AI risk isn't one thing.

It's four things.

93% of security leaders expect daily AI attacks.
But most are only watching **one direction.**

Here's the full picture...

swipe →

The One-Dimensional Trap

🛡️ Most AI risk frameworks only cover threats **FROM** AI

🚫 They miss threats **TO** your models, the cost of **NOT** using AI, and the risks of **USING** AI poorly

⚠️ This leaves **75% of your risk landscape** unmanaged

You can't defend what you can't see.

swipe →

The Four Threat Quadrants

💥

FROM AI

Hallucinations, deepfakes, bias, defamation, workforce reduction

🎯

TO AI

Prompt injection, data poisoning, model theft, backdoor attacks

⏳

NOT Using AI

Competitive gap, security holes, operational inefficiency, missed insights

☠

USING AI

Bad actors, cyberattacks, fraud, propaganda, surveillance

Each quadrant demands different strategies, stakeholders, and investment.

swipe →

QUADRANT 1

Threats FROM AI Models

Risks posed by AI capabilities being used against you

- 💬 Hallucinations
- 🎭 Deepfakes
- ⚖ Bias & Discrimination
- 🔒 Data Privacy
- 📢 Reputation Damage
- 👥 Workforce Reduction
- 📜 Regulatory Risk
- 🗡 Defamation

⚠ **93%** of security leaders are bracing for daily AI-enabled attacks. This isn't a future concern -- it's present reality.

The same tech helping you is being weaponized.

swipe →

QUADRANT 2

Threats TO AI Models

Your AI systems themselves are attack surfaces

- 🔥 Prompt Injection
- 🕷 Model Stealing
- ☢ Data Poisoning
- 🔐 Data Exfiltration
- 🐛 Backdoor Attacks
- 📄 Plagiarism
- $ Tokenisation Exploits
- 📜 Compliance Risk

🛠 **MITRE ATLAS** provides a structured taxonomy of these threats -- the ATT&CK framework for AI systems.

If it has an API, it has an attack surface.

swipe →

QUADRANT 3

Threats from NOT Using AI

The risk of standing still

📈 Market Competitiveness

📊 Scaling to Demand

🛡️ Security Gaps

⚙️ Operational Inefficiency

🔍 Missed Data Insights

📈 Organizations seeing real AI returns aren't experimenting. They're **operationalizing**. They're redesigning workflows, not just adding AI as a feature.

Inaction is a strategy. A losing one.

swipe →

QUADRANT 4

Threats USING AI Models

When AI becomes the weapon

- 👻 Bad Actors
- 💻 Automated Cyber Attacks
- 📷 Deepfakes & Misinfo
- 👁️ Surveillance & Control
- 📣 Propaganda
- 💰 Financial Fraud
- 📦 Dropshipping Scams
- ⚖️ Legal & Ethical Risk

⚖️ **EU AI Act:** penalties up to **7% of global revenue** for serious violations. The cost of getting this wrong is existential.

Your AI initiatives can create as many problems as they solve.

swipe →

AI risk is four-dimensional.

Is your strategy?

📝 **Read the full framework**
myyearindata.com

👥 **Follow me on LinkedIn**
Scott Bell

DailyDatabricks.Tips

Databricks.News

Powered by Rapid Data