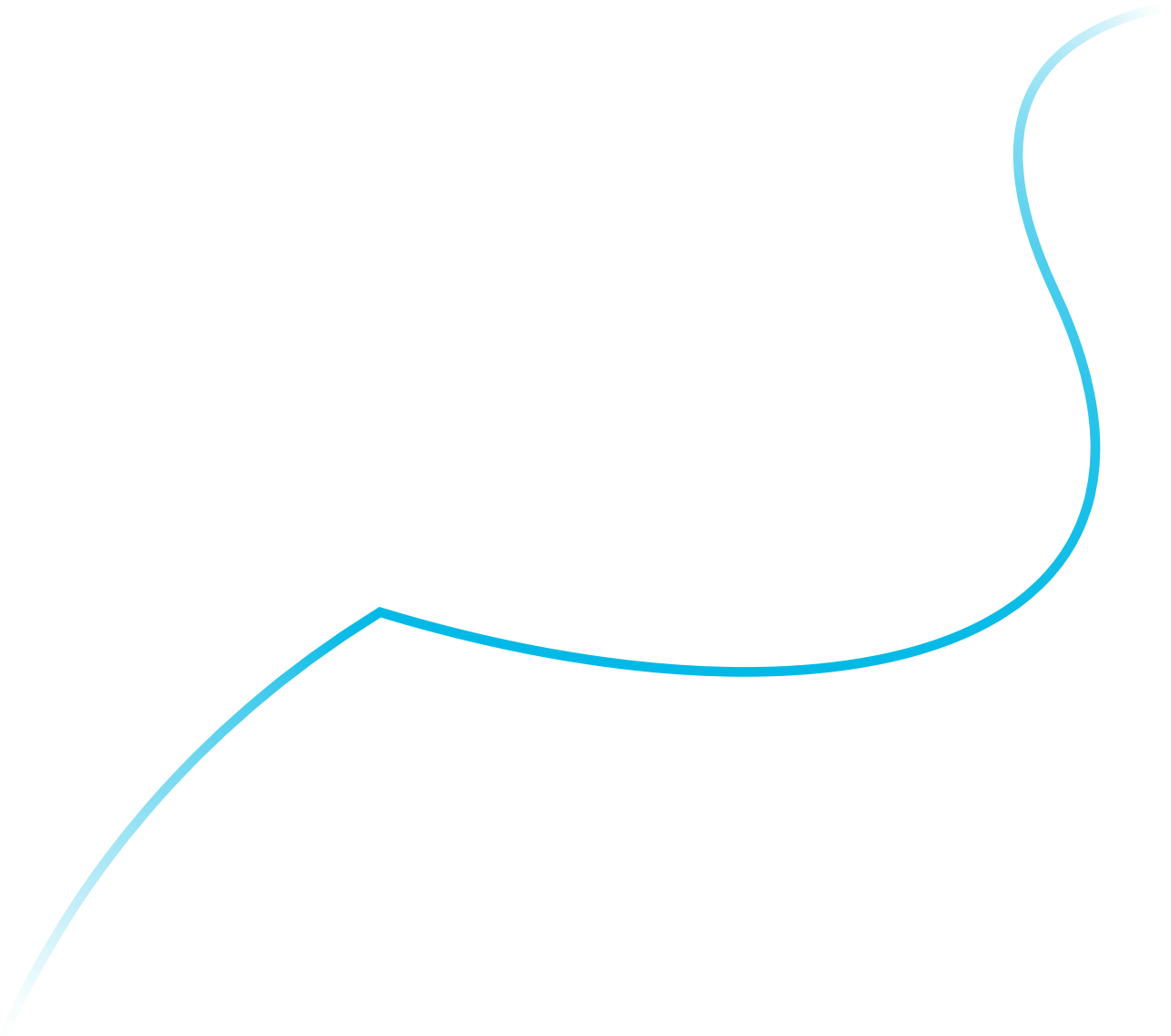
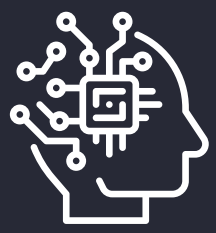
Trends in *Cybersecurity* 2025/2026

Cybersecurity Beyond Tomorrow

Capgemini





Trends in *Cybersecurity* 2025/2026

Cybersecurity Beyond Tomorrow

Index

Security Governance & Compliance

Future of Cyber

Preface: Cybersecurity Beyond Tomorrow

The digital world stands at a pivotal crossroads. Once a supporting function for operations, technology has now become a decisive factor in strategic positioning, competitiveness, and societal resilience. At the same time, complexity is mounting: cyberthreats are growing more sophisticated, global tensions expose the fragility of digital dependencies, and regulation demands demonstrable resilience.

In this landscape, cybersecurity is no longer a technical domain but a strategic imperative. The ability to manage digital risks while seizing opportunities increasingly defines the agility, innovation, and trustworthiness of both public and private organizations.

With the theme “Cybersecurity Beyond Tomorrow”, this report turns its focus firmly to the future. Cybersecurity today requires more than control. It demands adaptability, vision, and courage. Organizations that aim to be prepared for the unexpected must embed cybersecurity into strategy, culture, and technology.

We will explore four interconnected themes that will shape the cybersecurity agenda in the coming years: Artificial Intelligence (AI), Digital Sovereignty, Security Governance & Compliance, and The Future of Cyber. These themes transcend technology. They touch leadership, decision-making, and collaboration across an increasingly dynamic digital ecosystem.

AI: from tool to trust enabler

AI is evolving rapidly from a supportive technology into a strategic driver. In cybersecurity, it offers opportunities for real-time threat detection, predictive risk management, and operational efficiency. Yet AI also introduces new risks: inaccurate outputs, opaque decision-making, and ethical dilemmas. Robust governance is essential: ethics, transparency, and human oversight cannot be optional.

Organizations that adopt AI strategically and responsibly do more than improve processes. They strengthen trust with customers, regulators, and partners.

Digital Sovereignty: control over data and infrastructure

The demand for digital autonomy is intensifying. Cloud adoption, conflicting international legislation, and geopolitical uncertainty force organizations to make conscious decisions about data storage, encryption, and access.

Digital sovereignty is not achieved through technology alone. It requires governance, architectural foresight, and ecosystem collaboration. By embedding sovereignty into design, organizations can safeguard operations in a world where the rules shift constantly.

Security Governance & Compliance: from obligation to advantage

Regulation is becoming stricter and more specific. Frameworks such as NIS2, DORA, and the EU AI Act require clear governance, real time detection capabilities, and a strong security culture. Compliance is no longer just about meeting basic requirements; it must become a strategic driver of resilience, efficiency, and trust.

This shift requires change at multiple levels: structure, processes, and culture. Security is no longer a bolt-on; it is an integral part of business models, ecosystems, and digital transformation.

Future of Cyber: preparing for uncertainty

Tomorrow's threats are already taking shape. Quantum computing will disrupt current encryption standards. AI-driven attacks, automated exploitation, and deepfake-based social engineering represent new risks for which existing defenses are often inadequate.

Organizations that want to remain resilient must invest in crypto-agility, strategic risk profiling, and scenario planning. Equally important is the human factor: awareness, accountability, and collaboration across sectors and borders. The future of cyber will be defined not by reaction but by proactivity, adaptability, and resilience.

The trends highlighted in this report underscore one truth: cybersecurity is no longer a defensive shield but a strategic lever to navigate uncertainty and change. In a world where technology, geopolitics, and regulation intersect at speed, reactive measures are insufficient.

Focusing on "Cybersecurity Beyond Tomorrow" is not an aspiration but a necessity. Organizations that invest today in digital resilience, agility, and governance will not only protect themselves; they will create space for innovation, trust, and strategic advantage.

With this report, we provide insights into the challenges and opportunities that will shape digital resilience in the years ahead. We hope it inspires organizations to embed cybersecurity at the core of their strategic agenda and to take proactive steps toward building a secure, resilient, and future-ready digital ecosystem.

Devana Thonhauser

AI

Interview: How NS Makes Cybersecurity and Compliance Future-Proof

Dimitri van Zantvliet,
CISO and Cybersecurity Director at NS

> At NS, cybersecurity is not the department that hits the brakes, but a partner to the business. Our goal is to add value, not to be known as the office that says 'no'."

Safety and security are nothing new to the Netherlands' national rail operator Nederlandse Spoorwegen (NS). Ever since 1839, when the first train ran between Amsterdam and Haarlem, safety has been at the heart of the company's operations: from railway and fire safety to food safety, to name just a few of the ten different forms of safety NS manages. But while the railways have been firmly in place for nearly two centuries, digital security is a much newer dimension. "Cyber has only relatively recently appeared on our security radar," says Dimitri van Zantvliet, CISO and Cybersecurity Director at NS. "But today, we have no choice but to embed cybersecurity deeply into our business operations."

The catch-up advantage

When Van Zantvliet joined NS at the end of 2021, he found an organization that was about to be formally designated as a provider of critical services. This placed NS under the Dutch Network and Information Systems Security Act (Wbni), the predecessor of NIS2. "We were lagging behind compared to sectors like finance, which have been subject to stricter regulation for decades," Van Zantvliet recalls. "But we caught up decisively: setting up new teams, establishing governance, investing millions. Our maturity in cyber competencies has increased enormously."

That progress did not happen on its own. As Van Zantvliet puts it: "At NS, cybersecurity is not the department that hits the brakes, but a partner to the business. Our goal is to add value, not to be known as the office that says 'no'."

From AI pioneering to integration

NS is by no means a newcomer when it comes to artificial intelligence. As early as 1986, an AI expert system was already in use to calculate international freight tariffs. Since then, the application of AI has evolved widely. What was initially designed to predict maintenance needs for brakes and doors is now being used to optimize shunting yard planning algorithms.

In recent years, NS has also turned its attention to generative AI (GenAI). Van Zantvliet explains: "We have tested models and run them on our own infrastructure. Before ChatGPT became mainstream, we were already experimenting. Thanks to our tech culture, we were able to move quickly. I'm incredibly proud of that."

Those efforts have already produced dozens of use cases. For example, the internal cyber policy framework is accessible via a chatbot. NS employees can ask questions about password policy or incident reporting and receive instant answers. Outside the office, safety and service officers (BOAs) who issue fines at stations also receive AI support. AI helps them collect evidence and apply the correct legal grounds. “That has improved enforcement, because the fines are actually more likely to be collected,” says Van Zantvliet.

AI governance in practice

Speed should never come at the expense of diligence. That is why NS invested early on in an AI governance framework. “We started with a provisional policy: good enough to begin with, not perfect,” says Van Zantvliet. “That was a conscious choice. With the pace of developments, it was impossible to design a flawless framework from the start. So, we made a start and continue to develop it together with the organization. In this way, the policy grows along with practice.”

NS is now running its first AI Management System (AIMS), based on ISO 42001. This standard covers eleven risk domains, ranging from bias and fairness to ecological impact and privacy. “For every major change or go-live, we conduct a risk analysis,” Van Zantvliet explains. “That requires discipline and proper tooling, because it means that every project must be checked against those eleven domains.”

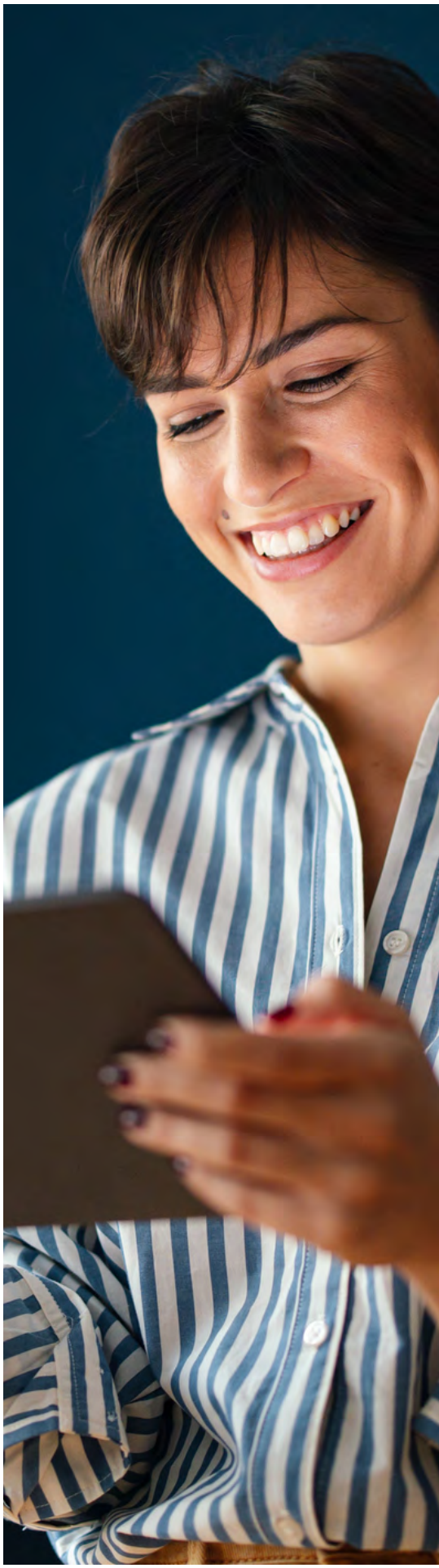
This process check is embedded in the Data Usage Board for AI (DUBAI), which evaluates proposals for proportionality, transparency, and social desirability. “We combine technical analysis with governance and ethics,” Van Zantvliet says. “And that is essential, because AI systems have a profound impact on people, data, and processes, especially at NS.”

Supply chain risks

As a public organization, NS takes digital resilience very seriously. Van Zantvliet explains: “We have added AI procurement requirements to our cybersecurity terms. Every supplier must specify how AI is used, for what purpose, and under what conditions. We want to know whether there is any shadow AI or hidden functionality.

With this, NS is anticipating the NIS2 Directive, which imposes additional requirements on cybersecurity for essential services. AI can support risk detection, monitoring, and compliance reporting, but it must also meet strict rules itself. “We are combining our existing Information Security Management System (ISMS) with the new AIMS,” Van Zantvliet says. “This creates a single, integrated approach that addresses both traditional IT security and AI-related risks.”

Even so, he remains concerned about the supply chain: “We can manage things fairly well ourselves, but many SMEs are still working on the basics. AI is now embedded in software by default, whether you want it or not. Therefore, bring-your-own AI can easily become a risk.”



AI as reinforcement of the cyber model

Does NS see AI as an additional layer on top of the existing security model, or as a fundamental overhaul? Van Zantvliet offers nuance: "AI strengthens existing processes. We use it for anomaly detection in trains, predictive maintenance, and incident recognition. But we are not moving toward autonomous agents that decide on their own whether a train should stop. We are simply not there yet."

Still, plenty of innovation is happening. In a recent pilot, a series of trains was equipped with ruggedized servers and AI at the edge. "We are running a next-gen firewall and intrusion detection in an entirely decentralized way. The system detects abnormal behavior in real time and sends events to our Security Operations Center. That is highly innovative, but integrating it properly takes five years," says Van Zantvliet.

People, mindset, and speed

AI in cybersecurity also requires change on the human side. Van Zantvliet explains: "Our cyber organization has only existed in its current form for a few years. We have grown into a functional cluster of about 120 people, 40 of whom are in my own team. I have personally hired many of them. We also have an AI Officer in the team, which means that cyber and AI governance are fully integrated."

Collaboration with the business is crucial: "You cannot impose AI top-down. We work iteratively and adaptively, in close cooperation with domain experts. That also means helping people understand the risks, frameworks, and opportunities. We have invested in awareness, training, and governance. The mindset is: It is fine to experiment, but within clear boundaries."

Still, there are challenges. "We are already at the maximum speed that NS as an organization can handle," Van Zantvliet says. "We are dealing with assets that last forty years, processes that are certified, and very strict procurement rules. We cannot simply order a hundred new trains for next Monday. That takes years."

Vital infrastructure in a geopolitical context

As CISO at NS, Van Zantvliet is responsible for the digital security of one of the most vital infrastructures in the Netherlands. That also requires vigilance against geopolitical threats. "Since the war in Ukraine, we have been monitoring more intensively for APTs, malware, and potential disruptions in the mobility sector. We work closely with the Dutch National Coordinator for Counterterrorism and Security (NCTV), the Military Intelligence and Security Service (MIVD), and the National Cyber Security Centre (NCSC), and feed our systems with up-to-date threat intelligence. Everything we learn, we try to share through ISACs and sector collaborations."

Within the CISO-NL community, where Van Zantvliet serves as chair, he also advocates for greater cooperation and stronger focus on basic hygiene: "Most breaches still result from very simple issues: no MFA, reused passwords, clicking on an unreliable link. We prefer to talk about hyper-modern, sexy applications. But as long as the basics are not in place, that remains a false sense of security."

> "We are doing well, but we need to move faster."

Van Zantvliet is proud of the progress NS has made. "We have achieved a lot in a short time. AI is now far more than just a gimmick: it has become a structural part of our cybersecurity strategy. We have governance, tooling, and use cases in place. And all development is done together with the business. But there is still work to be done. We have made big strides, but we are not there yet. The exponential speed of technological change demands maximum adaptability. And that is our greatest challenge: how do we keep up with that pace without losing control?"

His message to the sector? "Keep investing, keep collaborating. AI is an ally, but only if it is deployed responsibly and under strict control."

01

From Policy Paralysis *to Clarity*

How AI turns compliance into confidence

Highlights

- Complex cybersecurity policies are often misunderstood, increasing risk and reducing compliance.
- Tools like Microsoft Copilot simplify dense policies into clear, actionable language for all employees.
- Policy language can be tailored by role, improving understanding and daily use.
- Human review is essential to catch AI errors, reduce risks, and maintain trust and compliance.
- Policy transformation is a low-risk AI initiative offering immediate benefits and lasting strategic value.

