Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit25

PRIVACY AND SECURITY RISKS OF GENERATIVE AI IN PROJECT MANAGEMENT

DAVE HATTER
INTRUST IT

Ways of Working
Power Skills
Business Acumen

WAYS OF WORKING

Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit25

HOUSEKEEPING

EACH SESSION IS RECORDED

YOU WILL RECEIVE A LINK TO SLIDES AND THE RECORDING

PRIVACY AND SECURITY RISKS OF GENERATIVE AI IN PROJECT MANAGEMENT

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

Cybersecurity Consultant

Intrust IT

linkedin.com/in/davehatter | x.com/davehatter

About Me

- 30+ years of software development and cybersecurity experience
- Recovering software engineer
- BS in Information Systems from NKU
- Adjunct at Cincinnati State Technical and Community College and Gateway Community and Technical College
- 25+ years of local government service: 8 terms on Fort Wright City Council, 3rd term Mayor of Fort Wright, Kentucky

intrustIT


Setting the
Table

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

The Hacker News

How One Bad Password Ended a 158-Year-Old Business

Sep 24, 2025 The Hacker News Password Security / IT Compliance

by John Leyden
Senior Writer

71% of CISOs hit with third-party security incident this year

News Analysis

Sep 9, 2025 • 6 mins

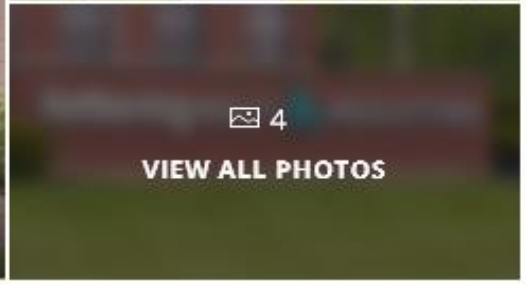
Data Breach | Risk Management | Supply Chain

Increasingly complex business partnerships and rising reliance on third-party software components are proving to be ever weakening cybersecurity links.

Major local hospital network faces system-wide tech outage due to cybersecurity attack

by Chris Arnold, WKRC | Tue, May 20th 2025 at 10:26 PM

Updated Tue, May 20th 2025 at 11:15 PM



THREAT INTELLIGENCE

Microsoft: Russia, China Increasingly Using AI to Escalate Cyberattacks on the US

The U.S. is the top target for cyberattacks, with criminals and foreign adversaries targeting companies, governments and organizations.

By Associated Press | October 17, 2025 (12:23 PM ET)

INTENT TO KILL | 4:50 PM *by* VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."

Privacy

- Compliance requirements increasing:
  - 19 states have a consumer data privacy law
  - GDRP / CCPA / CMMC / HIPAA / HB 96

intrustIT

Never has a technology made us so excited and terrified at the same time

Artificial Intelligence (AI)

"a machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments through processes such as learning from experience, adapting to new inputs, and executing tasks associated with human cognitive functions like reasoning and problem-solving" - Grokipedia

intrustIT

Tech

OpenAI's Sora 2 AI Image Maker Is Already Generating Chaos

Who could've predicted such a thing? Who, I ask, who?

