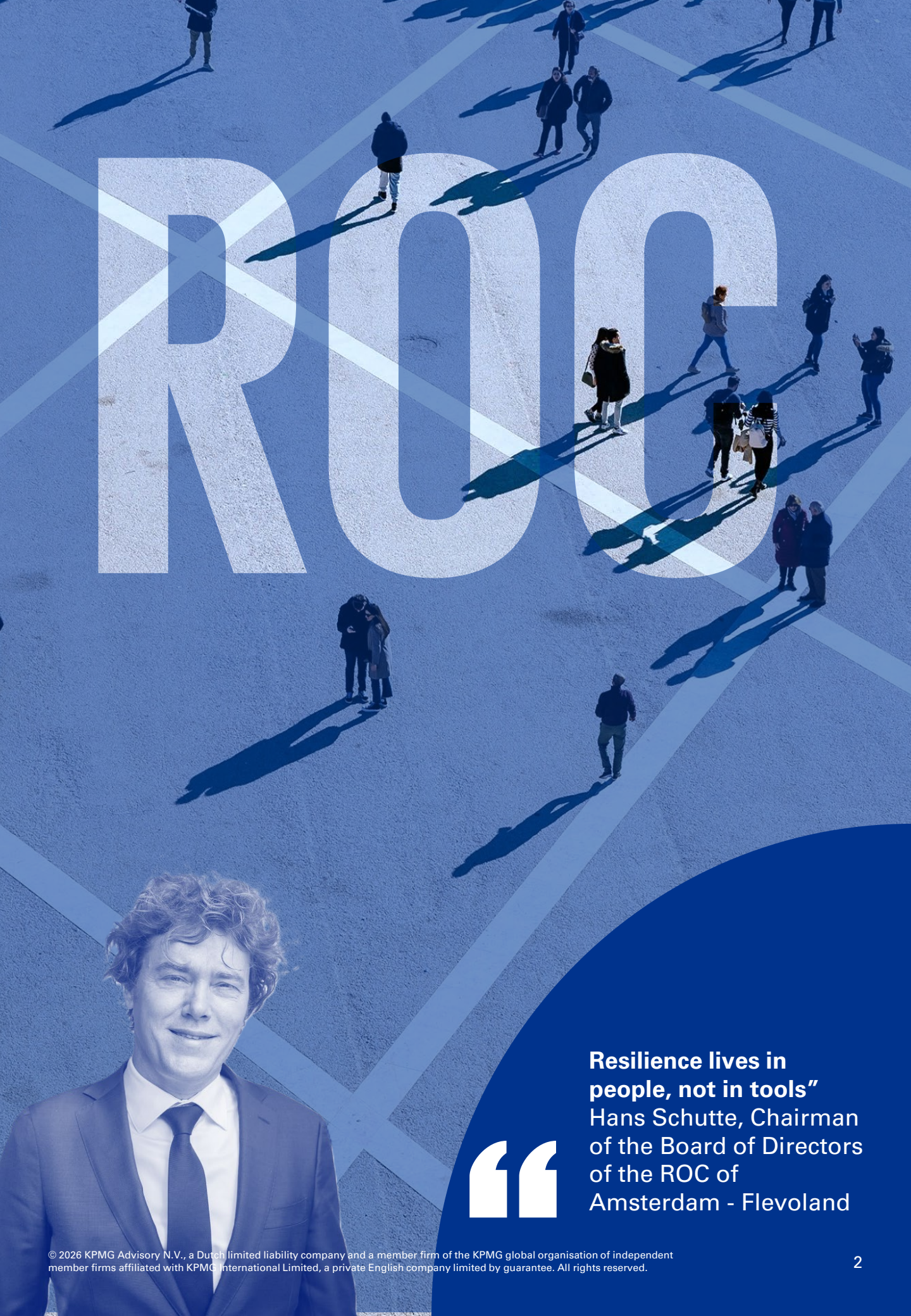
KPMG

Europe at a crossroads

Resilience lives in people, not in tools

Hans Schutte

February 2026



Resilience lives in people, not in tools”
Hans Schutte, Chairman of the Board of Directors of the ROC of Amsterdam - Flevoland

One Saturday morning, Mondriaan College, an ROC with 25,000 students, found itself cut off from its own systems, staring at a multimillion-euro demand and a long list of unknowns. What followed was a tense mix of moral decision-making, improvised problem-solving and technical triage. At that time, Hans Schutte was leading this ROC. He explains why refusing to pay mattered more than convenience, with one simple principle at the core: it's unacceptable to spend public money on criminal negotiations and it will set a precedent.