In today's digital world, clear security policies are vital for all employees. Large Language Models (LLMs) can transform dense regulatory documents into clear, actionable guidance that ensures compliance, cuts risk and promotes a proactive security culture.

Why accessible security policies matter

Cybersecurity policies play a crucial role in safeguarding an organization's assets. Yet when these documents are overly complex and filled with technical jargon, employees struggle to understand what is expected from them. This lack of clarity can lead to poor compliance and risky behaviors, ultimately undermining and thus weakening overall security. Making policies accessible ensures every employee, from frontline staff to top management, clearly understands their responsibilities. Modern AI technologies such as Microsoft Copilot and OpenAI's ChatGPT provide a powerful way to transform complex policies into clear and actionable guidance. By improving understanding, they also encourage proactive security practices that strengthen an organization's defenses.

The communication gap in cybersecurity policies

Security policies are usually developed by specialized teams that prioritize accuracy and compliance, resulting in dense documents filled with legal terms and technical details. Over time, these policies typically evolve into elaborate guides intended for expert-only audiences. Consequently, non-technical staff (such as those in sales, human resources, or middle management) receive instructions that are difficult to decipher. Critical guidelines, such as procedures for reporting phishing attempts or handling sensitive data, can become buried under layers of complex language. This disconnect leads to misinterpretation or neglect, leaving employees uncertain about their responsibilities and increasing the organization's cyber risk.

Modern AI technologies such as Microsoft Copilot and OpenAI's ChatGPT provide a powerful way to transform complex policies into clear and actionable guidance.

Why LLMs provide a breakthrough opportunity

Enter LLMs. With their ability to analyze expansive datasets and generate human-like text, LLMs have the potential to bridge the earlier explained communication gap. They can take complex, jargon heavy documents and transform them into clear, concise guidance that preserves the core message, while removing barriers caused by technical language.

Imagine an employee reading a simplified six-step guide instead of a 50-page technical manual.

The instructions clearly explain that if they receive an unexpected email with a suspicious link, they should report it immediately to the helpdesk. For instance, instead of explaining "multifactor authentication protocols" in technical terms, an LLM can simply say: "Always use two ways to prove who you are when logging in." This kind of simplification not only improves understanding but also prompts faster and more confident responses. Table 1 shows a comparison between original policy language and plain language generated by AI.

By generating tailored summaries, LLMs enable communication on multiple levels. For example, an IT director might require a high-level overview that highlights compliance responsibilities and risk factors, while a frontline employee may benefit from clear, step-by-step instructions. LLMs can customize a single document to address the needs of those in different roles.

Table 1: Original policy language versus plain language generated by AI

Policy Term	Original Formal Policy Text	AI-Generated Plain Language
Privileged Account Security	All privileged accounts must undergo multifactor authentication enforcement, continuous session monitoring, and strict credential rotation protocols to prevent unauthorized access and insider threats.	• Turn on two-step (multi-factor) verification for any account with extra permissions. • Monitor all sessions to spot unusual activity. • Change passwords on a regular basis to keep accounts safe.
Identity Access Management (IAM)	All user accounts must be governed by Role-Based Access Control (RBAC) policies that enforce least privilege principles. Access permissions must be reviewed quarterly to remove excess rights, and all access requests require multi-level approvals with full audit logging to maintain security and compliance.	• Review user permissions every three months. • Require multiple approvals for access requests. • Keep records of all access changes.

How LLMs work for policy transformation

LLMs are trained on vast amounts of written material, including legal documents, technical manuals, and everyday conversation. This training enables them to understand context and generate plain-language explanations, even for complex subjects. In the context of cybersecurity policies, the process usually involves several steps:

Data preparation
Security policies must be digitized and standardized. This often means formatting documents consistently, tagging sections, and clearly identifying definitions and key phrases. These steps help the LLM interpret the content accurately and generate reliable results.

01

Translating policies into plain language
Once the documents are prepared, the LLM generates a simplified version. Advanced techniques such as Retrieval Augmented Generation (RAG) may be used to include relevant references from verified policy texts, helping ensure that the output is accurate and aligned with regulations. The result is a more readable version that reduces complexity while preserving the core security requirements.

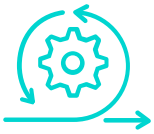
02

Human review and quality control
Although LLMs are powerful, they are not flawless. One known risk is that they can occasionally produce information that sounds correct but is factually wrong or fabricated. This is known as a “hallucination”. To avoid this, it is essential to include a human review step. Certified policy experts and auditors must carefully check the AI output to ensure that no important details are lost or distorted. This also creates an audit trail, where each change is traceable and compliant with regulatory standards.

03

Safe Adoption of LLMs

While the promise of LLMs is clear, it is important to acknowledge that this technology is a double-edged sword. On one hand, it notably lowers the barrier for understanding and complying with policies. On the other hand, it introduces risks such as potential misinterpretation or the generation of hallucinations, especially if the input data is not carefully managed. To prevent this, organizations must establish strong oversight mechanisms, ensuring that human experts review AI-generated outputs. This combination of automation and human expertise keeps the system both innovative and secure.



The adoption of LLMs in security policy management is at an exciting turning point. With technology advancing rapidly and interest throughout the cybersecurity sector reaching a critical mass, now is the time for organizations to experiment with and adopt these innovations.

Ensuring Auditability and Trust

A recurring theme in successful policy transformation is auditability. With LLMs generating user-friendly content, every automated transformation should include proper source referencing, linking back to the original text, and be logged for audit purposes. This practice establishes a clear and traceable record of how guidance was derived, reinforcing transparency and trust. Policies remain legally robust while being presented in a format that motivates compliance. Additionally, a human-in-the-loop strategy ensures that policy translations are subject to expert scrutiny. This not only limits the risk of errors but also provides a safety net when AI outputs deviate from approved guidelines. A well-documented process of oversight is critical for satisfying both internal and regulatory audits.

While much of the AI conversation is still dominated by hype, cybersecurity policy translation represents a rare and relatively safe entry point for applying LLMs. Unlike customer-facing tools that may affect brand perception or lead to legal complications, internal policy transformation provides clear value with controlled risk. It serves as an ideal testing ground for developing AI capabilities before expanding into more visible or high-stakes applications.

The adoption of LLMs in security policy management is at an exciting turning point. With technology advancing rapidly and interest throughout the cybersecurity sector reaching a critical mass, now is the time for organizations to experiment with and adopt these innovations. Forward-thinking enterprises are beginning to see measurable improvements in policy engagement and compliance, which bode well for broader industry applications. Early-adopter projects provide valuable insights and help establish best practices. We estimate that organizations that embrace LLM-driven policy accessibility now not only prepare themselves for future regulatory challenges but also foster a more informed, agile, and secure workforce.

Clear security policies are not just a compliance box; they are a frontline defense. LLMs give organizations a powerful tool to make policies actionable for everyone, not just IT and legal teams. The key is balance: combine automation with human review, ensure auditability, and keep outputs specific to each role. Organizations that begin with focused applications such as policy simplification will be in the best position to scale AI safely. Instead of waiting for the perfect moment, start where the risk is low and the payoff is immediate. Policy clarity is not just helpful, it is critical.

About the authors:

Folkert Visser

Managing Consultant
Cyber Defense

Folkert is a Cyber Defense enthusiast who excels at bridging the gap between theory, policy, and real-world practice. With a background in the telecom sector, he is currently focused on strengthening cybersecurity within the public domain.

www.linkedin.com/in/fkvisser
folkert.visser@capgemini.com

Mithras Kuipers

Cybersecurity Consultant
specialized in pentesting

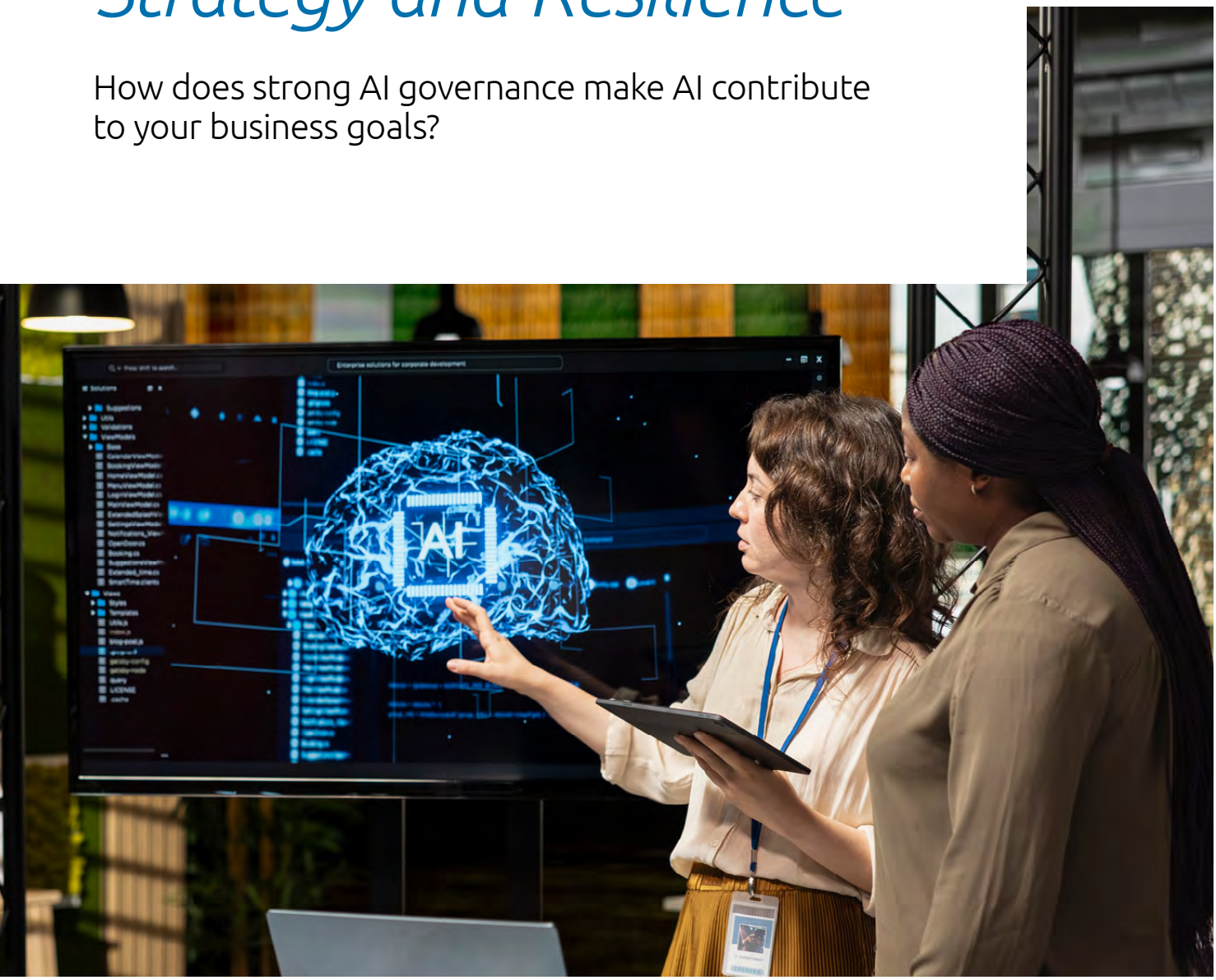
Mithras combines his expertise in pentesting with hands-on experience in machine learning and software development. He applies this skill set to explore how AI can support and enhance pentesting, while also identifying connections with other areas of cybersecurity.

www.linkedin.com/in/mithraskuipers
mithras.kuipers@capgemini.com

02

AI Governance: Focus on Trust, *Strategy and Resilience*

How does strong AI governance make AI contribute to your business goals?



Highlights

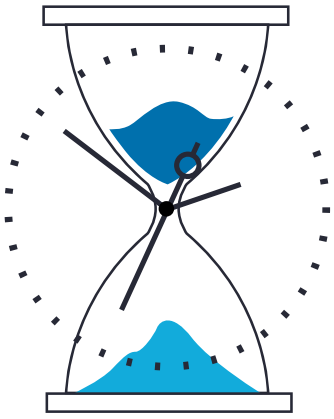
- AI governance is essential to align AI initiatives with strategic organisational goals and prevent them from becoming disconnected from broader policy.
- Effective AI governance requires cooperation within the organisation to manage risk and ensure compliance.
- AI governance touches on multiple domains such as IT, data, and ethics and requires a broader approach due to the unique challenges of AI.
- A robust AI governance framework provides insight into the strengths and weaknesses of AI applications, enabling organisations to better respond to opportunities and risks.
- By clearly defining tasks and responsibilities and making the right information available, it is possible to respond quickly and appropriately to an AI incident.

Artificial intelligence (AI) is rapidly changing business. It opens doors to innovative solutions and offers new growth opportunities, increases productivity and contributes to the organisation's profitability. At the same time, it also entails risks: from ethical dilemmas and bias to increasing pressure on compliance, transparency and responsible use. With clear frameworks, AI can develop into a strategic opportunity within an organisation and potential risk is limited.

In order to effectively regulate the opportunities and risks of AI within the European Union, the European Union has introduced an AI Regulation (AI Act) that sets rules for the development and use of AI systems.[1] This Regulation, which comes into force in phases from February 2025, applies to all companies that offer or apply AI. Other standards such as the NIST AI Risk Management Framework and the ISO 42001 AI Management System also offer practical guidelines for responsible AI use and are consistent with the requirements of the EU AI Act.

In this article, we will explain how AI governance can be implemented in practice, and why it is essential for organisations that want to use AI responsibly and future-proof.

The use of AI is growing rapidly in a variety of domains, from business to consumers' everyday lives. From an AI chatbot that supports a call centre to an AI-assisted drug research, this development also brings with it a growing responsibility for organisations. To be able to bear this responsibility and successfully use AI, it is not enough to simply look ahead. Careful management is required as well. Well-designed and effectively implemented AI governance is essential.



[1] Regulation (EU) 2024/1689.

AI governance

It is important for all companies and institutions that develop, deploy, or manage AI to establish clear agreements, processes, and responsibilities under the AI Act. This is called a governance structure. Such a structure ensures that AI systems not only function well technically, but are also ethically responsible and compliant with legislation. Without such a structure, there is a risk of AI systems generating undesirable or harmful outcomes, such as errors, discrimination, or even violations of fundamental rights. The introduction of AI governance helps to mitigate these risks and contributes to the responsible and transparent use of AI within organisations.

In addition to mitigating risks, AI governance also contributes to maximising the financial return on AI investments. By implementing AI systems in a controlled and reliable way, organisations can work more efficiently, cut costs, and generate value more quickly. Consider, for example, automated decision-making in customer service, where well-regulated AI leads to lower operating costs and higher customer satisfaction.[2]

Due to the above aspects, AI governance also affects other forms of governance within an organisation.[3] For example, it must be aligned with broader social responsibilities, which affects the corporate governance of an organisation.

Consider, for instance, ensuring ethically responsible decision-making when using AI in recruitment and selection, to prevent discrimination and guarantee transparency towards stakeholders.

AI governance not only influences social and administrative responsibilities, but also has a direct impact on IT governance. The integration of AI requires revision of architecture principles and security standards. For example: an AI system that analyses network traffic for cyber threats must be continuously monitored and integrated into existing incident response processes. IT governance ensures that this is in line with the IT strategy, compliance and risk management.

Data governance also plays a crucial role. Due to their autonomy and learning ability, AI systems require specific governance. Data governance ensures that the data used is representative, so that the system makes reliable decisions. For example, an AI model that reorders inventory in a supermarket may make mistakes if it has been trained on data from an exceptional period, such as a heat wave.

Effective AI governance starts with a clear structure and allocation of responsibilities, and requires an organisational culture in which AI is embraced as a strategic theme. Its purpose is to guide and control the use of AI within the organisation, so that it contributes to reliable, transparent, and ethically responsible decision-making.

[2] Why AI is the key to automation and cost savings ~ Wisemen

[3] AI and ethics – Volume 2, pages 603 – 609, (2022)-defining organizational AI governance: Defining organizational AI governance | AI and Ethics

Organisational

An effective AI structure and culture requires cooperation between different disciplines. By appointing AI Managers and an AI Officer for each department as a central point of contact, the policy is anchored in practice and the coherence between policy, technology and ethics is monitored. This approach is in line with previous organisational developments, in which central roles have been introduced to broadly safeguard issues such as privacy and information security.

In addition, setting up an AI Board or AI Committee is crucial. With representatives from legal affairs, business, compliance, IT and other departments, AI projects are not developed in silos, but are assessed holistically in terms of risks, impact and compliance with laws and regulations.

Legal and compliance teams play a key role in this: they translate legislation, such as the AI regulation and anti-discrimination laws, into practice. The AI regulation introduces a risk-based classification, whereby AI posing an unacceptable risk, such as social scoring, is explicitly prohibited.

For high-risk systems, the EU AI Act imposes additional requirements in terms of transparency, data documentation and human oversight. These requirements are intended to ensure safety, reliability and protection of fundamental rights in applications that can have a significant impact on people, such as in law enforcement, recruitment, or infrastructure. Legal and compliance teams supervise internal audits in this context and ensure that the organisation can demonstrate compliance with legal requirements and is prepared for external supervision.

In practice, this is reflected in the collaboration between the Privacy Officer and the AI Officer. By working together, they help ensure that AI systems comply with privacy legislation such as the GDPR, and that risks related to data use are identified and addressed in a timely manner.

A shared responsibility for AI in practice

How do you ensure that working responsibly with AI is not just a ‘tick-in-the-box’, but also becomes an attitude within your organisation? Not only is change required at the organisational level, but active involvement at the operational level is essential as well.

By appointing AI managers for each department, a network of shared responsibility is created. In this network, AI is not only seen as a technical issue, but as a theme that requires cooperation, transparency and continuous coordination.

Case study: AI chatbot in customer service

A designated AI manager quickly identifies incorrect responses and immediately contacts the AI team, privacy officers or IT security. This way, working responsibly with AI becomes part of daily practice and a culture of continuous improvement emerges.