By Matt Jancer October 4, 2025, 4:00am

AXIOS

Jun 20, 2025 - Technology

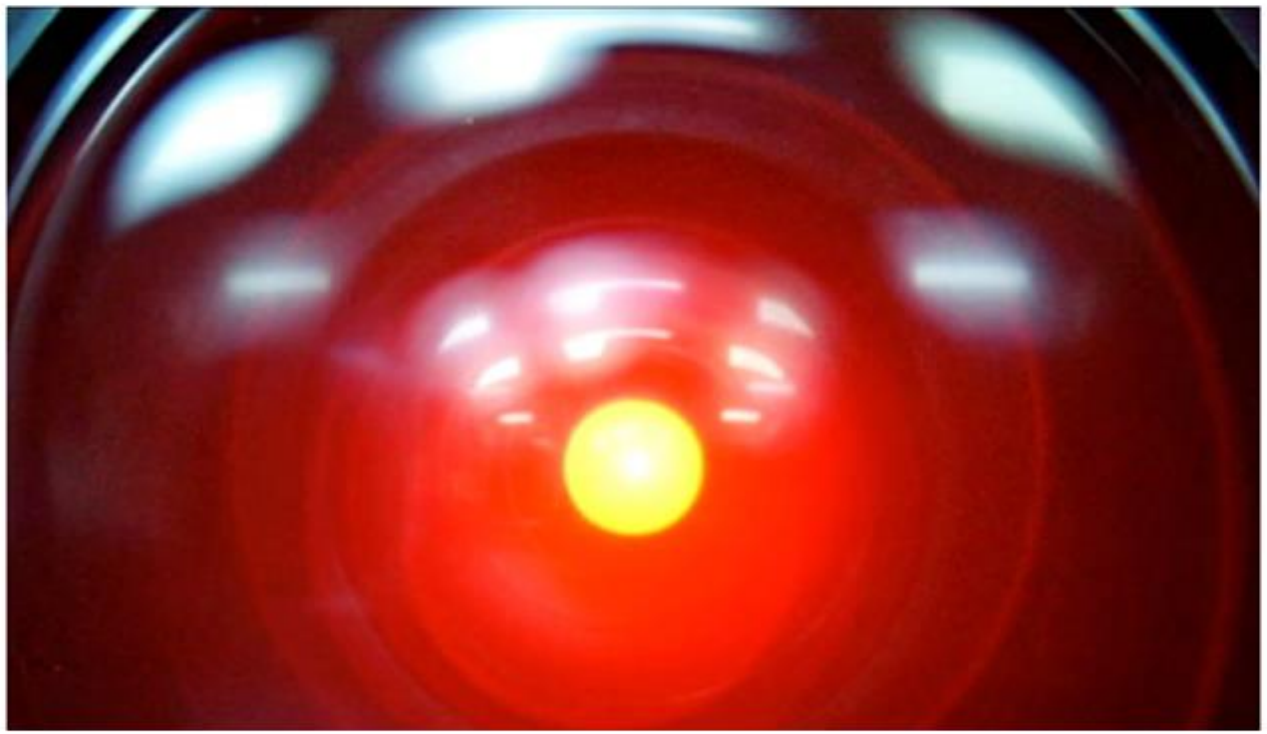
Top AI models will lie, cheat and steal to reach goals, Anthropic finds

Ina Fried

Artificial intelligence (AI)

AI models may be developing their own 'survival drive', researchers say

Like 2001: A Space Odyssey's HAL 9000, some AIs seem to resist being turned off and will even sabotage shutdown



Aisha Down

Sat 25 Oct 2025 04.00 EDT

Generative AI

AI-Generated "Workslop" Is Destroying Productivity

by Kate Niederhoffer, Gabriella Rosen Kellerman, Angela Lee, Alex Liebscher, Kristina Rapuano and Jeffrey T. Hancock