Let's go back to how this started, a couple of years ago, when you were heading the Mondriaan ROC in The Hague. When did you realise things were going off the rails?

"A quiet Saturday morning did the honours. The IT team noticed odd behaviour in a few systems. I was abroad and got a phone call. Within hours the whole digital landscape folded in on itself: HR, student administration, finance, access control. Even the coffee machines and the entrance systems to buildings and rooms were unusable. We were facing a classic ransomware hit. With a classic demand: the attackers demanded we pay several million euros in bitcoin and promised to leak data if we didn't meet their demands."

This must have been a nerve-wrecking few days for you and your team. Yet you decided almost immediately not to pay. Why so firm so fast?

"It boils down to a cocktail of things. Initial assessment suggested the compromised data had limited sensitivity. Large part of this data is publicly available which makes it worthless in terms of blackmailing. Secondly, we were quite convinced about the fact that we would be able to get things running again based on our backup plans that had been tested. That was the technical backbone of the decision. But perhaps the most important factor was the public-sector reality: it's simply unacceptable to spend public money on criminal negotiations. Furthermore, paying the money would send a signal that crime pays off. Once one institution pays, attackers would probably start treating the entire sector as an ATM. So, the choice not to pay was defensive, principled, and yes expensive in the short term."

Paying would send out a wrong signal, so much is clear. Yet, this must have been a big decision weighing on your shoulders?

"Of course there's the doubt that sits quietly in the background. You know refusing to pay is the right stance, but you also know that if backups fail or leaked data turns out worse than expected, the entire decision will be questioned publicly. You carry that weight while still moving at full speed. One of the things that made things easier was that we had a response team of experienced external specialists at our disposal. Which is not self-evident: the uncomfortable truth is that external specialists are scarce. There is a serious risk that when you need them, you might find every capable responder already booked."

Restoring operations is not a matter of days but may take weeks or months. But I guess telling all these 25,000 students to do nothing for such a long period was not an option?

"Most certainly not. What happened was that the pressure to get things going again resulted in creativity. Departments improvised, teachers switched to paper, students were informed by messaging apps. People relied on experience and judgment instead of dashboards and digital tooling. Especially our older employees were very capable in this respect. All in all, this was a reminder that technology supports our mission but doesn't define it."

The best experiences emerge under high pressure. What are other key takeaways to share with C-level suite?

"Preparation works. That sounds like a cliche, but there is so much truth to it. We had trained for incidents. The crisis structure existed on paper and, more importantly, in people's heads. Another key lesson is that a cyberattack is never just technical. It's organisational, human, or even political. And as I said: the striking thing is that, even with all systems down, the core mission of teaching continued. That's the real lesson: resilience lives in people, not in servers. And to conclude, there is also a silver lining to the incident: we are now pooling our risks with others."

Tell me more about this?

"We now have a collective pool in place with others in our sector with one basic rule: no ransom payments. Every member of the pool puts in money and is committed to reach a certain level on the benchmark for resilience. Should one of us be under attack, the pool can provide money to this individual organisation."

Viewpoint
Dennis Waalewijn

In case of an incident, tested contingency plans make the difference

Threat-informed practices promote knowledge sharing with peers and industry groups, strengthening collective cybersecurity defences. These practices enable enhanced cyber incident response and recovery by aligning defences with specific and current threats. During incidents, a threat-informed approach allows response teams to focus on the profiling of well-known cyber-criminal groups and their modus operandi, optimising containment and resolution efforts.

All of this could result in significantly reducing the impact of a large-scale cyber-attack. However, it is not easy to get beyond procedures and plan on paper. Many organisations struggle with obtaining the right level of expertise or are too slow to adjust appropriately given increasingly more complex architectures and third-party dependencies. Proper contingency plans are a must have. The most overlooked part of this is planning for staff augmentation and executing incident simulations on a regular basis with both executives and technical IT staff independently.

An incident will always come as a surprise; a tested and proved plan helps. A lot.