Supervision and adjustment: Another aspect of AI governance

Appointing the right people and establishing a clear structure is only one aspect of effective AI governance. Equally important is the active monitoring of AI systems in practice. For example, an insurer that uses AI for claims assessment should check for unintended biases. This requires log keeping, bias testing, and human control. Therefore, regular checks are necessary to ensure accuracy, fairness and legal compliance. The AI Regulation requires continuous monitoring.

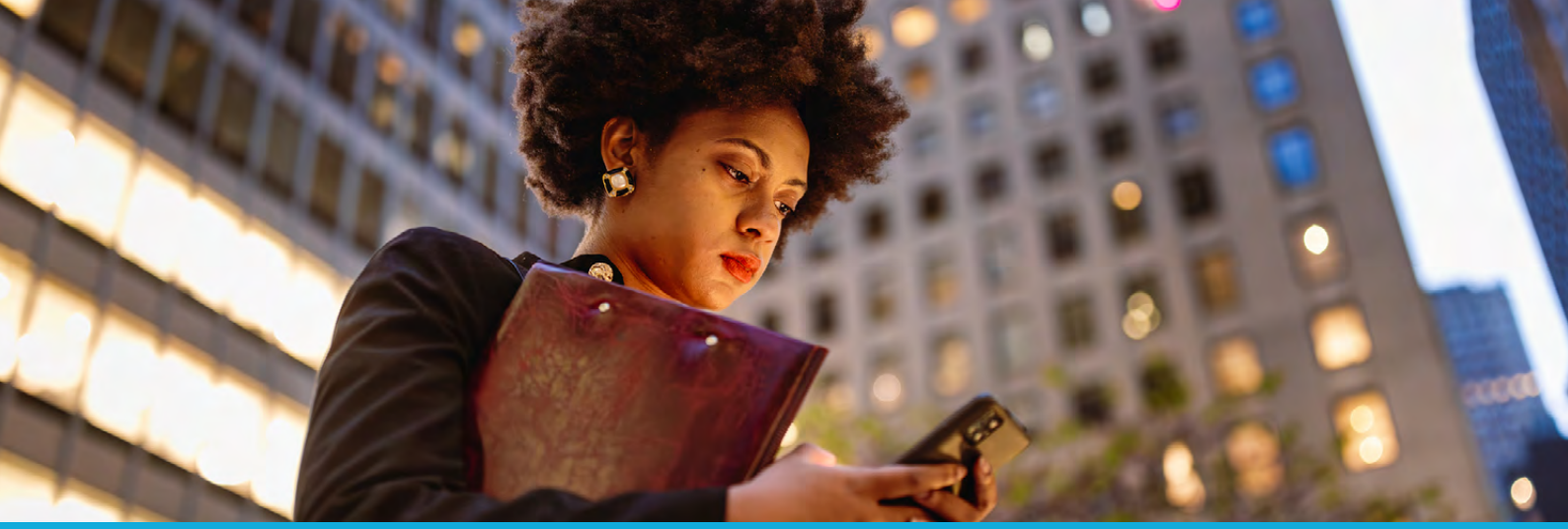
Case studies

Numerous studies have been conducted on the use of AI and the importance of strong governance. Such a study has also been undertaken by the Centre for Long-term Cybersecurity of UC Berkeley.[4] The report emphasises the importance of translating abstract AI principles into concrete applications.

Based on three case studies, this report shows how organisations are able to translate abstract AI principles into tangible policies and practices. The key insights that arise from this are:

1. AI principles are only valuable if they are supported by concrete actions, structures and culture change;
2. Internal governance (such as ethics committees) and external collaboration (such as international standards) go hand-in-hand;
3. Transparency, documentation, and engagement of various stakeholders – both within and outside the organisation – increase the acceptance and effectiveness of AI policies.

[4] Decision points in AI Governance, Three case studies explore efforts to operationalize AI Principles', CLTC White Paper Series. Decision_Points_AI_Governance.pdf



Opportunities through AI governance

A well-thought-out approach to AI governance helps organisations get a clear picture of both the opportunities and risks associated with AI. This allows them to invest strategically in technology, offer training courses and comply with laws and regulations, while increasing efficiency and profitability.

In practice, AI governance is not an abstract policy, but a concrete set of measures for responsible and effective use of AI. Below we explain **five essential building blocks** that contribute to the successful implementation of AI governance. Each of these elements not only protects against risks, but also opens the door to new opportunities.

1. **Training as the key to acceptance**
   A well-designed AI governance structure not only helps organisations manage risks, but also strengthens support and develops the right skills. ING research shows that 38% of respondents fear that AI deployment will cost their jobs in the coming years.[5] The same research shows that 9% of respondents believe that AI will create additional jobs. These figures emphasise the importance of a well-considered approach: By offering targeted training, AI can contribute to resolving staff shortages, reducing staff costs and increasing support.

2. **Ethical anchoring**
   An AI system must act in line with the same corporate standards and values that apply to employees. With well-designed AI governance, the system can focus on ethical principles such as honesty, inclusivity, responsibility, transparency, safety and reliability.

   Governance also ensures that this policy is assessed against the relevant legislation and regulations.

3. **Continuous monitoring**
   Ethical principles should not only be considered when developing an AI model, but should also be monitored throughout its entire lifecycle. After the development and testing phase of an AI model, 'model drift' may occur during use: the AI model gradually deviates from the original behaviour and over time no longer meets the ethical standards. Robust AI governance makes it possible to identify these risks in a timely manner, for example through monitoring or periodic audits or reassessments. This allows for timely intervention and ensures that the system remains reliable and responsible.

4. **Being prepared for incidents**
   Incidents are never completely preventable, which also applies to AI-related incidents. Solid AI governance helps organisations respond effectively.

   By establishing clear tasks and responsibilities in advance and making the right information available, it is possible to respond quickly and appropriately when an AI incident occurs. In addition, AI governance enables incident response processes to be tested, limiting the impact of incidents and helping prevent financial damage.

5. **Cooperation in the chain**
   AI systems and models are rarely developed or used in isolation; multiple internal and external parties are involved. Clear communication and the establishment of roles, responsibilities and agreements throughout the entire chain, including suppliers, are essential for effective AI governance. These parties are the primary target group for communication in the case of an incident. By organising this in advance, the risk of misunderstandings or delays in the event of an incident is significantly reduced, which not only ensures continuity, but also limits financial risks.

These five building blocks show that AI governance is much more than just rules: it is a strategic tool for deploying AI in a responsible, effective and future-proof manner. Investing in skills, ethics, monitoring, incident preparation, and collaboration helps manage risks and capitalise on opportunities.

[5] Bijna vier op de tien Nederlanders vreest dat AI banen gaat kosten - Sign Benelux

Strong AI governance is not only a tick on a checklist, but also a strategic weapon. Organisations that invest in clear roles, rigorous monitoring and interdisciplinary collaboration now are not only using AI safely, but are also actively building trust among customers, partners and regulators. This trust is more than just a reputational advantage; it forms the basis for competitive strength. By properly regulating AI, tasks can be automated more efficiently, and decision-making can be improved, leading to cost savings and greater operational effectiveness. At the same time, strong AI governance accelerates innovation and limits legal and reputational risks. This way, organisations not only claim their place in a digital future, but also strengthen their profitability and innovation.

Now is the time to go beyond compliance. By embedding ethics, training, and transparency, you transform AI from a risk into a strategic advantage. Not just to keep up, but to lead the way.

About the authors:

Lorin Derwish

Senior Consultant
Cybersecurity Compliance

Lorin specialises in compliance frameworks, including the AI Act. She helps organisations navigate legal changes, assess gaps, and develop strategies to meet evolving standards.

www.linkedin.com/in/lorin-derwish-523037100

lorin.derwish@capgemini.com

Rahul Rauniyar

Managing Consultant
Cybersecurity Compliance

Rahul is specialised in interpreting and applying requirements to strengthen operational resilience and cybersecurity controls across organisations, with a focus on compliance and adherence to industry standards.

www.linkedin.com/in/rahul-rauniyar

rahul.rauniyar@capgemini.com

Jeroen Nederlof

Senior Consultant
Cybersecurity Compliance

Jeroen is an experienced cybersecurity consultant in the area of governance, risk and compliance, holding multiple certifications and with a diverse technical background.

www.linkedin.com/in/jeroen-nederlof

jeroen.nederlof@capgemini.com

Digital Sovereignty

Cloud Autonomy:
The Need for Sovereignty
in the Netherlands

Highlights

- Disruptive geopolitical events in 2025 emphasize the need for digital sovereignty and autonomy.
- Both public and private organisations face cyber threats and dependence on foreign technology.
- It is no longer a luxury, but essential for control over data and infrastructure.
- Questions about whether this will become the new standard and what it means for innovation versus safety.
- Accelerated policies and investments in Europe-centric cloud and AI solutions show a growing urgency to achieve technological independence while continuing to innovate.

Our society and economy are becoming increasingly dependent on digital infrastructure, much of which lies beyond our national control and is shaped by international corporations and geopolitical tensions. Digital sovereignty is about maintaining control over technology that drives our daily lives and vital sectors, with resilience, independence, and direction at the heart. The rise of the sovereign cloud raises the question of whether this will become the new standard, or whether innovation becomes secondary to safety and stability. This discussion is not limited to the Netherlands and its vital infrastructure but also touches on broader European ambitions and even beyond for technological autonomy. In the articles that follow, we will further explore this topical and urgent theme of Digital Sovereignty, from different perspectives.

Is sovereign cloud computing the future and only standard moving forward? Or will this result in a complete shift in the digital landscape, with innovation taking a back seat to safety and stability? And does this only apply to Dutch society and its associated vital infrastructure services?

The geopolitical turmoil of recent years and the shift in the first half of 2025 have highlighted the urgency of digital autonomy in the Netherlands. Both public and private organisations face increasing cyber threats, dependence on foreign technology, and a growing need for control over data and infrastructure. The sovereign Cloud is no longer a luxury, but a strategic necessity.

Why sovereign cloud in all Industries?

In the public sector, dependence on foreign hyperscalers (such as AWS, Azure, and Google Cloud) is a risk to the continuity of essential services. Consider secure entrance to digital public services, tax portals, and municipal systems that are vulnerable to DDOS attacks or geopolitical pressures. We are now seeing a shift in standards and values, which means that this is not only relevant in the public sphere.

In the private sector, there is another risk: competitively sensitive data and intellectual property may be subject to foreign legislation, such as the US CLOUD Act. This can lead to legal conflicts and reputational damage. At the same time, access to innovation – such as AI and scalable infrastructure – is essential for competitiveness. The balance between autonomy and innovation requires a hybrid approach.

We are now seeing a shift in standards and values, which means that this is not only relevant in the public sphere.

Cybersecurity and risk management trends

The rise of state actors and hybrid threat scenarios requires robust digital resilience. Cybersecurity is no longer just an IT issue; it is a strategic governance challenge. Important elements in this context, especially in terms of organization-wide security and compliance, include the following:

1. **Zero-trust architectures** are becoming the norm, with access to systems being continuously and dynamically verified.
2. **Encryption under own management** (Client-side encryption, own key management) will become crucial for compliance and control, focusing on post-quantum cryptography-resistant set-up.
3. **Federal standards and Cloud models** such as NIS-2, Gaia-X and SECA (Sovereign European Cloud API) offer interoperability and scalability within European frameworks.
4. **Certifications such as SecNumCloud, C5, and ISO 27001** are becoming leading factors in tenders and risk assessments.
5. **Survivability** the ability to keep digital services operational in crisis situations requires redundancy, distribution, and fallback scenarios that can be initiated immediately.

Risk management is an integral part of cloud strategy. Instead of opting for a single infrastructure or supplier, this calls for a mix & match approach that focuses on clear data classification, flexibility, interoperability, and exit strategies. This means preventing a single point of failure, a solid risk analysis as a foundation, a holistic approach to safety.

The future: a sovereign digital infrastructure

Continue to rely on foreign hyperscalers or invest in a resilient digital infrastructure that extends beyond the public sector and its associated critical infrastructure.

Digital autonomy is not a return to the analogue era, but a forward-facing strategy for a resilient, innovative, and secure digital society. Both public and private organisations in the Netherlands must act now: not by choosing between innovation or control, but by combining both in a well-considered and integrated Cloud strategy. Sovereign cloud is not a goal in itself, but a means to put citizens and society first – with safety, flexibility, and personal control as its foundation.

Generally speaking, CxOs focus on legislation and regulations, the entire supply chain, the knowledge and skills of the staff and, above all, which data (from whom? Which classification? Which importance?). The risk picture on all these categories often trickles down to the operational and actual impact. This has given CISOs and cyber experts an additional threat scenario to consider, alongside the existing objectives of ensuring safety, compliance, and business resilience in a world of complex data regulations and geopolitical uncertainties.

The five key areas that CISOs should focus on:

1. Data governance and data classification: Know your data kingdom, which in many cases can still be unruly.
2. Data-centric security model: Protect the crown Jewels.
3. Cloud and infrastructure sovereignty: Choose your distribution and proportions carefully.
4. Supply chain and third party risk management and have a solid exit plan demonstrably effective in practice.
5. Navigate the regulatory landscape and comply with EU standards that are still evolving, partly as a result of the disruptive phase we are now in.

About the author:

Jurjen Thie

Cloud strategist

Jurjen has extensive experience ranging from Cloud Strategy consulting to Transition and Transformation projects at several large companies. He plays a critical role in increasing the value of cloud technology, Cloud mindset and applying it across organisations. As part of the Dutch Cloud CoE, as a Cloud strategist with a passion for complex, holistic issues and strives to solve the right problem in a creative way.

www.linkedin.com/in/jurjenthie

jurjen.thie@capgemini.com

03

Trust No One, Govern Everything: How Zero Trust Enables *Cloud Sovereignty*

A pragmatic approach to cloud guarding

Highlights

- Zero Trust shifts control from vendor defaults to organization-defined access policies.
- Sovereignty is earned through architecture, not provider geography.
- The Clarifying Lawful Overseas Use of Data (CLOUD) Act challenges jurisdiction; design choices mitigate exposure.
- Metadata control is essential and often overlooked in sovereignty models.
- A real-world case proves external access can be secure and sovereign.

Let's start with the dilemma. Many organizations are being pulled in two directions. On one hand, there's a clear need to modernize infrastructure, support hybrid workforces, and adopt best-in-class cloud services. On the other hand, there are growing concerns - especially in Europe - about data sovereignty, compliance, and geopolitical independence that need to be addressed, such as cloud providers with different legal jurisdictions.

At first glance, the Zero Trust model and digital sovereignty might seem incompatible. After all, the market leaders of advanced security solutions, particularly Zero Trust technologies, originate outside Europe. But here's the truth:

Zero Trust is not a threat to sovereignty. It is the mechanism that enables it.

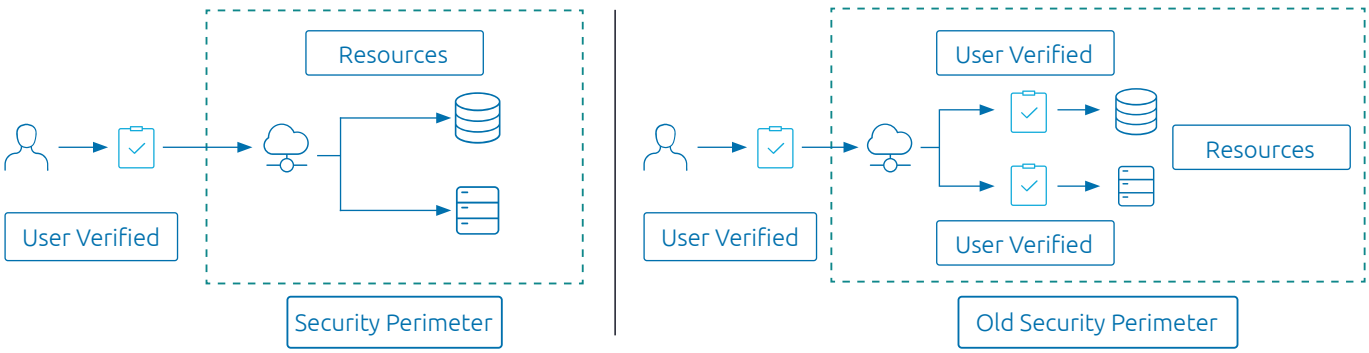
Nowadays, European institutions can exert greater control over their digital infrastructure by adopting Zero Trust regardless of where the technology was developed. In a landscape increasingly shaped by cyber diplomacy and digital dependency, leveraging Zero Trust means Europe can maintain resilience and autonomy while still integrating in global best practices. This shift, more stategic than technical, allows an organization to secure their data flows, enforce jurisdictional boundaries and assert their digital rights in a multipolar world where data is both currency and a weapon.

Zero Trust is not a threat to sovereignty. It is the mechanism that enables it.

The control shift

Traditional, perimeter-based security assumes that once you're inside it, you are trusted. This model, while functional in former security contexts, has become obsolete and hazardous due to contemporary threats. Zero Trust flips that thinking; you verify every identity, every device, every session, continuously and contextually. Zero Trust ensures access is granted not just at the perimeter but at every layer, network, application, and data access point in the enterprise. Both insiders and outsiders are treated with the same level of scrutiny. No one is trusted.

Figure 1. A comparison between Perimeter Based and Zero Trust Security models.



As defined by the National Institute of Standards and Technology (NIST) and embraced by the European Union Agency for Cybersecurity (ENISA), Zero Trust is a framework that assumes breach and verifies each request as though it originates from an open network. This approach initiates a fundamental shift in how organizations conceptualize their digital architecture, prompting a transformation towards more secure design principles and novelty governance frameworks.

In practice, adopting Zero Trust means regaining full control over access decisions independently of where your infrastructure or tools are geographically located. Whether your applications run on AWS, Azure, or a SaaS platform based outside the EU, it is the design of your security architecture, the precision of your access controls, and the enforcement of your organizational policies that define sovereignty.

