CIONET X LCL WHITE PAPER

Data Sovereignty

The foundation of digital resilience

A CIO conversation in Belgium about how Europe can turn digital sovereignty from ambition into operational control.

Baudouin Corlùy
Chief Market Development Officer at LCL

DO YOU REALLY KNOW YOUR DATA?

THE QUESTION BEHIND EVERY SOVEREIGNTY DECISION

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

Where does it reside?
Who can access it?

How does it move between systems?

Data governance is not an operational problem.
It is closely linked to digital sovereignty, cybersecurity and AI.

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

THE DIGITAL IMMUNE SYSTEM IS UNDER PRESSURE

DEPENDENCE, CYBER TRUST AND AI READINESS ARE THE SYMPTOMS

1. **How dependent are we on foreign**

DIGITAL SOVEREIGNTY

2. **Can we trust our data after a cyberattack?**

CYBER RESILIENCE

3. **Are we ready for AI?**

AI GOVERNANCE

We keep hearing questions about the state of that immune system and whether we should worry

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

WHAT WE STUDIED

THE DIGITAL RESILIENCE SURVEY WITH CIONET

We wanted to understand how CIOs look at these challenges and whether their organisations are up to the task

19 CIOs

CIO survey across the CIONET network

In-depth interviews

Qualitative input from Belgian digital leaders

LCL subscriber survey

Broader market perspective from the LCL community

The white paper message is clear: in a digital world, data governance is not optional - it is essential

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

THREE INSIGHTS FROM THE WHITE PAPER

DIFFERENT CHALLENGES. ONE FOUNDATION: DATA.

1 **Europe wants digital sovereignty**

But organisations remain highly dependent. The appetite is there. The market is not yet.

2 **Cyber risk awareness is high. Resilience confidence is not.**

Everyone expects an attack. Few feel truly prepared. A failing immune system lacks trust.

3 **AI is changing the rules**

AI strengthens cyber defence, but it also creates new risks around shadow AI and data integrity.

Sovereignty becomes the center of gravity:
because Europe can only be resilient if it can see, control and trust its critical data

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

THE SOVEREIGNTY PARADOX

EUROPE WANTS SOVEREIGNTY. CIOS STILL NEED CREDIBLE ALTERNATIVES.

Among 19 CIOs surveyed, dependence is the starting point, not the destination

"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."

LCL NEWSLETTER RESPONDENT

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

SOVEREIGNTY IS NOT ISOLATION

IT IS CONTROLLED INTERDEPENDENCE AND STRATEGIC OPTIONALITY

Not a binary debate

- Replace every global platform overnight
- Slow down innovation in the name of purity
- Treat cloud location as the only sovereignty question

A practical control model

- Know which data and workloads require European control
- Use global innovation where it is safe
- Keep exit, recovery and negotiation options open

For Belgian CIOs, sovereignty should increase choice, not reduce it.

Sources: European Commission tech sovereignty pages; CIONET x LCL white paper.

HOW EUROPE NEEDS TO POSITION ITSELF

FROM POLICY AMBITION TO MARKET CREDIBILITY

1

Scale infrastructure

European cloud, data center, AI compute and connectivity capacity must become a strategic asset.

2

Federate the ecosystem

Europe should compete as a network of interoperable providers, not as fragmented national islands.

3

Make portability enforceable

Data, metadata, contracts and architectures must make exit possible before a crisis.

4

Use procurement as demand creation

Public and regulated sectors can create the customer base that European alternatives need to scale.

5

Prove trust operationally

Auditability, resilience, cyber controls and governance must be visible to CIOs.

Europe does not need to cut itself off.
It needs the capacity to choose, switch, audit and recover.

Sources: European Commission tech sovereignty and Cloud/AI Development Act pages; CIONET x LCL white paper.

CYBER RESILIENCE IS THE FIRST SOVEREIGNTY TEST

CAN YOU RECOVER TRUSTED DATA AFTER AN ATTACK?

