, or **biased**, it can expose the organization to **regulatory** or **reputational risk**.
- Automation increases the **speed and scope of errors**, one bad algorithm can do more harm than a thousand employees.
- Third-party tools (especially GenAI) often integrate with internal systems—do you know what **permissions** they're granted?

OVERSIGHT PRIORITIES

1. **Ensure** management has an inventory of all AI and ML tools currently deployed—including shadow IT.
2. **Ask** whether AI tools undergo cybersecurity review before deployment. Are these tools explainable and auditable?
3. **Request** a briefing on the organization's AI governance policies—if they don't exist yet, that's a risk signal.
4. **Confirm** alignment with broader frameworks (e.g., NIST AI Risk Management Framework, ISO/IEC 42001).

BOARD PRACTICES

- **Require** periodic updates on AI risk from the CIO/CISO or equivalent.
- **Mandate** internal audit or external assurance over AI systems if they support core operations or reporting.
- **Push** for cross-functional AI governance committees—don't let IT operate in a vacuum.
- **Establish** clear escalation paths for AI incidents or anomalies.
- **Ensure** training for board members on emerging technologies and AI governance.

Trustworthy AI starts with governance.

Curious how BACKSTOP can support your AI risk strategy?

Contact us →

support.demo@backstop.ca
+1 (403) 701-2244