This places emphasis not on vendor geography, but on your ability to shape and implement rules of access, accountability, and protection. Sovereignty emerges from deliberate architecture and not assumptions about locality. This is why European organizations must scrutinize how platforms handle administrative privileges, enforce isolation, and empower customer-defined boundaries.

These technical and operational choices are what truly ensure sovereignty in a cloud-dominated world.

The sovereignty angle

The European Commission's Digital Decade strategy defines digital sovereignty as the ability to control data access and usage regardless of where infrastructure or service providers are located. For security leaders, this is not an abstract principle, but a strategic imperative. Sovereignty then means having the power to enforce governance, maintain autonomy, and protect data integrity across increasingly global and complex digital ecosystems.[1]

Preserving this sovereignty hinges on architectural choices because it is not enough to choose vendors based on geography alone. True control depends on the ability to define who can access what, under which conditions, and through which verified identities. The Zero Trust model makes this possible shifting organizations away from implicit trust and towards dynamic, policy-driven access controls shaped by risk and context.

However, this autonomy faces tangible legal challenges. Laws like the U.S. CLOUD Act empower American authorities to request data from U.S.-based cloud providers regardless of where that data is physically stored, thus creating a sovereignty dilemma: organizations may lose control over sensitive data simply by choosing widely adopted global platforms. So, how can this be addressed?

Fortunately, security architecture can mitigate these risks.

Sovereignty can be preserved even when working with non-EU vendors if the organizations proceed with some key elements of security within the solutions that may be affected by the legal challenges:

- Technical solutions like the implementation of customer-controlled encryption keys (BYOK/HYOK), ensuring that no external party can decrypt the stored data.
- Governance solutions like the adoption of federated identity and access models that decentralize control and minimize admin reach.
- Geopolitical decisions like the enforcement of data residency within the EU borders, using providers that allow features like localized storage and access policies.
- Access solutions such as opting for solutions with Zero operator access, preventing providers from having backend privileges over the tenant environments.

Sovereignty is not promised by a provider's physical address, but earned through architecture, accountability and control.

[1] European Comission. (2021). 2030 Digital Compass: the European way for the Digital Decade. Brussels: EU For Digital.

A real-world use case: securing external access without losing sovereignty

Let's take a look at this leading multinational logistics and facility services provider. The challenge they faces was quite complex: how to give hundreds of external contractors secure access to core building management systems without compromising compliance, visibility, or control. These systems - some cloud-based, other on-premises - handled operational data subject to EU sovereignty requirements and GDPR.

The organization's priorities were clear. External users could not be included in the internal identity systems. Direct network access was out of the question and every access session from user behavior to security telemetry had to remain under European jurisdiction.

As their solution, the company adopted an architecture built on Zero Trust principles and sovereignty-first thinking. Instead of relying on perimeter-based security or vendor defaults, they implemented solutions that provided seamless app-level access while keeping operational and policy enforcement entirely within EU boundaries. User verification, access decisions, and data flows were managed in a way that upheld the organization's governance regardless of which tools or cloud platforms were involved. This means they relied on processes and policies as their primary means of preserving sovereignty.

Critically, the approach addressed a sovereignty blind spot often overlooked: metadata. While some services operated globally, the company ensured that all metadata logs, telemetry, and user session data were processed and stored within their sovereign infrastructure. Control over identities and encryption keys remained exclusively in the hands of the organization.

The result? External users gained access without friction, the network remained shielded, and sovereignty was preserved not by vendor geography, but by architectural intent. The case shows that sovereignty is not an abstract ambition but a practical, enforceable standard that begins with how you design access.

The paradox and the answer behind it

After all, not just one but probably all organizations reach a point where they must ask the big question: how do you build a security model that "trusts no one" but must trust the providers and the solutions they bring to the table? That is the paradox that comes with the choice of technology, but the answer, surprisingly, is not complex at all:

You do not need to trust the technology; you need to control it.

According to Forrester Research, Zero Trust is not a product; it is a strategy, and when aligned with data governance and SaaS control, it serves as a mechanism for digital independence.[2] Sovereignty exists when it is the decisions made by the organization what builds security and the technology that backs it up, and not the other way around. You define who gets access, under what conditions, and with what oversight – not the vendor. That is operational sovereignty in action.

Security and sovereignty are not opposing goals, but co-dependent disciplines.

And that is the shift that leadership must embrace: sovereignty in the digital world is not given, but designed and shaped. It is not about trusting vendors implicitly but about building a model that can operate securely regardless of who provides it. Zero trust enables design and enforces the boundaries where geography and legal jurisdictions cannot.

In a world where jurisdictions are mixed, infrastructures shared on cloud platforms and global breaches occurring daily, the Zero trust model not only becomes a safeguard, but a statement. It declares that your organization defines its own perimeter, that it governs not by default, but by deliberate choice.

Zero trust will not be the answer to every question, but it is the strategy that turns sovereignty from an aspiration into an architecture.

That is not only security, but innovation and leadership.

When implemented with intent, Zero Trust becomes the bridge between innovation and control.

[2] Rivera, C., & Mullins, H. (2023, September 19). Forrester Research. Retrieved from www.forrester.com/report/the-forrester-wave-tm-zero-trust-platform-providers-q3-2023/RES179872

About the authors:

Alfredo Acuña Salswach

Senior Data & App Security Specialist

Alfredo is a Zero Trust and IAM lead for Capgemini Netherlands. He is a builder of secure and modern identity architecture with a passion for translating complex tech into clear business value.

www.linkedin.com/in/alfredo-acuna-salswach

alfredo.acuna-salswach@capgemini.com

Nilasha Sloeserwij

Cyber Security Consultant

Nilasha is a Cyber Security consultant with a strong focus on identifying risks and implementing security measures. She has developed a strong passion for IAM and has experience creating security awareness programs to enhance organizational security.

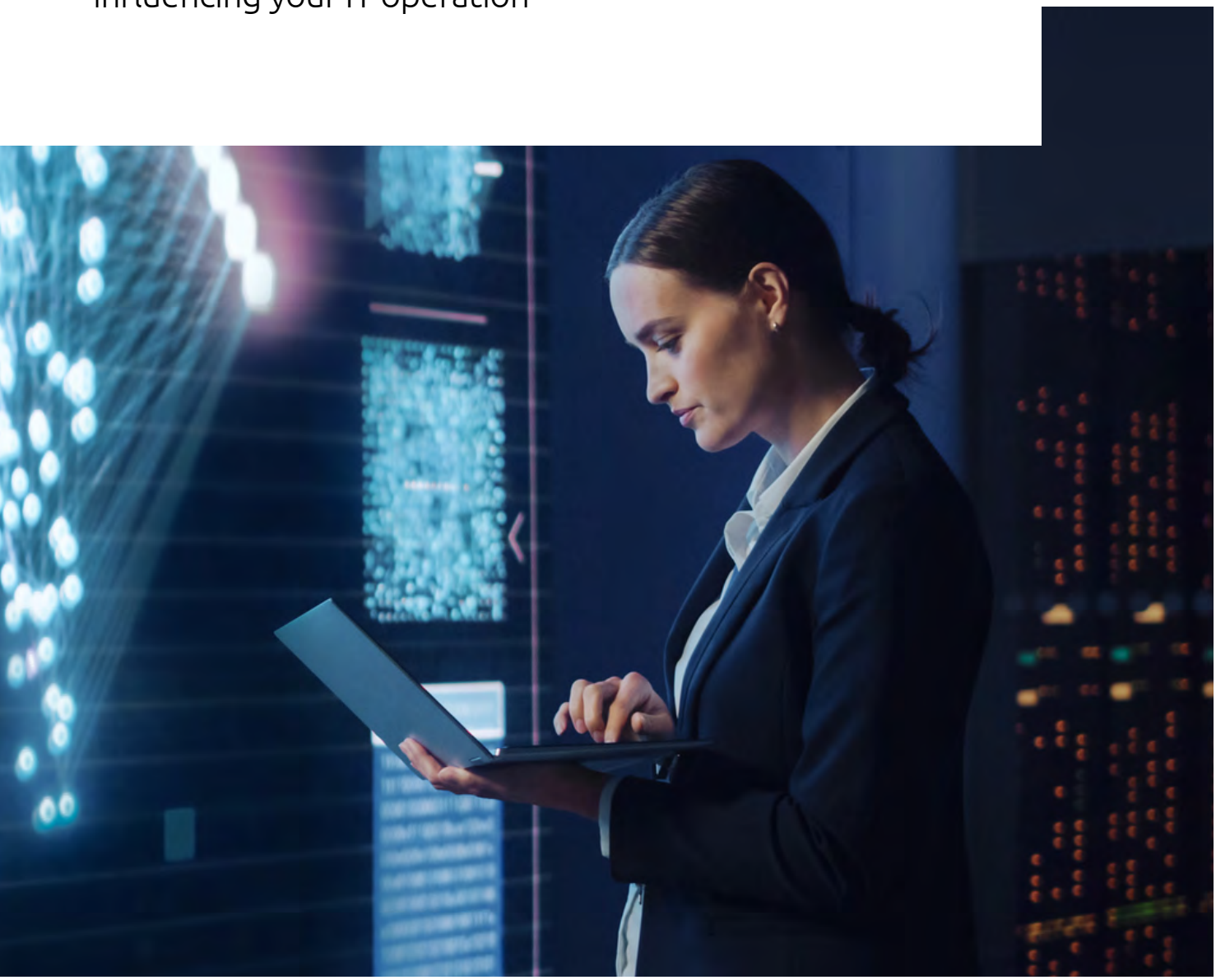
www.linkedin.com/in/nilasha-sloeserwij

nilasha.sloeserwij@capgemini.com

04

Ensuring *Data Sovereignty* through Encryption

How to protect your data against global politics influencing your IT operation



Highlights

- Specialization has enabled technology providers to provide tremendous benefits of scale.
- Various legislations around the globe conflict with local laws and regulations that protect data.
- Without proper caution, users of cloud services face a lose-lose choice between giving up their data sovereignty or losing the benefits of cloud services.
- Encryption provides an alternative to protect your data while using cloud services.
- Proper implementation of encryption requires users to be in full control of the encryption keys.

While changes in legislation have impacted the trust in cloud services of American hyperscalers, these products remain of great value.

Encryption provides a path to continued, trustworthy use of cloud services, as long as you are in full control of your keys, allowing continued use of cloud services without compromising control over your data.

Specialization pays off

Historically, society has tended towards specialization over self-sufficiency. Hardly any of us build our own houses, grow our own food, or mine our raw materials. Instead, we rely upon and trust an organically grown network of specializations, for bricklaying, farming, mining… for everything.

The same principle applies to IT operations, particularly within larger organizations that have the volume to allow for specialization. A network engineer is better suited to manage a network than a system administrator, and database administrators should not be responsible for managing firewalls. Today, the hardware of on-premises data centers has largely been replaced by virtual systems from hyperscalers, delivering the true benefits of scale.

However, it has become apparent that this increased specialization can no longer rely solely on a solid foundation of trust.

Dissecting the legal foundations of trust

It is unrealistic for any organization to completely and thoroughly evaluate its entire technology stack that is in use. Routers, switches and servers are traditionally viewed with caution because of their large reach and are more commonly subjected to code reviews and pen testing. However, a similar approach could be argued for less obvious devices like phones, computer mouses, building sensors, and more. Nearly every connected device can somehow be exploited for malicious purposes.

For most organizations, full control is an illusion. To achieve some level of control, organizations typically implement a third party risk management or supply chain risk management process. These processes allow an organization to balance control, risk, evidence, and trust. Still, some level of trust in technology providers remains inevitably necessary.

In western society, trust in Chinese technology providers has traditionally been low. They have been suspected of enabling the Chinese government to access data or even client infrastructure. In 2023, the European Commission approved the ban of specific Chinese technology providers in essential parts within member-state critical infrastructure.[1] As a result, Huawei has effectively been banned from Dutch critical telecom infrastructure.

The US has long been considered an ally of European countries. An unquestioned level of trust in US technology providers cemented itself in our western European society. However, in 2018, the US enacted the CLOUD Act.[2] This established that for American companies, US jurisdiction applies for data requested by warrants or subpoenas, regardless of the physical storage location. The CLOUD Act effectively overrides local laws and regulations that protect data. In other words, American companies can be legally required to hand over data that falls under EU regulatory protection.

Although the CLOUD Act was already established in 2018, it initially received little attention in western European IT operations. American hyperscalers remained the go-to solution for IT server infrastructure. However, the sentiment on data sovereignty changed noticeably after the political shift of the US government in early 2025. The virtually unquestioned trust in the services, security, and trustworthiness of the main hyperscalers took a hit. Companies started to look for more robust ways to protect the data that was entrusted to them.

Looking for alternatives to ensure trust

Since the introduction of cloud-based IT services, companies have started to move their IT infrastructure into the cloud. Buying cloud-based IT infrastructure and IT services provides all kinds of benefits, not just economic ones. Reversing that trend and building private and on-premises data centers has become appealing.

However, operating and managing a data center negates the economic benefits of cloud services in times when IT budgets remain tight. IT cost increases could be detrimental to the existence of some companies. This suggests that companies need to choose between a lose-lose scenario: giving up their data sovereignty or losing the benefits of cloud services.

Fortunately, data encryption provides a third choice that allows organizations to retain the benefits of cloud services and remain in control of their data. Proper encrypting ensures data can only be read by those who have access to the decryption keys. While encryption does not protect against the execution of warrants or subpoenas, it does protect against foreign agencies reading that data. This benefit also applies to hyperscalers based outside of the US.

Introducing encryption is not an easy task and should not be taken lightly. The choice of a specific encryption algorithm matters. Different ciphers have different characteristics when it comes to implementation effort, scalability, protocol overhead, performance, trustworthiness, and even post-quantum readiness.

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309

[2] https://en.wikipedia.org/wiki/CLOUD_Act

Encryption without Key Management is meaningless

In cryptology theory, it is recommended to be transparent about the encryption protocol and only treat the key as secret. A public review of the encryption protocol ensures weaknesses can be, and typically are, identified faster. Since the protocol should be considered public knowledge, it is the key that provides all the protection of data. Therefore, key management is most essential when using encryption to safeguard data. Unsafe storage of keys could negate all efforts put into encryption.

In an on-premises setting, using a Hardware Security Module (HSM) would be the go-to solution. For a cloud setting, hyperscalers offer services like that of an HSM, or even an actual HSM. However, using these services is equivalent to writing the code to your vault on a sticky note next to it. To protect our data, we need independence.

Fortunately, features like Bring Your Own Key or implementing an architecture that integrates an on-premise HSM with cloud services provide a useful alternative. These methods ensure that you remain in control of your keys, keeping your data secure.

While changes in legislation have impacted the trust in cloud services of American hyperscalers, these products remain of great value. Moving away from cloud services would result in significant divestment and would require building a new data center capacity and increasing operational costs. Encryption provides a path to continued trustworthy use of cloud services as long as you are in full control of your keys allowing continued use of cloud services without compromising control over your data.

About the author:

Folkert Visser

Managing Consultant Cyber Defense

Folkert is a Cyber Defense enthusiast who excels at bridging the gap between theory, policy, and real-world practice. With a background in the telecom sector, he is currently focused on strengthening cybersecurity within the public domain.

www.linkedin.com/in/fkvisser

folkert.visser@capgemini.com

Security Governance & Compliance

Interview: How Odido Accelerates Innovation and Resilience Through Compliance

Martijn Ronteltap,
CSO and GRC
Director Odido

> We have become an increasingly important critical infrastructure player and now critical infrastructure depends on us."

Compliance is sometimes seen as a burden, an arsenal of checkboxes to tick off just to satisfy the regulator. That mindset can be fatal for a telecom company that is part of the critical infrastructure. At Odido, compliance is instead regarded as the foundation of governance, innovation, and resilience. Martijn Ronteltap, CSO and GRC Director, explains how Odido uses compliance strategically to become stronger, more agile, and future-proof.

From challenger to key player

The telecom sector has traditionally been a strictly regulated playing field. Odido started out as a challenger in the market but has since grown into one of the largest players in the Netherlands. This transition came with a shift in responsibilities. "As a challenger, we could still rely on speed and boldness," says Ronteltap. "But we have become an increasingly important critical infrastructure player and now critical infrastructure depends on us."

In this context, compliance is no longer optional but a requirement. "You have the responsibility to keep your network reliable, because emergency services depend on it," Ronteltap continues. "Our corporate clients also use our network for their critical processes. That puts enormous pressure on our compliance approach, but it also creates an opportunity: if you manage it well, you gain trust – and that gives you a competitive advantage," he adds.

Compliance as a strategic lever

How do you make sure compliance does not become a box-ticking exercise? Ronteltap: "It is about mindset. You shouldn't see it as an obligation, but as a way to structure your organization and enable innovation. You can never design everything perfectly in advance, but you can position yourself to document thoroughly, explain, and substantiate. That creates room for agility."

He emphasizes that compliance at Odido is also a form of storytelling: "Tell me, show me, prove to me. We have to demonstrate that we have everything in order. Not only for regulators, but also for customers, shareholders, and our own people. Transparency and accountability are key."

