Advancing security and governance across emerging technologies

The second session of the Highly Resilient Organisations (HRO) Programme, featuring insights from Martin de Vries (CISO at VDL Groep) and Aernout Reijmer (Former CISO at ASML), discussed the strategic step that CISO's should make: moving beyond legacy compliance focus toward dynamic governance that can withstand the volatility of the emerging tech landscape.

While the first session focused on resilience as a measurable business capability, this session utilised interactive Mentimeter discussions to discuss upcoming threats and opportunities of emerging technologies (e.g. generative AI, low-code development, edge computing and post-quantum cryptography (PQC). These innovations can drive competitive advantage, while simultaneously introducing new risks, regulatory uncertainty and governance complexity.

> "We should stop being the department of 'no'. Applying to too many control kills an initiative. The goal is to move from merely 'secure innovation' to 'security innovation', using the speed of new technology for our own advantage."
>
> 
>
> **Martin de Vries**
> CISO at VDL Groep

Insights from industry leaders to navigating the technology roadmap

Martin and Aernout shared practical experiences regarding the balance between innovation enablement and long-term resilience. Martin focused on the practical realities of the Emerging Technologies Roadmap 2025-2026, ranging from Agentic AI systems to IoT security. He distinguished between simply securing new technology and actively using innovation for enhancing security management. One of the key takeaways was the warning that 'applying too many controls will kill the initiative'. Security must move at the speed of business requests rather than just being a technology push. Drawing on lessons from the TU/Eindhoven cyber-attack, Martin emphasized that resilience relies heavily on non-technical factors. He also warned not to forget physical security, citing the recent robbery at the Louvre as a reminder that vulnerability often sits in an unexpected corner. Monitoring must span both digital and physical domains.

Figure 1: Word cloud based on the emerging technologies seen by the participants.

The bigger picture of emerging threats & technologies
Aernout Reijmer placed emerging tech within the "bigger context" of a global cyber arms race, where threats are growing exponentially. Referencing the insights from the Peter Wennink report, Aernout stressed that 'Security & Resilience' is a foundational pillar for the Netherlands' future earning capacity. He warned against naivety regarding strategic autonomy in the current geopolitical technology situation.

A major challenge discussed was how to anticipate "Unknown Unknowns", threats for which use cases cannot yet be created, especially given how fast the adversary's use of AI is growing. He argued that working in silos makes defenders too slow. By applying Metcalfe's Law, organisations break those silos and can boost the value of their network exponentially by connecting nodes, sharing knowledge to "become more resilient in the technology war".

"For critical continuity, some leading organisations are currenlty adopting the 'ultimate measure' of resilience: implementing "three ways for backup" and multi-cloud strategies, sometimes even running multiple applications for the same functionality to ensure availability under any circumstance."

Arnout Reijmer
Former CISO at ASML

How significant is the potential impact AI related threats on your operational continuity?

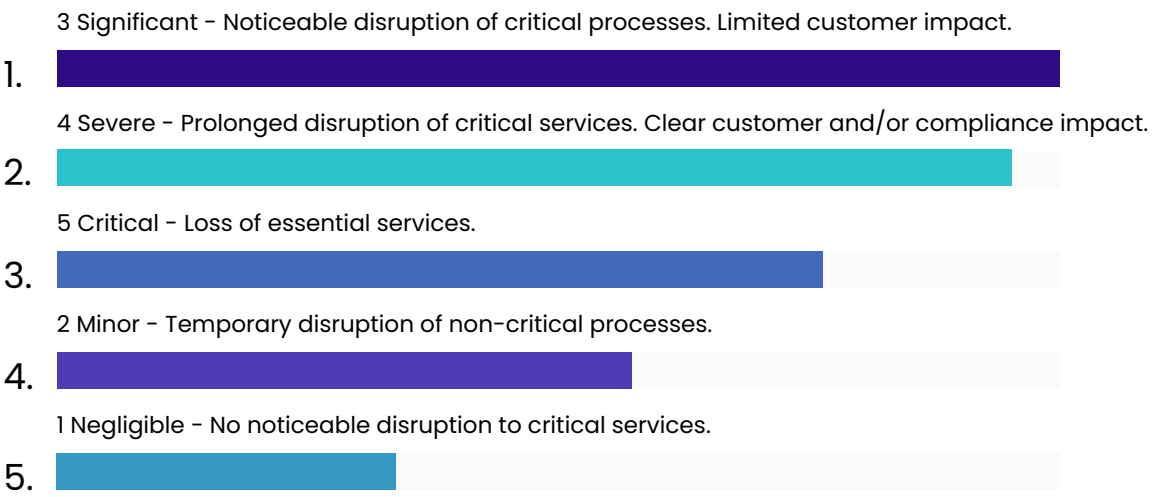

Figure 2: Impact of AI related threats by the participants.

Strong governance is like a piece of art, like the inside ceiling of the Rotterdam Market Hall. An "aesthetic chaos" with an "invisible structure" where resilience is designed in, not observed until it is missing.

Suzanne Janse
Lecturer and research supervisor at
Erasmus Economics & Business Executive Education

The evolving role of the CISO
A central theme during the session was the changing approach of forward thinking CISO's, supported by discussions on guiding principles such as:

- Behaviour through quality, not fear: A fundamental shift was proposed regarding culture and behaviour. Instead of driving compliance through fear (FUD), leaders should improve behaviour based on quality. Security must be framed as a mark of craftsmanship and professional excellence. This approach aligns with the insight that "most people are good" and want to do their work well, rather than needing to be policed.
- Transparency over collaboration: While collaboration is often touted as the goal, the session introduced a sharper principle: Transparency over collaboration. Collaboration without transparency is ineffective. True resilience requires radical transparency about risks and incidents as the absolute prerequisite; only then can effective collaboration (internal and external) follow.
- Strategy & risk appetite: It is vital to explicitly define the organisation's risk appetite and strategic choice: will you be a "laggard" or an "innovator"? This choice, alongside guiding principles like a Cloud Manifesto, forms the foundation of the security strategy.
- The ultimate redundancy measures: For critical continuity, some leading organisations are adopting the "ultimate measure" of resilience: implementing "three ways for backup" and multi-cloud strategies, sometimes even running multiple applications for the same functionality to ensure availability under any circumstance
- Governance & reporting: The discussion highlighted the Security Target Operating Model (TOM). The consensus moves towards a hybrid model, increasingly decentralized execution to support innovation speed, but strictly under central governance 'guardrails' conditions. The success of this model often depends on where and how the CISO reports within the corporate structure, preferably direct reporting line to the board.
- From enforcer to enabler: Leaders are moving from enforcing static controls to enabling agile, risk-aligned innovation. "Shift Left" remains a critical principle in this transition, ensuring security is embedded early in the lifecycle.

What cyber threats and trends do you foresee?

Figure 3: Word cloud of cyber threats seen by the participants.

Preparing for a Safe Quantum Horizon
Regarding the shift toward future-proof security, Post-Quantum Cryptography (PQC) emerged as a primary concern; participants overwhelmingly identified it as a critical "harvest now, decrypt later" threat. While the majority of the participants has already begun internal investigations into its impact on long-term data integrity, the discussion highlighted a concerning gap: public sector awareness and broader institutional attendance remain limited, leaving a potential blind spot in collective national resilience.

"You cannot build true resilience on fear; fear only leads to compliance. We need to build on quality and the belief that most people are good. Security should be treated as a mark of craftsmanship, not just a necessary evil."

Aernout Reijmer
Former CISO at ASML