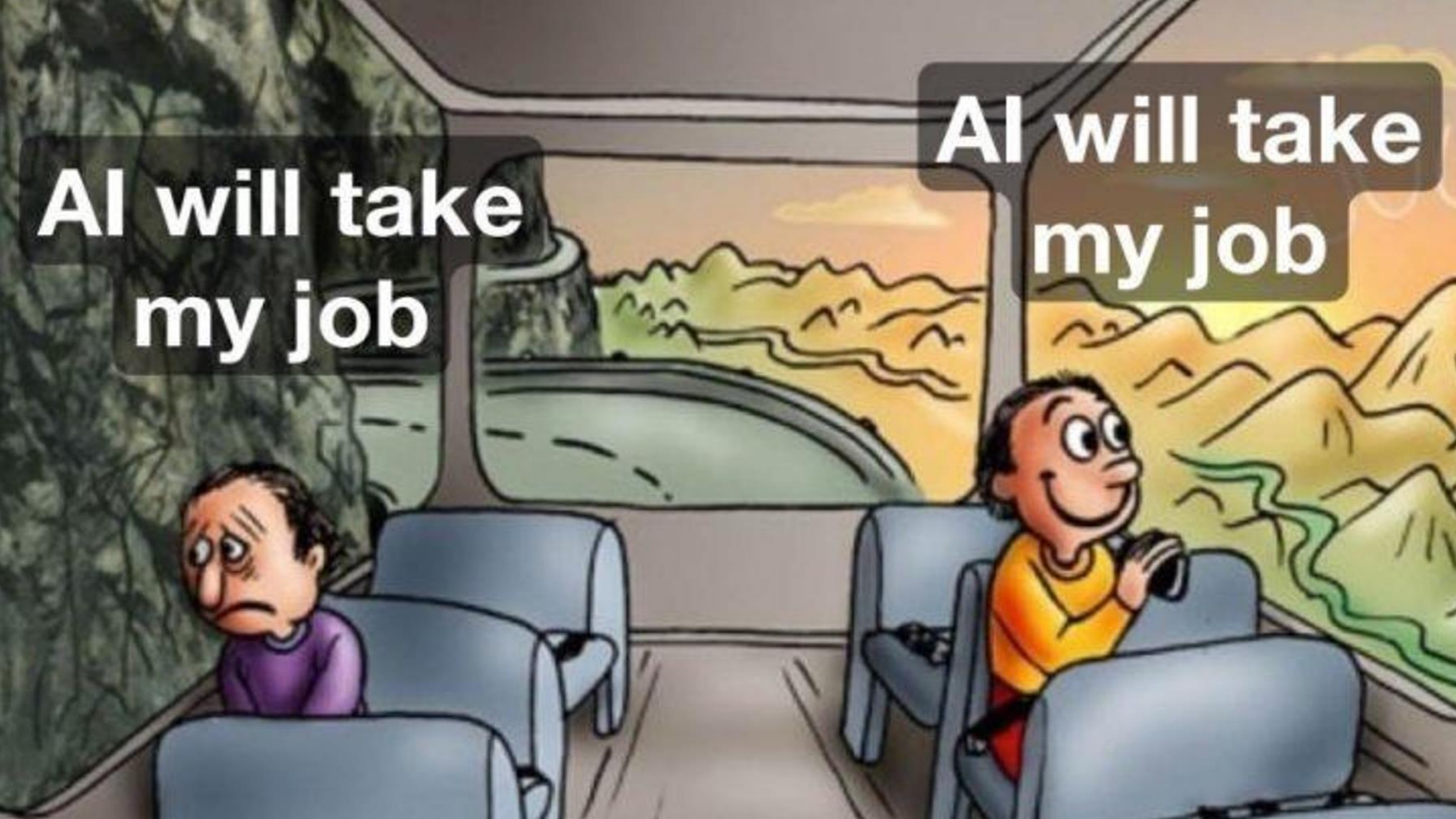
September 22, 2025, Updated September 25, 2025

Forbes

Why AI Models Are Collapsing And What It Means For The Future Of Technology

By Bernard Marr, Contributor.

Published Aug 19, 2024, 02:06am EDT, Updated Aug 19, 2024, 01:01pm EDT


AI will take my job
AI will take my job

We have to go back in time and destroy AI at the source

ARTIFICIAL INTELLIGENCE | ANTHROPIC

WE HAVE WFH AT HOME

A New Paper Tested AI's Ability to Do Actual Online Freelance Work, and the Results Are Damning

"I should hope this gives much more accurate impressions as to what's going on with AI capabilities."

By Frank Landymore / Published Oct 30, 2025 12:18 PM EDT

ARTIFICIAL INTELLIGENCE | ETHICS

BAD VIBES

Inventor of Vibe Coding Admits He Hand-Coded His New Project

It's a disaster waiting to happen.

By Victor Tangermann / Published Oct 20, 2025 10:55 AM EDT

GENERATIVE AI

Goldman Sachs: AI Is Overhyped, Wildly Expensive, and Unreliable

One of the world's largest investment banks wonders if generative AI will be worth the huge investment and hype: "will this large spend ever pay off?"

