
MILEVA
SECURITY LABS
TURN RISK INTO
OPPORTUNITY

TURNING **AI RISK OPPORTUNITY**

Artificial intelligence is revolutionising the way modern organizations operate, driving rapid innovation and offering new means for achieving a competitive edge. It can be an instrument for positive change – empowering individuals, improving services and benefiting businesses and societies. However, AI incidents can cause substantial monetary and reputational losses to organisations. New AI risk compliance obligations require organizations to manage their AI risk alongside their cyber and information security risk. **Risk managers must strike a difficult balance: addressing emerging vulnerabilities without overly restricting AI's innovative potential.**

n 2024 we conducted a survey of over 100 professionals from different organizations and industries, all grappling with AI adoption. We also conducted interviews with over fifty CISOs and risk professionals to understand their biggest concerns and what they wish other organizations knew about AI risk.

We share this knowledge with you here.

At Mileva Security Labs, we equip professionals with the tools to manage AI risks and be empowered to harness its full potential. **Allowing fear to govern AI use will stifle innovation, undermine competitive advantage, and weaken a company's ability to defend itself against AI-driven threats.**

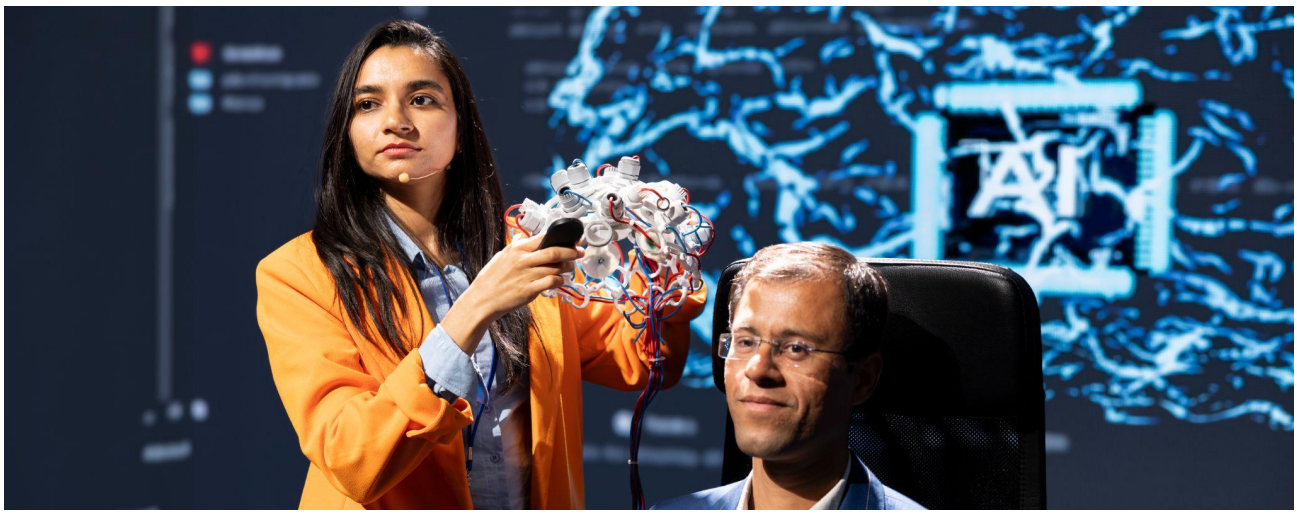
We believe in a future where AI is safe, secure and democratized. For this to happen, we need to build an ecosystem. This ecosystem must comprise knowledge, tools and collaboration. We are working on the knowledge and the tools, but we need you.

Will you join us to ensure the future of AI is one we want to have?

AI incidents cost businesses **$150 billion** in 2023.

Of these **70%** could have been prevented with **basic AI risk mitigations.**

Managing AI risk effectively requires more than just technical solutions; it demands a focus on people and processes.



AI RISK
A NEW DILEMMA

"My AI risk keeps me up at night"
- Fortune 500 CISO

In 2023, over 100 new AI standards were released. Many of these are compulsory, especially for highly regulated industries like healthcare, finance and Government. Proposed legislation like those in the European Union (EU) and the USA are landmark laws that will greatly impact the operations of any organization in or interacting with those states. These wide-ranging policy instruments speak to the critical recognition of AI risk.

AI increases your enterprise's attack surface at every level of operation. Some of these attacks are familiar, and others are entirely unique to AI technologies. AI systems are more dynamic, interactive, and customised than traditional IT environments. Unlike traditional computer systems, which are deterministic and follow a predictable logic, AI is probabilistic, demanding specialized knowledge to secure them effectively. In this environment, the line between AI systems being a tool for progress and a vector for attack is razor-thin.

Just as cyber security applies to every organisation with any information technology, AI security applies to every organisation with AI infrastructure.

Enterprises must now manage their AI risks alongside their safety and security risks to remain compliant.

