INSIGHT SERIES · GOVERNANCE, RISK & HUMAN FACTORS

The Art of Knowing What You Don’t Know

Risk intelligence is not about predicting the future. It is about building the clarity, the signal detection, and the institutional confidence to navigate it.

Author: E van Doorn **Date:** June 2024 · **Topic:** Risk Management

EXECUTIVE SUMMARY

Most organisations are not as good at risk intelligence than they believe. This article argues that risk intelligence — the organisational capacity to detect signals in uncertain environments, interpret them honestly, and act on that interpretation in time — is distinct from risk management and more fundamental to it. Drawing on the 2003 Columbia disaster and Estonia’s 2007 cyber response, it identifies three core dimensions of risk intelligence: clarity (seeing without distortion), signal detection (finding weak signals before they become loud ones), and calibrated confidence (making committed decisions under genuine uncertainty). Organisations that invest in these capacities make different mistakes — smaller, less avoidable, and more instructive.

Introduction

In the summer of 2007, a number of quantitative analysts at major financial institutions began to notice something strange in their models. The mathematics of mortgage-backed securities was producing outputs that rested on assumptions about house prices that had never, in the modern era, been seriously tested. The correlations embedded in the pricing of collateralised debt obligations assumed that regional housing markets behaved more or less independently of one another. They did not. The models were elegant. The signal they were generating — quietly, insistently — was that something was wrong. Almost no one acted on it. This was not, in the main, a failure of intelligence. It was a failure of what might be called risk intelligence — the organisational and individual capacity to detect signals in uncertain environments, to interpret them with appropriate confidence, and to translate that interpretation into action before the cost of inaction becomes unbearable.

> *"Risk intelligence is a different thing from risk management. Risk management is a process. Risk intelligence is more fundamental — the capacity that makes risk management possible."*

The Signal and the Noise

The problem of risk intelligence begins with epistemology — with how we know what we know, and how we know the limits of what we know. In risk environments, the fundamental challenge is not the absence of information. It is the presence of too much of it, most of it irrelevant, some of it actively misleading, and a small but critical portion of it genuinely important. The capacity to distinguish the signal from the noise is the foundational skill of risk intelligence, and it is far harder than it appears. Cognitive research — accumulated over decades and summarised most accessibly in the work of Daniel Kahneman — has established that human judgment under uncertainty is systematically biased in ways that are predictable, consistent, and largely immune to good intentions. We overweight recent experience. We seek confirmation of what we already believe. We are, in short, poorly designed for the kind of cold, probabilistic reasoning that genuine risk intelligence requires.

How Biases Undermine Risk Assessment

These biases are not merely academic curiosities. They have direct and documented consequences for the quality of risk assessment. An organisation that has never experienced a major cyber incident tends, systematically, to underweight the probability of one. A risk committee told for three consecutive quarters that a particular exposure is stable will find it harder to take seriously the analyst who says it has quietly changed. A board that has had a good run is structurally inclined toward overconfidence in the quality of its own judgment. The first task of risk intelligence is to build awareness of these biases into the risk assessment process itself — not to eliminate them, but to design processes that counteract them systematically.

> **Key Point:** The organisations with the most sophisticated risk intelligence are almost invariably those that have learned to distinguish between good decisions that led to bad outcomes and bad decisions that happened to lead to good ones — and to ask consistently which kind they are making.

Three organisational patterns consistently undermine risk intelligence before a crisis arrives:

- Optimism bias: assessors who are invested in a project systematically resolve ambiguous signals in its favour and interpret contrary evidence with a rigour that favourable evidence never faces.
- The normalisation of deviance: organisations that have managed to avoid the consequences of a known risk for an extended period revise their assessment of that risk downward not because the risk has diminished, but because the catastrophe has not yet arrived.
- False precision: expressing a risk as probability suppresses the uncertainty that is itself the most important piece of information and creates a spurious sense of analytical rigour.

Three Dimensions of Risk Intelligence

Risk intelligence has three core dimensions, each necessary and nonsufficient on its own. Clarity is the capacity to interpret data in ways that are honest about uncertainty, free from motivated reasoning, and appropriately sceptical of the models through which data is processed. Signal detection is the capacity to see early — to identify the patterns that precede consequential events before those events have announced themselves. And calibrated confidence is the capacity to make committed decisions under conditions of genuine, irreducible uncertainty. Together, they describe what it means for an organisation to be genuinely equipped to navigate a complex and rapidly changing risk environment.

A practical programme for improving risk intelligence in any organisation rests on five commitments:

- Invest in calibration by building into risk processes the regular, honest comparison of past predictions with actual outcomes not to assign blame, but to identify where assessments are systematically biased.
- Formalise the search for weak signals through horizon scanning, scenario analysis, and red team exercises as recurring, resourced activities not one-off projects commissioned after a crisis has begun.
- Protect the people who raise uncomfortable signals. In most organisations, consistent identification of risks others prefer to ignore is not rewarded. Risk intelligence requires the structural protection of exactly this kind of dissent.