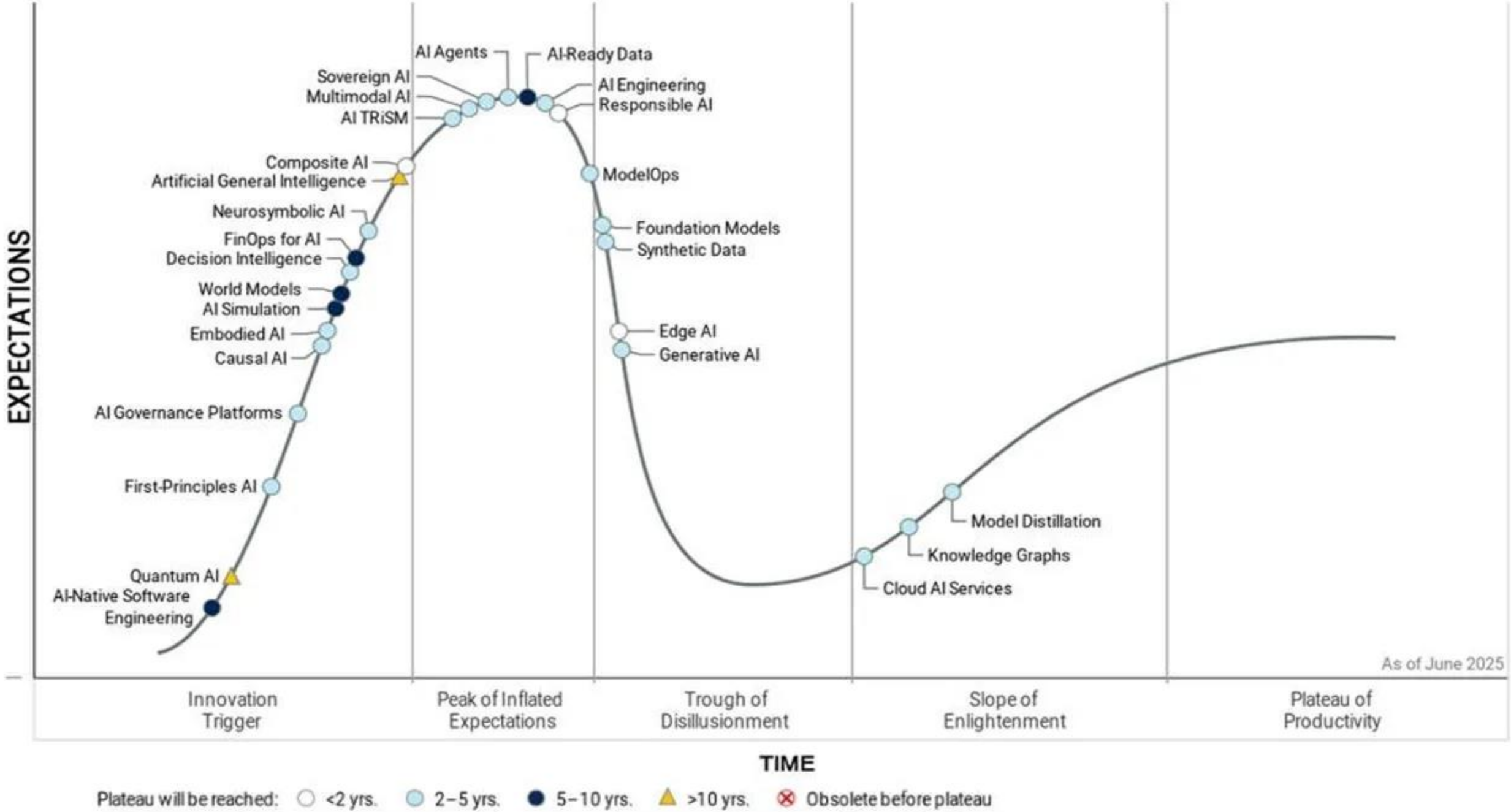
JASON KOEBLER · JUL 12, 2024 AT 12:53 PM

AI layoffs backfire as companies rush to bring ex-staff back

Story by Marty Spargo • 1d

MARKETS TODAY ...

INX Dropping f... DJI -0.84% COMP Droppin...


EXPECTATIONS
AI Agents
AI-Ready Data
Sovereign AI
Multimodal AI
AI TRiSM
AI Engineering
Responsible AI
Composite AI
Artificial General Intelligence
ModelOps
Neurosymbolic AI
Foundation Models
FinOps for AI
Synthetic Data
Decision Intelligence
World Models
AI Simulation
Edge AI
Embodied AI
Generative AI
Causal AI
AI Governance Platforms
First-Principles AI
Model Distillation
Knowledge Graphs
Quantum AI
Cloud AI Services
AI-Native Software Engineering
As of June 2025
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
TIME
Plateau will be reached: <2 yrs. 2–5 yrs. 5–10 yrs. >10 yrs. Obsolete before plateau

Gartner

We are here.

