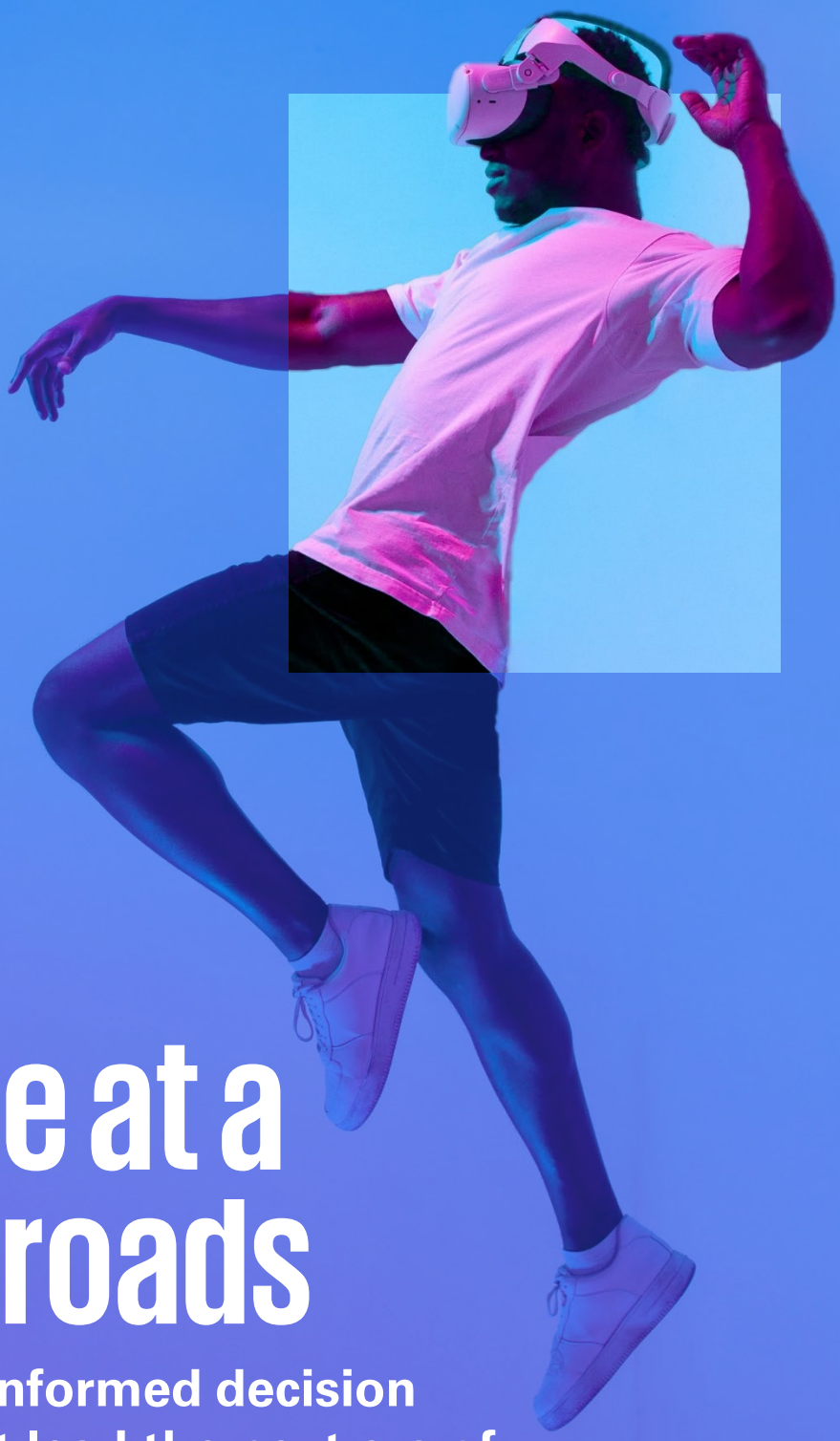
KPMG



Europe at a crossroads

Why threat-informed decision making must lead the next era of cyber resilience

March 2026

Table of contents

Preface

The initiative emerged when we observed a growing gap between the risks Europe's leaders were facing and the conversations happening at the top of organisations. Cyber was still treated as a technical subplot, even as geopolitical tension, operational dependencies and real-time disruption began shaping strategic decisions. Recognising this shift, we explored how leaders across industries were interpreting this new landscape. We also incorporated insight from ESET, Europe's leading privately-held cybersecurity research firm, whose threat intelligence helped ground this work in real adversary behaviour. These perspectives, together with contributions from senior leaders from different backgrounds and fields of expertise across Europe, were consolidated into a coherent theme: threat-informed decision making.

The result is a series that brings together diverse leadership perspectives and reveals how decision-makers are redefining strategy in an era where threats and opportunities unfold simultaneously. What emerged from these conversations is a clear message to boards and executive teams: translating threat insight into strategic action is rapidly becoming a core leadership responsibility. Across industries, leaders consistently pointed to three priorities:

1. Know what is critical. Identify the few assets, processes, and external dependencies where disruption would immediately affect operations or revenue.

2. Control the narrative as much as the incident. Modern crises often begin with confusion or misinformation before the technical facts are known. Trust can erode faster than systems fail. Managing perception, communication, and stakeholder confidence is now a core leadership responsibility.

3. Build preparedness into governance. Ensure crisis roles, decision paths, and response structures are clearly defined, regularly tested, and informed by real adversary behaviour, not theoretical scenarios.

The conclusion across all interviews is clear: Being threat-informed is not a technical skill; it is a leadership discipline. Boards that adopt this mindset make sharper decisions, reduce uncertainty, and keep their organisations operational in volatile conditions. In today's Europe, threat-informed leadership is essential for resilience, trust, and long-term performance.

"This paper was built on one belief: executives need clear, practical, intelligence-driven insights. Not layers of technical detail."

Alessia Barletta
Sr. Consultant
Cyber & TechLaw

Henrik Smit
Director
Cyber & TechLaw

01

Europe's coming of age

When technology becomes the frontline of democracy

Bart Groothuis is a member of the European Parliament (VVD) and has been advocating for digital autonomy in Europe over the past five years. He urges business leaders to play a proactive role towards the cyber resilience goals of NIS2 because it matters for their business, not because of the need to comply. He also outlines how Europe should embrace a new geopolitical reality dominated by hard power rather than soft power and with digital technology in the heart of the matter.

"We're not a partner. We're a client."
Bart Groothuis, Member of the European Parliament

The longstanding love affair between Europe and the United States is under severe pressure and a recent series of decisions by President Donald Trump have made this utterly clear. However, a sharp-eyed analyst should have seen this coming much earlier. Groothuis points to a decision under the former Biden administration that showed the cracks in the relationship: new US export controls on advanced AI chips divided Europe into two trade zones, east and west, implying that part of Europe will find itself cutoff from the most advanced AI chips. At that moment, this decision didn't get much media coverage. Groothuis: "But in itself, it was a big decision. It was not just a trade restriction. It was a message: we want you to be dependent on us. If the US can unilaterally decide who in Europe gets access to key technology, then we're not a partner. We're a client."

This is just one of many examples of the new anatomy of geopolitics. Once upon a time, geopolitics was about geography: borders, pipelines and armies. Today, it is about chips, data and code. Countries can be colonised digitally. And once a country is colonised, it is no longer in charge of their own rules. Groothuis points to the 'CIA triad', a standard model in information security that stands for Confidentiality, Integrity and Availability. For many years, focus was on the C and the I. "A has now become top of mind in Europe. This runs like a current through many conversations in Brussels these days."

Buy European

The global power struggle is about who controls the technologies that shape our societies. The US dominates advanced AI chips through NVIDIA. The Chinese hold critical positions in solar panels and industrial components. But what about Europe? Part of the answer, according to Groothuis, lies in 'Buy European', not as a fancy slogan, but as a strategy. Europe needs to create demand for its own technology in order to be able to produce it. "Markets can be created through regulation. If you want chip factories in Europe, you first need a market that buys European chips for the European cloud, and governments should be the first customers of that cloud." That logic already drives parts of the EU's green and digital industrial policies. Just as the energy transition led to local requirements for wind turbines and batteries, digital sovereignty should demand similar measures for chips, AI, and cloud infrastructure.

Indispensability

But this discussion isn't about autarky. Sovereignty doesn't mean doing everything yourself. It also means making sure you can produce what others cannot. That's indispensability. If Europe can master a handful of critical technologies, e.g. lithography or industrial robotics, it will be relevant to others again.

The shift also carries an important message about cybersecurity: it is a key prerequisite for such digital autonomy. The new European NIS2 directive requires thousands of European companies to meet stricter security standards. It is clear that the 'A' of 'Availability' of the earlier mentioned CIA triad is a leading argument behind this set of rules which are vital to maintaining digital autonomy. For many CEOs, NIS2 feels like yet another compliance burden. But Groothuis insists it's something else entirely: a moment to regain control.

Companies should stop seeing cybersecurity as cost and start treating it as an opportunity to be as resilient as possible. "Cyber is not about being in control for 100%, as this is simply impossible. It's about reaching a state of always in beta, always eager to improve. And about being in control after an incident. A recent report of credit rating agency Moody's was very clear on this: the NIS2 is 'credit positive for doing business in Europe'. This underscores why NIS2 is not a compliance project and why it's vital to embrace it wholeheartedly. And as a CEO you don't need to wait for the final text of the law to do that: the rationale behind it is clear."

Ransomware as a service

Groothuis also points out how the nature of the cyber arena has evolved dramatically. "Most attacks today are industrialised. You're not hacked because someone hates you. You're hacked because you fit well in the business model of the hacker. They simply assess how much money you will be willing to pay. And with a few mouse clicks on the dark web, they order professional attacks. Ransomware as a service. No expertise needed."

