HIGHLY RESILIENT ORGANIZATIONS - WRITE UP

Digital Knowledge Institute
CISO community NEDERLAND

Resilience as business capability

The first session of the Highly Resilient Organisations Programme examined how leading companies are redefining resilience as a measurable business capability. Security and risk leaders discussed the evolution from technical maturity models towards governance, metrics and culture that link cyber resilience directly to enterprise value.

Resilience in today’s enterprise

In the current threat environment resilience has become a central component of business strategy. Continuous disruption, digital interdependence and rapid technological change are reshaping how organisations manage operational stability. From AI risk to increasingly complex supply chain and systemic dependencies, digital risks are expanding in new ways.

These enterprise risk developments were the focal point of the first session of the HRO (Highly Resilient Organisations Programme), where executives, regulators and researchers discussed how resilience can be defined, measured and embedded in governance. The discussion reflected a clear shift: resilience is moving from a compliance exercise to a strategic business capability that supports continuity, trust and long-term performance.

Beyond cybersecurity metrics

Participants noted a transition from traditional cyber maturity frameworks to data-driven resilience indicators that connect technical performance with business outcomes. Some organisations are already applying quantitative analysis to assess the operational and financial impact of incidents, giving boards greater visibility into resilience performance.

This evolution is further encouraged by regulatory expectations. Frameworks such as NIS2 and DORA require firms to quantify the operational consequences of cyber incidents, not just the technical causes. The discussion underscored that resilience now extends beyond IT, encompassing governance, finance and reputation.

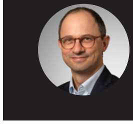
The importance of resilient employees

Technology alone does not make an organisation resilient. All speakers highlighted that culture and leadership are equally important. Clarity of roles, open communication, decision-making autonomy and trust help teams respond effectively to disruption. Training and simulation exercises (as most larger organisations pursue yearly) also reinforce collective preparedness and situational awareness.

Leadership behaviour emerged as a determining factor. Consistent and transparent communication during high-pressure events sets the tone for the organisation and enables faster recovery. Speaker Jan Joost emphasised the importance of building resilience through people: “Ask employees about their training needs, ambitions and wellbeing and how they want to balance work with family life. Create quiet time when there is no crisis, so you can rely on them when something inevitably occurs. Resilience is both a technical and a behavioural capability, it starts with spending time with your people.”

Collaboration across the ecosystem

No organisation can build resilience in isolation. Shared infrastructures and supply chain interdependencies mean that disruptions often have systemic effects. The session emphasised the importance of collaboration with peers and public bodies such as the NCSC and DIVD. Information sharing, joint incident simulations and coordinated recovery planning were seen as practical ways to reduce collective exposure. Emerging technologies such as multi-party computation may further enhance secure data collaboration. Early work with partners shows potential for privacy-preserving analysis that could strengthen system-wide resilience. We will deep dive into this promising concept with new research on HRO’s.

> Resilience is becoming a core business metric. the capability to continue performance and trust when disruption hits the fan.
>
> 
>
> **Andrea Bergamini**
> Vice President & Chief Information Officer at Orbia

Linking resilience to business value

As resilience initiatives mature, boards are increasingly focused on tangible contribution to business value. The ability to express resilience through measurable indicators related to financial stability, operational continuity and stakeholder confidence, is becoming a key element of governance reporting.

The conversation also touched on cyber insurance. While it remains part of the broader risk management approach, participants noted that coverage limitations and rising costs are driving a greater emphasis on intrinsic resilience as a more effective long-term safeguard. A good way to start is to quantify P2, P3 incidents that occurred.

Looking ahead in the HRO programme

Future sessions in the HRO will explore governance models that link cyber risk management to enterprise value creation. The research will focus on how resilience metrics can be integrated into regular performance reporting and used to support strategic decision-making at executive level. Participants will gain early access to benchmark data, peer comparisons and an executive-ready report on emerging resilience practices. The aim is to help define what high organisational resilience will look like in 2025 and to support leaders in aligning security, risk and business outcomes.

The second HRO session will address the challenges and opportunities presented by emerging technologies, including generative AI (agents), edge and quantum computing. These technologies offer competitive advantages but also introduce new risks, regulatory uncertainty and governance complexity. CISO’s are increasingly moving from enforcing static controls to enabling agile, risk-aligned innovation. The session will examine how organisations gain visibility over technology adoption, manage emerging technology risks across centralised and distributed teams and communicate potential business impacts to executives and boards, balancing innovation enablement with long-term resilience.

> Resilient organisations start with resilient people. Leaders who invest in wellbeing and trust, build teams that stay steady under pressure.

Jan Joost Bierhoff

COO Nationaal Cyber Security Centrum (NCSC-NL)