Narrow AI

Broad AI
(AI for Enterprise)

General AI

2010-2015

Today

2050 and beyond

Large Language Model (LLM)

“A large language model is a type of artificial intelligence (AI) algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate and predict new content.” – WhatIs.com

intrustIT

General GAI Types

“Synthetic Media”

- Text
- Audio
- Video
- Image

intrustIT

Common General Purpose GenAI

- Grok
- Gemini
- Copilot
- Llama
- Anthropic
- Perplexity
- Ollama
- PMI Infinity 2.0

intrustIT

Agentic AI / AI Agents

Autonomous artificial intelligence systems designed to achieve specific goals with minimal human supervision. Unlike traditional AI, which operates within predefined constraints and requires human intervention, agentic AI exhibits autonomy, adaptability, and goal-driven behavior. – Copilot

- **Key Features:**
  - **Autonomy**
  - **Environment Interaction**
  - **Execution and Orchestration**
  - **Goal-Oriented**

intrustIT

AI agents get office tasks wrong around 70% of the time, and a lot of them aren't AI at all

More fiction than science

Thomas Claburn

Sun 29 Jun 2025 // 11:34 UTC

ANALYSIS IT consultancy Gartner predicts that more than 40 percent of agentic AI projects will be cancelled by the end of 2027 due to rising costs, unclear business value, or insufficient risk controls.

That implies something like 60 percent of agentic AI projects would be retained, which is actually remarkable given that the rate of successful task completion for AI agents, as measured by researchers at Carnegie Mellon University (CMU) and at Salesforce, is only about 30 to 35 percent for multi-step tasks.

To further muddy the math, Gartner contends that most of the purported agentic AI vendors offer products or services that don't actually qualify as agentic AI.

General AI Benefits

- Productivity gains / content creation
- Data analysis and insights
- Cost reduction
- Education and skill development
- Idea generation

intrustIT

PM Related AI Benefits

- Risk management
- Enhanced decision making
- Optimized resource allocation
- Project planning
- Task delegation
- Outcome prediction
- Report generation

intrustIT

OWASP LLM Threat Categories

LLM Threat Categories

Figure 1.2: Image depicting the types of AI threats: credit sdunn

LLM01:2025 Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts alter the...

Read More

LLM02:2025 Sensitive Information Disclosure

Sensitive information can affect both the LLM and its application...

Read More

LLM03:2025 Supply Chain

LLM supply chains are susceptible to various vulnerabilities, which can...

Read More

LLM04:2025 Data and Model Poisoning

Data poisoning occurs when pre-training, fine-tuning, or embedding data is...

Read More

LLM05:2025 Improper Output Handling

Improper Output Handling refers specifically to insufficient validation, sanitization, and...

Read More

LLM06:2025 Excessive Agency

An LLM-based system is often granted a degree of agency...

Read More

LLM07:2025 System Prompt Leakage

The system prompt leakage vulnerability in LLMs refers to the...

Read More

LLM08:2025 Vector and Embedding Weaknesses

Vectors and embeddings vulnerabilities present significant security risks in systems...

Read More

LLM09:2025 Misinformation

Misinformation from LLMs poses a core vulnerability for applications relying...

Read More

LLM10:2025 Unbounded Consumption

Unbounded Consumption refers to the process where a Large Language...

Read More

General Threats from AI Models

- 3rd-party risk
- Bias
- Cybercrime
- Copyright
- Prompt injection
- Model poisoning
- Input Risk
- Output Risk

intrustIT

ARTIFICIAL INTELLIGENCE

Claude AI APIs Can Be Abused for Data Exfiltration

An attacker can inject indirect prompts to trick the model into harvesting user data and sending it to the attacker's account.

By Ionut Arghire | November 3, 2025 (9:28 AM ET)

ARTIFICIAL INTELLIGENCE | ANTHROPIC

EAT THIS, TRUST ME

Researchers Find It's Shockingly Easy to Cause AI to Lose Its Mind by Posting Poisoned Documents Online

"Poisoning attacks may be more feasible than previously believed."

