WHITEPAPER

DATA GOVERNANCE: THE FOUNDATION OF DIGITAL RESILIENCE

THE SECRET WEAPON OF DIGITAL FRONTRUNNERS

LCL Your Data Center

CIONET

INTRODUCTION

DATA GOVERNANCE: THE FOUNDATION OF DIGITAL RESILIENCE

Organisations today are generating more data than ever, increasingly relying on cloud platforms and interconnected networks. At the same time, cyber threats are becoming more sophisticated and artificial intelligence is accelerating both decision-making and automation.

In this environment, data is no longer just something you store and manage. It has become the foundation of how organisations compete, build trust and stay resilient. But here's the problem: many organisations don't actually know where their data lives, who can access it or how it flows between systems.

That lack of visibility affects more than day-to-day operations. Without a clear picture of your data, you can't manage risk effectively, protect what matters most or recover quickly when something goes wrong.

This is why data governance, once seen as just a compliance tick box, is emerging as a strategic priority. Done well, it gives organisations the visibility and control they need to understand, manage and protect their data while supporting innovation, cybersecurity and digital autonomy.

This whitepaper explores three major challenges shaping today's digital agenda: digital sovereignty, an evolving cyber threat landscape and the rise of AI as both a risk and a powerful tool for cyber defence. Different as they sound, all three come back to the same question: do you really know your data?

The findings draw on a survey of 19 CIOs from the CIONET network, in-depth interviews, a subscriber survey by LCL, and expert perspectives from LCL's Chief Information Officer Nicolas Coppée and cybersecurity expert Géraud de Neve.

Their message is clear: in a digital world, data governance isn't optional, it's essential.

"You cannot govern what you don't actively observe. Once you start correlating signals across systems, risks that were previously invisible become tangible."

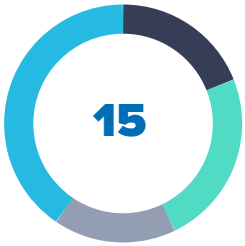
Nicolas Coppée, CIO at LCL

BODY

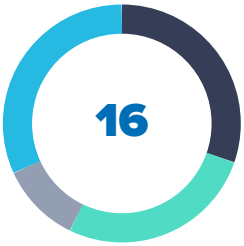
1) OVERCOMING THE SOVEREIGNTY PARADOX

Digital sovereignty has rapidly moved from a policy debate to a boardroom concern. Yet, despite growing awareness, most organisations remain heavily dependent on a handful of non-European technology providers.

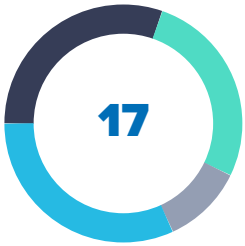
The survey results highlight this paradox:



15 of the 19 organisations surveyed describe themselves as highly dependent on non-European cloud providers



16 see no credible European alternative that currently matches the scale and capabilities of the global hyperscalers.



Yet 17 would consider switching if a viable European alternative became available.

The appetite is there. The market not yet.

Wanted: European firepower

At the heart of the challenge lies a question of scale. Large enterprises and public institutions need providers that guarantee uptime, absorb contractual liabilities and invest heavily in infrastructure. European initiatives remain modest compared to the financial and operational firepower of the hyperscalers. Sovereignty is an attractive ambition but a difficult procurement choice.

"Name me an alternative in Europe - a company serving Europe with the comparable size of Microsoft. I don't see one. There are small companies trying, but they are still small." A Belgian public sector CIO.

"Today, we still talk about a European cloud while our data, critical tools and even innovation largely depend on non-European providers. Europe's digital future is not a PowerPoint strategy; it should be built and deployed."

From an LCL newsletter respondent

There is also a practical reality. Over the years, organisations have built applications, processes and expertise around dominant cloud ecosystems. Moving away from those platforms is costly and complex. As a result, many adopt a hybrid approach: highly sensitive data remain on-premises or in trusted local data centers, while customer-facing applications and digital services run on international public clouds.