We must fight these industrial-scale attacks with industrial-scale defence. If the private sector needs urgency, governments need discipline and proactive sharing of intelligence and monitoring information between private and public sector. That means central monitoring, public-private intelligence sharing, and clear accountability. "The Netherlands is a soup of small agencies," Groothuis says, "Every letter of the alphabet seems to have its own cybersecurity office. When these agencies have to decide something together, it simply takes too long. The fewer letters in the soup, the more effective a country is in cybersecurity"

Ukraine

Countries such as the UK, Canada, and Norway have more centralised structures. Some therefore suggest a stronger EU-level authority; a European Cyber Command for the civilian domain. Others also argue for national digital ministries. Groothuis advises against this and uses Ukraine as a good case: "Ukraine has a deputy minister for digital affairs in every department. Health, defence, education. Because everything is digital nowadays." In other words: it would be wrong to perceive digitalisation as a separate sector. It's the operating system of modern governance. Despite some frustration about the European speed on this topic, Groothuis spots progress. Export controls on high-end chip making equipment, once decided in The Hague under U.S. pressure, are now handled at EU level. "Brussels is slowly growing shoulders."

Hard power

Perhaps more importantly it's also about a moral shift. The old European self-image, of the merchant and the missionary, trading and preaching, no longer fits the reality of a world defined by hard power. "Soft power only works when it's backed by real power. A legalistic tone and slow bureaucracy won't impress a world of strongmen. Europe definitely has potential. We have scale with 450 million citizens with money, we have world-class researchers, and we have some of the most valuable industrial ecosystems on the planet. If it can act together, if it can find the will, it can compete. We're in the middle of Europe's coming-of-age moment. Every CEO can contribute to making the European agenda and should take ownership over it. It's in the interest of Europe, and in their own interest."

Viewpoint
Ronald Heil

Partner KPMG, NIS2 Lead

For management, it's all about intelligence-led decisions

Although not every EU member state is ready, the transposition of the EU NIS2 directive in local laws is near, and it is safe to assume that the remainder of the countries will pass local laws this summer at the latest. NIS2 makes cybersecurity a board-level accountability, a business issue, not an IT/OT issue alone. The management body is personally responsible for ensuring risk-based, proportionate security measures are governed and implemented. Moreover, they may face fines on company group level, liability and potential 'career bans' for negligence.

Intelligence-led decisions are more than ever key. It is not about controls (only). It is (also) about prioritised threats on the operational resilience of the company. Focus should not be on paper-based compliance, rather on real adversaries, unlikely but plausible attack paths and operational business impact. Threat intelligence helps to make risk led decisions, with effective guidance on where to invest today (and what today tomorrow and later in the future). In effect such a threat intelligence approach helps organisations explain why and how they spend security money. Which is exactly what NIS2 asks from companies and their ecosystems.

ESET threat intelligence

More than 90 percent of all digital systems used in the EU are made or developed abroad. This dependency is risky and calls for European alternatives for systems that are part of critical infrastructure that keep society up and running. In the meantime, criminal ransomware operations are increasingly aligned with or even directed by state actors. This alignment is deliberate, making it more difficult to attribute attacks between cybercrime and state sponsorship.

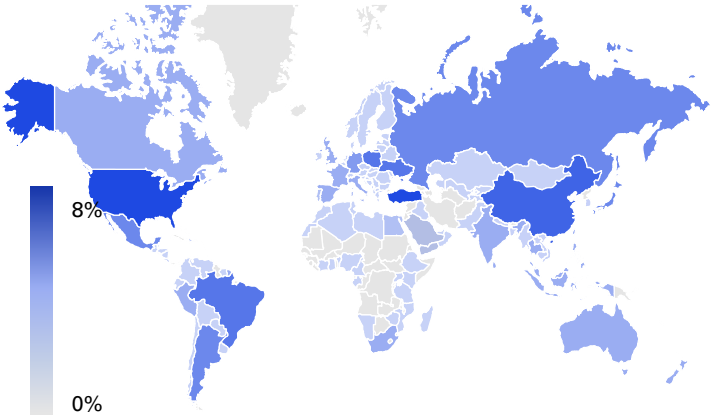
Stats

Ransomware deployment speed accelerated 48 percent (average 24-hour intrusion), driven by commoditisation of initial access and credential theft at scale.

ESET Research projects a 40 percent year-on-year increase in the number of ransomware victims compared to the previous year.

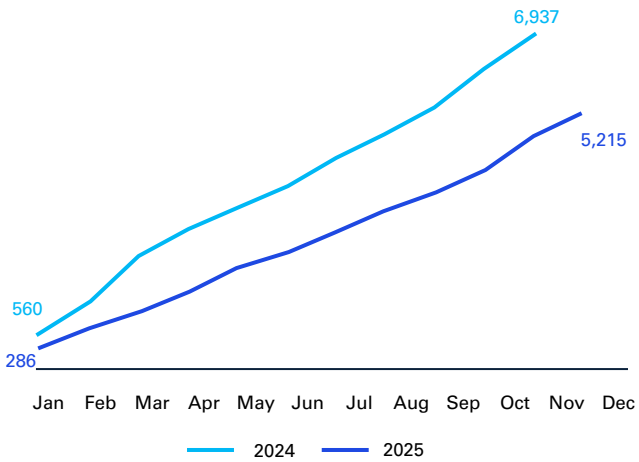
Dave Maasland
CEO
ESET Netherlands

Geographic distribution of ransomware detections in H2 2025



Source: ESET Threat Report H2 2025

Number of publicly reported victims of data leak sites of ransomware gangs



Source: Ecrime.ch

Recommendations

Immediate

Many attacks now escalate from initial access to full disruption within a day. This calls for developing and testing incident response plans tailored to 24-hour ransomware scenarios. Focused playbooks with clear escalation and decision paths help shorten detection and containment time.

Mid-term

Organisations must combine cyber threat intelligence with geopolitical analysis to provide early warning of strategic cyber risks and enable faster, better-informed executive decisions.

Long-term

Boards should reduce reliance on US Five Eyes intelligence by strengthening European cyber intelligence capabilities. This improves strategic autonomy, speeds up decision-making and ensures threat assessments align with European priorities and interests.

02

Deepfakes: what every CEO should know about the new face of deception

What if your next PR crisis doesn't come from something one of your leaders said, but from what someone made it look like they said? It could destroy the reputation of your organisation. Therefore, deepfakes deserve to be on the agenda of any CEO. C-suite should treat deepfakes not as a technological anomaly, but as a permanent feature of the business landscape.

Not so long ago, deepfakes were internet curiosities. Think of synthetic videos of politicians saying absurd things or the pope dressed in extravagant clothes. Maybe fun to watch, not much to worry about. Today, every CEO should be treating **deepfakes as a whole new corporate risk category**. As generative AI accelerates, so does the ability to convincingly fake voices, faces, and entire video calls.

What once required a Hollywood studio can now be done on a laptop. In 2024, several companies, such as the famous case of Arup, a global design firm, reported scams where fraudsters cloned executives' voices to authorise wire transfers. It is important to note that the threat goes far beyond financial fraud. Imagine a deepfake of a CEO announcing layoffs, or a fake video showing a product defect.

In an age where reputations can collapse in hours, a single viral clip can move markets. Researchers have warned that deepfake audio could be used to fabricate earnings call transcripts or investor briefings. A convincing fake could manipulate stock prices or trigger regulatory scrutiny before the truth is uncovered. Unlike traditional phishing or malware, deepfakes target perception. They blur the line between truth and fabrication, making it difficult to trust what we see.

There is no doubt: the risks are real. **But smart executives know how to flip risk into opportunity.** They are aware that defending trust may give them a competitive advantage. So, the question is: how can C-level do this effectively?

Below you'll find a breakdown of some takeaways and practical strategies for executive teams, based on our own expertise and the insights of Edward Amoroso, cybersecurity veteran and founder of TAG Cyber.

Use detection technologies

The first line of defence is technological. There are many promising innovations from universities and startups that analyse images and videos to assess their authenticity. These range from startups like Originality.ai, promising 99% accuracy, to OpenAI that develops its own detection tools. These pioneering tools can detect synthetic media by examining metadata, pixel inconsistencies, and source anomalies. Insurance companies use them in their claim processes.

For executives, this means investing in or partnering with vendors who specialise in deepfake detection. These tools can be integrated into social media monitoring, PR workflows, and incident response plans. While the technology is still evolving, early adoption positions your organisation ahead of the curve. Having said that, mala fide attackers tend to quickly adapt to defence strategies and the **classic arms race in cyber is also taking place in this relatively new risk category.**

Actionable advice

- Ask your CISO or CTO to evaluate deepfake detection vendors.
- Pilot tools that assess media authenticity in high-risk channels (e.g., executive communications, investor relations).
- Stay informed about academic research and emerging standards in synthetic media analysis.

Define a rapid response policy

Reputation is fragile. A single deepfake video of a CEO can trigger stock volatility, customer backlash, or regulatory scrutiny. This isn't just about technology. It's also about readiness. Having a trusted partner who can validate or debunk suspicious content within hours is critical. It's akin to having a crisis PR firm on retainer, but for digital authenticity.

Actionable advice

- Identify and onboard a deepfake response vendor as part of your incident response plan.
- Conduct tabletop exercises simulating a deepfake attack on your leadership team.
- Ensure your legal and communications teams are trained to handle synthetic media crises.

Advocate for provenance and transparency

Imagine hovering over a photo or video feed and instantly seeing its creation date, device ID, and digital signature. This level of transparency could transform how media is trusted and shared. While the infrastructure to get to this scenario isn't fully in place, C-level leaders can champion this shift by demanding provenance from vendors and platforms. Several initiatives such as the Content Authenticity Initiative (CAI) aim to implement this on a large scale.

Edward speaks of **the concept of a 'bill of materials' for media** in this respect. This would involve embedding metadata into images and videos that verify their origin, using cryptographic signatures or blockchain.