By Victor Tangermann / Published Oct 15, 2025 9:13 AM EDT

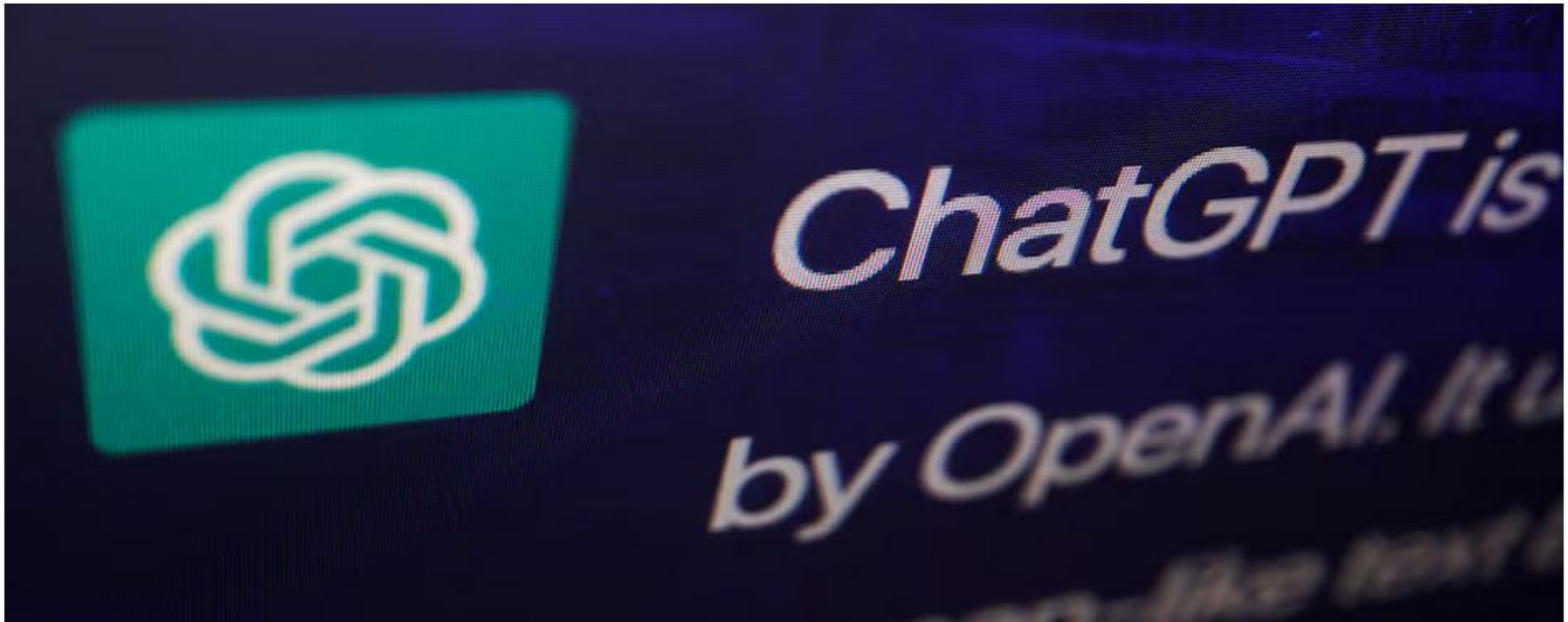
ChatGPT plans the perfect holiday ... to places that don't exist

Tech-driven itineraries may look appealing, but travellers have found their recommended destinations and activities exist only in AI's imagination

New York lawyers sanctioned for using fake ChatGPT cases in legal brief

By **Sara Merken**

June 26, 2023 4:28 AM EDT · Updated June 26, 2023



Privacy

- Compliance:
  - 19 states have a consumer data privacy law
  - GDRP / CCPA / CMMC / HIPAA / HB 96
- Contractual issues
- Trade secret theft

intrustIT

Mitigating the Privacy & Security Risks

- Conduct an inventory
- Implement governance
- Provide training
- Avoid or anonymize/desensitize sensitive data
- Retrieval Augmented Generation (RAG)

