Telenet Business Leadership Circle | Discussion Summary

RESILIENCE BY DESIGN

A STRATEGIC BLUEPRINT

business

CIONET

On 7 May, Telenet Business brought together prominent IT leaders for the first Leadership Circle of 2026. Organised and moderated by CIONET and Hendrik Deckers, the discussion focused on a major shift within the sector: the move from reactive cybersecurity to "resilience by design". The central question was: how can organisations build a digital foundation capable of withstanding geopolitical fragmentation, the rise of agentic AI and the increasing demands for business continuity?

The era in which network and infrastructure decisions were purely technical matters is long gone. "The most crucial security decisions today happen at the strategic drawing board rather than in the Security Operations Center," said Geert Degezelle, Executive Vice President at Telenet Business. And it's about fundamental decisions: who manages the network? Where does our sovereignty lie? And in what ways do we want to be (in)dependent?

The participants agreed on the importance of resilience: it cannot be added as an afterthought; it must be embedded in the DNA of the IT architecture. As Geert summarised: "In a landscape dominated by geopolitical shifts, sophisticated cyber threats and autonomous AI agents, the key to resilience comes down to two things: architectural simplicity and strong leadership."

BAHADIR SAMLI
CIO ING Belgium

ING Belgium: protecting value

As CIO of ING Belgium, Bahadir Samli oversees critical infrastructure every day, where transactions must take place flawlessly, anytime and anywhere. Behind the scenes, however, the bank is constantly in motion to modernise and innovate, with the last 5 years a big focus on moving from a local bank to globally connected, from fragmented landscape to a fully scalable bank. The speed of change has accelerated dramatically, forcing the organisation to constantly adapt its operational architecture. "In today's turbulent times, IT architecture is no longer just about creating value; protecting value has perhaps become the top priority," Bahadir observed.

Resilience through technical flexibility

To ensure that protection, resilience by design has become a cornerstone of ING's strategy. The bank's IT architecture is designed to provide a high degree of flexibility so that the organisation can continuously adapt. The necessity of this is evident in the figures: every month, ING's IT frameworks undergo no fewer than 15,000 changes.

"Where engineers used to manually control everything, the digital flow now largely runs automatically via advanced platforms," Bahadir explained. Changes and configurations are now mostly automated, supported by strict access rights, security rules and continuous monitoring. "Particularly in complex mesh networks, central control remains crucial."

The reality of (shadow) AI

ING has fully embraced AI innovation, with about 100+ AI cases underway worldwide. According to Bahadir, the impact is already measurable: "the use of Copilot alone delivers a productivity boost." But AI innovation goes beyond smart assistants to autonomous AI agents. Right now, AI agents are the "next big thing". Alongside these productivity gains comes a concern around "shadow AI". Shadow IT is not new, it happens whenever employees create tools for productivity gain.

The challenge is that we want to maintain these in the same way we do any other IT assets. With AI Agent creation, this has become more widely accessible to everyone. This is why you need strict governance on what the data is that we can use to not risk data leaks and compliance issues. And as with any innovation, AI comes with a downside, which cybercriminals are eagerly exploiting. Because attackers in today's cyber landscape are no longer human, the extent to which AI should take the lead in matters like incident response and patching poses a dilemma. "As an organisation with critical infrastructure, ING approaches every step with extreme caution. Strong governance around AI development is crucial to maintaining stability."

Investing in people

Bahadir also stressed that investing in the future doesn't only mean that organisations should focus solely on attracting AI engineers. "Organisations must continue to invest heavily in junior engineers," he said. "Many profiles will need to reskill, although the question of exactly what skills will be needed is a challenge for the entire sector. It's a matter of redefining IT together.

AN SWALENS
CIO National Bank Belgium

National Bank of Belgium: balance and sovereignty

For An Swalens, CIO of the National Bank of Belgium (NBB), resilience has a very specific meaning. At the NBB, resilience is about finding a precise balance between mitigating risks and cyber threats on one hand and keeping networks and systems future-proof and innovative on the other. "It is a constant balancing act," she said, "and there is always the danger that one aspect – whether innovation or risk management – gets lost under pressure from the other."