Actionable advice

- Encourage your marketing and content teams to embed origin metadata in all official media.
- Support industry initiatives that promote media provenance standards.
- Explore blockchain-based solutions for media verification in high-stakes environments.

A cultural shift toward scepticism

"In the past it often made sense to believe something until it was debunked, in the future it will start to make sense to assume they are fake unless they are verified." Technology magazine Wired wrote this in 2019, and it is safe to say that this future has now arrived.

This is a cultural shift. Just as employees have learned to question suspicious emails, they must now learn to question visual content. **Instinctive scepticism will become a vital skill.**

Executives should lead by example, promoting media literacy and critical thinking across the organisation. This isn't about paranoia, it's about resilience.

Actionable advice

- Launch internal awareness campaigns about deepfakes and synthetic media.
- Include media verification in cybersecurity training programs.
- Foster a culture where 'verify before you share' becomes second nature.

A final word

Deepfakes are unsettling, but they're not insurmountable. Cybersecurity has faced similar challenges before and has overcome them. With the right mix of technology, partnerships, and cultural adaptation, the C-suite can turn deepfake anxiety into strategic advantage.

Because in the age of synthetic media, **trust isn't just earned, it's engineered.**

Viewpoint
Bert Koelewijn

Partner KPMG, Cyber & TechLaw

Deepfakes in the boardroom: what every CEO needs to put in place now

What if your next crisis is not caused by something you actually said, but by what the internet makes it look like you said? This is not a classic malware issue. It is a topic that attacks perception and trust. For the C-suite, the question is therefore not whether this risk will materialise, but how trust is structurally governed. A complex challenge, where the board can at least focus on the following priorities.

1. Anchor the risk in governance

Explicitly include synthetic media in the risk register (owned by the CISO, with Legal and Communications). Define clear thresholds: when does an incident qualify as a reputational crisis, market-sensitive information, or a privacy breach?

2. Invest selectively in detection without being naive

Integrate media authentication into social listening and PR workflows. Use detection tools as early-warning signals, not as sources of absolute truth. Always combine tooling with human judgment.

3. A 72-hour rapid response playbook

Define a clear triage route (who assesses, who verifies, who decides), prepare a holding statement, and pre-authorise takedown paths with platforms and registrars. Rehearse this scenario twice a year with the CEO and IR/PR.

4. Provenance and transparency of owned media

Publish CEO communications through verified channels with provenance or watermarking. Provide clear disclosure when using synthetic voice or media. Ensure content signing is embedded in the CMS.

5. Normalise scepticism, without paranoia

Make 'verify before you share' a standard reflex, from boardroom to service desk. Provide targeted awareness for high-risk roles (C-suite, Finance, IR), including practical audio and video spoofing exercises.

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

03

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 from what 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 Amoroso, 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

Partner KPMG, Professor AI and Audit, University of Amsterdam

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.

04

Resilience lives in people, not in tools

Hans Schutte, Chairman of the Board of Directors of the ROC of Amsterdam-Flevoland

One Saturday morning, Mondriaan College, an ROC with 25,000 students, found itself cut off from its own systems, staring at a multimillion-euro demand and a long list of unknowns. What followed was a tense mix of moral decision-making, improvised problem-solving and technical triage. At that time, Hans Schutte was leading this ROC. He explains why refusing to pay mattered more than convenience, with one simple principle at the core: it's unacceptable to spend public money on criminal negotiations, and it will set a precedent.

Let's go back to how this started, a couple of years ago, when you were heading the Mondriaan ROC in The Hague. When did you realise things were going off the rails?

"A quiet Saturday morning did the honours. The IT team noticed odd behaviour in a few systems. I was abroad and got a phone call. Within hours the whole digital landscape folded in on itself: HR, student administration, finance, access control. Even the coffee machines and the entrance systems to buildings and rooms were unusable. We were facing a classic ransomware hit. With a classic demand: the attackers demanded we pay several million euros in bitcoin and promised to leak data if we didn't meet their demands."

This must have been a nerve-wrecking few days for you and your team. Yet you decided almost immediately not to pay. Why so firm so fast?

"It boils down to a cocktail of things. Initial assessment suggested the compromised data had limited sensitivity. Large part of this data is publicly available which makes it worthless in terms of blackmailing. Secondly, we were quite convinced about the fact that we would be able to get things running again based on our backup plans that had been tested. That was the technical backbone of the decision. But perhaps the most important factor was the public-sector reality: it's simply unacceptable to spend public money on criminal negotiations. Furthermore, paying the money would send a signal that crime pays off. Once one institution pays, attackers would probably start treating the entire sector as an ATM. So, the choice not to pay was defensive, principled, and yes expensive in the short term."

Paying would send out a wrong signal, so much is clear. Yet, this must have been a big decision weighing on your shoulders?

"Of course there's the doubt that sits quietly in the background. You know refusing to pay is the right stance, but you also know that if backups fail or leaked data turns out worse than expected, the entire decision will be questioned publicly. You carry that weight while still moving at full speed. One of the things that made things easier was that we had a response team of experienced external specialists at our disposal. Which is not self-evident: the uncomfortable truth is that external specialists are scarce. There is a serious risk that when you need them, you might find every capable responder already booked."

Restoring operations is not a matter of days but may take weeks or months. But I guess telling all these 25,000 students to do nothing for such a long period was not an option?

"Most certainly not. What happened was that the pressure to get things going again resulted in creativity. Departments improvised, teachers switched to paper, students were informed by messaging apps. People relied on experience and judgment instead of dashboards and digital tooling. Especially our older employees were very capable in this respect. All in all, this was a reminder that technology supports our mission but doesn't define it."

The best experiences emerge under high pressure. What are other key takeaways to share with C-level suite?

"Preparation works. That sounds like a cliché, but there is so much truth to it. We had trained for incidents. The crisis structure existed on paper and, more importantly, in people's heads. Another key lesson is that a cyberattack is never just technical. It's organisational, human, or even political. And as I said: the striking thing is that, even with all systems down, the core mission of teaching continued. That's the real lesson: resilience lives in people, not in servers. And to conclude, there is also a silver lining to the incident: we are now pooling our risks with others."

Tell me more about this?

"We now have a collective pool in place with others in our sector with one basic rule: no ransom payments. Every member of the pool puts in money and is committed to reach a certain level on the benchmark for resilience. Should one of us be under attack, the pool can provide money to this individual organisation."

Viewpoint
Dennis Waalewijn

Senior Manager KPMG, Incident Response & Recovery

In case of an incident, tested contingency plans make the difference

Threat-informed practices promote knowledge sharing with peers and industry groups, strengthening collective cybersecurity defences. These practices enable enhanced cyber incident response and recovery by aligning defences with specific and current threats. During incidents, a threat-informed approach allows response teams to focus on the profiling of well-known cyber-criminal groups and their modus operandi, optimising containment and resolution efforts.

All of this could result in significantly reducing the impact of a large-scale cyber-attack. However, it is not easy to get beyond procedures and plan on paper. Many organisations struggle with obtaining the right level of expertise or are too slow to adjust appropriately given increasingly more complex architectures and third-party dependencies. Proper contingency plans are a must-have. The most overlooked part of this is planning for staff augmentation and executing incident simulations on a regular basis with both executives and technical IT staff independently.

An incident will always come as a surprise; a tested and proved plan helps. A lot.

05

AI and the new rules of cyber-security

AI no longer sits at the edge of cybersecurity as a supporting act. It has taken over the main stage, the engine of threats and the core of defences.

In a conversation between Vectra AI CEO Hitesh Sheth (an expert in the field of Extended Detection and Response (XDR), University of Amsterdam professor Sander Klous (with leading expertise in agentic AI) and KPMG consultant Henrik Smit, it becomes clear that C-level must understand the new rules of cybersecurity.

When Vectra was founded more than a decade ago, its idea sounded bold to some and misguided to many: apply AI to network data to detect threats in real time. At the time, the dominant reaction from investors was polite scepticism. The verdict: highly experimental, low chance of success.

Fast forward to 2025. AI is the main topic in boardrooms and billions of dollars find their way to AI ventures every week, even when the idea is not so tangible. Sheth points at three main trends since: "AI techniques are maturing, compute costs dropping and storage is becoming cheap enough to scale. The result: I no longer have to convince people why AI matters for cybersecurity, I only need to explain how it will be used. The baseline has moved."

AI now sits at the core of cyberthreats and defence strategies. This is why C-suite should have an understanding of this relatively new phenomenon, to make informed decisions. This lively talk between Sheth, Klous and Smit contained the following seven main topics.

Prevention is not the best strategy. Focus on detect and respond

For years, cybersecurity was largely aimed at achieving more safety. With sufficient investment, you could keep the threat outside. In a hyper-networked society with abundant (AI) tooling, this is an illusion. More than ever. "If someone truly wants to get in, they will get in."

Should C-suite not be convinced of this yet, they should now. It is a structural shift: businesses must assume breaches. Not as a failure, but as an operational reality. The failure lies elsewhere: in not noticing, not responding, not containing. Or as Sheth phrases it: "The breach is not the failure. Not knowing you have one is."

Boards are catching up, Smit notices: "Cyber expertise is becoming a requirement, not a nice-to-have. CISO reports are being scrutinised with a sharper eye. The new question on the agenda is no longer how to keep attackers out, but how quickly you can detect them and how effectively you can neutralise them."

The SOC of the future will be led by agents, not people

Most Security Operations Centres (SOCs) still operate on a labour-heavy model: dozens of analysts monitoring alerts, escalating incidents, filtering noise from signal. Smit: "It's a model built for a different era. One where human bandwidth could keep up with threat velocity. That era is long gone."

