



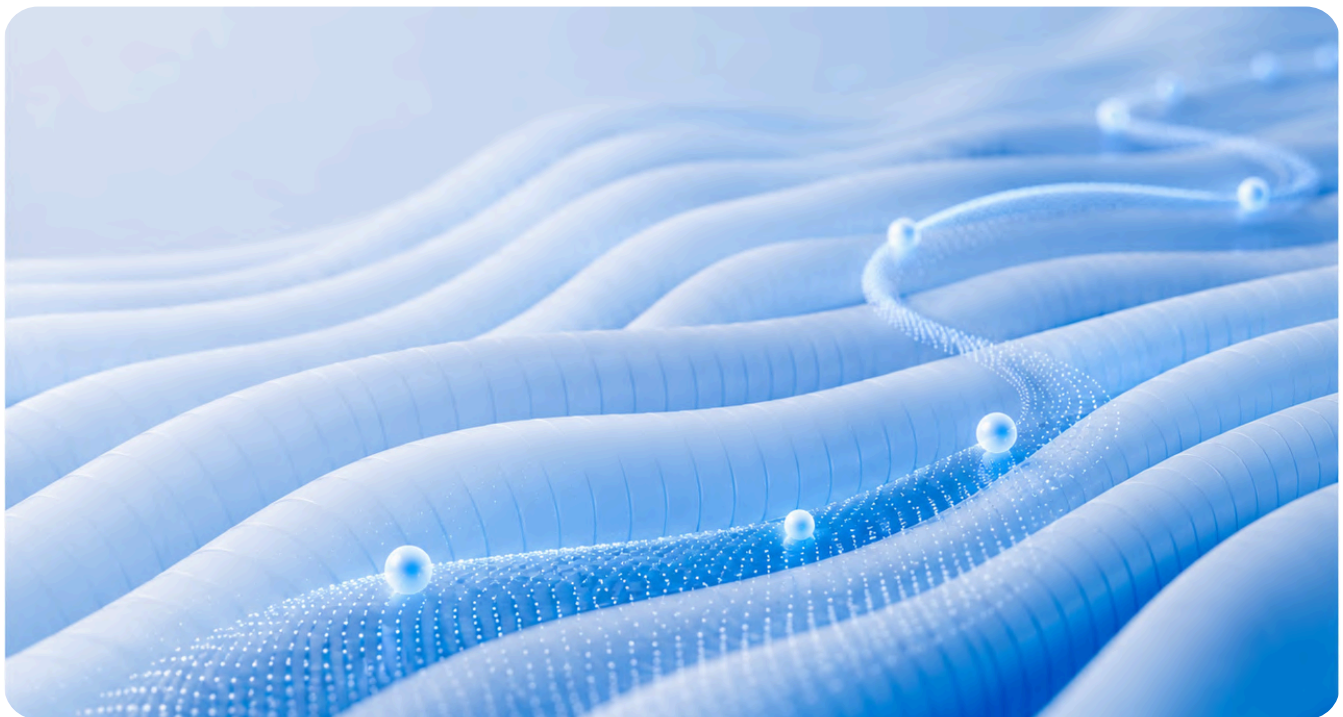
**Nemko**  
Digital

# **What Business Leaders Are Getting Wrong About Digital Trust in 2026**

Five years ago, digital trust was largely a compliance discussion. Today, it is increasingly influencing procurement decisions, customer confidence, partnership agreements, access to markets, and board-level investment priorities.

Yet many organisations continue to approach digital trust as a regulatory exercise rather than a strategic capability. The biggest risk facing many organisations is not non-compliance. It is investing significant time and money in digital trust programmes that fail to address their most material business risks.

In conversations with executives across the Benelux region, six themes consistently emerge.



# Key Findings

## 1. Organisations Focus on Compliance Before Understanding Their Exposure

### The Wrong Starting Point

The first question I often hear is: "How do we become compliant?"

In practice, the organisations making the fastest progress start somewhere else: "What actually applies to us?"

### Understanding Your Actual Obligations

Both the [EU AI Act](#) and the Cyber Resilience Act contain obligations that depend on organisational role, product type, use case, and risk classification. Yet many organisations begin building policies, controls, and governance structures before establishing a clear understanding of where their actual exposure lies.

This often results in resources being directed toward low-priority activities while more significant risks remain unaddressed. The organisations pulling ahead are not necessarily spending more. They are investing with greater precision.

The lesson is simple: clarity of exposure drives better investment decisions.

## 2. Governance Is a Bigger Challenge Than Technology

### The Misconception About Technical Solutions

Many leaders assume [AI governance](#) and cybersecurity readiness are primarily technical challenges. In reality, technology is rarely the biggest obstacle.

The more difficult questions are organisational. Who owns AI governance? Who approves new AI use cases? Who is accountable for AI-related risks? Who decides when innovation goals conflict with risk considerations? As highlighted in [The enterprise guide to AI governance by the IBM Institute for Business Value](#), establishing governance guardrails for trustworthy AI is a critical trust factor that cannot be ignored.

Most organisations already have capable technical teams. What they often lack is a governance model that clearly defines accountability and decision-making authority.

Technology can be purchased. Accountability must be designed.

Organisations that establish ownership early move faster, make better decisions, and respond more effectively when challenges emerge.