Case Study I: The Intelligence That Was There — NASA and Columbia

On the morning of February 1, 2003, the Space Shuttle Columbia disintegrated during re-entry. All seven crew members were killed. The proximate cause was a piece of foam insulation that struck the shuttle's left wing during launch, damaging the thermal protection system. The foam strike had been observed. Engineers were aware of it. Their concerns were filtered through a decision-making process that systematically downgraded their significance. The Columbia Accident Investigation Board did not describe the disaster as a failure of technical knowledge. It described it as a failure of risk intelligence — of the structures and culture that should have allowed a weak but genuine signal to travel upward and be acted upon.

The Board identified what it called "the normalisation of deviance" — the gradual acceptance of known anomalies as tolerable because they had not previously produced catastrophe. This is one of the most important insights in the literature on organisational risk intelligence: that success is a poor teacher. Organisations that have managed to avoid the consequences of a risk for an extended period tend to revise their assessment of that risk downward — not on the basis of new evidence that the risk has diminished, but on the basis of the absence of adverse outcomes. In risk intelligence terms, this is a failure of calibration, and it tends to recur in precisely the places that should know better.

Case Study II: The Signal That Was Heard — Estonia's Digital Resilience

In April and May of 2007, Estonia was subjected to coordinated cyberattacks targeting government ministries, parliamentary systems, banks, and media organisations — widely attributed to actors associated with Russia in the context of a political dispute over the relocation of a Soviet-era war memorial in Tallinn. These attacks represented the first major test of a nation-state's digital infrastructure under coordinated assault. Estonia not only survived; it recovered rapidly, maintained essential services, and emerged from the experience with its digital infrastructure substantially more robust.

What Estonia had was risk intelligence infrastructure. It had invested in its Computer Emergency Response Team (CERT-EE) as a genuinely capable, well-resourced organisation with clear decision rights and direct lines to government. It had scenario-planned for exactly this class of attack and pre-established relationships with European and NATO partners that could be activated quickly. Its response was not improvised under pressure — it was the realisation of investments in clarity, signal detection, and decision-making process that had been made when the environment seemed calm enough to make investment seem unnecessary. The paradox of risk intelligence is that the best time to build it is precisely when it seems least urgent.

Confidence Under Uncertainty: The Decision-Maker's Dilemma

There is a final dimension of risk intelligence that is perhaps the most underappreciated: the capacity to make confident decisions under conditions of genuine, irreducible uncertainty. This is distinct from the capacity to assess risk accurately. It is the capacity to act on that assessment — to convert an honest acknowledgment of what is not known into a timely, committed decision. Genuine intellectual honesty about uncertainty can become, in practice, a form of paralysis. An organisation that has truly internalised the limits of its own knowledge may find itself unable to act, waiting for a level of certainty the environment will never provide. This is not risk intelligence. It is risk anxiety — a different pathology, but a pathology nonetheless.

The resolution lies in what decision theorists call calibrated confidence: the ability to hold uncertainty and commitment simultaneously. A calibrated decision-maker is not someone who is certain they are right. They are someone who has assessed the available evidence honestly, acknowledged what they do not know, formed a view about the most probable outcome, and made a decision coherent with that view — while remaining genuinely open to revising it as new information arrives. This requires a culture in which it is acceptable to say "I think this is the most likely outcome, but I hold that view

with significant uncertainty," and in which that honesty is met with engagement rather than a demand for false confidence. The great enemy of calibrated confidence is the institutional demand for certainty that most large organisations impose on their decision-makers — driving the false precision that distorts clarity, suppressing the honest acknowledgment of what is not known, and producing decisions that look confident but are merely unreflective.

Conclusion

Risk intelligence is not a capacity that can be purchased or installed. It cannot be outsourced to a consulting firm or delegated to a risk function, though both can help. It must be cultivated — in individuals, through the development of genuine probabilistic thinking and honest self-assessment; in organisations, through the structural and cultural changes that make clear sight possible; and in leaders, through the kind of intellectual humility that can hold uncertainty and commitment in the same hand. The organisations that are best at this do not make fewer mistakes. What they do is make different mistakes — less catastrophic, less avoidable, and more instructive. In a world where the pace of change makes prediction increasingly unreliable, and where the complexity of interconnected systems makes the consequences of risk increasingly difficult to contain, that capacity is not merely useful. It is the defining strategic advantage of the next generation of institutions. Uncertainty cannot be eliminated. The ability to navigate it intelligently can be built.