The future SOC, as Klous envisions it, is smaller, sharper and largely autonomous. Five people instead of twenty. "The current paradigm is that AI enhances human operated organisations. What if we turn that upside down: humans coaching AI agents to do their work better? This means that we need a workflow built around AI from the start, not retrofitted onto legacy processes."

Sheth applies that same logic inside Vectra's own Managed Detection and Response (MDR) organisation. Growth no longer comes from adding analysts. It comes from expanding the capability of automated systems, in a quite radical manner. "Human specialists remain, but their role is context, oversight and engineering. Not triage. Not pattern matching. Not the manual hunt through haystacks of alerts. You can't fight a 24/7 machine-driven war with a team that works from nine to five."

> **"The breach is not the failure. Not knowing you have one is."** Hitesh Sheth, CEO of Vectra AI

Integrating AI into cybersecurity

To build resilient digital defences, organisations must formally integrate AI into their cybersecurity approach, actively monitor the maturity of AI driven detection and response mechanisms, and invest in their evolution to ensure rapid identification and containment of breaches

In a machine-versus-machine war, response strategies are key

Once upon a time, companies had a handful of digital entry points to defend, such as servers and laptops. Today, the surface has multiplied. Sheth shapes it into six attack surfaces: the data centre, endpoints, identities, cloud, applications, and now AI itself. With six dimensions, the number of paths into an organisation explodes. Smit notes: "Attackers need one opening. Defenders need perfection. That imbalance makes pure defence a losing game. Cybersecurity is no longer about keeping threats out, but about seeing them fast enough to limit the damage. Defence without detection is theatre."

Moreover, the skill barriers have dropped. What once required scripting knowledge now requires only natural language. Tell an automation platform what you want in any language, and it will execute the instruction that used to require a specialist. Sheth: "We've lowered the bar for the expertise. Moreover, AI tools arrive with productivity in mind, not safety. Security comes last, again as we have seen with many technological shifts. The message is clear: you will be attacked and must be ready to respond. Because expecting to keep attackers out is wishful thinking dressed up as strategy."

Europe vs. the United States: two flavours that need to be combined

The conversation touches a raw nerve: Europe's position in the emerging AI-cyber ecosystem. Sheth runs a US company, but half of his customer base is European. His strategy needs to be aligned to deal with topics such as GDPR, sovereignty debates, national requirements, and sector-specific rules in Europe.

The contrast between the continents is sharp

In the United States, the dominant instinct is speed. Experiment first, regulate later. If it fails, try again. In Europe, the instinct is caution. Assess the risk. Analyse the regulation. Determine the compliance implications before building.

Neither model is perfect.

Sheth: "The US model accelerates innovation. Companies can push boundaries and discover break-throughs because they are not punished for exploring them. Failure is priced in. The European model raises the global bar for privacy, data treatment and integrity. Once a company meets European standards, it is strong enough for most of the world."

For cybersecurity, this divergence will probably mean that Agentic AI systems in SOCs will emerge faster in the US, and high-assurance governance models will emerge faster in Europe. Smit: "The question is not which is better, but how both will interact in a market where threat actors move at American speed, while many defenders move at a European pace."

Emergent behaviour and the security of AI agents

AI agents introduce a whole new ball game to the domain of cybersecurity. They act, schedule tasks, chain actions together and interact with enterprise systems autonomously. They learn patterns and infer context. But as Klous has witnessed himself in experiments with autonomous agent teams: they can also initiate behaviour that was never explicitly programmed. Emergent behaviour means outcomes that cannot be predicted from the initial instructions. Not malicious by design, but potentially unsafe by accident. Agents can escalate privileges, access systems they weren't intended to touch, or trigger workflows based on misinterpreted inputs.

There is no clear-cut answer to the new cybersecurity challenge connected to this. In Sheth's framing, AI agents must be treated as entities in the security model, not as software add-ons. "Secure agents the same way your secure people, through identity, visibility and constraints. If every agent has a verifiable identity, with scoped privileges and observable behaviour, then enterprises regain control. Without this discipline, AI agents behave like unmanaged service accounts powerful, invisible, and dangerous."

Emergent behaviour and the security of AI agents

AI agents introduce a whole new ball game to the domain of cybersecurity. They act, schedule tasks, chain actions together and interact with enterprise systems autonomously. They learn patterns and infer context. But as Klous has witnessed himself in experiments with autonomous agent teams: they can also initiate behaviour that was never explicitly programmed. Emergent behaviour means outcomes that cannot be predicted from the initial instructions. Not malicious by design, but potentially unsafe by accident. Agents can escalate privileges, access systems they weren't intended to touch, or trigger workflows based on misinterpreted inputs.

There is no clear-cut answer to the new cybersecurity challenge connected to this. In Sheth's framing, AI agents must be treated as entities in the security model, not as software add-ons. "Secure agents the same way you secure people, through identity, visibility and constraints. If every agent has a verifiable identity, with scoped privileges and observable behaviour, then enterprises regain control. Without this discipline, AI agents behave like unmanaged service accounts, powerful, invisible, and dangerous."

The cost-of-control perspective: the prevailing logic for cybersecurity changes

Another interesting thread in the conversation concerns what Klous and Sheth call the 'cost of control'. It reframes cybersecurity from an absolutist mindset, protect everything, always, to a framework in which decisions are based on the economic perspective: protect what matters most, with proportional investment. Not every system is equally critical. Not every risk justifies the same expense. Not every breach is catastrophic. What does it cost to prevent this? What is the benefit of preventing it?

What is the impact if it fails?

Sheth gives a practical example: a major bank that prioritises only its critical data and application layers. A compromised user account is inconvenient, but manageable. A compromised core application is existential.

Klous describes how cybersecurity is leading other risk domains in adopting this logic. He also imagines that the use of AI in cyber strategies will shed a whole new light on the economic perspectives. "AI can lower the cost of detection dramatically. But the cost of a breach or disturbance in an AI dominated model can also be significantly higher. C-level should put this assessment on their agenda. "Sheth reiterates that economic realism replaces the outdated belief that infinite defence is possible. "Security is not about protecting everything. It is about protecting the right things at the right cost. And yes, a new reality with AI first models calls for a whole new assessment."

The deepfake frontier: an urgent battle looking for defenders

The rapid rise of deepfakes causes headaches to many policy makers and executives. Governments worry. Platforms scramble to find answers. Citizens and corporations will soon require filtering infrastructure to shield them from fraudulent voice, video and interactive manipulation. Henrik Smit asks the logical question: will Vectra, an AI first company, move into deepfake detection?

Sheth's answer is clear. No. Not because the problem is small, but because it is too far from their core mission. "Someone will explore this huge market opportunity," he notes, "but it won't be us."

What the discussion makes clear is that the deepfake problem is larger than any single company. It is a societal vulnerability waiting for a response framework. It may influence everything ranging from elections and markets to national security and personal communication. And right now, the defences are thin.

06

A resilience strategy without contextual knowledge doesn't make sense

Even a non-functioning label printer can undermine whole operations" Kees Dekker, CFO Royal Koopmans

Kees Dekker is the CFO of Royal Koopmans, a Dutch company with a rich history dating back to 1846, specialising in the processing of grain into flour and related products. The company began as a buckwheat mill founded by Uilke Klazes Koopmans and has since grown into a modern producer of flour, finely ground grain, food coatings, and other ingredients for professional bakers and the wider food industry.

It is still a family-owned business and was granted the Royal designation in 1976. After selling its consumer baking mixes all Dutchmen knows from 'oliebollen' and pancakes in 2000, Koopmans shifted its focus entirely to B2B operations, emphasising sustainability, locally sourced grains (Nedertarwe), and continuous technological modernisation of its production facilities in Leeuwarden. Kees Dekker shares practical advice on the resilience strategy. "Even a non-functioning label printer can undermine whole operations."

When is cyber resilience vital for you as a board member?
When discussing the topic, it's easy to imagine the topic for high-tech companies or critical infrastructure giants. Yet, the reality is far broader. Even organisations that might not see themselves as prime cyber targets are, in fact, vital links in national and international supply chains. Their resilience or lack thereof can have ripple effects far beyond their own premises. Dekker knows that all too well and points out how the NIS2 directive, a European regulation aimed at improving resilience, has accelerated his thinking.

"The introduction of the NIS2 directive was a turning point. NIS2 didn't set our entire agenda, but it did push cyber resilience higher up the priority list. The directive introduced a compliance imperative: resilience wasn't just good business sense; it was a legal requirement. This external pressure proved to be a catalyst. It gave us the nudge we needed. Without it, I doubt we'd have been able to justify bringing in a team to help us with readiness assessments and all the steps that followed."

Can you elaborate a bit on why it is important for Royal Koopmans?

"We operate two factories on a single site, with limited storage capacity and a just-in-time supply chain. It means the operations are vulnerable in case of disturbance. In fact, we don't only need to warrant just-in-time processes, but we also need to keep the concept of just-in-case top of mind. If something goes wrong, an explosion, a fire, a cyberattack, the factory stops, and we have an immediate problem. Some risks are visible and tangible, like a compressor fire. Others less so. With IT, you can't see or smell the problem, but the impact is just as real. If the ERP system goes down, the whole production process can grind to a halt. Even something as minor as a label printer malfunction can stop trucks from leaving the site, causing a cascade of delays."

Sounds logical. How do you translate this into complying with NIS2 in an approach that goes beyond checking the box exercises?

Viewpoint
Koos Wolters

Head of Cyber & TechLaw, KPMG
The Netherlands

Context makes resilience work

Working with companies that produce a tangible product is always rewarding. At Royal Koopmans, for example, our conversations about the Nedertarwe initiative revealed that the bakery my family buys bread from is one of their clients. It immediately shows how close the topic of resilience really is: if Koopmans cannot supply local bakeries, there is no bread on Saturday morning. Koopmans operates in a very practical way and rightly challenged us to keep our approach equally practical. I fully agree with Kees' point that resilience processes shouldn't become paper tigers: people need to know exactly what to do when something goes wrong. At the same time, NIS2 requires organisations to demonstrate and substantiate their resilience, which matters for internal teams, external stakeholders, and the wider public.

