CYBERSECURITY SURVEY 2025: EU CYBERSECURITY REGULATIONS NOW SHAPE IT STRATEGIES, WHILE CIOS CALL FOR EUROPEAN PROVIDERS

Sovereignty Moves To The Boardroom – 48% Of Security Executives Demand European Providers, While Regulatory Pressure Reshapes Strategy And Budgets

ZURICH, SWITZERLAND, June 27, 2025 /EINPresswire.com/ -- Cybersecurity decision-making in Europe is undergoing a quiet transformation — driven by rising regulatory pressure and growing demands for digital sovereignty at the executive level. A new report from Open Systems reveals that 48% of CIOs and CISOs now explicitly demand European-based security providers, while 43% of all organizations — and nearly three quarters of C-level executives — say that frameworks like NIS2, DORA and the Cyber Resilience Act directly shape both their security investments and vendor choices.

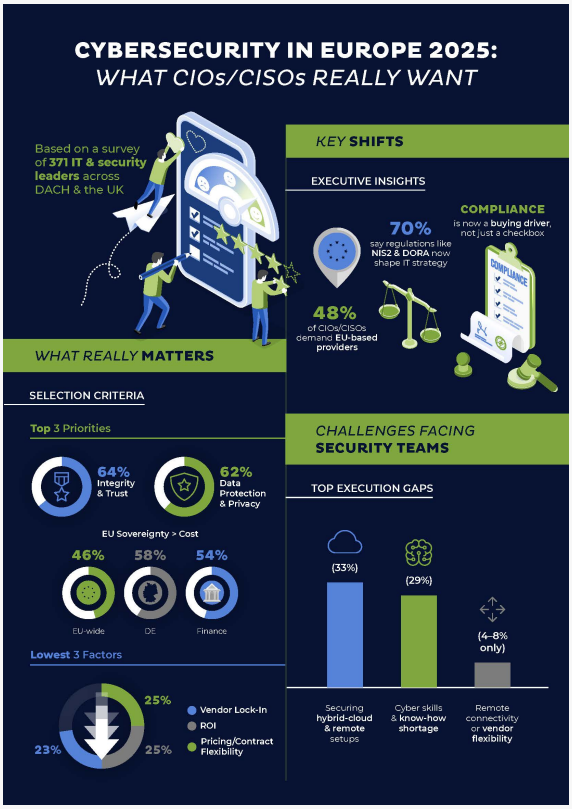
> The sovereignty debate has entered the boardroom. We're seeing a decisive shift: compliance is no longer a final checkpoint, but a driver of strategy, architecture and supplier shortlists."
>
> *Daniel Gerber, Chairman of the Board, Open Systems*

The study is based on a survey of 371 IT and security decision-makers across Germany, the UK, Austria, and Switzerland.

"The sovereignty debate has left the back office and entered the boardroom," said Daniel Gerber, Chairman of the Board at Open Systems. "We're seeing a decisive shift: compliance is no longer a final checkpoint, but a driver of strategy, architecture and supplier shortlists."

What today's security leaders say:
Criteria like sovereignty, regulation alignment and certifications far outweighing lock-in concerns including vendor dependency.
- 48% of CIOs/CISOs demand European-based providers
- 43% of all organizations — and 72% of the C-suite — say EU regulations dictate both strategy and supplier selection
- Hybrid-cloud protection and the cyber-skills drought remain the top execution gaps

“Security leaders are not just responding to regulation — they’re building architectures and teams around it,” said Markus Ehrenmann, CTO of Open Systems. “And they’re demanding platforms that combine EU-hosting, zero-trust control, and out-of-the-box audit readiness.”



Cybersecurity in Europe 2025: What CIOs/CISOs really want

New Role Of Managed Services
The limited concern around vendor dependency likely reflects a shift of organizations towards regulatory fit and service quality. While only 25% still consider vendor lock-in a relevant factor, 55% now prefer European-based providers, and 70% feel tangible pressure from frameworks like NIS2 and DORA. This underlines a growing demand for partners who not only meet compliance requirements but also support operational execution.

The top IT challenges cited in the study clearly relate to complex technical environments — including hybrid infrastructure, multi-cloud adoption, and skills gaps in network and security operations. This makes it increasingly important that managed services combine consulting expertise with the underlying technology.

Providers must offer:
- Effective architecture design that works in practice with the technology deployed and is tailored to each organization’s structure and risk profile.
- Close support during configuration and operations, filling internal gaps and acting as an extension of the team.

Survey respondents also listed the following top three IT projects driven by new regulations:
- Security operations and incident/audit handling (45%)
- Data transparency and processing (e.g. SIEM visibility) (37%)
- IT/OT convergence and OT security (36%)

These Trends Place New Demands On Security Providers:
- There must be a plan for ongoing operations, particularly for organizations without the capacity to manage incidents, changes, or reviews internally.
- Transparency is critical: how and where security data is processed, whether it remains in the EU, and how it is accessed (e.g. via real-time dashboards, drill-downs, APIs).
- OT security must be addressed beyond manufacturing: 48% of industrial companies, and 44% of finance and healthcare respondents cite this as a pressing need. Providers must go beyond

technology (e.g. ZTNA, OT firewalls) to help design secure architectures and realistic transformational planning and successful migration strategies.

About the Survey
The research was conducted in Q2 2025 and includes responses from 371 qualified IT/infrastructure/security leaders, spanning C-level executives, mid-management, and technical roles. Respondents represent a wide spread of industries and company sizes, with balanced representation across the DACH region and the UK.

About Open Systems
Open Systems is a leading provider of native Managed SASE solutions, converging network and security functions on a cloud-native platform. Founded in 1990, the Swiss cybersecurity company, headquartered in Zurich, supports businesses and organizations in more than 180 countries with a holistic, customer-centric service model that guarantees 24x7 expert support. The combination of an innovative platform, integrated solutions, and excellent service ensures secure, reliable, and worry-free network operations – even within the complex IT infrastructures of global manufacturing companies and NGOs. Open Systems not only enhances security but also boosts operational efficiency and accelerates innovation.

Barbara Jaeggi
Open Systems
bjaeggi@open-systems.com