18 / 19

consider a cyberattack likely or very likely within 12 months

4 / 19

are very confident they can withstand a targeted attack

"Restoring systems took weeks. Restoring trust took six months."

DIGITAL LEADER INTERVIEWED FOR THE WHITE PAPER

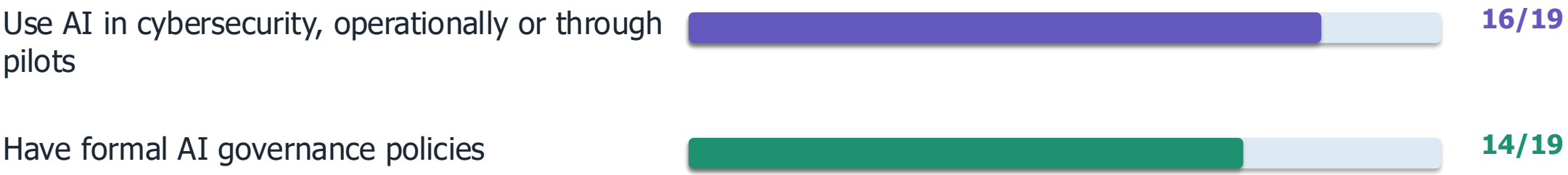
Sovereignty lens

A sovereign organisation does not only prevent downtime. It knows which data is still trustworthy, what to restore first and how to prove integrity after an incident.

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

AI CHANGES THE SOVEREIGNTY QUESTION

CONTROL THE DATA BEHIND AI, OR AI AMPLIFIES YOUR DEPENDENCIES



"What worries me more than AI itself is open data. If we distribute false information, the impact will be on everyone who relies on that data."

BELGIAN PUBLIC SECTOR CIO

Sovereignty lens

- Shadow AI makes data leakage a governance issue
- AI decision-making shifts the risk from data loss to data integrity
- European AI competitiveness depends on trusted data and compute capacity

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

THREE CHALLENGES. ONE FOUNDATION.

DATA GOVERNANCE TURNS VULNERABILITY INTO RESILIENCE

SOVEREIGNTY

Where data resides

Visibility and control over critical data location, jurisdiction and dependencies

RESILIENCE

Which data can be trusted

Integrity, recovery and prioritisation after cyber incidents

AI

Quality of data consumed

Traceability, lineage and governance of the data AI uses

DATA GOVERNANCE: OBSERVE, CLASSIFY, CONTROL, TRUST AND RECOVER

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

THE DATA SOVEREIGNTY OPERATING MODEL

HOW TO MAKE CONTROL MEASURABLE

1 → 2 → 3 → 4 → 5

Observe

Discover where data lives and flows

Classify

Define criticality, sensitivity and legal exposure

Control

Manage access, location, contracts and providers

Trust

Prove integrity, lineage and AI readiness

Recover

Test recovery, portability and reversibility

What gets measured becomes governable.
What is governable becomes defensible.

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

CIO AGENDA: THE NEXT 90 DAYS

TURN SOVEREIGNTY INTO DECISIONS

DAYS 1-30

Create the sovereignty heatmap

Top critical datasets, providers, jurisdictions, access paths and recovery dependencies.

DAYS 31-60

Rewrite procurement criteria

Add location, jurisdiction, reversibility, interoperability, auditability and incident-trust requirements.

DAYS 61-90

Prove one sovereign anchor workload

Select a critical workload and prove European control operationally, not only contractually.

Start with visibility. Build governance into every initiative.
Treat sovereignty, cyber and AI as one challenge.

Source: CIONET x LCL white paper, CIO survey (n=19), in-depth interviews and LCL newsletter survey.

Data sovereignty

is built where critical data lives.

Read the white paper.
Let's talk about how to make sovereignty operational for your critical data.

Baudouin Corlùy | Chief Market Development Officer at LCL
baudouin.corluy@lcl.be

LCL Your Data Center

TOGETHER WE EXCELL