### 3. AI Adoption Is Moving Faster Than Organisational Readiness

#### The Speed of Enterprise AI Adoption

Few developments are moving faster than enterprise AI adoption. Across almost every sector, employees are already using generative AI tools to support research, content creation, coding, analysis, and decision-making. What many organisations underestimate is how quickly governance gaps emerge when adoption outpaces organisational readiness.

A simple question often reveals the issue: if ten employees were asked about the organisation's AI usage rules, would they give the same answer?

Frequently, they would not.

The resulting risk is not primarily technical. It stems from thousands of everyday decisions made throughout the organisation, often without clear guidance or oversight. The leaders getting ahead are treating AI literacy as an organisational capability rather than a training requirement. They recognise that responsible AI adoption depends as much on people and culture as on technology itself, supported by [AI management systems](#).

### 4. Many Organisations Still Assume Their Vendors Carry the Risk

#### The Misconception About Vendor Accountability

One misconception continues to surface repeatedly.

Many organisations assume that purchasing an AI solution transfers a significant portion of the regulatory burden to the vendor. It does not.

As AI becomes embedded across business processes, organisations remain accountable for how those systems are used, governed, monitored, and overseen within their own operations.

This distinction is becoming increasingly important as AI moves from experimentation into critical business functions.

The leaders navigating this most effectively understand that while technology can be outsourced, accountability cannot. Digital trust ultimately remains a leadership responsibility.



## 5. Cybersecurity Is Becoming a Business Capability

### Moving Beyond Compliance

For many organisations, cybersecurity is still viewed primarily through a compliance or risk-management lens. Increasingly, that perspective is becoming too narrow.

### Security as a Strategic Business Driver

Driven in part by regulations such as the Cyber Resilience Act and the [New Information Security Directive \(NIS2\)](#), organisations are strengthening capabilities around vulnerability management, software transparency, incident response, and product security. The most forward-looking organisations are not doing this because regulation requires it. They are doing it because business resilience requires it.

Security weaknesses create more than regulatory exposure. They create operational disruption, supply-chain risk, reputational damage, and growing barriers to market access.

In this sense, security debt is increasingly becoming business debt.

The organisations making the greatest progress are embedding cybersecurity into core business operations rather than treating it as a standalone compliance initiative.



## 6. Digital Trust Is Becoming a Competitive Advantage

### The Shift Beyond Compliance

Perhaps the biggest shift I have observed over the past year is that digital trust is moving beyond compliance altogether. Research by McKinsey on [why digital trust truly matters](#) indicates that consumer faith in data privacy and responsible AI can directly lead to business growth, with trusted organizations more likely to see significant annual growth rates.

Customers, partners, procurement teams, investors, and regulators are all asking increasingly similar questions: How do you govern AI? How do you manage cyber risk? How do you handle vulnerabilities? Who is accountable when something goes wrong?

In many sectors, the answers increasingly influence purchasing decisions, supplier selection, partnership opportunities, and access to new markets.

We are already seeing procurement teams and enterprise customers asking suppliers to demonstrate AI governance practices, cybersecurity maturity, and structured risk-management processes. Increasingly, trust is becoming part of the buying decision, not just a compliance requirement.

### Digital Trust as a Strategic Asset

The organisations furthest ahead no longer view digital trust as a defensive activity. They see it as a business capability that strengthens resilience, accelerates decision-making, builds customer confidence, and supports growth.

The organisations gaining advantage are not necessarily the most compliant. They are the ones that can demonstrate trust at scale.

## FROM COMPLIANCE TO COMPETITIVE ADVANTAGE

*The Digital Trust Maturity Progression • Nemko Digital*



*"The right question is not 'Are we compliant?' — it is 'Are we building the right capabilities?'"*

*From reactive compliance to strategic leadership — the four stages every organisation must navigate to turn digital trust into a competitive advantage.*

## Conclusion

### *The Wrong Question*

One of the most common questions I hear from executives is: "Are we behind?"

In my experience, that is the wrong question.

### *The Right Question*

The more useful question is: "Are we building the right capabilities?"

The organisations creating the most value are not treating digital trust as a collection of compliance activities. They are building governance structures, accountability mechanisms, workforce capabilities, and cybersecurity practices that will remain valuable long after individual regulatory deadlines have passed, guided by global standards such as those established by the [Digital Trust Institute](#).

### **The Strategic Imperative**

The biggest mistake business leaders are making in 2026 is viewing digital trust as a compliance project, rather than embracing a comprehensive AI trust hub strategy.

The organisations pulling ahead increasingly view it as something far more strategic: a capability that reduces risk, strengthens resilience, enables innovation, builds customer confidence, and increasingly determines competitive advantage.

## About the author

---



### Angelo Saji

Angelo Saji is Global Sales Lead at Nemko Digital, where he helps organisations turn the complexity of AI governance into commercial opportunity. With extensive experience in B2B sales, business development, and market expansion, he focuses on helping organisations navigate the EU AI Act, ISO/IEC 42001, and the evolving responsible AI landscape. His career spans the Dutch startup and scale-up ecosystem, including roles at Startupbootcamp, Growth Tribe, and True Growth, as well as co-founding gaming startup SZZITCH. With a builder's mindset, Angelo specializes in creating scalable sales processes, opening new markets, and translating complex solutions into clear business value.