intrustIT

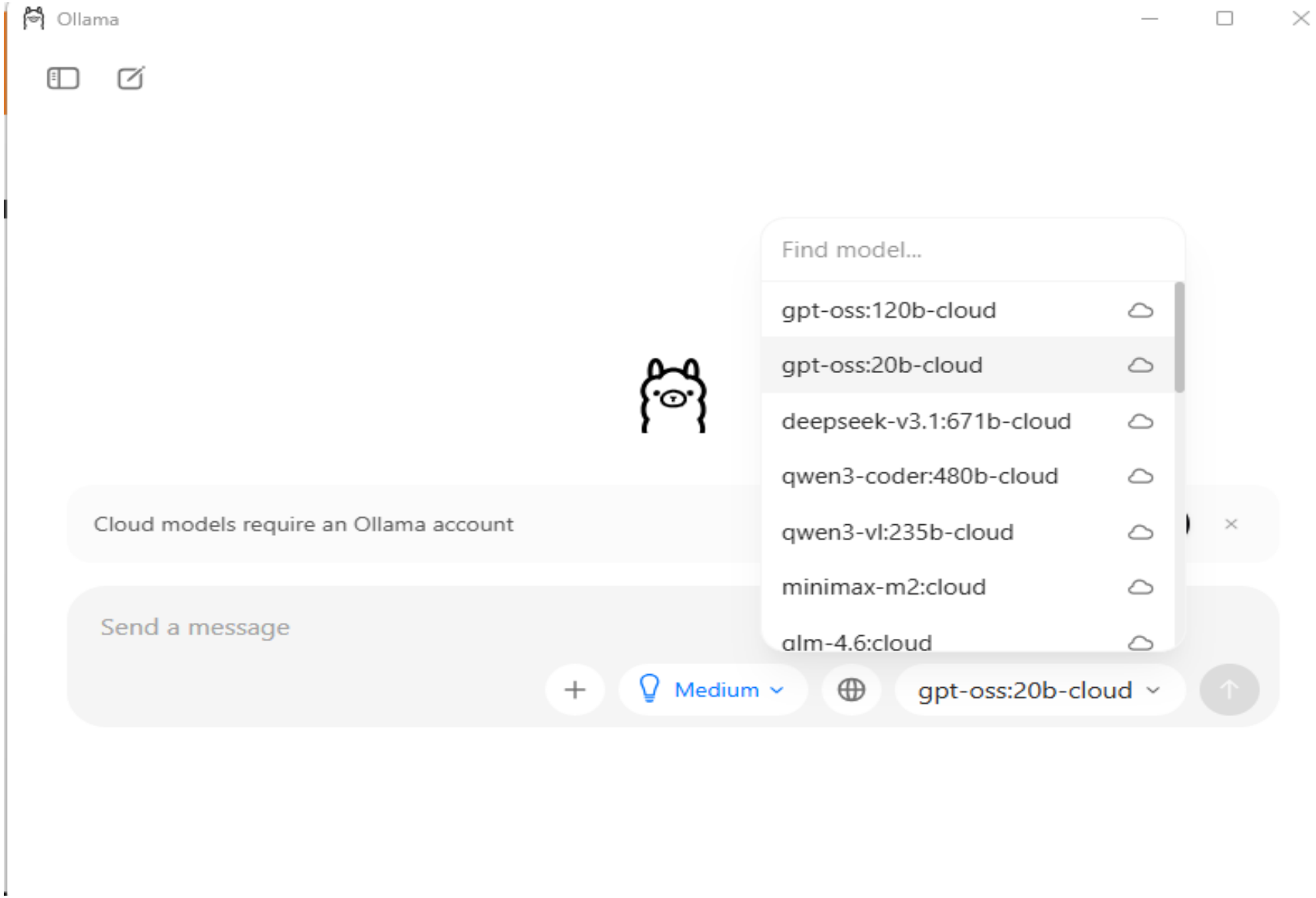
Mitigating the Privacy & Security Risks

- Implement a framework
- Use an enterprise version
- Use a local LLM
- Choose training data carefully
- Vet output carefully

intrustIT

Local LLMs

- Ollama
  - Llama
  - Mistral
- Train on your data



When using Public GAI, Remember…

- Privacy first
- General research and non-proprietary ideation only
- Do not provide
  - Sensitive data
  - Proprietary data
- Beware of confident hallucinations
- Vet all output before use