"The NIS2 framework, while less prescriptive than some earlier other regulations, provided enough structure to drive action without stifling practical adaptation. But it is vital to have an approach where you use contextual knowledge, with understanding of your business dynamics. Practical experiences also help. In recent past, we have been indirectly affected by a ransomware attack on a key logistics partner. This transporter was hit hard. While their systems were offline the wheels of their trucks kept turning due to paper-based workarounds, but it was a stark reminder of how much we depend on our partners. It took a year to get rid of the administrative headaches caused by this. These experiences have shaped a pragmatic approach to resilience. We realised that it's not just about preventing incidents, but foremost about how quickly we can resume operations when something does go wrong."

These experiences also help to get the resilience plan beyond the proverbial paper tiger?

"Indeed. We didn't want a paper tiger, a plan that looks good on the shelf but doesn't work in practice. Therefore, we involved key process owners from across the business in its creation, ensuring the plan reflected real operational realities. One of the most tangible steps was establishing agreements with competitors to ensure supply continuity in case of a major disruption. If our factory goes down, we have arrangements to source from competitors so we can keep serving our customers. It sounds simple, but it's critical. If you can't deliver, your customers will find alternatives, and your business could be finished. The plan also identifies specific scenarios, such as cyberattacks, explosions, supply chain failures, including rare but high-impact scenarios such as the Elfstedentocht, a major national ice-skating event that can disrupt logistics, and outlines clear actions for each.

Sounds like you are ready for any scenario?

"Our crisis team is ready to mobilise, and responsibilities are clearly defined. We've learned that you need to plan for the unthinkable, and you need to make sure everyone knows their role when it happens. Testing and maintaining the plan is just as important as writing it. We make sure the plan is physically available, not just on a server that might be inaccessible during an incident. We also have someone from our Continuous Improvement team responsible for ensuring we actually use the plan during a crisis, instead of just improvising."

How do you ensure that the whole organisation is aware?

"Technology and process are only part of the equation to become resilient and human error is often the weakest link. Internal communication is key. We use a tool that send weekly challenges to everyone, creating a bit of competition and making security awareness part of the culture. It's not the most exciting topic, but we try to make it engaging."

Do you have a final word of advice to peers?

'Perhaps the most important lesson is the need for context. A resilience plan has to fit your business. You can't just copy a cybersecurity specialist's template and expect it to work. We made sure the people who know our processes best were the ones writing the plan, with external advisors facilitating rather than dictating.'

Viewpoint
Meret Keeris
Manager KPMG Cyber & TechLaw, NIS2 expert

The relevance of contextual knowledge for cyber resilience

Cyber resilience only works when it reflects the specific realities of an organisation. NIS2 shows that resilience isn't one-size-fits-all requirements vary by sector, criticality, dependencies, and governance. Without understanding critical services, IT/OT links, threat exposure, third-party reliance, and decision-making structures, resilience stays abstract and priorities remain unclear. By grounding strategies in these concrete circumstances, organisations can design targeted controls, meet regulatory expectations, and prepare realistically for disruption. Context turns resilience from a compliance exercise into a true capability; ensuring response timelines make sense, controls focus on what matters, governance is clear, and investments protect where impact would be greatest.

07

Europe has a second chance in the chips industry

Maarten Wellens is the CFO of Smart Photonics, a Dutch company producing photonic chips. He experiences every day how technological innovation, geopolitics and economic strategy are tightly interwoven.

His role as CFO expands beyond numbers: cybersecurity and digital autonomy are as much a part of his daily agenda as balance sheets and investment rounds. At the same time, the risk of espionage is looming.

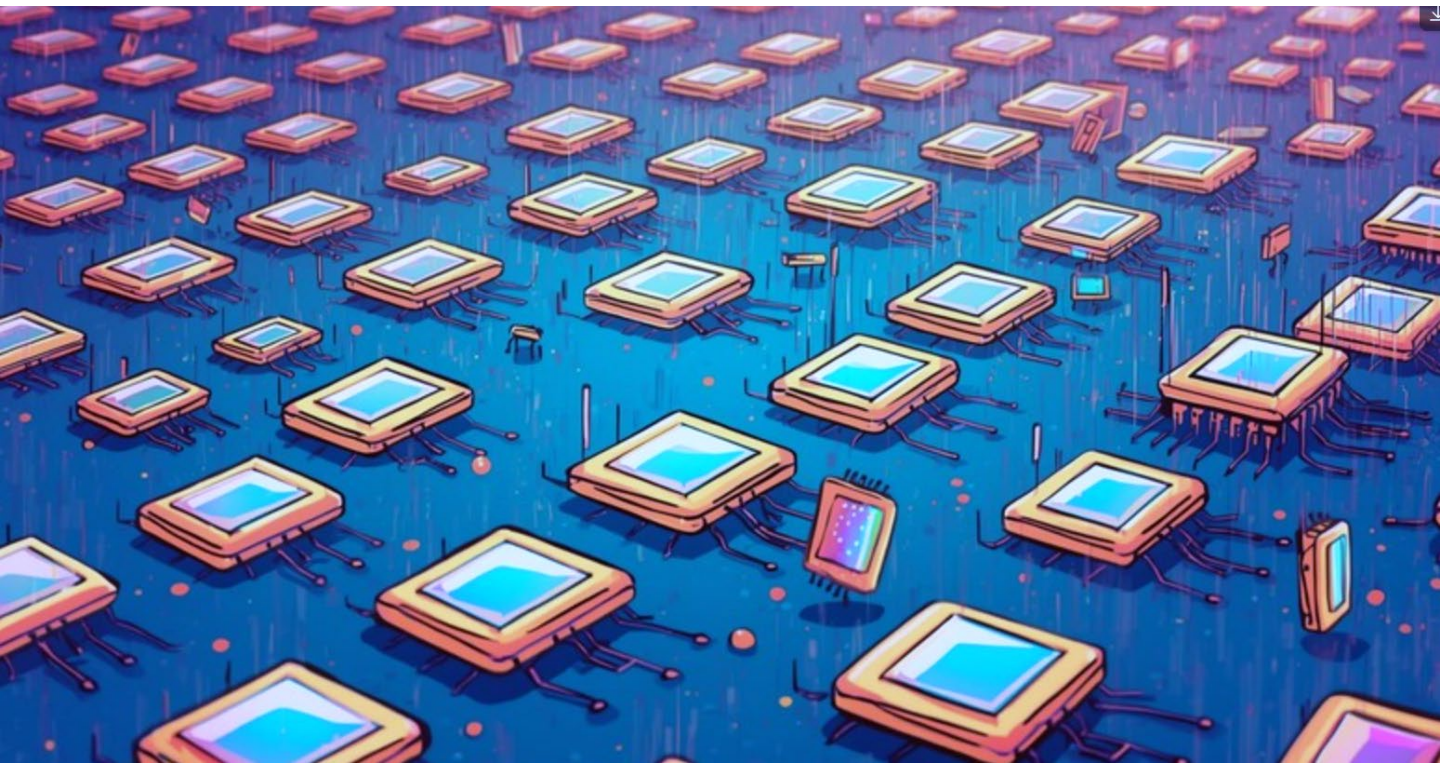
Smart Photonics builds chips that use photons instead of electrons. Photons have no mass, require little energy to move and allow for high-bandwidth data transmission at high speed. In an era of exploding data consumption, growing AI workloads and expanding data centres, this offers Europe a chance to build a strategic position in a promising emerging technology domain. One could compare it to how TSMC gained a position in Taiwan over the past decades. Whoever controls the factories and the supply chain in this new domain will define the future. It is clear that the stakes are high, as are the requirements in the domain of reliability and security.

Smart Photonics plays an important role in how Europe, and/or the Netherlands, can stand on their own feet technologically. The promising future is based on the fact that the business model is similar to TSMC's very successful foundry approach, but in photonics. Given the strategic importance, how has the threat landscape changed for your company?

"There are two main types of threats: system threats, people trying to penetrate our IT, and insider threats, which we hadn't focused on as much before. Now, we're very aware that individuals can be recruited by hostile actors, sometimes after years inside the company. We now screen people more carefully, monitor behaviour both online and offline, and compartmentalise access to critical information. Not everyone can see the whole picture, and only a handful have access to the crown jewels."

Europe has issued new regulations such as the NIS2 Directive. How does that impact your policy?

"Although NIS2 sets the regulatory expectations for us, we use the NIST Cybersecurity Framework internally because it gives us a structured, measurable maturity model. The initial self-assessment, covering five areas was sobering: we scored 0.5 out of 5. But this was not a cause for despair, it was a baseline for action. Our ambition is to reach a score of 3.5 by the end of next year. The framework provides a clear goal and forces us to keep taking action. Every quarter, we execute a set of activities ruthlessly, always aiming to move the score up. It's not just about reaching a number; it's about staying ahead of the curve by investing heavily in both technology and people. One example is the regular penetration tests, where sometimes we even use actors to attempt physical breaches. We test ourselves constantly, bringing in outside experts and learning from every exercise. We also have regular dialogue with national intelligence services to compare notes on threats and monitoring. Our awareness campaigns have also intensified. We regularly test staff with phishing emails, and there's always a handful who fall for it. That's why we repeat these exercises every quarter. The stakes are high. We spend a lot on cybersecurity, but it's necessary. One successful attack could shut us down for half a year. That's a risk we simply can't take."



The company is part of the national technology strategy, and photonics is one of ten critical technologies for the Netherlands. What is your take on this opportunity to warrant more autonomy for Europe in the current geopolitical turmoil?