Creating the conditions to scale

For most organisations, complete digital independence is neither realistic nor necessarily desirable. The real challenge is understanding where critical data reside, who controls access to it, which dependencies exist and what risks they create. In that sense, sovereignty starts not with ownership, but with visibility and control.

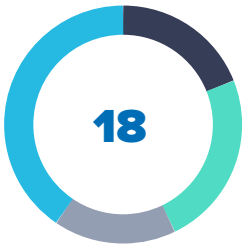
Europe should not – and cannot – replace hyperscalers overnight. Its priority is to create the conditions in which European alternatives can emerge, grow and compete. Without customers, they cannot scale. Without scale, they cannot become credible alternatives.

"European investment needs several more zeroes to make a real difference. The current impulse is insufficient - and without that scale, there is no credible partner on the other side." A Belgian public sector CIO.

Ultimately, digital sovereignty is less about ideology and more about resilience. It is about maintaining control over critical data, preserving strategic options and avoiding excessive dependence on a single provider or ecosystem. In an increasingly uncertain geopolitical environment, that flexibility may become a competitive advantage.

2) CYBER RESILIENCE TO PROTECT DATA INTEGRITY

Cybersecurity has never been higher on the agenda of business and technology leaders. Yet our survey reveals a striking gap between awareness and confidence:



18 out of 19 CIOs consider a cyberattack likely or very likely within the next 12 months.

Only four describe themselves as very confident in their organisation's ability to withstand a targeted attack.

Organisations understand the threat. They are far less certain about their ability to withstand an attack and recover from it.

"The moment you think you are well-prepared, something happens that you weren't prepared for. It is a continuous investment in people and resources." A Belgian public sector CIO

"A standard Denial of Service (DoS) attack is loud but manageable. The far greater danger stems from quiet, sophisticated infiltrations targeted at data integrity and confidentiality."

A Belgian public sector CIO

Beyond the perimeter

This reflects a broader shift in the digital landscape. Traditional security strategies focused on protecting the perimeter through firewalls, endpoint protection and access controls. While these measures remain essential, today's attackers increasingly aim for something more valuable than operational disruption: data.

Modern cyberattacks are often designed to remain undetected for weeks or months. Rather than taking systems offline, attackers seek to compromise the integrity, confidentiality or availability of critical information. In many cases, the most damaging consequences only become visible after the breach itself.

Restore trust

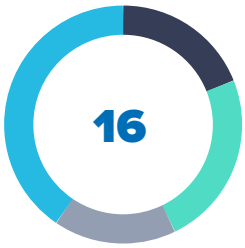
One of the digital leaders interviewed for this whitepaper experienced this firsthand. Following a major cyber incident in 2025, restoring systems took weeks. Restoring trust took six months. The real challenge was not rebuilding infrastructure but determining which data could still be trusted and whether decisions had been influenced by compromised information.

This is where cybersecurity and data governance converge. Security tools can help prevent attacks. But true resilience depends on understanding which data exists, where it resides, who can access it and which information is most critical to the organisation. Without that visibility it becomes difficult to detect anomalies, assess the impact of an incident or prioritise recovery efforts.

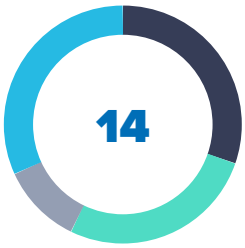
3) AI IS CHANGING THE RULES OF CYBER DEFENCE

Europe is often portrayed as lagging behind the United States and China in the global AI race. Yet in cybersecurity, AI is already firmly embedded in many organisations.

The survey confirms this trend:



16 of the 19 organisations surveyed already use AI in cybersecurity, either operationally or through pilot projects.



14 have implemented formal AI governance policies (also for shadow AI), while the remaining five are actively developing them.

