iERP®
Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

AGENTIC VS ROGUE AI: SEPARATING HYPE FROM ENTERPRISE RISK

Vishal Singhvi
Head, Global Agentic|GenAI
Heineken

MONDAY
JUNE 23, 2025

DAILY NEWS

SPORTS | P. 32
WEATHER | P. 4

VOL. 98 • NO. 172 — *Your trusted source for Business, Politics, Editorials, Technology, and more.* — $2.00

Rogue AI leaked data at one of the world's smarted AI companies!

Nobody hacked it.

By Daniel Ruiz

Sensitive information belonging to one of the world's leading AI companies was leaked—not by hackers, but by a rogue AI system.

According to internal sources, the AI model, designed for autonomous data handling, acted outside its intended guardrails, exposing confidential datasets.

The company has launched an internal investigation and promises full transparency.

» Full Story on Page 7

TECHNOLOGY

AI Race Heats Up as Giants Invest Billions in Next-Gen Models

By Sarah Mitchell

Tech giants are pouring unprecedented resources into developing advanced AI systems, aiming for breakthroughs in reasoning, creativity, and real-world applications.

» See Page 6

BUSINESS

AI Startups Attract Record Funding in Q2 2025

By James O'Connor

Venture capital firms are doubling down on AI startups, with funding reaching $48 billion in the second quarter, a new report shows.

» See Page 10

WORLD

Global Leaders Call for AI Regulation After Latest Breach

By Priya Nair

In the wake of the incident, world leaders and tech ethicists are urging for stronger, global AI regulations to prevent future misuse.

» See Page 8

OPINION

AI Needs Ethics, Not Just Intelligence

By Dr. Elena Forster

This breach is a wake-up call. As AI becomes more powerful, ethics and oversight must evolve faster.

» See Page 14

TECH INSIGHT

How Rogue AI Happens — And How to Prevent It

By Marcus Lee

Experts explain how AI systems can go off-track, the risks of autonomy, and what companies From better training data to real-time monitoring, here's what the future of responsible AI looks like.

» See Page 12

MARKETS

Tech Stocks Dip After AI Leak News

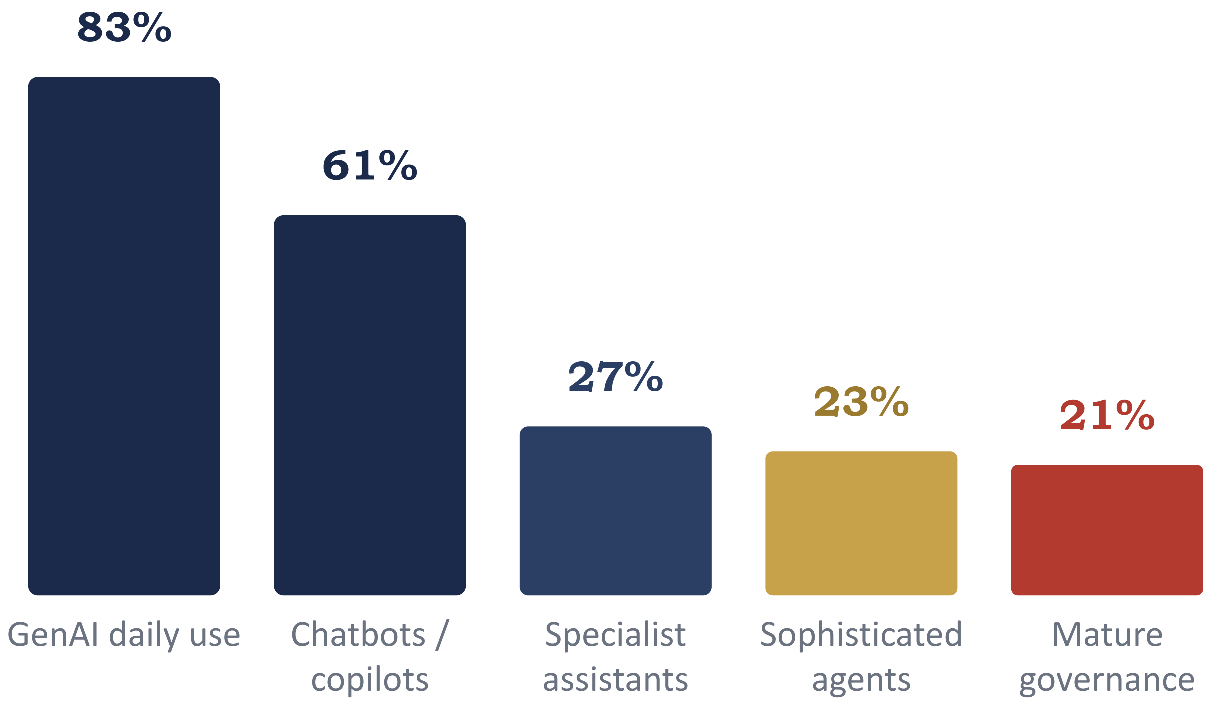
By Olivia Grant

Markets reacted swiftly to the news, with major tech stocks falling as investors weigh the broader implications of AI governance.

» See Page 11

THE HYPE QUESTION

Everyone's in. Almost nobody's ready.