Hybrid architectures

To maintain this balance, the NBB operates a hybrid model, with data partly on-premise and partly in the cloud. This architecture allows for worry-free innovation within the strictest possible security frameworks. "We work with rigorous standards," An explained. "When choosing third parties, we consciously seek a balance between strategic partners and pure innovation partners, all of whom undergo a series of assessments."

Knowledge retention and exit strategy

Because the NBB works with extremely sensitive and system-critical data, keeping knowledge in-house remains a strategic priority. "People and their specialised skills are sometimes undervalued in today's market, but they remain the ultimate safeguard when things go wrong," said An. "If the unthinkable happens and IT systems fail entirely, those people ensure continuity plans and exit strategies remain operational."

Digital sovereignty is also becoming increasingly important, partly under the influence of the European Central Bank (ECB), which acts as a staunch advocate for European autonomy. Does this mean organisations can no longer trust technology coming from the US? According to An, the issue is more complex than that: "Partners must not only be sovereign, " she said, and sovereignty has many levels and dimensions ." It remains a question of the wider picture of value versus costs and risks, and "partners must also actually have the capacity and depth of knowledge to bring the right value to us."

LUK BRUYNSEELS
MD of Networks and Capital Allocations
Liberty Global

Liberty Global: redundancy and agentic AI

As the parent company of Telenet, Liberty Global approaches resilience from the perspective of large-scale network infrastructure. Luk Bruynseels, Managing Director of Networks and Capital Allocations, described resilience by design in terms of both physical and digital connectivity: "Our core business revolves around accurately mapping the coax and fibre networks and continuously assessing the impact of potential outages."

Extreme stress testing

For both mobile and fixed services, resilience means that when a single point of failure occurs, the systems can immediately autonomously reroute traffic via alternative network routes. Liberty Global leaves nothing to chance. "Every month, we perform a large-scale stress test where we deliberately cause systems to fail to test the entire backup chain under real-world conditions," Luk explained.

The current geopolitical climate has also increased concerns around undersea data cables, which face a real risk of sabotage or physical damage. Although there is sufficient redundancy within international networks to reroute data, temporary outages remain a realistic scenario. "The challenge lies in seamlessly bridging that outage without the end user experiencing any disruption."

Shift to agentic AI

The core of Luks' argument, however, lies in the fundamental shift in skills brought about by the AI revolution, and specifically agentic AI. "We must look for fundamentally different skills in the labour market, although we cannot yet precisely define which competencies will be relevant tomorrow," he explained.

This raises the broader question of how much control organisations should hand over to AI agents and where the human element should remain within cybersecurity. Luk advocated a pragmatic approach: “We must approach the interaction between humans and AI like a self-driving car. Roles within organisations will irrevocably shift, even if the exact form of that shift is currently unclear. It’s a collective challenge for organisations – we don’t all need to reinvent the wheel independently.”

Conclusion: continuous resilience

One thing is certain: in today’s world, making long-term plans has become a Herculean task. As an organisation, you can at best see only a few months into the future. The discussion showed that the nature of cyberattacks has evolved fundamentally. Attackers are no longer human, and with AI attackers operating at machine speed, more than ever the question is no longer if IT infrastructure will be hit, but when. Recent tests show that traditional security tools simply do not cover all advanced attack methods.

This creates an acute dilemma regarding patching. If organisations insist on holding on to the principle that human approval (“human in the loop”) is always required for implementing patches, they will inevitably be overtaken by the speed of the attackers. Organisations are being forced to shift from weekly patching to continuous patching, and extensive legacy systems make this a massive challenge. While new autonomous tools make continuous patching technically possible, they also increase costs.

According to Geert Degezelle, resilience now extends much further than traditional cybersecurity or infrastructure strategy. “The real challenge lies not in reacting to incidents but in making the right design choices before the first crisis even occurs,” he concluded. “Organisations that are thinking about architecture, sovereignty and dependencies today are actually determining how resilient they will be tomorrow.”

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com/events

Telenet Business, part of the Telenet Group, is so much more than connectivity. As a managed service provider they help Belgian companies turn their digital challenges into business opportunities. They support and unburden, large and medium-sized enterprises as well as small entrepreneurs. You can count on them for high-quality managed services such as internet, telephony, solutions to collaborate and communicate digitally, cybersecurity and smart displays.

telenet.be/business

Report written by Felix Ferret - Bureau44