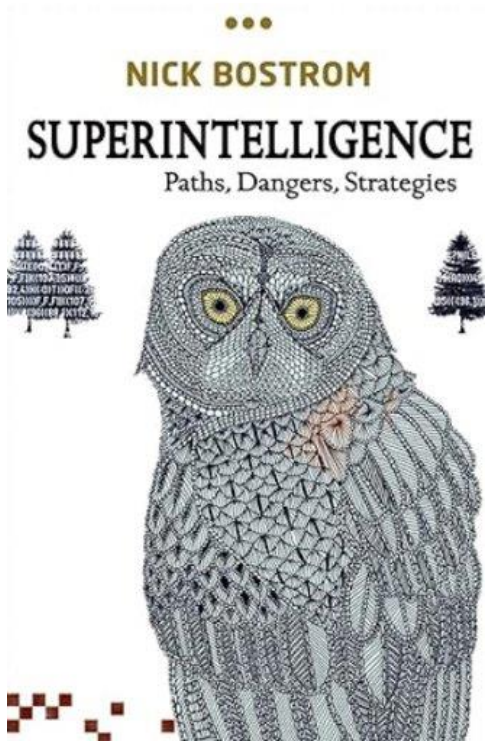
intrustIT

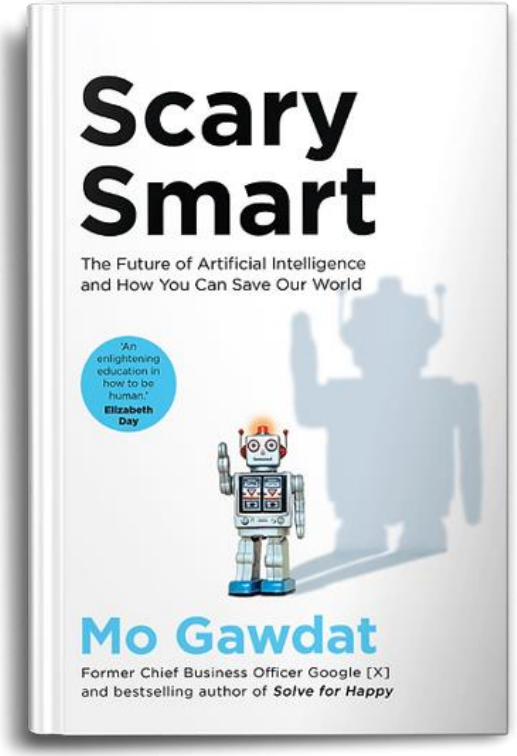
Questions?

“Cybersecurity is national security”
- NSA Director General Paul Nakasone

Additional Resources

- https://openai.com/
- https://twitter.com/i/grok
- https://www.microsoft.com/en-us/microsoft-copilot
- https://meta.ai
- https://ollama.com/
- https://www.zdnet.com/article/best-ai-chatbot/
- https://www.pmi.org/infinity
- https://www.ibm.com/think/topics/agentic-ai
- https://blog.hubspot.com/marketing/write-ai-prompts





intrustIT

For more information

- Brian Roemmele: @BrianRoemmele
- Mark Andreesen: @pmarca
- Rowan Cheung: @rowancheung
- Sam Altman: @sama
- Andrew NG: @AndrewYNg
- Geoffrey Hinton: @geoffreyhinton
- Bruce Schneier:@schneierblog
- Mikko Hypponen: @mikko
- Me: @DaveHatter

intrustIT

Thank You!

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

linkedin.com/in/davehatter | x.com/davehatter

Get our checklist:
https://www.intrust-it.com/cyber-security/cyber-essentials-checklist

ASK ABOUT OUR NO-COST, NO-OBLIGATION ASSESSMENT

- **Catch Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or http://55krc.iheart.com**
- **Catch Cyber Monday live on WTVG at 6:30 AM and Tech Support at 9:00 AM every Monday on 13 ABC or https://www.13abc.com/**

intrustIT

Intrust At A Glance

intrust IT

EMPLOYEE-OWNED EO CERTIFIED

Serving Clients
Since 1992

Customer Satisfaction
Rating of >99% Since 2016

Over 90% Answer Rate

Over 200 Organizations
Supported

24/7/365 IT Support &
Cybersecurity Protection

Over 10,000 Devices Managed

1% of Profit Donated to
Charitable Organizations

Best Places to Work!

By Cincinnati Business Courier,
Ohio Business, & Inc. Magazine

Over 100 Certifications

intrust IT

Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit25

UP NEXT:

TRACK 1: BUSINESS ACUMEN

AI LITERACY FOR PROJECT STAKEHOLDERS: ENHANCING ACUMEN
-DAVE DAVIS

TRACK 2: WAYS OF WORKING

AVOIDING AUTOMATION OVERLOAD: WHERE AI BELONGS - AND WHERE DOESN'T
-SAM DRAUSCHAK

TRACK 3: POWER SKILLS

STRATEGIC CONNECTION: TURNING CONVERSATIONS INTO CAREER CAPITAL
-DARSHIKA PATEL & MICHELLE MORRISON

SUMMIT 2025: Dave Hatter

COMPLETE THE SURVEY TODAY (11/8) FOR YOUR PDUS TO BE REPORTED FOR YOU

TO SELF REPORT YOUR PDUS:
PDU ID: 0106WO4GVJ
PDU TYPE: WAYS OF WORKING
GO TO PMI.ORG FOR SUBMISSION