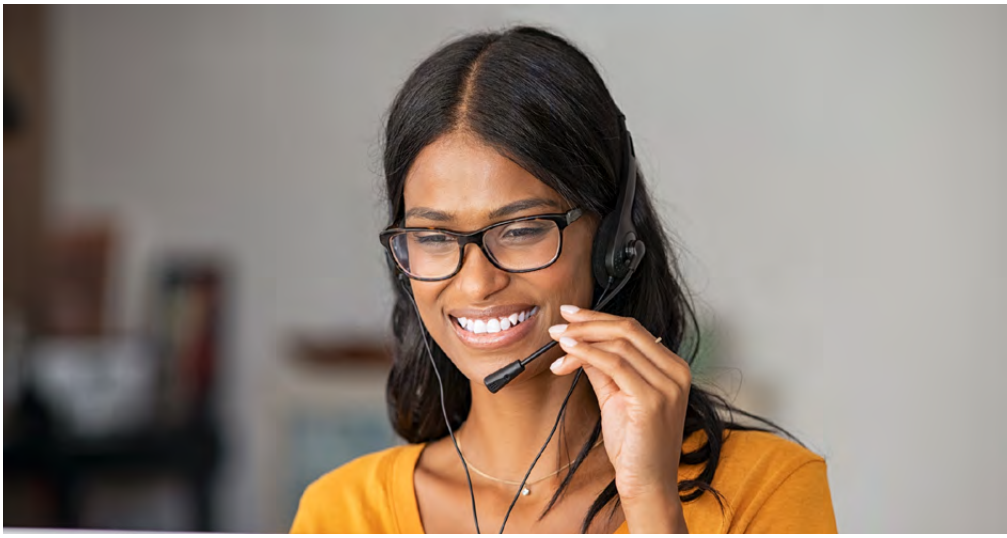
Resilience versus agility

As part of critical infrastructure, Odido constantly balances strict regulations with the need for speed. Ronteltap explains: "That has two sides. In the network domain, which supports emergency services, we are extremely cautious. We don't run that part in an agile way. At the same time, on the commercial side, we want to be fast and agile. So you end up with different speeds within one organization."

This tension makes compliance at the very least challenging: multiple regulators, diverse requirements, and at times even conflicting expectations. "In the Netherlands, we deal with the Radiocommunications Agency, the Data Protection Authority (DPA), the Authority for Consumers and Markets (ACM), and the Authority for Financial Markets (AFM). Each sets its own requirements, with separate audits and reports. That's why we have built a robust framework to help us maintain oversight and plan audits within an annual cycle," Ronteltap explains.

Automation as an enabler

At Odido, compliance and automation are closely intertwined. "Automation makes compliance sustainable," says Ronteltap. "You can't go through hundreds of audits and checks manually every year. We build tools that automatically generate reports, provide real-time monitoring where possible, and flag deviations even before we or an external party conduct an audit. In this way, compliance does not become a burden, but a natural part of our operations."



NIS2: consolidation rather than revolution

While many organizations are struggling with the implementation of NIS2, Ronteltap sees it primarily as a tightening of existing processes. "For telecom operators, many requirements were already covered in the Telecommunications Act," he says. "We've always had to deliver reports, notify incidents, and so on. What NIS2 adds is the emphasis on documentation and accountability at the board level. That takes time and effort, but in terms of content we were already doing a lot."

"The discussion with the government is more about the details: What exactly does the reporting obligation look like, what does it mean for customers in practice, and how far does the chain of responsibility extend? This is a logical step in the maturity of our sector. We see it as an opportunity to further strengthen our governance."

Lessons identified, then learned

Compliance only truly comes to life when it becomes part of behavior and culture. That is why Odido places great emphasis on practice and simulation. "We simulate a lot," Ronteltap says with a smile. "Not just tabletop exercises, but also red teaming and awareness activities. Naming and sharing incidents helps enormously. If you show how an attack came in, and which team was the entry point, it becomes tangible."

What matters is that incidents do not lead to finger-pointing but to constructive learning. Ronteltap: "We have a culture where you don't get in trouble but actually score points when you report something. That encourages openness. Lessons identified really do become lessons learned with us."

IAM as a foundation

Identity & Access Management (IAM) also plays a role in Odido's compliance approach. "IAM is important for control and security," says Ronteltap. "It determines who has access to what, how scalable your security model is, and how quickly you can respond. For us, IAM is not just a technical solution but also a strategic theme. It has to grow with the organization and be flexible enough to support new business models and partnerships, while at the same time robust enough to meet regulatory requirements." Odido is therefore investing in a scalable IAM platform that covers the internal organization as well as partners and suppliers.

The gap between governance and operations

Ronteltap acknowledges that there is always a gap between strategy on paper and operational reality: "We work in networks within networks. Everything is interconnected, intertwined internationally. That makes 'zero breach' as a principle unrealistic for us.

What we focus on is resilience: how quickly can you respond, how do you become antifragile? It is not about preventing everything, but about bouncing back quickly and stronger." This approach requires continuous adaptation: "You always have to adjust. Compliance helps with that, because it provides a structure to organize that adaptability."

Supply chain responsibility and accountability

In a world of suppliers, subcontractors, and partners, compliance is increasingly becoming a supply chain issue. Ronteltap: "You can't just look at yourself. Our responsibility extends far into the chain. That's why we set agreements on security standards, access, and monitoring with our partners. In the end, It is about unity of direction and clear accountability."

To achieve this, Odido has built a governance structure in which second-line functions support and challenge the business units. Ronteltap: "You then don't burden internal stakeholders with endless compliance discussions, but you do ensure that decisions are made with security and compliance in mind."

Awareness and training

Compliance does not work without people and Odido therefore invests heavily in training and awareness. "We use incidents as learning moments, but also gamification," Ronteltap explains. "People score points when they report phishing or suggest improvements, and they receive feedback as quickly as possible. That works better than dull e-learning. You want people to understand that compliance is not a burden, but something that makes the organization stronger."

Compliance in 2028

How does Ronteltap see the future of compliance? "It has to evolve into something that no longer feels like compliance. The general assumption is that security will only become more complex, that we will be permanently fighting AI, and that the world will continue to change. That means we need a different mindset: a shift from 'prove you follow the rules' to 'prove you can survive and adapt'. Regulators should also move away from 'How do you prevent?' to 'How do you survive?' We can learn a lot from crisis management organizations. How have they set up their organization for crisis? How do they build on preventive measures during the response phase, and how can you improve and adapt as quickly as possible? Compliance must continue to reinvent itself in order to stay relevant."

05

Strengthening National *Cyber Resilience*

How NIS2 and the National Detection Network strengthen the cybersecurity of the Netherlands

Highlights

- The NIS2 Directive requires continuous, risk-driven monitoring of the infrastructure.
- Many organisations lack the maturity to effectively respond to or detect threats.
- The NDN provides real-time threat information, but requires proper monitoring and integration of the entire IT infrastructure.
- Governance and detection capabilities are crucial conditions for NIS2 compliance.
- Through cooperation between the NIS2 entities, the NDN increases the resilience of the Netherlands.

The cybersecurity threat landscape remains persistently high-risk. The NIS2 Directive sets a high bar for organisations. They must not only protect their digital systems, but also detect and respond to threats quickly, proactively and effectively. However, many companies still struggle to make effective use of available threat intelligence. A crucial but often overlooked link in this chain is the National Detection Network (NDN), a partnership coordinated by the National Cyber Security Centre (NCSC), where cyber threat intelligence (CTI) is shared in real time with affiliated organisations. Despite this, many organisations covered by the NIS2 Directive are still not making full use of the threat information provided.

In this article, we explain how connecting to the NDN not only supports compliance with the technical requirements of NIS2 but also helps meet the directive's reporting obligations.

The NIS2 Directive, which is being implemented in the Netherlands through the Cyber Security Act (Cyberbeveiligingswet, Cbw), introduces significantly stricter and more specific requirements than the original NIS Directive. These include stronger obligations around monitoring, detection and response. Organisations subject to NIS2 are expected not only to protect their digital infrastructure but also to demonstrate compliance with a broad set of technical and organisational requirements. This includes continuous monitoring, mature risk management, and effective incident detection and response.

From awareness to active resilience

Emphasis on the effectiveness of security measures in practice is what sets NIS2 apart from the first version of this Directive. It is no longer sufficient to simply record measures on paper: they must be proven effective. Where NIS1 focused primarily on establishing and implementing awareness and policy within the organisation, NIS2 requires validated effective processes for risk management, monitoring and incident response. Cybersecurity is not merely a policy on paper; it is a continuous practice of active resilience.

One of the components of NIS2 is the obligation to continuously monitor the IT infrastructure. This means that organisations should be able to detect anomalies, suspicious patterns, and potential threats immediately. Of course, there are plenty of products on the market for this purpose. Solutions such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Extended Detection and Response (XDR) collect infrastructure data, which can then be analysed by a Security Operations Centre (SOC) and correlated with current threat intelligence.

Technology alone is not enough. Without clearly defines processes, communication, trained people, and defined responsibilities during an incident, detection efforts tend to be reactive instead of proactive. Especially in complex attack chains, humans are often the most vulnerable link. This is only becoming more challenging due to the rise of AI[1], the commercialisation of cybercrime[2] and the ever-increasing role of state-owned actors such as Advanced Persistent Threats (APTs). These developments are making it increasingly challenging for employees to recognise threats, while attackers are exploiting human vulnerabilities more frequently to gain initial access to an environment. However, the arrival of NIS2 offers an opportunity to significantly enhance the detection and response capabilities required – an expectation also embedded in the legislation.

The NCSC collects these signals, enriches them with additional context and then shares them via composite feeds with other affiliated parties.

The NDN: strengthening resilience together

The National Detection Network (NDN)[3] is an initiative of the National Cyber Security Centre (NCSC), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) to exchange threat information with the affiliated parties. The objective is to warn the affiliated parties in a timely manner of active threats and to share 'sightings' (i.e. observations, detections) for this. When an organisation receives threat indicators via the NDN and detects suspicious behaviour within its own infrastructure on that basis, this sighting is automatically shared with the NCSC. This feedback is valuable: the NCSC collects these signals, enriches them with additional context and then shares them via composite feeds with other affiliated parties. This creates a dynamic and up-to-date threat picture, based on collective observations, which strengthens the resilience of all participants. Based on this feedback, the NCSC can paint a clear picture of cybersecurity and act on it both strategically and operationally, for example, by providing targeted advice on emerging threat trends or by conducting further research into specific actors.

Previously, this threat information was only available to affiliated parties of the central government and vital organisations. However, with the introduction of NIS2, organisations beyond the government in critical sectors will also fall within its scope. This information can be of great value if organisations can effectively integrate it into their own detection system. The arrival of NIS2 creates a powerful opportunity to not only expand detection capabilities, but to improve them, based on up-to-date and collective threat information. When an organisation has sufficient detection capabilities and joins the NDN, it can make a valuable contribution to the cyber resilience of the Netherlands. In doing so, the organisation also receives specifically collected threat information, tailored to the sector in which it operates. This includes closed, commercial, and open sources, internal research and data shared by affiliated organisations. For example, indicators of an actor actively targeting NetScaler equipment in the Netherlands that is susceptible to the Citrix Bleed 2 vulnerability.[4] Although such abuse is often difficult to detect, specific indicators can support the identification of potential steps in the attack chain.

[1] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai?hl=en

[2] https://cybersecuritynews.com/cybercrime-as-a-service/

[3] https://www.ncsc.nl/aansluiten-en-samenwerken/aansluiting-bij-het-ndn

[4] https://www.ncsc.nl/actueel/nieuws/2025/07/21/informatie-over-kwetsbaarheden-in-citrix-netscaler-adc-en-netscaler-gateway

From maturity to resilience

To comply with NIS2 requirements and make effective use of initiatives such as the NDN, organisations must achieve a certain level of security maturity. Detection and response processes should not be ad hoc or reactive, but should be standardised, repeatable and proven effective. Only then can observations or detections from monitoring and threat intelligence, such as those shared via the NDN, be properly contextualised and followed up. In addition, detections may also occur based on abnormal or malicious behaviour that would typically only be identified in a later phase of the attach chain.. For example, actions that generate many signals (such as alerts) within the environment, such as exfiltration.

Governance plays a vital role in this as well. If there is a lack of ownership, management or the board of directors is not involved, and cybersecurity is not properly embedded in broader risk management, it often remains a separate and undervalued activity. NIS2 specifically calls for cooperation in which technical measures are combined with organisational involvement. Fortunately, maturity is both measurable and essential, for example, through NIS2. NIS2 provides a solid foundation for developing a realistic roadmap and investment plan aimed at achieving sustainable and structural resilience. Experience within SecOps shows that no process is ever perfect; there are always lessons to be learned, often revealed during crisis simulations. Unfortunately, investments in such simulations are not always made or broadly supported within organizations.

Where to start in the NIS2 process

Organisations often lack sufficient security maturity to effectively detect, utilise and respond to threat intelligence. This is often due to insufficient detection or monitoring, gaps in infrastructure monitoring, or a lack of processes to respond quickly and effectively. It is important that organisations that fall under NIS2 set up a process to become NIS2-compliant. The first step is to gain insight into the current level of maturity: where does the organisation stand now? A good assessment can be made using risk analyses, crisis simulations, and audits, among other things. It is also wise to engage an experienced party to assess whether the IT infrastructure is adequately protected and whether the processes are in order. A cost-benefit analysis can support decision making: what does an incident at scale X cost, and can the impact be limited by early detection?

NIS2 as an opportunity, not just as a checklist

NIS2 is not simply a checklist to tick off, but also an opportunity to structurally improve cybersecurity within the organisation. By investing in mature detection capabilities, good governance, and collaboration through the NDN, organisations not only meet the requirements of NIS2, but also better protect themselves and actively contribute to the resilience of digital Netherlands. This is a major challenge as a defensive party. After all, attackers have the luxury of time, preparation, and focus, and basically only need to gain initial access once.

Defensive parties, on the other hand, need to be constantly alert, monitor their entire infrastructure, and respond quickly to signals that are often vague or complex. This is precisely why it is essential to not only meet the minimum requirements, but also to proactively invest in mature processes, collaboration, and up-to-date threat intelligence. Fortunately, initiatives by the NCSC, such as the NDN, show that organisations are not alone. Together we are strengthening the digital resilience of the Netherlands.

About the author:

Tim van Nederveen

Senior Cyber Security Consultant

Tim is a passionate Cybersecurity specialist with a strong background in both operational and technical security and a focus on Threat Hunting and Cyber Threat Intelligence. As a subject matter expert, he improves detection and response, as well as optimising the processing and exchange of threat information to make organisations more resilient.

www.linkedin.com/in/timvannederveen

tim.van.nederveen@capgemini.com

06

Shift Left, Scale Right: *Accelerating the Future* of DevSecOps Security

How can governance keep up with agile delivery without slowing innovation?

Highlights

- Security governance must keep pace with fast-moving DevSecOps teams.
- Security by Design enables proactive, contextual risk management.
- Security Assessment Questionnaire (SAQs) and automation empower squads without slowing delivery.
- Security advisors coach teams through design reviews, SAQ interpretation, and risk-based decisions enabling secure delivery without enforcing controls.
- Security Governance becomes a strategic enabler, not a bottleneck aligned with agile delivery and business impacts.

In today's digital-first economy, speed is survival. But as organizations race to innovate, security must evolve – not as a checkpoint, but as a catalyst. Traditional governance models are too slow, too siloed, and too reactive. The future lies in embedding Security by Design into DevSecOps workflows where governance scales with agility, and security becomes a shared responsibility.

Security governance must evolve to match the speed and scale of DevSecOps. Traditional security governance models, built on manual processes and siloed approaches, are no longer effective in today's agile and cloud native environments. Organizations that embed Security by Design and context-aware governance into their DevSecOps workflows can ensure compliance, reduce risk, and drive innovation at scale. This shift reframes governance not as a bottleneck, but as a strategic enabler. One that empowers squads through automation, self-assessment (SAQs), and risk-based design validations.

In today's digital-first world, agility is king, but security remains the cornerstone. The increasing adoption of DevSecOps reflects a critical mindset shift: that security must be integrated, not imposed. In 2025, the governance teams see this transformation deepen. Security by Design is not just an aspirational goal; it is an operational necessity.

Security leaders have witnessed the growing pains organizations face while balancing speed, innovation, and compliance. By embedding scalable governance processes into DevSecOps lifecycle, teams ensure security standards are met without compromising delivery timelines.

In a landscape where speed and scale define success, organizations often struggle to balance that speed, security and compliance. This article redefines how governance should operate: embedding security early and scaling it effectively across teams.

