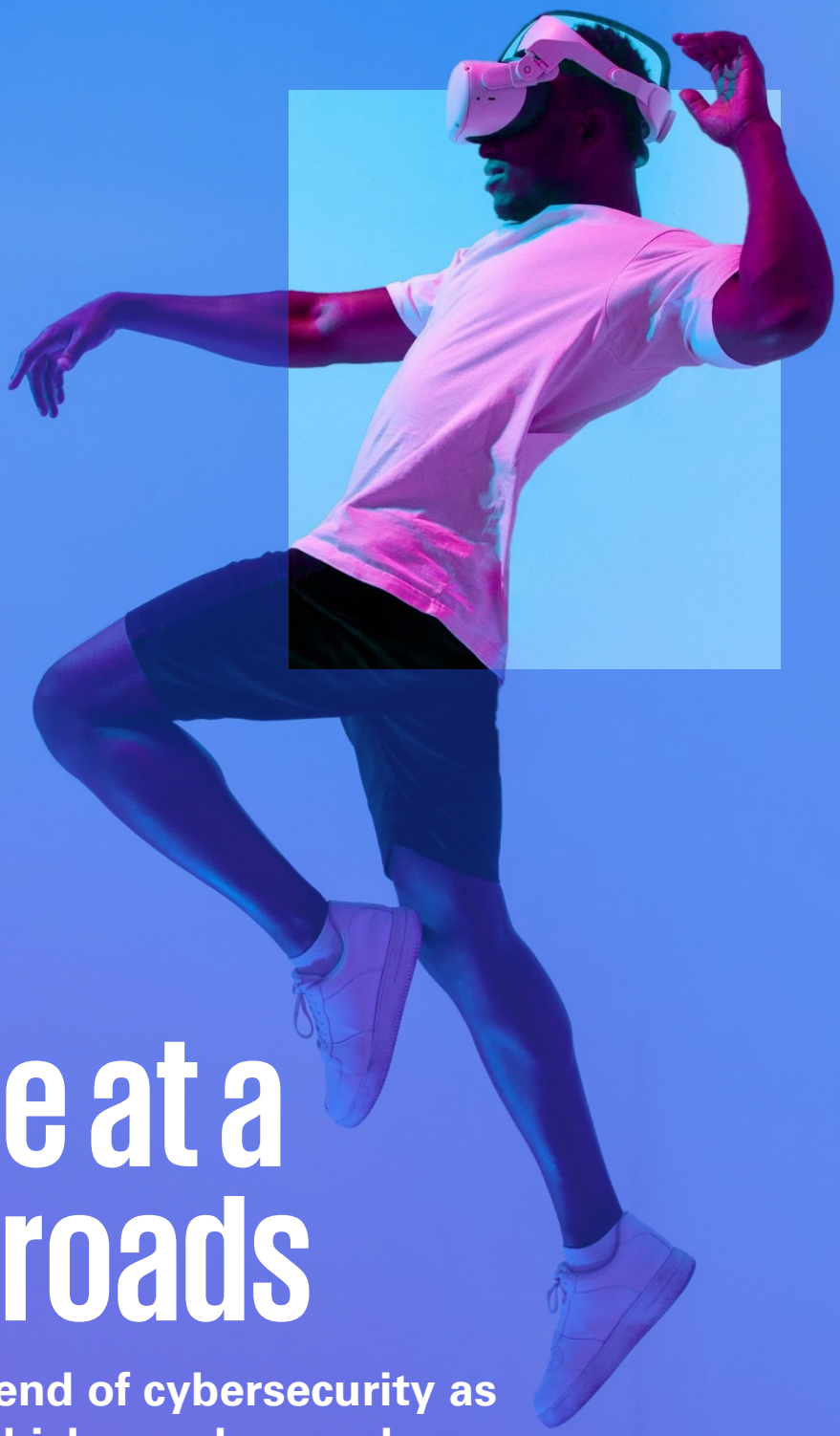
KPMG



Europe at a crossroads

AI means the end of cybersecurity as we know it, which may be good news for you

Edward Amoroso

February 2026

AI means the end of cybersecurity as we know it, which may be good news for you

Is the rapid advent of AI a threat or an opportunity for executives who want to protect their organisation? It's the wrong question, according to Edward , CEO of TAG Infosphere and Distinguished Research Professor in the NYU Center for Cybersecurity. He argues that AI will be the great leveller. Cyber will become business as usual, a business largely conducted by machines. And your capabilities to defend against threats will also become a commodity. "Tomorrow's cyber guardians don't clock in, they boot up."

You can't have missed the news: Artificial Intelligence (AI) is rapidly reshaping business processes. A multitude of research papers points out that AI will also give mala fide parties new weaponry to disturb business or infiltrate in systems.