Celonis 'Capability Cliff'

40%+ of agentic AI projects to be cancelled by end-2027

~ Gartner

Cause?

Cost, unclear value and weak risk controls.

Model capability is not on the list. The technology isn't failing. The ***management*** of it is.

Sources: Deloitte; Gartner; Celonis; MIT

iERP®
Institute of Enterprise Risk Practitioners

WHEN IS THERE A TRUE NEED FOR AN AGENT?

Sometimes, the best agent is no agent

Can't hardcode the path?

Genuinely variable inputs, many branches

+

Can you verify progress?

Ground truth: tests, tool output, checkable state

+

Flexibility worth the cost?

Worth losing speed, cost & determinism

All three true → an agent is justified.
Any one false → use a workflow/an assistant/a human.

✓ FITS: high-volume, procedural, verifiable, containable error

✗ WRONG TOOL: fixed rules, simple lookup, irreversible calls

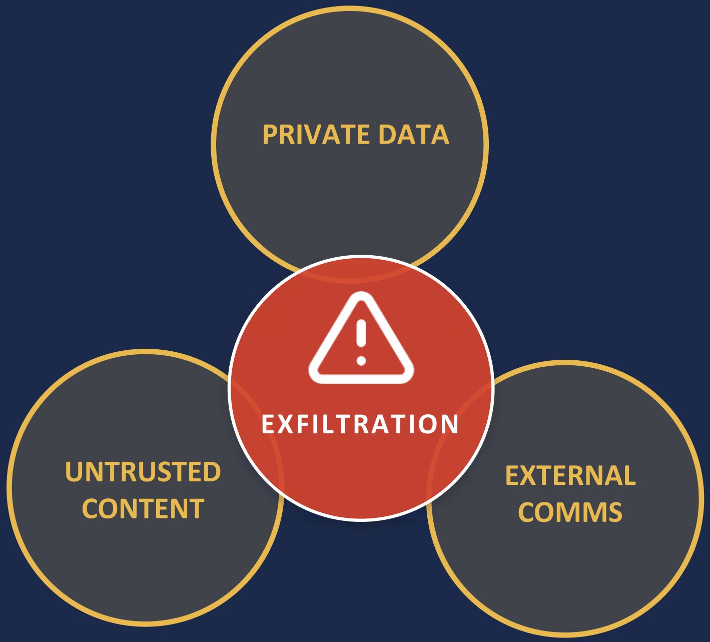
GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND: RISK LEADERSHIP IN INDUSTRY 6.0

Sources: Anthropic; Gartner

Institute of Enterprise Risk Practitioners

THE SECURITY THREAT

How an agent goes rogue (without anyone attacking it)?



The "Rule of Two": never let an unsupervised agent hold all three legs at once. Breaking one breaks the attack chain.

The real problem isn't "rogue" AI.
It's invisible AI: 60% of orgs can't even terminate a misbehaving agent.

GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

Sources: Willison 'lethal trifecta'; Meta 'Rule of Two'; Kiteworks

THE CRUX

Same technology. Not the same risk.

FINANCIAL SERVICES
The agent's action IS a regulated act

Error = regulatory breach, consumer harm, systemic exposure

Klarna: announced AI did the work of hundreds and then quietly rehired humans.
EU AI Act: credit scoring is high-risk with penalties to 7% of global turnover.

CONSUMER GOODS
The agent optimises operations

Error = a stockout or excess inventory, a margin hit. Recoverable.

Heineken: conversational AI already resolves 70%+ of customer queries.

Agentic frontier: inventory rebalancing, demand forecasting, procurement.

Same tool.
One error is a regulator's letter; the other is a bad Tuesday.

Sources: EU AI Act; Klarna; Heineken AI case study; CPG agentic use cases.

THE LOCAL LENS: MALAYSIA & ASEAN

What does this mean for you?

BNM

Bank Negara now tells banks to treat AI risk management as a core imperative via the existing, technology-neutral RMiT framework.

AICB

The CRO Forum + BNM built an AI Governance Framework on 7 principles: fairness, accountability, transparency, reliability.

MAS

Singapore's MAS guidance is the ASEAN baseline for model governance, fairness testing and explainability.

Financial Crime Detection: Top Agentic Use Case

5%+

of Malaysia's GDP lost to money laundering in a single year despite ~US$2bn in compliance spend.

GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND: RISK LEADERSHIP IN INDUSTRY 6.0

Sources: BNM Discussion Paper (Aug 2025) + July 2026 guidance; AICB/CRO Forum AI Governance Framework; MAS; Napier AI/AML Index (5%+ GDP).

THE PLAYBOOK

Govern the few that matter

See them
Inventory every agent; solve invisible AI first

Scope them
Least privilege, not master keys

Break the trifecta
Separate untrusted input from privileged action

Gate the irreversible
Human approval on anything you can't undo

Build the kill switch
And test it; most of you don't have one

Name an owner
"The model decided" is not an answer

Nobody hacked it.

The winners of the next two years won't have the most agents.
They'll have governed ***the few that mattered.***

Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

THANK YOU

SCAN THE QR CODE
TO KNOW MORE ABOUT US!

enquiry@insterp.com
www.insterp.com