TECHNOLOGY TRANSFERS CAPABILITY.

IT ALSO TRANSFERS RISK.

The providers don't carry it. You do.

Every technology adoption decision your organisation makes comes with an undisclosed passenger: a field of risk that transfers entirely to you at the moment of deployment. The vendors who built these systems have systematically excluded themselves from liability for the failure modes they know best — leaving adopting organisations to carry exposure they cannot see, cannot quantify, and were never equipped to manage.

01

THE BUILDER KNOWS THE RISK

Their contracts ensure they don't own it

02

THE ADOPTER OWNS THE RISK

And rarely has the context to price it

03

THE GAP BETWEEN THEM

Is where breaches, penalties, and losses live

THREE FORCES THAT KEEP THE RISK INVISIBLE.

01

KNOWLEDGE ASYMMETRY

Technology providers hold material intelligence about their products' failure modes — vulnerability classes, systemic weaknesses, emergent risks at scale. That knowledge does not transfer to adopters. What transfers is the capability. The risk profile remains behind a wall of engineering documentation, legal indemnity, and competitive confidentiality.

02

TEMPORAL MISMATCH

Adoption decisions are made today. The risk materialises later — under conditions that didn't exist at deployment. AI systems are trained on architectures whose failure modes aren't yet observable. Cloud dependencies create concentration risks that only become visible when a systemic event occurs. The market learns the lesson after the damage is done.

03

TRANSLATION DEFICIT

Even where risk information exists, it speaks the wrong language. CVSS scores and CVE databases are built for engineers. Risk committees, CFOs, and boards govern in a different language: financial exposure, regulatory liability, business continuity. The gap between those two languages is where most organisational cyber risk lives — unquantified, unpriced, unmanaged.

WE MAP WHAT IT COSTS YOU TO USE IT.

The Hanois Intelligence Practice is the market's first dedicated institutional function for technology adoption risk — built to close the gap the providers left open.

VISIBILITY

We quantify the actual risk field that specific technologies create for specific adopter profiles — in Rands, not theory. Real operating conditions. Real financial exposure.

TRANSLATION

We convert technical risk into governance language: Rand-denominated liability, POPIA penalty exposure, business interruption probability. The right intelligence, for the people who must act on it.

ANTICIPATION

We get ahead of adoption curves. When a technology reaches scale, we produce its risk framework before the breach events that would otherwise teach the market what it needed to know.

The providers built the technology. ***Hanois maps what it costs you to use it.***