Cyber Threat Exposure & Response Readiness

Cybersecurity risks continue to grow in scale and sophistication, affecting the stability of critical business services across all sectors. Organisations increasingly face the challenge of ensuring digital continuity while modernising technology landscapes, managing third party dependencies and keeping pace with evolving attacker behaviour.
As part of the High Reliability Organisations (HRO) Program on Technology & Chain Resilience, hosted in collaboration with knowledge partners Okta and Rubrik, this session 2 focused on Cyber Threat Exposure & Response Readiness. Together, with a group of approx. 20 digital leads and knowledge partners we explored how organisations can strengthen their cyber resilience posture, reinforce sovereignty across cloud and data ecosystems, and build the controls needed to ensure continuity across the technology supply chain.

Key themes covered

1. **Anticipating Cyber Threat Exposure & Evolving Attacker Behaviour**
   With attacks becoming more targeted and disruptive, organisations must move beyond compliance-level defence and anticipate likely attack pathways. Early detection, expanded visibility and adversary modelling are becoming fundamental capabilities.
2. **Strengthening Response Readiness During Major Cyber Incidents**
   The ability to respond quickly and decisively remains one of the strongest predictors of resilience. Participants emphasised the need for cross-domain playbooks, clear decision rights and structures that support rapid escalation while limiting operational disruption.
3. **Minimising Business Disruption & Accelerating Recovery**
   As ransomware and supply chain attacks accelerate, the focus is shifting toward recovery assurance: immutable backups, rehearsed failover strategies and architectures designed for rapid restoration of critical services.
4. **Managing Third Party Dependencies & External Service Risks**
   Modern ecosystems create both value and vulnerability. Organisations increasingly recognise the importance of continuous assessment of external partners (not just at onboarding) and the integration of third party risk into operational resilience planning.

Identity is the New Attack Surface.

Pierre François Guglielmi
Field CTO EMEA at Rubrik

Session Perspectives
Suzanne Janse (program manager HRO from the Digital Knowledge Institute) and Kenny van Midden (ICT-Media) guided the session as moderators, facilitating an open dialogue across participating CISO's and knowledge partners. Jeroen van Kesteren from The Dutch National Bank (DNB) and Pierre François Guglielmi from Rubrik joined as guest speakers, providing strategic and technical perspectives on strengthening digital continuity. Their contributions highlighted the continuous pressure on CISOs to anticipate attacker behaviour while ensuring that business services remain resilient and recoverable.

Identity as the New Attack Surface
Pierre François addressed the topic **that Identity has become the primary target** in today's cyber threat landscape. While cybersecurity spending continues to rise, attackers increasingly bypass traditional malware and instead rely on stolen credentials, social engineering and identity system manipulation. Over 90% of organisations faced an identity related incident last year, and most modern attacks are now malware free.

Pierre François highlighted a case study on the Scattered Spider threat group (adaptive, financially driven attackers). He showed how quickly attackers adapt, using vishing and social engineering. They easily gain initial access, escalate privileges, and establish deep persistence inside identity providers such as AD, Entra ID or Okta, often remaining undetected even after malware is removed. This persistence creates significant recovery challenges: organisations are forced into weeks long AD rebuilds or destructive rollbacks that erase legitimate changes. It demonstrates how modern attackers bypass traditional malware based defences entirely.

This is a critical shift: **detection is no longer the problem, removal is.** Effective resilience now requires the ability to protect identity data, track every change, validate clean restore points, rebuild IdPs in a trusted environment and safely roll forward sanctioned updates without re introducing

attacker artefacts. This identity first approach is key to ensuring digital continuity and protecting the broader technology chain.

Adding field experience to the discussion several participants shared practical insights from incident response, cloud transformations and the operational realities of managing complex technology chains. Their contributions underscored **the need for an integrated business approach,** linking resilience, architecture, security operations and third party governance.

Cyber Resilience is more and more about Predictive Intelligence and Ecosystem Readiness
Jeroen van Kesteren highlighted in his presentation the growing urgency of moving from reactive cybersecurity to predictive intelligence. With major, recent incidents such as Odido and Ministry of Finance breaches, the central question is whether these are isolated events or signals of a larger trend. Geopolitical tensions (across the US, Russia and Iran) further increase uncertainty in energy deliveries and supply chains.

Jeroen emphasized a three layered intelligence model: strategic (threat evolution and systemic risk), tactical (actor behaviour and capability shifts) and operational (actionable indicators). This broader intelligence lens strengthens executive decision making and anticipatory defence.
Ecosystem and chain resilience emerged as a critical theme. Organisations must understand their critical third parties, manage concentration and dependency risks and embrace shared responsibility across the ecosystem. **Testing readiness is essential:** Threat Led Penetration Testing (TIBER) across the chain, advanced red teaming (ART) and realistic crisis scenarios provide measurable insights for joined learning.

Leadership under pressure plays an important role. Boards and Crisis Management Teams must be prepared to make strategic decisions under pressure with clear accountability and learn from each other. For DNB, cyber threats represent a strategic and systemic risk, resilience must be ecosystem wide, continuous exercising is mandatory, and strong executive leadership is indispensable. Conclusion

Cyber Resilience is about predictive intelligence and ecosystem readiness.

Jeroen van Kesteren
CISO at De Nederlandsche Bank (DNB)

Conclusion
The session made clear that organisations are entering a new phase of digital resilience. One defined by identity driven attacks, supply chain interdependencies and geopolitical uncertainty. Traditional security measures are no longer sufficient: resilience now depends on predictive intelligence, integrated response capabilities and the ability to recover cleanly from deep seated identity compromise.

Across all contributions (technical, strategic and operational) one message consistently resonates: **cyber resilience is no longer an internal capability but an ecosystem responsibility.** Organisations must strengthen collaboration with critical third parties, continuously test their readiness, and ensure leadership is prepared to act decisively under pressure.

As attackers evolve faster than ever, high reliability organisations will distinguish themselves by anticipating threats, safeguarding identity at the core and building recovery processes that guarantee continuity even in the most challenging scenarios.

Detection is no longer the problem, it's removal of the attacker who's already inside.

Suzanne Janse
DKI program manager Highly-Resilient Organisations