One thing is certain: AI's ability to automate attacks means that threats can become more sophisticated and relentless. Attackers can deploy AI-driven tools to probe defences, identify weaknesses, and launch coordinated assaults. Yet, the same certainty is valid on the defence side. New AI powered technology empowers your organisation to better visualise attack surfaces, predict threats, and respond in real-time.

Shield and spear

All in all, AI is both a shield and a spear when it comes to cybersecurity.

is convinced that machines will have a dominant role in tomorrow's cyber landscape and that human involvement will decrease: "As AI agents take over routine tasks, the industry will move away from labour-intensive processes toward autonomous, intelligent systems. AI can scan, analyse, and exploit vulnerabilities at a scale and speed unattainable by humans. **Tomorrow's cyber guardians don't clock in, they boot up."**

Cyber as a commodity

As an executive, should you be worried about this? Not per se. AI will probably act as the great leveller. Traditionally, hackers and defenders would have a battle of wits, each largely relying on their skill and intuition. We used to have an asymmetry between them. "Now that both sides will have access to the same technology, this will no longer be the case. One could compare it to how graphic design tools like PowerPoint and Adobe InDesign made professional visualisation accessible to all. In the same way, AI is poised to make advanced cybersecurity capabilities available to everyone. The result: **cybersecurity will no longer be the privilege of the few. It will be the commodity of the many.** And as a result, the cybersecurity industry will be fundamentally different than it is now."

There might also have an upside for you. Even smaller businesses can access the same powerful AI-driven defences as multinational corporations. The barriers of cost and expertise are lowered, enabling a broader range of organisations to protect themselves effectively. It's no longer a matter of having deep pockets. "And the real differentiator will not be the tools themselves, but how organisations choose to use them. Strategy, organisation, and agility will become the new competitive advantages."

"Tomorrow's cyber guardians don't clock in, they boot up" Edward , CEO of TAG Infosphere

Business as usual

For executives, it means that building a resilient business is no longer something exotic, but becomes business as usual, in a world where machines on both sides play their role, having the same access to tools and thus create a new equilibrium.

"My belief is that AI will drive cybersecurity risk into the same category as, say, physical bank robberies. There will certainly be incidents, but the intensity and frequency will drop to a level that no longer requires the same level of attention."

Although that may sound like an attractive scenario, points out that we also need to carefully watch some new risks following the advent of AI.

Emerging behaviour of AI agents

One of them is emergent behaviour in AI agents. While AI agents can act comfortably within well-defined tasks, problems may arise when they start reasoning and making decisions independently. There have been cases where agents started to operate in a way that human designers hadn't foreseen. This is one of the (new) risks of deploying agentic teams. This is bad news if you want to keep your organisation safe. **AI agents can expand the threat surface in ways that organisations may not anticipate.**

On a side note, notes that this challenge goes beyond cybersecurity, touching on broader ethical and regulatory issues. Not only does he stress the need for clear rules and kill switches to ensure humans retain control.

He also emphasises the need for ethical guidance and envisions a future where organisations may appoint a chief philosophy officer to help navigate dilemmas stemming from AI, ensuring that technology serves human values rather than undermining them. "My advice to computer science students is to take courses in ethics and philosophy. I believe the next big thing will be a shift back toward human interaction and moral reasoning."

Access to energy

One other important topic for the near future is a possible radical decentralisation of energy production and the rise of virtualised infrastructure. This will democratise the access to energy but also create novel attack vectors and create a totally different energy landscape than we have today. Protecting these systems will require innovative AI tools and a reimagining of security strategies, especially as we know that historically, the access to energy has been the main cause for wars and conflicts. "Apple's main business in twenty years might be energy, not iPhones. **If Apple, Google or some other big name becomes your energy company, what are the new security challenges?"**

Thinking about far-fetched scenarios like this, cyber may after all not be so 'business as usual'.

Viewpoint
Sander Klous

In this rat race, faster learning is the key

AI is reshaping cyber risk by expanding the attack surface and accelerating both offense and defence. Generative systems invite new failure modes, prompt injection, covert model routing, data poisoning, that weaponise business workflows. Not adopting AI is the higher-risk path: attackers will automate regardless; leaders must match that pace with governed, threat-informed use. Treat AI as critical infrastructure: harden models and agents, minimise permissions, instrument for runtime monitoring, and pre-commit to kill-switches. Continuously red-team with AI-driven adversaries, validate content provenance, and bake controls into MLOps (Machine Learning Operations) and product lifecycles.

We've entered a rat race where machines probe and protect at machine speed; advantage goes to teams that operationalise AI safely, augmenting detection, triage, and response while closing feedback loops to policy.

The goal isn't zero risk, but faster learning, containment, and recovery. Start with threat-informed objectives, measurable controls, and executive ownership to turn experimentation into resilient, responsible advantage at scale now.