CYBERATTACKS & IA

TRENDS 2026

ozngo

Implications for organisations

10 500 Md$

Global Cost of Cybercrime 2026

+72%

AI Cyberattacks YoY 2025

87%

Organisations targeted by an AI attack

LANDSCAPE OF 2026 THREATS

5 attack vectors redefined by AI

+1 265% — **AI Social Engineering**

in AI phishing since 2023. Arup case: $25.6M lost via video deepfake.

Click rate x4 vs human phishing.

97% — **Data poisoning**

of breached organisations had no access controls on their AI models (IBM 2025).

13% have already experienced a model breach.

+160% — **Model Inversion**

increase in AI credential theft in 2025. IP theft, industrial espionage, ransom via exposed model extraction.

69% — **Adversarial ML**

misdiagnoses on manipulated mammograms (UPMC/Nature). Invisible to the human eye — applies to any decision-making model.

79% — **AI/Cloud Supply Chain**

of cloud companies have suffered a breach. 'One-to-many' attack via compromised central provider.

Sources : IBM X-Force 2025 · Verizon DBIR 2025 · FBI IC3 · Microsoft Cyber Signals 2025 · SlashNext · CrowdStrike

THE HACKER 2026

He attacks

- Your data & AI models
- Your perception of Truth
- Your emotions & cognitive biases
- Your dependency chains
- MFA bypass
- Your cloud infrastructure

His objective

Credibility & Trust
Fragment internal truth

Cascading Loss
Assets, business, reputation

Biased Decisions
Via compromised AI models

Operational Paralysis
53 000$/h average downtime cost

93% of executives expect daily AI attacks by end of 2026 WEF Global Cybersecurity Outlook 2026

CONCRETE IMPLICATIONS

questions you must ask… among others

Crisis Communication

Do we have a ready narrative for an 'AI error'? Is our communication aligned with our cloud providers?

Truth Governance

Who owns the truth in the organization? How quickly can you counter a deepfake or a false report?

Culture & Human Reflexes

Can our teams identify signs of a manipulated AI? Do we have a 'stop-the-line AI' protocol?

AI Model Integrity

Are our AI models monitored against corruption? Do we have a non-AI fallback plan if a model is compromised?

Dependency Chains

Have we mapped our AI/cloud providers? Who controls the security of each link?

Intellectual Property

Are our AI endpoints protected? Do we have technical evidence if a proprietary model is stolen or cloned?

SIX IMMEDIATE LEVERS

The foundations of a modern defense

Truth Governance & Evidence Strategy

Define how the organisation establishes what is true vs. doubtful, who arbitrates, and how.Protect and authenticate sensitive official content.

Internal Alert & Critical Intelligence Channel (SME-friendly)

A simple pathway to report incidents, weak signals, AI inconsistencies, or online findings. Aggregate, filter and circulate useful info, even without a dedicated cyber team.

Expanded Resilience: Human, Cultural & Decision Reflexes

A psychological and systemic approach to build vigilance, cohesion and reliable reflexesunder uncertainty, doubt or manipulation.

Mastering Communications Under Pressure

Train executives and spokespersons to handle doubt, confusion and disinformation. The first minutes set the tone for the entire crisis.

Real-World Tests & Simulations

AI scenarios, fake messages, deepfakes, vishing, contradictory signals, etc.You don't discover your crisis plan on the day of the crisis.

Critical Thinking & Anti-Manipulation Reflexes

Train teams to detect cognitive red flags, react without panic, use protection reflexesand report anomalies factually.

A prepared leadership, without a massive cyber budget.

WHO IS OZNGO

Maryse Rebillot

Strategic Advisor on Cyber-AI crises and information integrity

- 20+ years in marketing-communication in High Tech, Cyber security
- Expert in Crisis Management, sensitive Communication, and Information Integrity
- International Executive Marketing Master, INSEAD

linkedin.com/in/maryse-rebillot

Experts Network

Cybersecurity

Cyber defense, White Hacking, Cyber Governance, Data Governance, Legal & Insurance

AI & Technologies

Gen AI, LLM, Vertical AI, Other AI

Human & Communication

Psychology, Medias & Journalists, Sociology

IN AN AI-DRIVEN WORLD, THE ONLY LASTING DEFENSE

Is Human Cohesion

ozngo

contact@ozngo.com