Kubus

The cost of the coverage you don’t have

An operational risk briefing for IT leaders

The gap between what enterprise IT teams are accountable for and what they can realistically cover has never been wider.

Estates have grown: more sites, more cloud services, more connectivity dependencies, more devices outside the office. Headcount has not grown in the same proportion. Cyber obligations have expanded faster than most internal teams can resource them, and budgets have remained flat or shrunk in real terms.

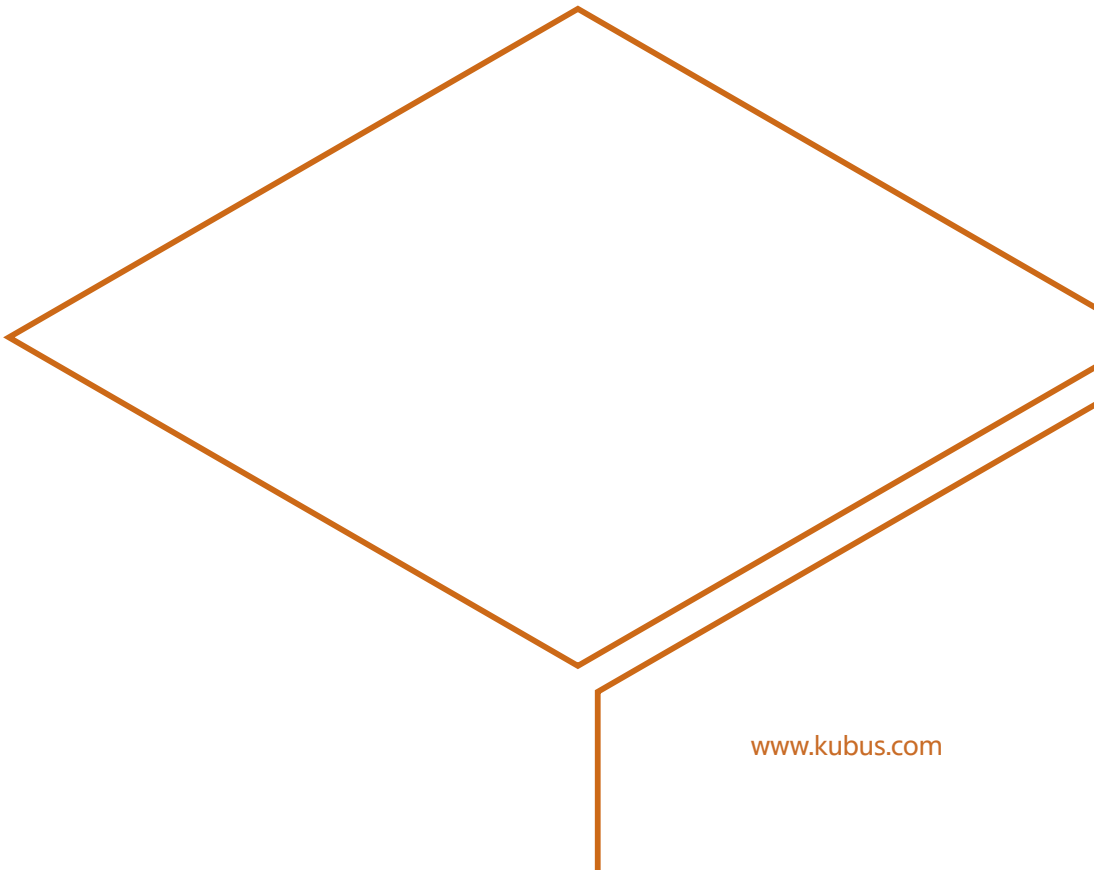
Most IT Directors recognise this condition instinctively, even if it has never been described in these terms: the organisation is already running a managed service. It was simply never designed as one.

No board decided to run monitoring only during office hours, or to make a single engineer the only person who understands a critical firewall configuration. These arrangements accumulated, incident by incident, hire by hire, until they became the operating model by default.

The question worth asking is not whether the organisation has a managed service. It already does. The real question is whether coverage has kept pace with accountability, or quietly fallen behind it.

What appears to be a lower-cost operating model often hides its largest costs.

Four indicators make that gap visible. Each is usually tracked on its own. Read together, they describe the same widening distance between what the organisation is accountable for and what it actually covers.



Where the cost actually sits

Each of the following is usually tracked in a different part of the organisation. Seen together, they are the same gap, measured from four angles.

The cost of unplanned downtime is well documented and consistently understated inside IT budgets, because it rarely lands as an IT cost. It lands in missed delivery dates, and in the assumption that Tuesday morning was simply lost to a switch failure.

Over 90%

of mid-size and large organisations put the cost of one hour of downtime above £240,000.

Source: ITIC, Hourly Cost of Downtime Survey

Unmeasured, this cost does not disappear. It resurfaces at budget time, unexplained.

Recruitment is the second, quieter driver, and it does not correct itself. IT and data skills have been the hardest category to recruit in the UK for five consecutive years, according to ManpowerGroup's UK Talent Shortage Survey. Every unfilled specialist role becomes coverage that someone already on the team absorbs, until the person who joined two years ago is the only one who fully understands a piece of the estate, and every leave request runs through them first. Coverage that depends on named individuals is not resilient, however capable those individuals are, and it rarely appears on a risk register because no one has been asked to write it down.

Cyber exposure has moved from an IT concern to a board one.

65%

of medium and 69% of large UK organisations reported a breach or attack in the past year. Only 25% hold a formal incident response plan.

Source: UK Government, Cyber Security Breaches Survey 2025/2026

That is the question insurers and auditors now ask first: not whether a breach occurred, but whether the response was rehearsed or improvised.

The same pattern shows up in costs that never reach a spreadsheet: the strategic project delayed because the team spent the sprint on an unplanned recovery, and the specialist contractor brought in at short-term rates because the gap could not wait for a normal recruitment cycle. Neither appears in the IT budget. Both appear in finance, and in delivery timelines that quietly slip.

Coverage that falls behind accountability doesn't save money. It simply moves the cost somewhere the IT budget doesn't reach.

Coverage by design, not by accumulation

Organisations that close this gap share a small number of characteristics, and none of them are about the size of their technology budget.

Organisations operating by design have clarity on:

Ownership

what the internal team owns and what a partner owns, without ambiguity at the boundary

Monitoring

where visibility begins and where it stops

Escalation

how an incident escalates and who is accountable at each stage

Accountability

a division of responsibility that can be explained to a board without hesitation

Out-of-hours coverage

hat happens when the office is empty

Kubus

By Default	By Design
Knowledge held by individuals	Knowledge retained by the organisation
Reactive recovery	Predictable resilience
Hidden operational cost	Planned operational investment
Implicit accountability	Explicit accountability
Coverage assumed	Coverage confirmed

Done well, this strengthens the internal team rather than displacing it. A co-managed structure removes out-of-hours load and the specialist gaps that no reasonable headcount plan can close, while leaving ownership and decision-making with the people who understand the organisation. The IT Manager keeps the estate. The IT Director gains a defensible answer to the questions a board will eventually ask.

The issue is not whether an organisation can afford managed support. Most already fund one, informally, through recovery time, unplanned specialist spend and the quiet cost of a team permanently working behind.

The first step is not a decision about outsourcing. It is an accurate account of the model already carrying the organisation, something most IT Directors have never seen assembled in one place. An operational coverage assessment provides exactly that: a structured view of where accountability already exceeds coverage, with no commitment attached and no sales conversation involved.

To arrange an operational coverage assessment,
contact your Kubus account team.

T: +44 1285 771600

E: sales@kubus.com