KPMG

Europe at a crossroads

Digital autonomy calls for harmonisation of baselines in cybersecurity

Sebastian Madden

February 2026

Digital autonomy calls for harmonisation of baselines in cybersecurity

Sebastian Madden
Chief Product Officer at CREST

When organising a major event such as the 2026 World Cup, the whole supply chain can become a target for digital threats. It is a perfect opportunity for criminals to embarrass a host nation. And it means that even organisations with a peripheral role must be prepared. This is one of the reasons why Sebastian Madden, Chief Product Officer at CREST, makes a case for coherent international baselines in security.

Amidst today's geopolitical turbulence, digital autonomy has become a strategic priority for governments and large companies. Politicians have also put it on top of their agenda. The rationale for this is solid. Organisations want to keep control over critical data, reduce geopolitical exposure, and avoid dependence on a small group of global technology providers. Yet there is also another side to this coin, says Madden. "There is a hidden cost to digital autonomy: complexity. It may lead to fragmentation of digital infrastructures and cybersecurity practices. That fragmentation increases cost, slows innovation, and tests the resilience of organisations that suddenly operate under stricter, more localised rules and frameworks."

The effects of this fragmentation? What once could be delivered from a single global team now requires local units, local licences, and local compliance procedures. Talent cannot move freely either. A professional certified individual in one country may not be recognised in another, even within the same company. This slows down skills development at a time when the global cybersecurity workforce is already overstretched.

The decentralisation also affects innovation. When teams operate in isolated pockets, their ability to learn from global best practices erodes. CREST, an international not-for-profit membership body representing the global cybersecurity industry, tries to counter this by encouraging the reuse of international standards. Madden cites Dubai's Cyber Force Programme as an example: companies must hold the same standards to qualify technically, and they only need to add local top-ups such as police checks or trade licences. The country thus adopts global quality baselines without reinventing the wheel.

C-level leaders have a role in acknowledging these trade-offs of digital autonomy. They must ensure their organisations build local capability where required, but without disconnecting from global best practices.

Digital autonomy is only one part of the wider resilience discussion now moving into C-suites. CEOs increasingly find themselves drawn into complex environments where geopolitical tension, public visibility, and digital risk intersect. Major events are a prime example of how this pressure builds up. One example is the upcoming 2026 World Cup, where any organisation in the supply chain can become a target. These threats range from politically motivated disruption to criminal activity or attempts to embarrass a host nation. Madden: "CEOs must assume heightened exposure the moment their organisation takes on even a peripheral role. This is precisely why we need international standards to manage the risks well."

In his view, effective resilience is built through preparation, and preparation requires (international) coordination. Resilience also calls for a realistic view of responsibility. Many organisations still approach crisis planning from a somewhat narrow, internal perspective. They look inward and downward, not upward and across. Events such as the 2026 World Cup, by definition, require coordination across public and private sectors, critical infrastructure operators, law enforcement, and specialised digital teams. If those links remain weak, even well-designed frameworks falter in practice.

Madden stresses that this lack of coordination leads to blind spots. A cyber incident that triggers a physical impact may for instance become the domain of fire brigades and emergency services. A digital intrusion driven by state actors may shift into the realm of intelligence or defence agencies. No single organisation can cover all dimensions. It's a matter of being able to connect the dots when it matters. Not only in elaborate plans on paper, but also in testing these plans for real.

Requests for proposal (RFPs) sometimes already reflect a shift in requirements: customers want to be assured of proper testing of crisis plans. The question that pops up when it becomes common practice to raise the bar in RFPs: why not see cybersecurity as an opportunity in the market, as a competitive factor? And why not use this opportunity to move from good enough to world-class?

It may be too early or too optimistic for this. But the broader message is clear: "The organisations that treat these topics as joint responsibilities rather than isolated duties will be the ones that stay adaptable in a more volatile digital landscape."