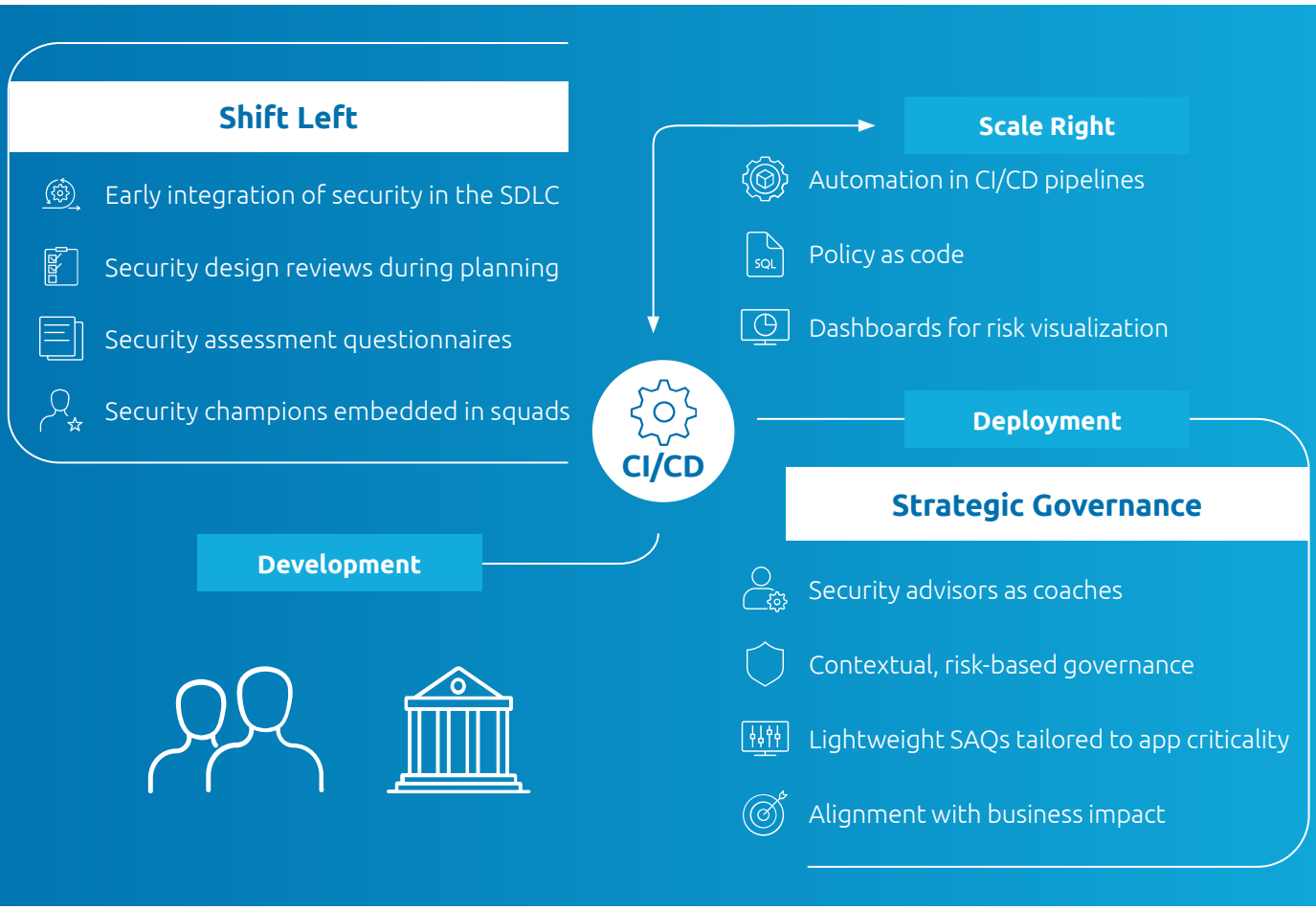
Why Security by Design matters more than ever

Security by Design has evolved beyond compliance – it is now a strategic enabler of digital trust and resilience. In today's fast-paced development environments, embedding security early in the Software Development Lifecycle (SDLC) is critical to reduce vulnerabilities and avoid costly rework.

- Design-time validation: Evaluate security controls during architecture planning, not post-deployment.
- Security maturity metrics: Track team progress and target improvements.
- Integrated compliance: Embed checks into DevOps workflows to reduce friction.
- Audit-ready evidence: Automate logs, snapshots, and security control validations for real-time assurance.

When executed effectively, Security by Design transforms security from a blocker into a business accelerator, building trust with users, regulators, and internal stakeholders alike.[1]

> "Security does not scale through enforcement – it scales through enablement. When teams understand the 'why' behind the controls, they are far more likely to own the 'how'."



[1] Black Duck's 2024 Global State of DevSecOps Report: Offers data from over 1,000 professionals on DevSecOps priorities, automation, and best practices. Read the report

CISA – Principles for Security by Design and Default: Highlights how secure-by-design practices reduce patching needs, configuration errors, and attack surfaces. View CISA's principles

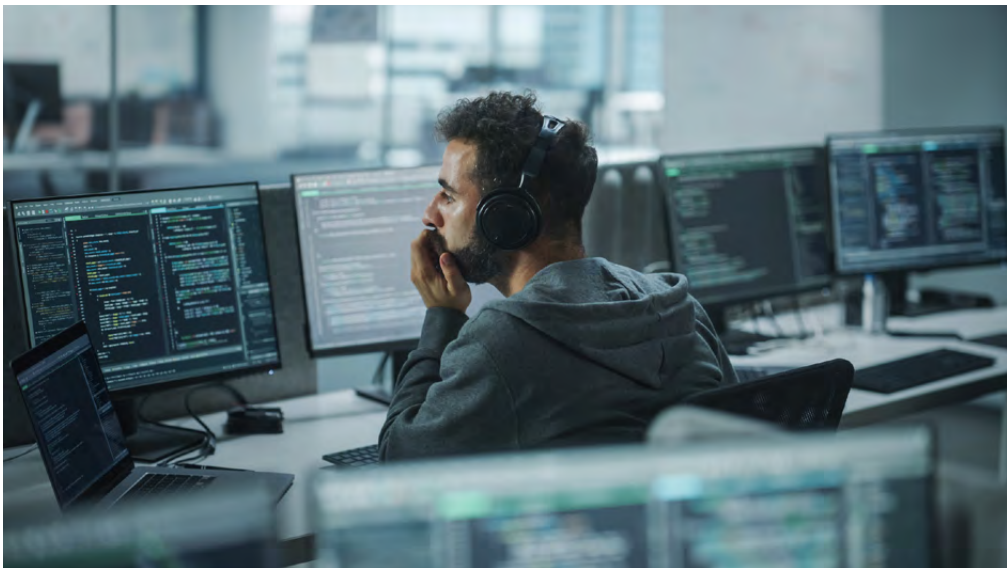
How DevSecOps Enables Proactive Governance

In many organizations, security traditionally entered the development process at a later stage often just before production release. This reactive model slowed down delivery, making meaningful risk mitigation difficult and costly.

DevSecOps challenges this traditional approach by shifting security left thus embedding it early in the development cycle. It incorporates:

- Security Design Reviews: Conducted during early architecture and feature planning stages, these reviews evaluate how systems manage identity, data classification, network architecture, logging, and monitoring. All are tailored to the applications criticality. For example, a customer-facing portal may require stricter access controls and logging than an internal utility tool.
- Security Assessment Questionnaires (SAQs): These lightweight yet powerful tools empower teams to self-assess their controls against a defined security standardized baseline. They are a set of minimum-security requirements tailored to the application's risk profile and business impact. Automated checks and scoring frameworks allow consistent governance without creating friction.

By integrating security reviews throughout the sprint lifecycle, not just during planning, teams retain ability to innovate while ensuring oversight and compliance. This approach fosters autonomy and accountability, making security a natural part of agile delivery rather than a late-stage hurdle.



Challenges in Scaling Security Governance

While the vision is clear, the theme is not without challenges:

- Diverse Tech Stacks: Modern applications span hybrid environments; microservices, APIs, containers, serverless. This makes creating one-size-fits-all security controls difficult.
- Stakeholder Alignment: Security, DevOps, architecture, and compliance teams often speak different languages. Creating shared understanding and ownership is critical.
- Security Fatigue: Teams overwhelmed with lengthy policies and unclear guidance often see security as a blocker. The solution? Contextual, risk-based governance that aligns with agile ways of working.

These challenges are solvable by establishing a centralized governance model that supports distributed execution. In this model Security advisors act as serve coaches, not gatekeepers guiding teams through security requirements into actionable development tasks. Design templates, SAQ tools, and feedback loops transform static documentation into practical, team friendly actionable insights.

Automation & Metrics: The Game-Changers

Modern DevSecOps practices rely on automated compliance validation tools that integrate with Continuous Integration and Continuous Delivery CI/CD pipelines (or deployment) to check for control adherence, design gaps, and collect evidence in real time.

Evidence collection refers to the automated gathering of artifacts such as:

- Audit logs showing access and activity
- Configuration snapshots of deployed environments
- Validation results of implemented controls (e.g., encryption, authentication)

This evidence supports audit readiness, continuous assurance, and real-time visibility into security posture.

Examples of automation:

Evidence collection refers to the automated gathering of artifacts such as:

- Auto-tagging sensitive data-based classifications rules like tagging customer Personally Identifiable Information (PII) or financial records for encryption and access control
- Detecting missing controls based on application criticality like flagging absence of multi-factor authentication on high-risk services
- Visualizing design risks through live dashboards that show control coverage gaps across microservices or environments
- Enforcing "policy as code" models that embed security rules directly into infrastructure and deployment scripts

Moreover, SAQs serve as a lightweight yet powerful mechanism for enabling secure-by-default thinking. Rather than waiting for security reviews at the end of the cycle, teams complete SAQs early – often during backlog grooming or sprint planning to surface potential risks upfront.

These questionnaires are risk based, derived from the security standards and tailored to application criticality.

For example:

1. A non-customer-facing utility may only require basic logging & access control.
2. A high-value customer portal may need encryption, multi-factor authentication, and detailed monitoring.

This differentiation improves efficiency, boosts developer buy-in and directs security efforts where they matter most.

By using SAQ scoring metrics, organizations can track security maturity across squads enabling targeted coaching, early intervention and consistent oversight where necessary. This shift helps move from subjective assessments to data-driven decisions.

Real-world benefits

Organizations adopting Security by Design report smoother releases, fewer audit issues, and stronger collaboration across disciplines. It helps development teams mature in their security understanding, while also giving risk and compliance functions a clearer view of security posture without additional paperwork.[2]

How to operationalize Security by Design

Build Security into the team's DNA: Security champions in each team act as the first line of defense, while processes reflect Security by Design.

- Use Lightweight, Contextual SAQs: Tailor SAQs to the application's criticality and integrate them into sprint rituals like planning and retrospectives.
- Automate What Matters: Leverage CI/CD hooks and automated triggers in the software delivery pipeline to run checks for missing security controls, data classification, and logging configurations. Security advisors act as coaches. They guide teams through security design reviews; help interpret SAQ results, and provide contextual advice based on application criticality. Rather than enforcing controls, they enable teams to make informed decisions and align security practices with delivery goals.
- Align Security to Business impact: Map every security recommendation to business value – protecting data, ensuring up time, or meeting compliance.

Looking ahead: What should organizations do?

- Treat security as a product, not a process: building feedback loops, user journeys, and Service Level Agreements (SLAs) around security tooling.
- Invest in security champions within teams; your best security ambassadors are your developers.
- Align governance to business impact, not only to technical stack.
- Automate, but validate; tooling is only as good as the trust and context behind it.
- Create a culture of secure design thinking: train, empower, and embed security as a shared responsibility.

> "The real shift left. It is not in the pipeline – it is in the mindset."

[2] Lombardi & Fanton, 2023, Springer Software Quality Journal https://link.springer.com/article/10.1007/s11219-023-09619-3

Security by Design is now a strategic imperative – not a luxury. Treating security as a product empowers teams to build resilience from the ground up, take ownership of security risks, and deliver with confidence. In a world where trust is earned through action, those who design securely by default will lead the future of digital innovation.
As cloud-native architectures, AI-driven development, and platform engineering reshape how software is built and deployed, security must evolve from static controls to dynamic, embedded capabilities. Organizations that operationalize secure design. Thinking through automation, contextual governance, and developer empowerment will not just keep pace with innovation; they will define it.

The future of DevSecOps belongs to those who scale security not through enforcement, but through enablement, intelligence, and shared accountability.

About the author:

Rahul Mishra

Managing Consultant – Cyber Security Unit

Rahul is a cybersecurity leader with over 14 years of experience across financial services and enterprise IT. He specializes in embedding scalable security governance into agile and DevSecOps environments, helping organizations align security with business goals and delivery speed.

www.linkedin.com/in/rahul-m-64990052

rahul.f.mishra@capgemini.com

07

The Strategic Rise of the CISO: *Securing a Seat at the Executive Table*

Leadership in a digital world

Highlights

- The role of the CISO is transforming from technical expert to strategic leader with direct influence on innovation and operations.
- Cybersecurity is no longer just about defence, but a strategic tool for trust, growth, and competitive advantage.
- A proactive approach and continuous threat analysis are crucial to addressing advanced cyberattacks.
- The modern CISO must strike a balance between robust security and the agility required for digital innovation.
- The modern CISO claims their place at the table by positioning cybersecurity as a strategic business enabler, whereby the CISO translates technical risks into tangible value for continuity, reputation, and growth.

Cybersecurity has become a critical pillar in modern organisations. Whereas it used to be seen primarily as a technical issue, it is now recognised as a strategic factor that determines business continuity, reputation, and competitive advantage.

Organisations are facing increasingly complex threats, ranging from ransomware attacks to social engineering via AI-driven techniques. Meanwhile, scientific research conducted by Computer Science, University College London, indicates that the human factor remains the weakest link.[1] The National Cyber Security Centre (NCSC) highlights in the Cybersecurity Picture Netherlands 2024 that human actions remain a key factor in the occurrence of digital incidents.[2]

In this dynamic environment, the role of the Chief Information Security Officer (CISO) is indispensable. They translate complex threats into strategic choices and ensures cybersecurity as an integral part of business operations. As a bridge between technology, governance and compliance, they not only monitor risks, but also encourage a culture of digital resilience. Without this coordinating role, there is a lack of alignment between policy, implementation and awareness, which leads to fragmented efforts and increased risk.

The evolution of the CISO

Traditionally, the CISO was seen primarily as a technical expert responsible for IT security such as firewalls and antivirus software.

Today, the CISO not only influences risk management and compliance, but also plays a key role in digital transformation. Under their direction, cybersecurity is integrated into development processes from the start. As a result, security is not an afterthought, but a core part of innovation. This proactive approach makes the CISO an indispensable link in ensuring sustainable digital resilience.[3]

[1] Transforming the "Weakest Link": A Human-Computer Interaction Approach for Usable and Effective Security, M.A. Sasse, S. Brostoff & D. Weirich, Department of Computer Science, University College London
[2] www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024
[3] www.intelligentciso.com/2025/03/27/the-evolving-role-of-the-ciso-from-security-expert-to-strategic-leader/

Cybersecurity as a competitive advantage

For a long time, cybersecurity was seen as a defence mechanism against digital threats, but in recent years it has also developed into a strategic asset that organisations can use to distinguish themselves in their market. Organisations that effectively integrate cybersecurity into their business strategy benefit from increased customer confidence, improved operational efficiency, and a stronger competitive advantage.[4]

In an era where data breaches and cyber incidents frequently make headlines, customer trust has become a critical asset. As awareness of cyber risks grows, consumers and stakeholders increasingly favour organisations that can demonstrably and effectively protect their data.[5]

Research shows that companies with a high level of cybersecurity awareness have higher customer satisfaction and loyalty. Organisations that communicate transparently about their security measures and act proactively in the event of threats strengthen their brand and improve their market position.[6]

From tech expert to strategic leader

In the current landscape, the CISO helps determine the course of the organisation by linking cyber security to business strategy.

The modern CISO operates at the intersection of technology, risk management and business strategy. Instead of acting reactively on security incidents, they proactively work with senior management and the management board to integrate cybersecurity into the core of business operations. This means that security is no longer an afterthought, but a fundamental part of innovation, compliance and digital transformation.

The following is an overview of the four key tasks of the modern CISO:[7]

1. **Risk management and cyber threat analysis**

   Proactive security against a constantly changing threat landscape.

   Cyber threats are constantly evolving, making it crucial for CISOs to not only act reactively, but also implement proactive strategies. One of the CISO's core responsibilities is to identify and manage cyber risks that can disrupt business operations. This requires a proactive approach using threat models and risk assessments to identify potential vulnerabilities.

   - **Threat monitoring:** continuously analyse internal and external threat landscapes using threat intelligence platforms.
   - **Risk analyses:** implementing frameworks such as the NIST cybersecurity framework and ISO 27001 to systematically identify risks.
   - **Preventive measures:** developing cybersecurity strategies to minimise vulnerabilities, such as network segmentation and strong access controls.

The business value of good risk management:
By proactively identifying and analysing risks and threats, the organisation protects its core processes against disruptions. This increases digital resilience, minimises financial damage and strengthens the confidence of customers and stakeholders.

[4] www.pwc.nl/nl/themas/blogs/cybersecurity-steeds-belangrijker-voor-waardecreatie.html
[5] www.customeyes.nl/kennis/de-rol-van-klanttevredenheid-in-de-snel-veranderende-wereld-van-cybersecurity/
[6] www.prnewswire.com/news-releases/nieuw-onderzoek-toont-aan-dat-bedrijven-met-een-sterke-cybersecurity-tot-7-beter-presteren-dan-de-benchmark-839220005.html
[7] www.cyberday.ai/nl/blog/10-belangrijkste-taken-voor-een-ciso-en-tips-om-succesvol-te-zijn

2. **Compliance and legal requirements**

Strict regulations require effective compliance

With the introduction and tightening of European legislation and regulations such as the General Data Protection Regulation (GDPR), NIS2 Directive and the Digital Operational Resilience Act (DORA), CISOs are expected to actively monitor compliance with complex legal frameworks that deeply impact the operational and strategic processes of the organisation. They also increasingly work closely with the legal and compliance departments within the organisation.

- **Regulations:** Ensure systems and processes comply with national and international laws.
- **Audits and reports:** Conduct regular internal and external audits to ensure compliance.
- **Collaboration:** Actively work with compliance officers and legal departments to properly implement legislation.

The business value of compliance: from obligation to strategic advantage

In a landscape of increasingly stringent regulations, compliance is not an administrative burden, but a strategic necessity. By complying with legislation and regulations such as GDPR, NIS2 and DORA, the organisation not only protects itself against fines and reputational damage, but also builds trust with customers, partners and regulators.

Close collaboration between the CISO, legal teams and compliance officers ensures an integrated approach that reduces risk, simplifies audits and positions the organisation as reliable and future-proof.

3. **Incident response and crisis management**

A quick and effective response to cyber incidents can minimise damage

Cyber incidents can have major consequences, ranging from data breaches to disruptions to business processes. The CISO must develop a robust incident response plan to respond quickly and effectively to threats.

- **Crisis response strategy:** Develop a response model that sets out the steps for limiting cyber incidents.
- **Advanced detection systems:** AI-driven threat detection to identify suspicious activity in real time.
- **Multidisciplinary teams:** collaborating with IT, legal affairs and communications departments to minimise the impact of an incident.