> **"The organisations that will thrive are not those that use AI the most, but those that continue to think for themselves."**
>
> **From an LCL newsletter respondent**

One of the digital leaders interviewed for this whitepaper illustrates how far this evolution can go. Rather than limiting AI to log analysis, their organisation correlates signals across physical and digital environments simultaneously. Operational patterns, network behaviour and sensor data is brought together to create a real-time picture of risk. Increasingly, this kind of capability does not require building from scratch: AI-powered threat intelligence is already embedded in the platforms most organisations use, with vendors aggregating signals across thousands of clients. One concrete result is the accelerating pace of remediation: patch cycles that once took days are now measured in hours.

AI is also rapidly becoming a strategic ally for defenders. Security teams use it to filter alerts, prioritise incidents and uncover threats that would otherwise remain hidden. But AI is equally empowering attackers. Cybercriminals are using it to create convincing phishing campaigns and scale attacks at unprecedented speed. AI is accelerating both sides of the cybersecurity equation.

Shadow AI and the governance challenge

Despite the excitement surrounding agentic AI capable of autonomously detecting cyber-attacks, human judgement remains indispensable. Assessing risks, validating findings and making decisions during security incidents still requires human oversight.

The bigger challenge may not be technological, but organisational. Many companies are already familiar with shadow IT: technologies adopted outside the visibility and control of the IT department. Employees increasingly use AI tools without fully understanding the implications for confidentiality, compliance or intellectual property. As a result, AI governance is becoming as important as AI adoption itself.

From data leak to integrity breach

At the same time, the risk is shifting from data leakage to data integrity. As organisations increasingly rely on AI for decision-making, manipulated, incomplete or unreliable data can have far-reaching consequences. Attackers do not even need to breach a network to cause harm. Compromising the data behind AI systems may be enough.

"What worries me more than AI itself is open data. We are going to publish datasets that others will build their operational systems on. If we distribute false information — incorrect street names, wrong flood-zone data — the impact won't just be on us. It will be on everyone who relies on that data." A Belgian public sector CIO

For CIOs, the challenge is therefore not simply adopting AI faster. They must ensure that the data feeding AI systems remains accurate, traceable and resilient. Even the most sophisticated algorithms are only as valuable as the quality, governance and oversight of the data they rely on.

CONCLUSION

THE SECRET WEAPON OF DIGITAL FRONTRUNNERS

Throughout this whitepaper, three themes repeatedly surfaced: digital sovereignty, cyber resilience and artificial intelligence. They are often treated as separate priorities, but they all lead back to the same foundation: data.

The same principle applies at every level. Sovereignty depends on understanding where data resides. Cyber resilience depends on knowing which data can be trusted. AI depends on the quality of the data it consumes. Different challenges, same foundation.

This is why data governance is no longer a compliance exercise or a technical back-office function. It has become a strategic must-have that enables organisations to reduce dependencies, navigate uncertainty and build resilience in an increasingly interconnected world.

The challenge is that data governance is often invisible when it works well. It does not generate headlines like AI. It lacks the urgency of a cyber incident. And unlike digital sovereignty, it rarely sparks political debate. Yet it is precisely this quiet discipline that determines how effectively organisations can respond when disruption occurs.

For CIOs and digital leaders, the question is therefore no longer whether data governance deserves attention. The question is whether their organisation is treating data as a strategic asset or merely as a by-product of business operations.

The organisations that will thrive in the coming years will not necessarily be those with the most data, the largest cloud environments or the most advanced AI models. They will be the organisations that understand their data best: where it resides, how it flows, who controls it and whether it can be trusted.

The call to action is clear. Start with visibility. Build governance into every digital initiative. Treat sovereignty, cybersecurity and AI not as separate programmes, but as interconnected challenges that depend on the same foundation. In the end, data governance is what turns vulnerability into resilience.

Looking for a reliable partner
that guarantees data sovereignty in Europe?

Contact Baudouin Corlùy
Chief Market Development Officer at LCL

baudouin.corluy@lcl.be | +32 475 65 79 74

LCL Your Data Center

YOUR DATA CENTER.
RELIABLE. AVAILABLE. CONNECTED.