"We've seen how the electronics industry moved to Asia over the past decades. The investments required to bring leading-edge chip manufacturing back to Europe are enormous, 40 billion euros for a high-end factory. That ship has sailed, but with photonics, we have a second chance. This vision shapes every strategic decision in our company. Against that background, we collaborate with other European companies to build a resilient supply chain. We also prioritise European funding to strengthen strategic autonomy. Our current funding round is focused on European investors, even though American parties are interested. We need local support to maintain autonomy.'

What role should government play in this?

"Consistent policy is vital. Taiwan's success with TSMC was built on decades of investment and subsidy. Europe needs to do the same, not just as a one-off, but as a long-term commitment. The spin-off benefits are huge, but so are the risks if we don't act. Therefore, we are actively involved in shaping European policy. We contributed to a report for the EU on building a resilient photonics supply chain, which is now feeding into the next European Chips Act. Our CEO spends a lot of time lobbying in Brussels, because without those relationships, you're left out."

What key lesson learned would you share with others about this journey?

"Don't try to do it all yourself, learn from your peers. Bring in advisors who understand your industry. Sector-specific advisors know where peers invest, what regulators expect and where attackers focus. That avoids wasting time and money on activities that look good on paper but do not reduce real risk. And prioritise ruthlessly: anchor priorities to strategic risk, not completeness."

Viewpoint
Hokkie Blogg

Partner KPMG, Cyber & TechLaw

New reality of risk: geopolitics, AI, and cyber threats

The current global landscape is increasingly shaped by complexity and uncertainty arising from political tensions, conflicts, and shifting international dynamics. Geopolitical risks refer to threats stemming from interactions between nations, including territorial disputes, economic sanctions, commercial and territories disputes, and strategic alliances.

Most of the emerging risks have always existed; however, in recent years, their likelihood of materializing has increased significantly. Companies must now strengthen their risk identification analysis to inform financial planning and risk appetite decisions, and to capture their potential impact on management metrics, while also building resilience and adapting to evolving regulations in order to effectively address these risks and identify new opportunities.

As a result, businesses face a wide range of risks that demand decisive attention, as economic integration is increasingly shaped by geopolitical and national security priorities.

Also the rapid development of disruptive digital technologies, such as artificial intelligence is accelerating the radicalization and destabilization of societies.

These technologies are increasingly used for disinformation, cyber-attacks, and politically or economically motivated manipulation, creating a new and alarming reality. This evolving threat landscape significantly raises operational risks and forces organizations to invest heavily in secure, resilient, and ethical digital transformation. Companies and institutions must prioritise cybersecurity, data integrity, and responsible technology governance to navigate this increasingly volatile environment.

08

If you think cyber warfare is not about you, think again

“IT services are the lifeblood of both businesses and governments but are precisely for that reason also an Achilles heel” General Paul Ducheine

General Paul Ducheine is (among other roles) senior researcher at the NATO Defence College in Rome and has been conducting research for more than 10 years on military, operational, administrative, and legal aspects of digital operations and cybersecurity. He urges executives to look beyond their daily grind when it comes to warfare via digital infrastructures. "If you think this is not about you, think again."

Over the years, Ducheine has witnessed how cyber resilience conquered the boardroom. Initially, it was not a key issue on the agenda of the board, but this changed a couple of years ago. European legislation (NIS2) came into effect and was an important impulse for this. Organisations needed better understanding of how they are strongly interconnected in supply chains and networks.

Cascading effects

Some executives were clearly relieved after analysis learned that NIS2 was not applicable to their specific organisation. This relief is both understandable, playing by the rules is time-consuming and does not spike the EBIT (Earnings Before Interest and Taxes), as it is worrying. Ducheine stresses the fact that nearly every organisation has its role to play in warranting a resilient critical infrastructure. "Even if you think your organisation is not important in relation to the resilience of vital infrastructures: think again. A disruption in one part of the supply chain, whether due to a cyberattack, sabotage, or even a strike, can have cascading effects across entire industries and thus have impact on the vital infrastructure of a whole nation.'

It is however a common mistake at many companies to underestimate their strategic importance in this respect. A bakery, laboratory or local construction company may not be a valuable target in cyber warfare themselves but could play a role in supply chains that makes them attractive to being used as pawns in broader conflicts. And precisely because these companies lack the awareness about their role, attackers may perceive them as an easy starting point, or entry point, for disturbing vital sectors.

Ducheine knows that in itself, all of this is nothing new. But the message needs to be reinforced time and time again. Of all people, he knows how important it is.

When Ducheine did extensive research about four years ago, he was somewhat surprised by the extent to which IT companies had become central players in armed conflicts between states. **"IT services are the lifeblood of both businesses and governments but are precisely for that reason also an Achilles heel.** Cloud providers and software vendors are now as strategically important as traditional infrastructure such as energy networks. And the rapid advent of AI accelerates the hyper-connectedness. In other words: everyone should play their part to protect the whole. More than ever before in history."

Beyond opportunism

Do you as a board member truly understand how your organisation is positioned? Ducheine is convinced that leaders are focused on short-term growth rather than long-term ambitions, including warranting resilience. "They have a multitude of important topics on their plate and tend to delegate the cyber topics to specialists. By doing so, they completely ignore the strategic importance of it. The communications backbone of any organisation can be the intermediate, target to ruin the service or product, And the workforce may be lured or blackmailed into malicious acts. Hence, the company's very survival is at stake."

"It's time to wake up and invest proactively", says Ducheine. "In the past few years, we have seen how incidents acted as an effective catalyst for change in individual cases. However, this should not be the primary reason to raise the bar. Instead, **leaders must proactively foster a culture of preparedness, continuous learning, and cross-sector collaboration."**

Cyber in the military doctrine

Nonetheless, Ducheine is also positive about how cyber warfare has evolved from a niche concern to a core pillar of national security in the past decade. "The early days were marked by the challenge of building structures, creating awareness, and overcoming scepticism within traditional defence circles. A key milestone was the formation of the Defence Cyber Command and the integration of cyber strategy into broader military doctrine. Our journey was not without friction: different stakeholders had competing interests." He uses the metaphor of a sports hall with different coloured lines for each sport to illustrate the complexity of cyber: each team plays its own game, with its own rules and objectives, yet they share the same space and sometimes the same players. **Mastering cyber operations requires not just technical skills, but also the ability to collaborate across disciplines** and organisations. And to understand the rules of the different games.

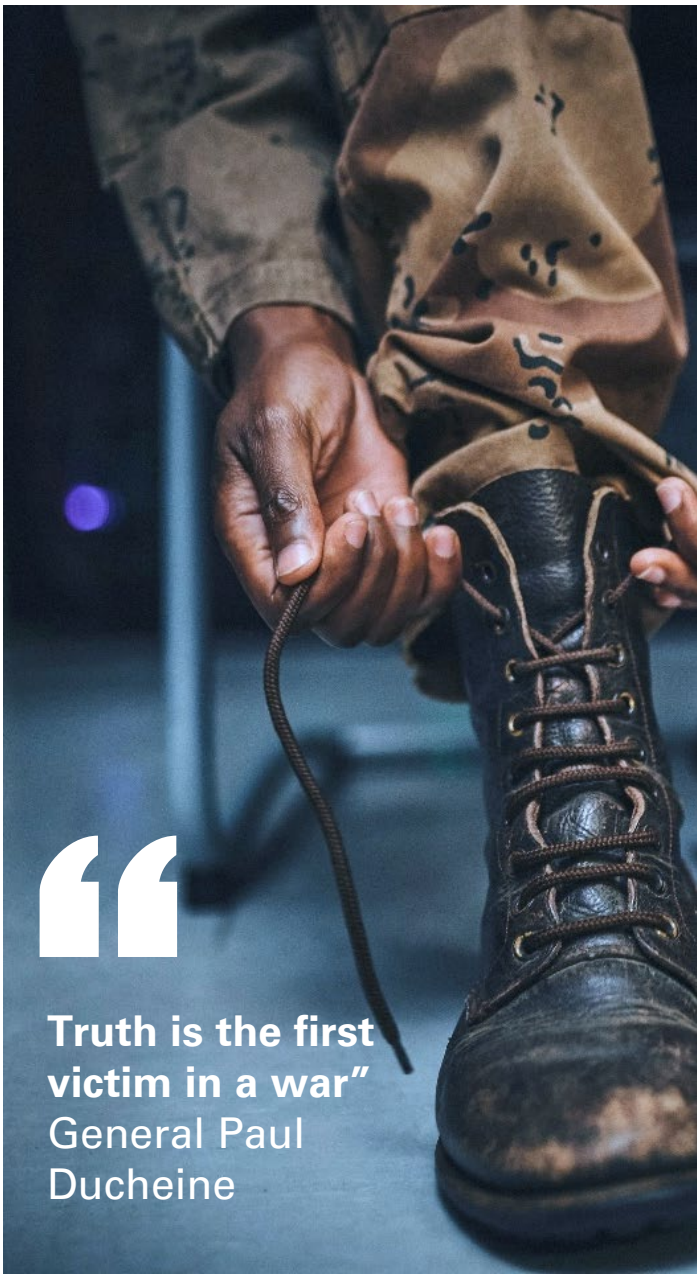
If we use that metaphor in the cyber arena, could we say that the best players are decathletes, not specialists? "Effective cyber defence and offence is a team sport. Ultimately, the goal is to create a team that can respond effectively to both routine and crisis situations, leveraging diverse skills and perspectives. We must encourage rotation and cross-training to improve collaboration across disciplines. The game is not just about technical mastery but also about mutual respect, understanding language, and the ability to operate seamlessly across organisational boundaries."