The business value of a robust incident response:

At a time when cyber incidents are not the question of if they will happen, but when, a quick and coordinated response is crucial. A well-designed incident response plan delivers immediate business value:

- **Limiting damage and downtime -** By responding quickly to incidents, operational disruptions are minimised, resulting in immediate cost savings and maintenance of productivity.
- **Reputational protection -** Transparent communication and controlled crisis response prevent reputational damage and strengthen the confidence of customers and stakeholders.
- **Faster recovery and continuity -** Multidisciplinary collaboration and advanced detection ensure efficient handling, allowing the organisation to resume operations quickly.
- **Learn and improve -** Incidents provide valuable insights that contribute to strengthening the security strategy and improving future response.

4. **Security architecture and technology leadership**

New technologies offer opportunities and challenges

With the rise of cloud computing, Internet of Things (IoT), and AI-driven cyber attacks, the CISO is forced to invest in innovative technologies that improve security.

- **Zero Trust architecture:** policy whereby every network request is verified to prevent unauthorised access.
- **Cloud security solutions:** Implement cloud-based security tools to safely support hybrid working models.
- **AI-based threat detection:** Using machine learning to predict cyber threats and neutralise them in a timely manner.

With the rise of advanced threats such as supply chain attacks, ransomware-as-a-service, and AI-driven attacks, the CISO faces the challenge of not only ensuring digital security, but also supporting operational efficiency and organisational agility. This requires a balance between robust security and facilitating innovation and growth.

The business value of smart security architecture and technology leadership.

By investing in innovative technologies such as Zero Trust, cloud security, and AI-driven detection, the organisation creates direct business impact:

- **Strengthening digital resilience -** Advanced architectures help to effectively guard against complex threats such as supply chain attacks and AI-driven attacks, helping the organisation to operate more securely.
- **Supporting innovation and growth -** A flexible and scalable security architecture enables new technologies and working models to be embraced safely, without slowing down business operations.
- **Efficiency and cost control -** Smart automation and integration of security tools streamline processes and reduce operational costs.
- **Confidence in digital transformation -** Technological leadership in cybersecurity strengthens the confidence of customers, partners and investors in the organisation's digital strategy.

Challenges faced

Today's cyber threats not only affect IT systems, but also put pressure on the entire organisation. Digital security has become a strategic business issue. The CISO must manage risks that have a direct impact on reputation, continuity, and growth potential, and that requires leadership at the intersection of technology and business.[8]

Three urgent challenges dominate the current cybersecurity landscape:

1. **Increasing cyber threats and AI-driven attacks**

   Cybercriminals are getting smarter and using new technologies

   AI has made ransomware and phishing attacks significantly more sophisticated. Ransomware 2.0 combines encryption with data theft and threat of publication, putting organisations under severe pressure. AI enables attackers to operate faster and in a more targeted manner, with automated scans and personalised phishing campaigns.

   This requires a proactive and adaptive strategy from the CISO to address these threats.

   - **AI-based phishing:** Hackers use AI to create personalised phishing attacks, making employees more likely to click on malicious links.
   - **Deepfake and social engineering:** It is becoming increasingly difficult to distinguish real communication from counterfeits, making it easier for criminals to access systems through social engineering techniques.[9]

2. **Cybersecurity talent deficiency**

   Demand for security experts exceeds supply

   The global shortage of qualified cybersecurity professionals continues to grow, and the Netherlands is no exception. CISOs are being forced to develop alternative strategies to strengthen their teams.

   - **Training and internal talent development:** Organisations invest in training programmes to train employees internally and develop cybersecurity skills.
   - **Automation of security processes:** By applying AI and machine learning, organisations can automate repetitive cybersecurity tasks and partially compensate the shortage of qualified staff.[10]

3. **Balance between security and business agility**

   Cybersecurity should not restrict innovation, but rather support it

   Strict cybersecurity measures are necessary, but can hinder innovation and flexibility. CISOs face the challenge of ensuring safety without slowing down operations. This asks for smart choices, integrating security from the start and strategically balancing risks against growth goals.

   - **Security by Design:** By making security part of production development and IT infrastructure from the outset, organisations can prevent cybersecurity from becoming a barrier later on.
   - **Risk-based decision-making:** CISOs must develop strategies that balance risk levels against operational objectives so that security supports rather than hinders business objectives.[11]

   By investing in advanced technologies, talent development, and risk-based decision-making, organisations can protect themselves against cyber threats while remaining competitive in a rapidly changing digital world.

[8] www.pvib.nl/kenniscentrum/documenten/de-spagaat-van-de-ciso-beheersbaarheid-versus-verantwoordelijkheid
[9] kpmg.com/nl/en/home/insights/2024/06/ai-cyber-security-challenge.html
[10] www.forbes.com/councils/forbestechcouncil/2023/06/12/the-impact-of-the-talent-shortage-on-cybersecurity-leaders/
[11] belgiumcloud.com/2025/02/11/onderzoek-van-gartner-slechts-14-van-cisos-weet-balans-te-vinden-tussen-effectieve-data-beveiliging-en-zakelijke-doelstellingen/

The modern CISO at C-level

The CISO is increasingly gaining a permanent seat at the table with senior management and the board of directors, particularly when it comes to determining cybersecurity budgets. This shift highlights the strategic importance of digital security within organisations. However, this also presents challenges: translating technical risks into understandable business impact, supporting investments in prevention and resilience, and competing with other strategic priorities for limited resources. To exert effective influence, the CISO must not only be strong in terms of content, but also possess financial and communication skills to create support and position cybersecurity as a valuable business enabler.[12]

While investments in digital security are crucial, they rarely yield direct profits. That makes justifying these expenses even more challenging: cybersecurity is about protection, not yield. For the CISO, this means continually demonstrating how cybersecurity contributes to business continuity, reputation protection, and preventing financial damage. By translating risks into tangible business impact and positioning security as a strategic prerequisite for innovation and growth, the CISO can effectively build support among senior management.

In this way, the modern CISO not only defends his seat at the table, but claims it as an essential part of the business strategy.[13]

The future of the CISO

The CISO is becoming increasingly important within the business strategy. In a landscape of AI, automation, and stricter regulations, cybersecurity is becoming a source of competitive advantage. The CISO plays a key role in keeping the organisation safe and agile, with direct influence on innovation, compliance and decision-making.[14]

8 strategic tools for the modern CISO of the future

The modern CISO demands a broad set of skills and insights to operate effectively in a dynamic and risky digital landscape. Below are eight strategic tools that help the modern CISO to embed cybersecurity sustainably within the organisation:

1. **Integrating cybersecurity into business strategy -** Position digital safety as a core part of innovation, risk management and growth.
2. **Translating risks into business impact -** Make cyber risks understandable for the board of directors by linking them to concrete operational and financial consequences.
3. **Apply security-by-design -** Ensure that security is incorporated into IT architecture, product development, and digital transformation from the start.
4. **Investing in talent development -** Build a future-proof team by investing in training, internal growth and attracting diverse talent.
5. **Effective communication with senior management -** Develop the ability to speak in business terms and create support for strategic investments.
6. **Collaborate with legal and compliance departments -** Ensure compliance with regulations such as GDPR, NIS2 and DORA, and avoid legal risks.
7. **Leveraging automation and AI -** Utilise smart technologies to automate repetitive tasks and respond to threats more quickly.
8. **Continuous evaluation and improvement of security strategy -** Adjust policies and measures based on new threats, technological developments, and business objectives.

[12] www.ibm.com/think/insights/ciso-vs-ceo-making-case-for-cybersecurity-investments
[13] www.forbes.com/councils/forbestechcouncil/2025/04/02/the-ciso-evolution-how-to-become-a-business-enabler/
[14] www.techzine.nl/experts/security/557108/hoe-nieuwe-technologieen-de-rol-van-de-ciso-transformeren/

Cybersecurity is a strategic priority and requires strong leadership

The role of the modern CISO is rapidly evolving from technical expert to strategic leader. At a time when digital threats are increasing exponentially, cybersecurity is no longer just an IT issue, but a core component of business strategy and continuity. Organisations that invest in this not only strengthen their digital resilience, but also create a distinctive competitive advantage.

At the same time, the CISO faces significant challenges: from attracting talent to navigating complex regulations and future risks and uncertainties. That is precisely why it is essential that the CISO is firmly embedded within senior management, with a direct influence on strategic decision-making. The eight handles for the modern CISO provide direction in this transition.

> “Cybersecurity is not a cost item, but a catalyst for trust, innovation, and sustainable digital growth. The modern CISO is the tour guide to that future.”

About the author:

Rafik Nasiri

Cybersecurity manager at the CISO Office & Cybersecurity and Privacy consultancy

After several years as a consultant in cybersecurity and privacy within international environments, Rafik now focuses on strengthening internal security processes and developing cybersecurity services that Capgemini provides to customers in various sectors.

www.linkedin.com/in/rafik-nasiri-9b9b64a9

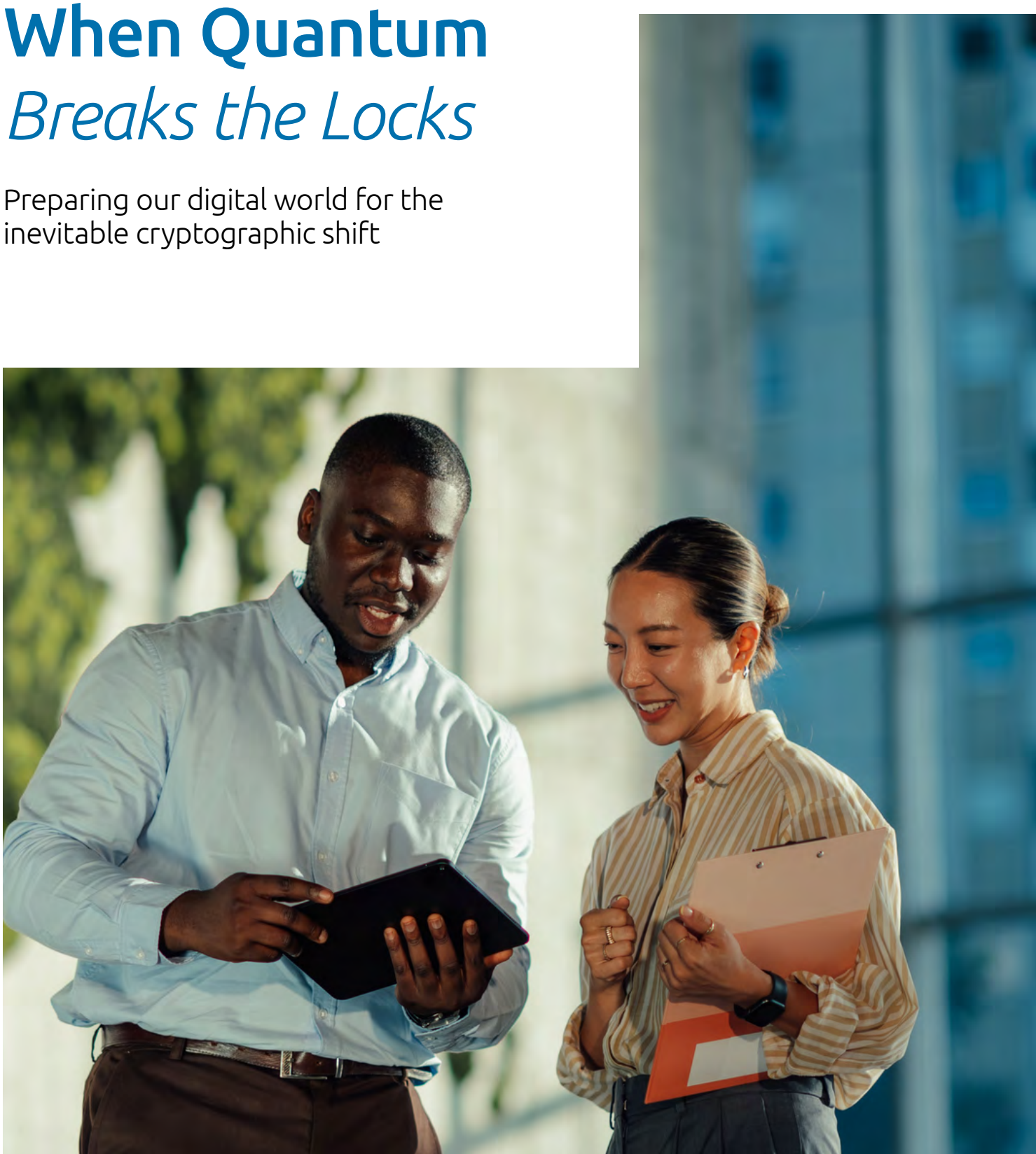
rafik.nasiri@capgemini.com

Future of Cyber

08

When Quantum *Breaks the Locks*

Preparing our digital world for the inevitable cryptographic shift



Highlights

- Quantum computers pose a serious threat to current encryption standards like RSA and ECC.
- Malicious actors can actively collect encrypted data now, anticipating future quantum capabilities. This makes quantum readiness a present-day concern, not just a future one.
- Transitioning to PQC is not plug-and-play. It requires years of planning, hardware/software updates, and overcoming compatibility challenges.
- Agencies like NIST, NSA, CISA, and the EU have published migration timelines. Most of these guidelines agree to have critical infrastructures migrated by 2030, and all migrations should be completed by 2035.
- Organizations must build in crypto agility—the ability to switch algorithms quickly—and foster quantum-safe ecosystems. This includes vendor alignment, board-level commitment, and governance to ensure resilience against emerging threats.

New and emerging technologies make the agenda of the CISO ever growing. Quantum computers are accelerating at an unprecedented pace; this development is bringing with it a growing threat to today's cryptographic foundations.

For decades, our digital world relied on encryption based on mathematical puzzles, like factoring huge numbers or solving complex curves. These puzzles were hard to solve for our current computers - often referred to as classical computers- which made them great for security. These classical computers compute mostly sequantially or paralelly, whereas quantum computers explore many possibilities simultaneously. Quantum computers can therefore solve complex mathematical problems within hours instead of many years. This includes breaking widely used encryption algorithms, which underpin secure communications, digital signatures, and data protection across industries.

Data intercepted today could be decrypted in the future, posing serious risks to privacy, regulatory compliance, and national security. As "harvest now, decrypt later" attacks become more prevalent, quantum security has evolved from a niche technical issue to a strategic priority for the C-suite. Even though quantum computers are not yet mature, rapid shifts in the technology landscape, regulatory mandates and the pursuit to maintain digital trust are all driving early adoption. Even though it is hard to predict when quantum computers will be mature enough to pose a threat to cybersecurity, current predictions by experts as when quantum computers will be cryptographically relevant (CRQC) range from 2029 to 2035.

To stay ahead, organizations must act now. This article explores the evolving Post Quantum Computing (PQC) landscape, key trends shaping the market, and why we should start now with preparing for a post quantum world.

Why is our current security not enough?

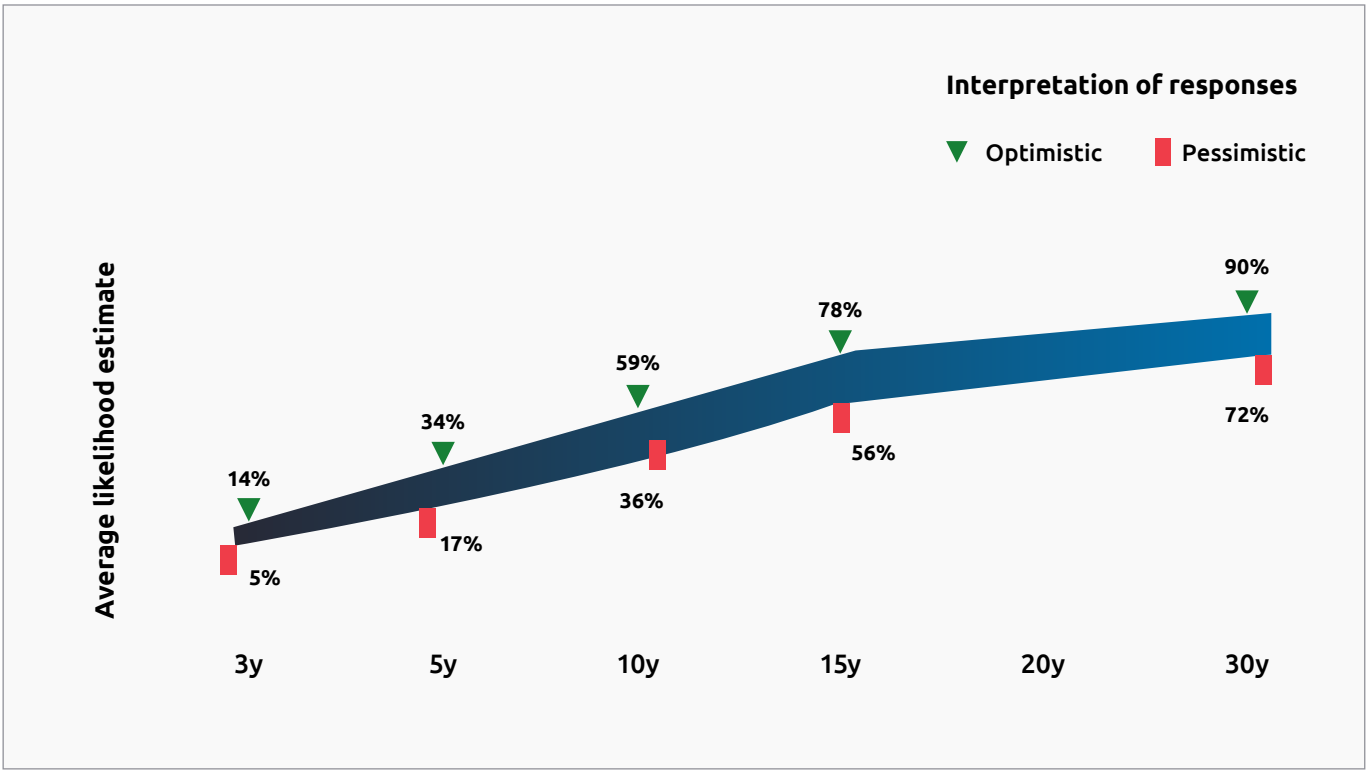
Most of the encryption we use today relies on mathematical puzzles that are very difficult for classical computers to solve. For example, RSA encryption is based on the challenge of factoring very large numbers. It is a task that would take a regular computer an impractical amount of time to complete. However, quantum computers can factor these large numbers in a fraction of the time. That means it could potentially break RSA encryption in minutes, rendering it useless.

