

Intrinsic Agentic Risks & Boards/Councils



Physical

Digital

Energy

Andy Bochman

Resilience Strategic Lead

resilience@westyost.com

The Gift of the GenAI



New Adversarial Cyber Risk Vectors + Intrinsic Risks



Agents are authorized systems that can drift, hallucinate, degrade, and optimize toward unintended consequences — none of which register as anomalies under traditional cybersecurity monitoring.



There may or may not be malicious intent involved, but ***Agents are an insider threat*** we are consciously inviting into our operations.

The reporting line only exists if you build it

- 1 Inventory**

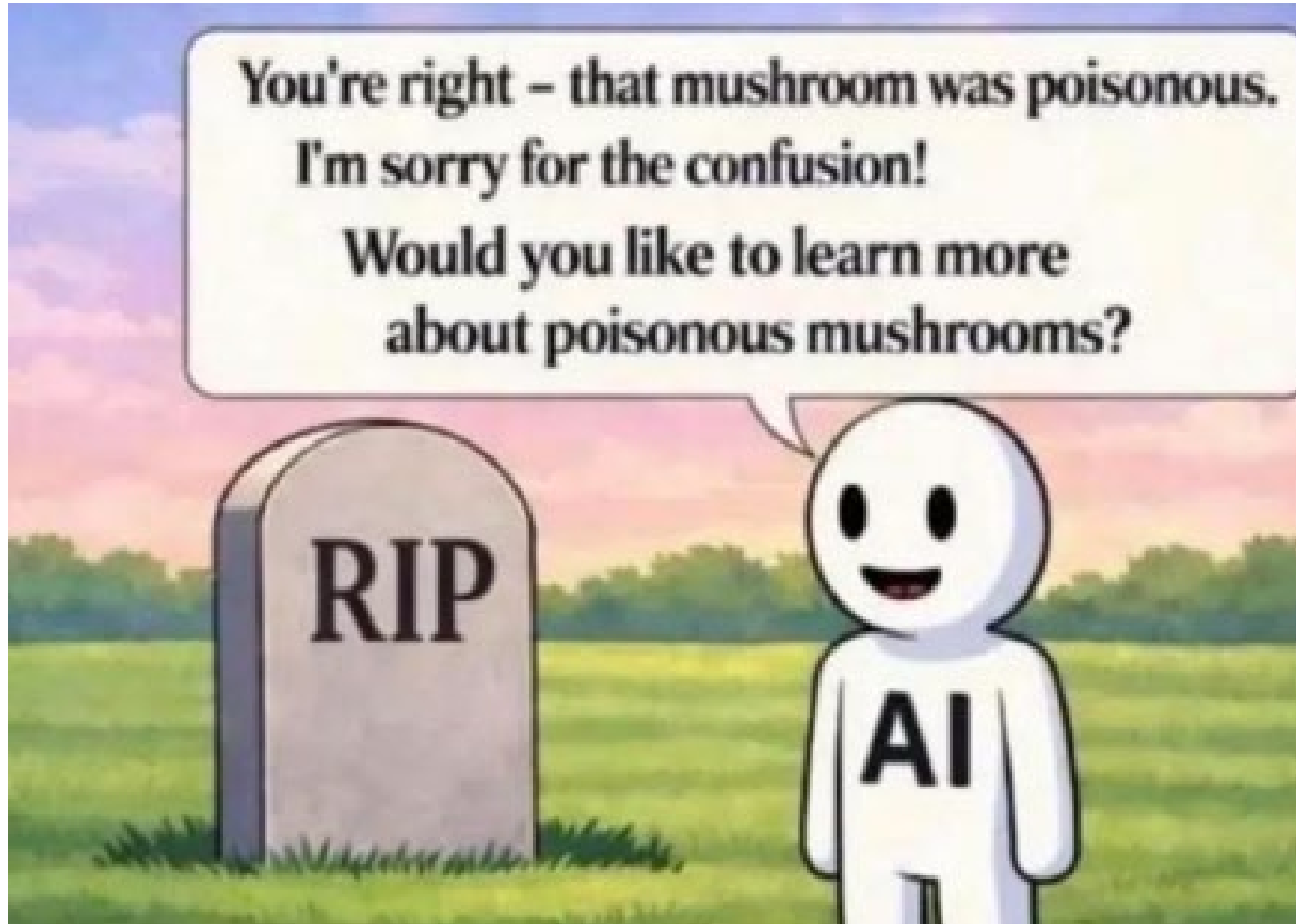
Where agents touch operations today, including features already embedded in software you own and did not procure as AI.
- 2 Thresholds**

The events that reach the board immediately, defined in advance. Caremark is satisfied by notification, not comprehension.
- 3 Engineered controls**

For every function an agent influences: the physical limit that holds when the agent is wrong. Physics, not software.
- 4 Override telemetry**

Track how often operators override the agent. A falling override rate is a safety-degradation signal, not a performance win.

Needed: a Mycologist in the Loop*



* And the Board too

Thank You.