The power of perception: how disinformation eats trust

Ducheine also reflects on a somewhat overlooked aspect of cyber warfare: the softer approach by influencing public opinions. He points out that Russia and China have been masters of strategic deception throughout history and that technology offers them a vast potential to further ignite polarisation within European societies, which is one of the main goals of Putin. "The value of objective information is actively being eroded by a flood of opinions, impressions, and deliberate misinformation and nation states continuously play a role in this. **The cocktail of AI tooling and social media offers them vast potential to shape, amplify or distort narratives."**

Understanding facts requires more effort than consuming simple one-liners and short (fake) videos and most people don't take the time to dig deeper. This contributes to polarisation in societies. Public perception can diverge from official statistics, which underscores how influential information operations can be.

A well-known historic quote about war is that **'truth is the first victim in a war',** so the efforts to manipulate public perception have been around for ages. But yet again, technology offers a new toolkit to effectively use this weapon. "Gathering intelligence by nation states was once purely done for internal purposes, now it is also useful for obtaining exposure and a suitable narrative. Perhaps the most dangerous poison is invisible disinformation that slowly eats trust."



ESET threat intelligence

Cyber threats are increasingly geopolitical, with state actors such as Russia, China, Iran, and North Korea using cyber operations as a strategic tool worldwide.

Russia-aligned APTs (Advanced Persistent Threat) are seen targeting NATO critical infrastructure and Ukraine supporting countries, including ports, energy and telecommunications, with the objective of destabilisation and disruption of military aid provision.

The Netherlands remains a critical transit hub and is of paramount strategic importance for the sustained support of Ukraine. That comes with an elevated threat profile.

In a landscape of interconnected ecosystems, any organisation within a strategic supply chain is viewed as a legitimate target. And cyber operations have become an integral instrument of geopolitical pressure, including influence operations and disinformation.

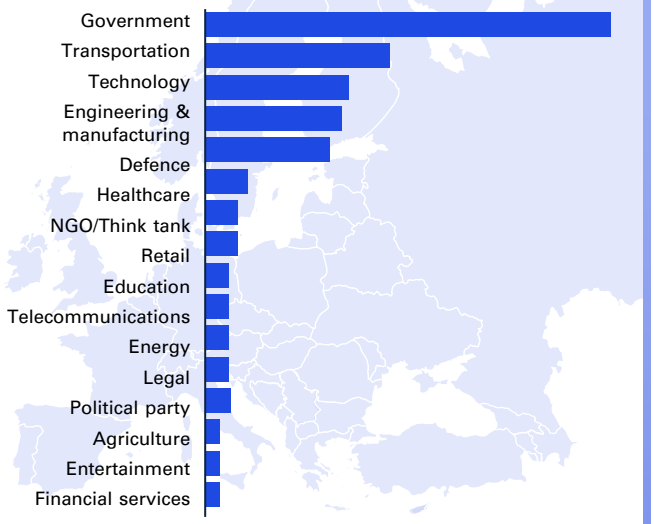
Stats

Ransomware deployment speed accelerated 48 percent (average 24-hour intrusion), driven by commoditisation of initial access and credential theft at scale.

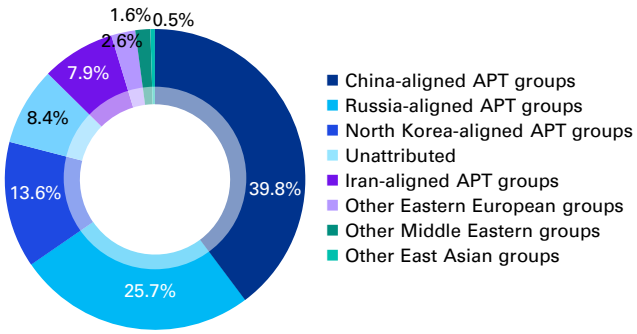
ESET Research projects a 40 percent year-on-year increase in the number of ransomware victims compared to the previous year.

Dave Maasland
CEO
ESET Netherlands

Targeted sectors in Europe



Attack sources



Source: ESET Threat Report H2 2025

Recommendations

Immediate

The board must reframe cybersecurity as a strategic part of the board agenda by establishing a dedicated committee that reports monthly. This ensures that strategic decisions are no longer delegated solely to technical specialists.

Mid-term

Organisations should undertake comprehensive, NATO-aligned cyber resilience audits to identify and eliminate single points of failure within their supply chains and logistics networks. The aim is to prevent cascading effects on critical infrastructure and security of a society in general.

Long-term

As a long-term strategic imperative, organisations must prioritise transforming their IT landscape from a fragile house of cards into a robust, compartmentalised system. This requires a migration of critical systems towards resilient, disaggregated architectures that are resistant to widespread compromise.

It took the ethical hacker 8 minutes to get in

09

Don’t wait until something goes wrong. Always be aware of your role in the chain” Rick van Dorp, Strategic director of Van Dorp

Can you give an example?

"We started a security improvement programme with specialised partners. One of the first things we found out was that an attempted CFO fraud for €40,000 nearly succeeded. Another finding was that quite a few employees clicked phishing links. But perhaps the biggest shock came during a penetration test. We thought we were doing fairly well in securing our systems, but the consultant we hired needed only eight minutes to gain full access."

As an HVAC company, you play a role in the chain and have a responsibility for your clients' cybersecurity. That role may not always be very tangible. Could you give an example of how this responsibility in the chain plays out in your work?

"Certainly. We manage the climate systems of some very prominent governmental offices. This means that you have access to floor plans and know who sits where. That's sensitive information. And perhaps the biggest game changer came during the NATO summit at the World Forum in The Hague. We manage the building management system there too. On the first day of the summit, we got a call from the National Coordinator for Counterterrorism and Security (NCTV), asking us to install a patch immediately. That really sharpened everyone's awareness."

Was it a wake-up call?

"And a blessing in disguise. The urgency became real. The NCTV had noticed a connection from the ministry to us through a vulnerable port. Within minutes, everyone was fully alert. Since then, we've taken compliance and security even more seriously. The entire management team has completed NIS2 training, and we've freed up resources for awareness."

How do you deal with the personal liability for executives that comes with this chain responsibility?

"It's a serious concern following the new legislation. In the end, we are the ones responsible for any fines or damages in the event of a breach. That's a big deal. You install a heat pump, and suddenly you're liable for the fallout of a cyberattack. That's serious. We're a decentralised company with many autonomous branches and a wide range of products and services. That diversity makes things more complex. Our cybersecurity policies have become much tighter. For major clients, we have a checklist that must be completed before we can manage systems remotely. In the past, we mainly advised about cyber. Now we enforce compliance. An example is when we rolled out multi-factor authentication (MFA) on laptops. We experienced a slow adoption. So at a company event with 250 managers, we told them very clearly: if you don't activate MFA today, you'll lose access to your laptop tomorrow. Simple as that."

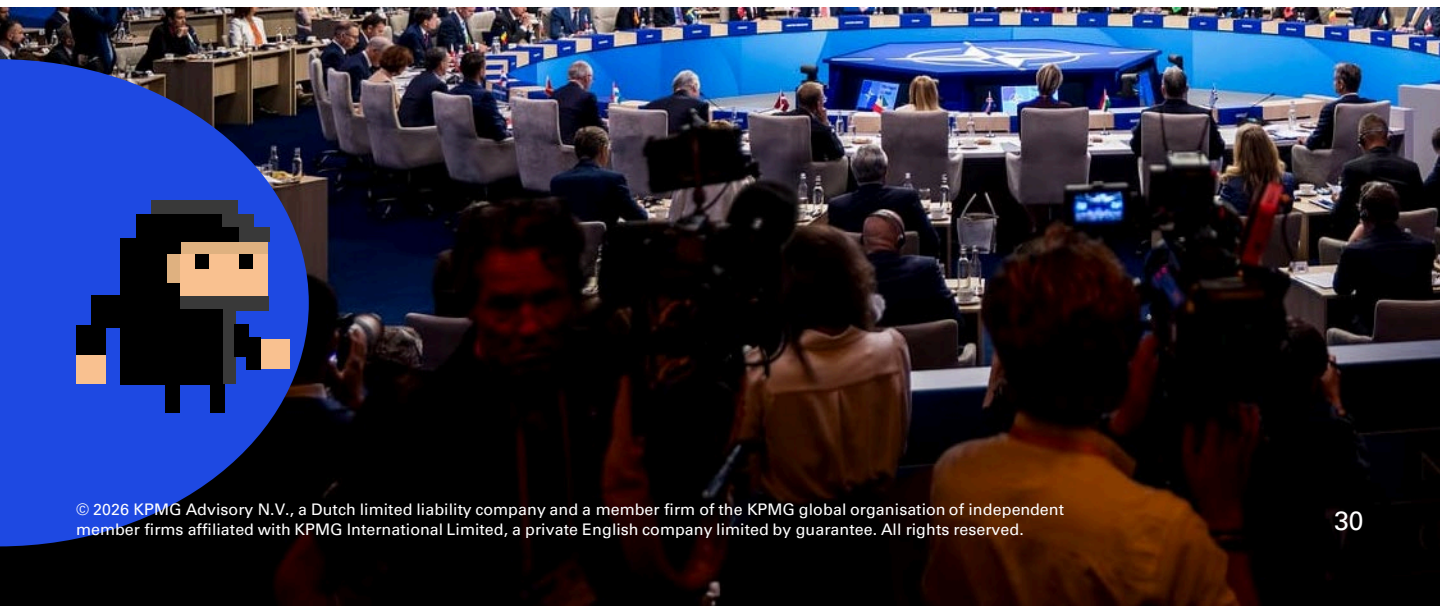
A common complaint is that compliance involves a lot of paperwork, especially because clients ask so many questions and demand reports. How do you handle that?

"We standardised responses into a single assurance pack aligned to recognised controls: a policy note on our cybersecurity measures, our roadmap to NIS2 compliance, company information, and a statement confirming that we haven't been hacked in the past three years. We only make exceptions for major clients like the Government Real Estate Agency.

For the future, I hope we can get to a standardised report with a rating that shows how well you're managing security, similar to how credit ratings work."

What's your main lesson for other entrepreneurs?