AI risk is comprised of AI Security - the dynamic technical and governance practices required for safeguarding AI systems from manipulation or disruption by human or AI adversaries - and AI Safety - harm due to misalignment, design flaws, or ethical concerns.

STATISTICS

AI incidents increased by

30%

in 2023.

82.5%

of organizations use AI.

The most concerning **AI risk** for respondents was

BIAS

69%

Of respondents are concerned about the **development and adoption of AI**

57%

Of respondents are confident they **understand what AI is**

45%

Of respondents are confident they **understand what AI Security is**

83%

Of respondents chose the **correct definition of AI**

Mileva's **AI-centric triad** complements the traditional CIA model by providing a practical model for classifying unique AI vulnerabilities into the categories disruption, deception, and disclosure.

DISRUPTION

Preventing interference with the normal functioning of AI

36% of those AI incidents were **disruption attacks**

DECEPTION

Countering manipulation of AI to produce false or misleading outputs.

49% of those AI incidents were **deception attacks**

DISCLOSURE

Protecting sensitive information from being extracted by adversaries.

20% of AI incidents were **disclosure attacks***

*categories are not exhaustive so do not add to 100%

A BETTER WAY TO **THINK ABOUT RISK**

"AI security is an essential component of information security"

- Fortune 500 CTO

In many fields, risk is not seen as a negative but a positive attribute. You cannot grow or find new opportunities without taking risks. The essential thing to know is which risks to accept, and which ones to prevent. Specifically, how to make a decision about how to allocate funds to prevent a risk from occurring.

You may be familiar with risk matrices of high, medium and low risks that do not have a meaningful impact on decision-making. We instead propose an evidence-backed quantitative approach to risk management that drives meaningful decision-making.

IN 2023:

There were
121
AI incidents.

The largest fine was
€20 million
for **AI misuse.**

Only
23%
Of organizations implement AI security controls

The best AI risk management approaches are:

- Data-backed, quantitative and measurable
- Offer clear financial decision allocation
- Map to standards, regulations and legislation
- Can be updated based on expert judgement

“My next biggest priority is AI security””
- Fortune 500 CISO

14.7% Of organizations say they **comply with AI risk standards. More than half** of those **don’t know which ones they comply with.**

OVER 2/3 of organizations rely on **third party AI.**

OVER 1/2 of organizations rely on adapting **existing open source AI.**

The challenge for CISOs is significant, but not dire. As with previous technological revolutions—cloud computing, BYOD—risk managers have proven that they can adapt and overcome.

TECHNOLOGY, PEOPLE + PROCESS: A HOLISTIC APPROACH

“I am still asked what a deepfake is”
- Cyber Security Professional

The current challenge in approaching AI security lies in its fragmented and often misunderstood landscape. Effective risk management does not just focus on technology, but on people and process.
Now is the time for risk managers to prioritise AI security; your adversaries already are. Properly securing AI is not about stifling innovation; it's about empowering organisations to harness AI's full potential without compromising security. With the right tools and expertise, you can stay one step ahead of AI-driven threats and maximise the returns on your AI investments.

AI innovation does not need to come at the expense of resilience, privacy, and data integrity, however every business needs to see AI risk management as one of the many technologies they incorporate in their business risk mitigation and strengthening cyber security posture. When you mitigate risk you can embrace opportunity. Every organization needs to have strategies and processes in place including that attempt to both measure and manage risk.

Imagine the year 2035, and AI is everywhere. To ensure a positive future, AI literacy needs to improve now - not just among technical professionals, but in every team. This is not just good but risk management, but essential opportunity creation.

LESS THAN **40%** Of organizations have an AI ethics policy or framework

ONLY **40%** Of organizations surveyed provide AI training for their employees.

10% Of employees aren’t sure if their organizations use AI or not.

MILEV.AI

“Understanding your AI risk is essential to embracing its opportunities”

- Harriet Farlow, CEO Mileva Security Labs

With Mileva, the path forward is clear. Organizations can confidently navigate the AI landscape, managing threats while driving innovation forward. Milev.ai, by Mileva, is a powerful AI risk management platform designed to identify, assess, and guide the mitigation of risks associated with AI systems. By translating AI vulnerabilities into corporate financial risk, condensing major industry frameworks and jurisdiction requirements into digestible, actionable controls, Mileva helps organizations tackle complex compliance processes and minimize their unique risk profiles, all in a cost-effective way.

While Milev.ai empowers risk managers, our training programs ensure staff across all levels of technicality understand their role in protecting organisations from risk and are well-equipped with strategies for leveraging AI securely. Our advisory services also offer expert guidance to promote long-term resilience and compliance with evolving regulations.

Mileva’s solution, grounded in requirements recognized by active cyber risk managers, provides a comprehensive AI risk management platform, targeted training and advisory for organizations.