This is tricky, since public key encryption is the silent engine that powers the digital economy. From online banking and e-commerce to government communications and enterprise systems, it ensures that sensitive data—credit card numbers, personal messages, business transactions—remains confidential and tamper-proof. It underpins digital signatures that authenticate software, emails, and documents, protecting against fraud and forgery. In essence, public key encryption is the foundation of digital trust. It is therefore safe to say that quantum computers will impact security in all types of industries. According to recent expert assessments, there is a 5 to 14% probability that quantum computers will be able to break RSA encryption within the next five years - a range that rises from 36 to 59% over the next decade (see Figure 1). These probabilities are too high to ignore, especially in critical industries.

Many organizations handle sensitive data that needs to remain confidential for years or even decades—think medical records, legal documents, financial transactions, or intellectual property. If this data is intercepted today and stored by malicious actors, it could be decrypted in the future once quantum computers become powerful enough. The impact this will have on organizations as trusted safeguards of data and information is high.

Whether it is health records, financial history or private messages, people want to know their personal data is safe, not just today, but years from now.

Figure 1: Becoming quantum-ready is not a one-time initiative, it's a multi-phase journey.



This is not a problem that we just recently encountered. The story goes back to 1994, when mathematician Peter Shor was interested in finding applications for quantum computers. At that time, quantum computers were even more theoretical than they are today but they had the promise of solving certain problems much faster than classical computers. One of the most famous problems in computer science then was factoring large numbers. Shor wondered: Could a quantum computer do it faster? He developed an algorithm that showed that a quantum computer could factor large numbers in polynomial time, which was a dramatic improvement over classical algorithms. This meant that RSA encryption could be broken by a sufficiently powerful quantum computer.

After the realization that quantum computers can break encryption, the U.S. National Institute of Standards and Technology (NIST) has worked on researching how quantum-safe algorithms should be designed to withstand an attack. In August 2024, NIST announced the first three standardized post-quantum cryptographic (PQC) algorithms: CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+. This marked the culmination of years of research since the early 2000s and an eight-year effort to develop quantum-resistant encryption. Currently, there are more algorithms in the process of being standardized (Falcon and HQC) and it is expected that more will be added overtime.

Why we should care today

While the arrival of mature quantum computers, often referred to as "Q-day", is likely still a decade away, the implications are already shaping today's cybersecurity priorities.

As previously explained, sensitive data that is secure today and remains valuable in the future can already be stolen. "Harvest now, decrypt later" is already an imminent threat and is actively reshaping the threat landscape. Malicious actors are collecting encrypted data today, anticipating the ability to decrypt it once quantum capabilities are mature. In a tense political climate, failing to prepare for this threat leaves governments and critical organizations exposed. It does not matter how secure our data is right now; it matters more how we secure our data for the future.

Q-day is often compared to Y2K; the year 2000 problem. Many older computer systems stored years as two digits (e.g., "99" for 1999). When the year rolled over to 2000, these systems would interpret "00" as 1900, not 2000. This was a massive global effort, and governments and companies spent hundreds of billions of dollars to audit, fix, and test systems. With Y2Q however, we do not know what year to prepare for. This attaches extra uncertainty that requires organizations not to wait and see what happens. We cannot afford to wait for 'that ChatGPT moment'. When we realize that quantum computers are near, we will already be too late.

The complexity of migration is often overlooked. Multinational organizations will require at least 3-5 years to migrate to quantum safe solutions, if it goes perfectly-to-plan. Realistically, we need to think more about 5-8 years. Transitioning to PQC is not plug-and-play. These new algorithms require updates to hardware or software which will introduce compatibility challenges. For example, longer key lengths will increase computing requirements.

Lastly, regulation is expected to follow. Most organizations see a "regulatory mandate" as a top factor in increasing urgency to adopt PQC.

Globally, we see a growing importance towards safeguarding against quantum computers. The U.S. National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA) and NIST have issued guidance on the impact of quantum on cyber security and are encouraging organization in critical infrastructure to start preparing early by developing readiness roadmaps. NIST is also encouraging the transition to quantum safe encryption by phasing out existing quantum vulnerable encryption from now till 2030. From 2030, algorithms with key lengths of 112 bits will be deprecated, meaning the algorithm and key length may be used, but the user must accept some security risk. By 2035, all quantum vulnerable algorithms should be transitioned, and algorithms such as RSA and Elliptic Curve Cryptography (ECC) will be disallowed by 2035. Which means that the algorithm or key length is no longer allowed for applying cryptographic protection.

The European Union has published a coordinated implementation roadmap to support a uniform approach towards PQC migration. Its roadmap advises all member states to begin transitioning to PQC by initiating a migration strategy, maintain a cryptographic inventory and start with a quantum vulnerability assessment by 2026. Between 2027 and 2030 high risk use cases should be migrated, with the full migration completed no later than 2035. The National Cyber Security Center (NCSC) in the Netherlands has issued guidelines specifically focusing on a hybrid key exchange.

The National Cyber Security Centre in the United Kingdom is recommending a similar phased approach with target dates for discovery and preparation in 2028, high priority migration in 2031 and full migration by 2035.

These developments signal a clear message: the global shift to quantum-safe cryptography is not just underway—it is accelerating.

“These developments signal a clear message: the global shift to quantum-safe cryptography is not just underway—it is accelerating.”

How to get ready for the shift towards quantum-safe encryption

What is certain is that PQC implementations will not be a plug-and-play solution, but one that needs careful consideration to meet both performance and new security requirements. There are multiple organizations that have started, and early adopters are in the defense and banking sector. Other sectors are still lagging in adopting quantum-safe solutions.

Many perceive quantum threats as a distant concern and prefer to wait for standardized protocols to mature. A lack of awareness and expertise; integration complexities with existing infrastructure; limited standardization; lack of availability of mature solutions; lack of clear timelines further contributes to the delay. Despite the urgency, progress towards preparedness remains slow.

Given the uncertain timelines of the maturity of quantum computers and the complexity of migration, becoming quantum-ready requires a structured and phased approach. Relying on future standardized protocols or waiting for regulatory mandates to enforce PQC migration is a high-risk strategy. It could lead to last-minute crisis management while critical data is already vulnerable to potential quantum threats.

Key questions to understand the current risks are:

1. Where am I using public key encryption?
2. What is the shelf-life of my data?
3. What areas are most at risk?

Having a continuous overview of the current state is important for building a comprehensive PQC migration strategy and is considered a no-regret move as having a comprehensive overview of your risk exposure is key towards digital trust and resilience against all types of cyber-attacks. Whereas the abovementioned steps focus mostly on understanding the current state of security, it is also important to look to build in a PQC component in new activities. With every new platform built, or every new vendor onboarded, building a quantum-safe component will be necessary. To ensure the possibility of continuously implementing new and updated quantum-safe algorithms is by becoming crypto-agile.

Achieving crypto agility - the ability to change to different cryptographic algorithms - is an important element in the transition towards becoming quantum-safe. Organizations that have high levels of crypto agility ensure that they can withstand sudden cyber-attacks, by being able to switch between different algorithms as a fallback scenario when a protocol is being attacked. Crypto agility ensures that systems can adapt without having to be shut down while waiting for specific hardware updates or having to re-architect the entire infrastructure.

It is important to make sure that the organization can support such a transition. Creating internal awareness is vital and treating quantum security as a board-level topic is essential to create the needed governance and budgets to build up internal capability and capacity. This means investing in training programs, making sure that internal teams are aware of company-wide initiatives and strengthening storage and computational bandwidth to handle updated hardware requirements. As with any transformation, change should not only be viewed on the technological dimensions but also on the process and people side.

Fortunately, organizations do not have to do this alone. Strengthening ecosystems and fostering partnerships help to make this transition. Ecosystems drive shared learning, faster adoption of standards, and innovation. Early adopters can help shape the best practices that others can follow, reducing the learning curve and implementation risks. Cryptographic systems rarely operate in isolation. They span across vendors, platforms, cloud services, and supply chains. A quantum-safe ecosystem ensures that every link in the chain—from hardware to software to third-party integrations—is aligned and secure.

Transitioning to quantum safe cryptography gives a perfect segue into upgrading current security policies and establishing a strong cyber foundation. The threat of "Q-day" can be used as a catalyst to modernize cryptography and become more resilient to emerging technology attacks beyond quantum computers alone, such as AI driven attacks. Organizations that have an active approach towards cyber security can enjoy a competitive advantage as customer trust will increase, especially in industries where this is highly valued such as in health care and finance. Being PQC compliant sends a clear message to investors, customers, and regulators: "We're not just reacting to threats, we're anticipating them." This kind of strategic foresight is increasingly valued in boardrooms and by shareholders.

> "We're not just reacting to threats, we're anticipating them."

Living in a quantum-safe world

As quantum computing advances from theoretical promise to practical reality, the urgency to transition to post-quantum cryptography (PQC) becomes undeniable. The transition to post-quantum cryptography (PQC) marks a pivotal moment in cybersecurity, demanding not only technological upgrades but a fundamental shift in how organizations approach digital trust. The threat of "harvest now, decrypt later" underscores the urgency to act today, not tomorrow. Migration to PQC is a complex, multi-year journey that requires crypto agility, collaboration, and board-level commitment. It is not just about replacing algorithms but about building resilient ecosystems, fostering vendor alignment, and embedding quantum-safe principles into every new system and partnership. Waiting for standardized protocols or mandates is a high-risk strategy that could leave critical data exposed. Instead, organizations should treat quantum readiness as a strategic enabler. One that strengthens cybersecurity posture, enhances customer trust, and positions them ahead of emerging threats. The shift to PQC is not a one-time fix, a continuous evolution. And those who start early will be the ones best prepared to thrive in a post-quantum world.

Here is how to get started:

Assess quantum risk

Maintain a live cryptographic inventory. Prioritize cryptographic assets based on sensitivity and exposure.

Drive enterprise awareness

Treat quantum safety as a board-level concern – with governance, sponsorship, and budget to match.

Plan the transition

Start with pilots. Use phased rollouts to integrate learnings into enterprise-wide programs.

Adopt crypto agility by design

Ensure infrastructure supports rapid algorithm replacement as standards mature.

Future proof legacy and edge systems

Embed update mechanisms that allow retrofitting of quantum-safe protocols.

Invest in talent and capacity

Upskill internal teams. Foster specialized expertise to manage PQC integration effectively and strengthen computational, bandwidth, and storage capacity.

Strengthen your ecosystem

Foster partnerships with partners and suppliers. Embed quantum-safe clauses in contracts.

About the author:

Nadine van Son

Quantum & Quantum Safe Lead

Nadine is an experienced manager in technology and innovation strategy, specialized in the impact of quantum technologies on our society. In her role she works with organizations globally to prepare themselves for quantum technology. She is passionate about new technologies and how these can contribute to an inclusive and sustainable future.

www.linkedin.com/in/nadine-van-son

nadine.van.son@capgemini.com

Other Publications

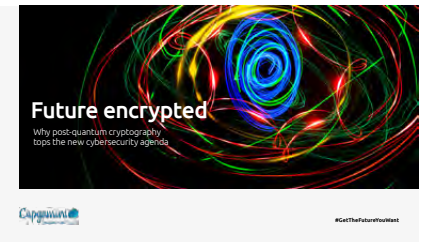
In addition to our 'Trends in Cybersecurity' report, we regularly publish other reports, studies, and white papers that may be of interest to you. Below is a brief selection. For the full overview, please visit: www.capgemini.com

TechnoVision 2025

Your gateway to cutting-edge innovation

In today's fast-evolving technological landscape, TechnoVision acts as a lighthouse for your innovation strategy, helping business and technology leaders stay ahead of the curve. This global program from Capgemini provides a comprehensive view of the world of technology, guiding decision-makers through the myriad of emerging trends to focus on those that will make their organizations more effective.

www.capgemini.com/insights/research-library/technovision-2025



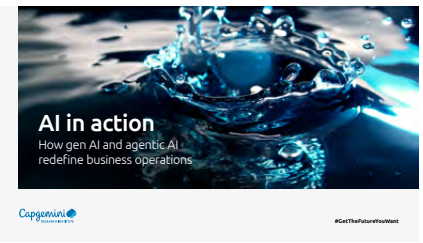
Future encrypted

Why post-quantum cryptography tops the new cybersecurity agenda

Quantum threats are no longer theoretical – they've become a strategic priority. This Capgemini report highlights how organizations are preparing for a quantum-safe future with post-quantum cryptography and crypto-agile architectures to protect critical assets and maintain trust.

Based on a global survey and expert interviews, it outlines challenges, progress, and best practices for staying ahead of emerging quantum risks.

www.capgemini.com/insights/research-library/post-quantum-crypto



AI in action

How Gen AI and agentic AI redefine business operations

AI is no longer just a pilot project. It is delivering real ROI and transforming core business functions. This Capgemini report explores how generative and agentic AI are driving efficiency, cost savings, and faster decision-making across supply chain, finance, customer service, and more.

With adoption accelerating rapidly, the report offers key insights and practical steps for scaling AI to unlock its full business potential.

www.capgemini.com/insights/research-library/ai-and-gen-ai-in-business-operations

COLOPHON

This edition of *Trends in Cybersecurity* was produced with contributions from:

Natasja Pieterman

Folkert Visser

Maarten Veldhuizen

Dennis Paardekooper

Alex de Vries

Joris Commissaris

Editorial, Design & Production

Marketing & Communications, Capgemini Netherlands B.V.

Devana Thonhauser

Thomas de Klerk

Nicole Hartung

Project Management

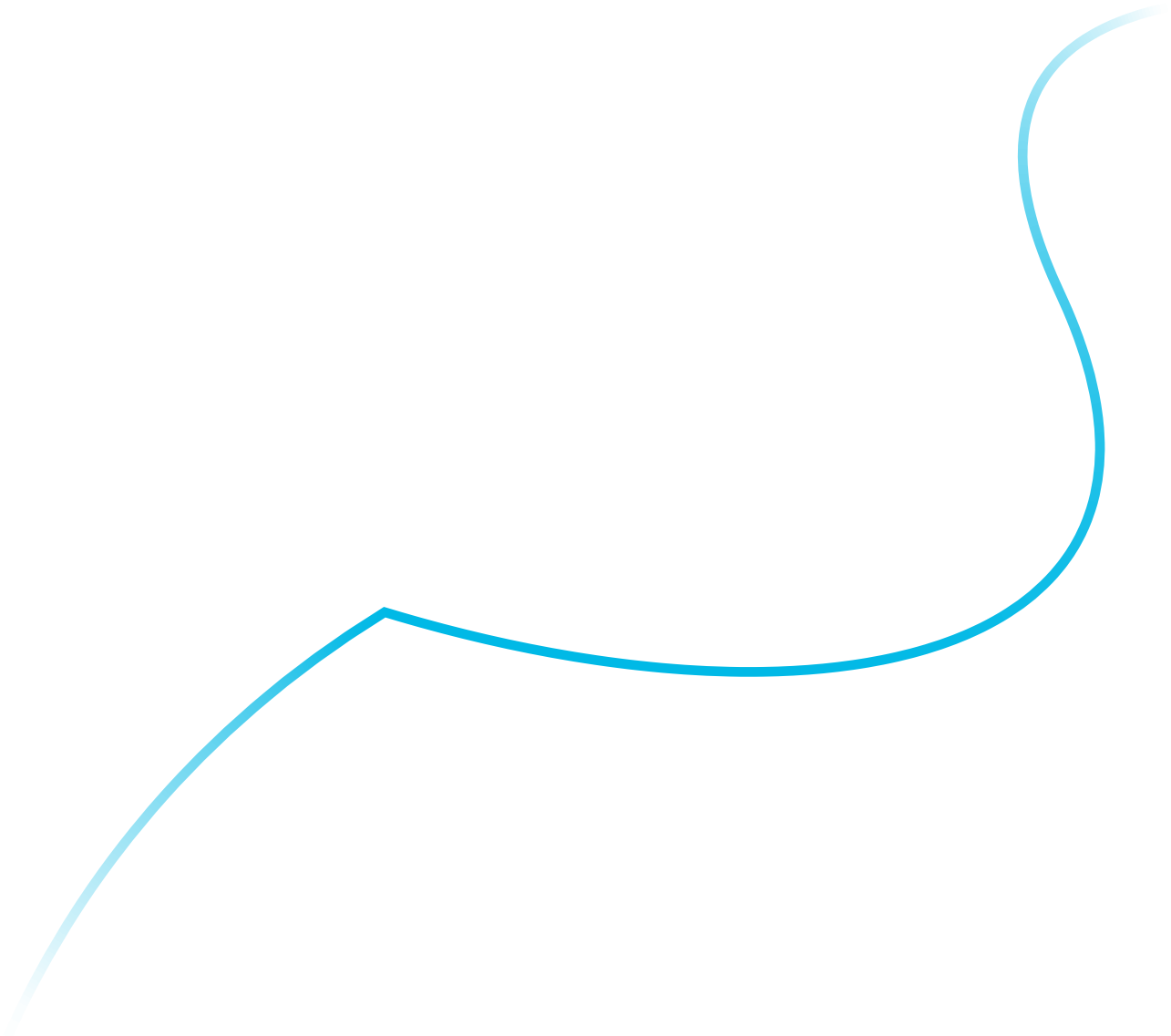
Devana Thonhauser

Capgemini Netherlands B.V.

P.O. Box 2575 – 3500 GN Utrecht

+31 30 689 00 00

www.capgemini.nl



About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Get the future you want | www.capgemini.com

Capgemini