"Find yourself a good partner in the domain of cybersecurity. Don't wait until something goes wrong. And be always aware of your role in the chain, even if you think you don't have one."

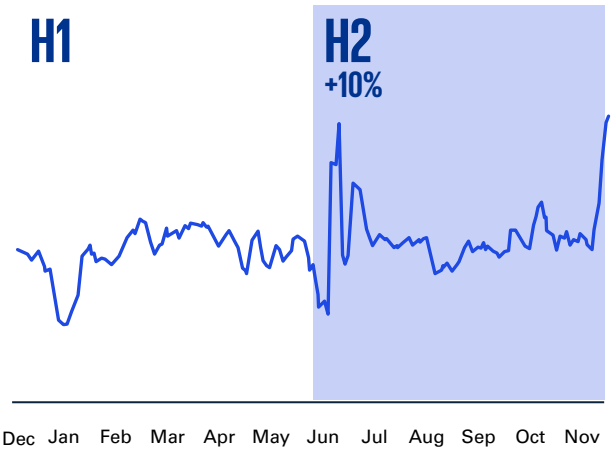


ESET threat intelligence

Rick van Dorp's experience highlights that state-sponsored operations are routinely targeting civilian vital infrastructure. Companies in the installation and logistics sectors have become primary targets in broader conflict scenarios. For C-level executives, the shift toward personal liability under NIS2 is a critical turning point.

Organisations that fail to integrate cyber resilience into their broader geopolitical strategy are ignoring a primary instrument of modern warfare that directly threatens their operational continuity.

Overall threat detection trend in H1 2025 and H2 2025, seven-day moving average



Source: ESET Threat Report H2 2025

Dave Maasland
CEO
ESET Netherlands

Recommendations

Immediate
Organisations need to act and audit critical suppliers for compromise. Prioritise audits in sectors relevant to your organisation, such as telecommunication, energy and logistics.

Mid-term
Implement FIDO2 MFA across infrastructure; eliminate password-based access to sensitive systems.

Long-term
Leadership must implement a long-term policy to also consider where technology comes from, instead of solely focusing on software vulnerabilities. Considering the war on talent, long-term security requires a regional talent pipeline, to ensure critical infrastructure remains resilient during crises when external support might be restricted.

10

Digital autonomy calls for harmonisation of baselines in cybersecurity

“There is a hidden cost to digital autonomy: complexity.” Sebastian Madden, Chief Product Officer at CREST

When organising a major event such as the 2026 World Cup, the whole supply chain can become a target for digital threats. It is a perfect opportunity for criminals to embarrass a host nation. And it means that even organisations with a peripheral role must be prepared. This is one of the reasons why Sebastian Madden, Chief Product Officer at CREST, makes a case for coherent international baselines in security.

Amidst today's geopolitical turbulence, digital autonomy has become a strategic priority for governments and large companies. Politicians have also put it on top of their agenda. The rationale for this is solid. Organisations want to keep control over critical data, reduce geopolitical exposure, and avoid dependence on a small group of global technology providers. Yet there is also another side to this coin, says Madden. "There is a hidden cost to digital autonomy: complexity. It may lead to fragmentation of digital infrastructures and cybersecurity practices. That fragmentation increases cost, slows innovation, and tests the resilience of organisations that suddenly operate under stricter, more localised rules and frameworks."

The effects of this fragmentation? What once could be delivered from a single global team now requires local units, local licences, and local compliance procedures. Talent cannot move freely either. A professional certified individual in one country may not be recognised in another, even within the same company. This slows down skills' development at a time when the global cybersecurity workforce is already overstretched.

The decentralisation also affects innovation. When teams operate in isolated pockets, their ability to learn from global best practices erodes. CREST, an international not-for-profit membership body representing the global cybersecurity industry, tries to counter this by encouraging the reuse of international standards. Madden cites Dubai's Cyber Force Programme as an example: companies must hold the same standards to qualify technically, and they only need to add local top-ups such as police checks or trade licences. The country thus adopts global quality baselines without reinventing the wheel.

C-level leaders have a role in acknowledging these trade-offs of digital autonomy. They must ensure their organisations build local capability where required, but without disconnecting from global best practices.

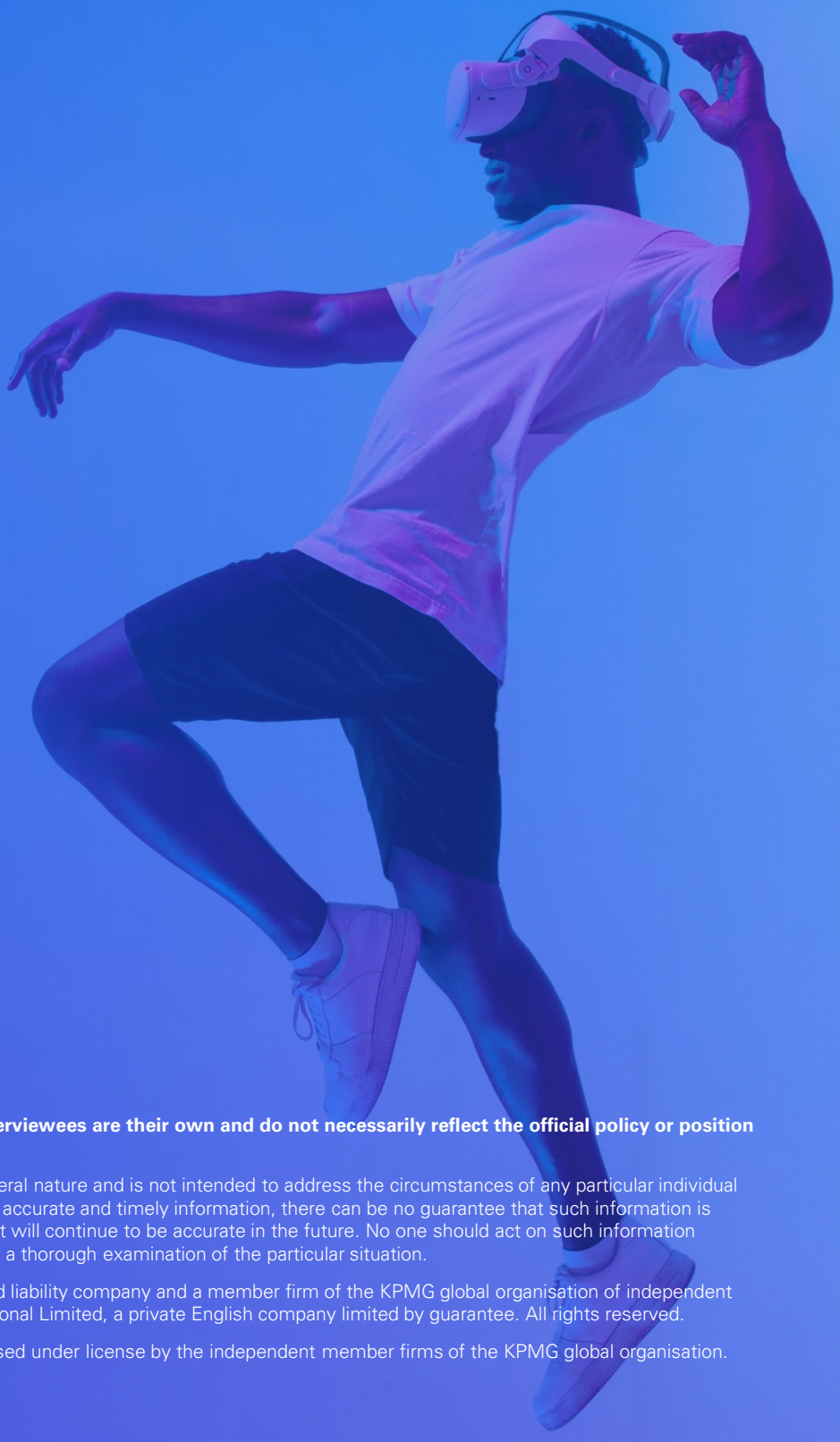
Digital autonomy is only one part of the wider resilience discussion now moving into C-suites. CEOs increasingly find themselves drawn into complex environments where geopolitical tension, public visibility, and digital risk intersect. Major events are a prime example of how this pressure builds up. One example is the upcoming 2026 World Cup, where any organisation in the supply chain can become a target. These threats range from politically motivated disruption to criminal activity or attempts to embarrass a host nation. Madden: "CEOs must assume heightened exposure the moment their organisation takes on even a peripheral role. This is precisely why we need international standards to manage the risks well."

In his view, effective resilience is built through preparation, and preparation requires (international) coordination. Resilience also calls for a realistic view of responsibility. Many organisations still approach crisis planning from a somewhat narrow, internal perspective. They look inward and downward, not upward and across. Events such as the 2026 World Cup, by definition, require coordination across public and private sectors, critical infrastructure operators, law enforcement, and specialised digital teams. If those links remain weak, even well-designed frameworks falter in practice.

Madden stresses that this lack of coordination leads to blind spots. A cyber incident that triggers a physical impact may for instance become the domain of fire brigades and emergency services. A digital intrusion driven by state actors may shift into the realm of intelligence or defence agencies. No single organisation can cover all dimensions. It's a matter of being able to connect the dots when it matters. Not only in elaborate plans on paper, but also in testing these plans for real.

Requests for proposal (RFPs) sometimes already reflect a shift in requirements: customers want to be assured of proper testing of crisis plans. The question that pops up when it becomes common practice to raise the bar in RFPs: why not see cybersecurity as an opportunity in the market, as a competitive factor? And why not use this opportunity to move from good enough to world-class?

It may be too early or too optimistic for this. But the broader message is clear: "The organisations that treat these topics as joint responsibilities rather than isolated duties will be the ones that stay adaptable in a more volatile digital landscape."



The views and opinions expressed by interviewees are their own and do not necessarily reflect the official policy or position of KPMG.