Cybersecurity is still treated like an IT problem, and that’s a problem.

Walk into a lot of organisations, and you'll find security buried somewhere under infrastructure, sitting alongside helpdesk tickets and patch cycles. It's seen as necessary. Expensive. Occasionally annoying. But rarely strategic.

And yet, when something goes wrong, it doesn't stay in IT for long.

It lands in the boardroom.

Cybersecurity is governance, whether you like it or not

There's a persistent misconception that cybersecurity is about tools. Firewalls. Endpoint protection. Identity platforms. All important. None sufficient.

Cybersecurity, in practice, is about risk. Business risk.

Who owns it?
Who understands it?
Who is accountable when it fails?

Those are governance questions.

If the board doesn't actively govern cyber risk, the organisation isn't managing it, it's hoping the technical team can contain it. That's not a strategy. It's wishful thinking dressed up as delegation.

And it rarely holds up under pressure.

I've seen well-funded security teams struggle because they lacked clear direction from leadership. No defined risk appetite. No agreed priorities. Plenty of tools, but no mandate to make hard trade-offs.

So they defend everything. Which means, in reality, they defend nothing particularly well.

What "hand in hand" actually looks like

The phrase gets thrown around a lot. Governance and cybersecurity must align. Sounds sensible. But what does that mean on a Tuesday morning?

It's less about frameworks and more about clarity.

Clear reporting lines matter. The board (or a relevant committee) should receive regular, structured updates on cyber risk, not just incident reports, but forward-looking assessments. What's changing? Where are we exposed? What are we choosing to accept?

Risk appetite isn't a document you write once and forget. It's a working agreement. How much disruption can the business tolerate? How much data exposure is unacceptable? These aren't technical decisions. They're business decisions.

And then there's accountability.

Not shared accountability. Not vague ownership. Real, named responsibility.

- The board owns oversight of cyber risk.
- Executives translate that into operational priorities.
- Technical leaders implement and report back without sugarcoating reality.

If any of those links are weak, the whole chain fails.

Why this matters more than most think

Many organisations only connect governance and cybersecurity after an incident. By then, the conversation is very different.

It’s no longer about risk tolerance. It’s about damage control.

When governance and cybersecurity work together from the outset, the benefits show up in ways that are hard to ignore.

Reputation holds.
Customers stay.
Regulators ask fewer uncomfortable questions.

Investors notice, too. Not because they expect perfection, but because they value predictability. A well-governed organisation signals that risks are understood, not ignored.

There’s also a quieter benefit: better decisions.

When boards engage meaningfully with cyber risk, funding conversations improve. Priorities sharpen. The business stops chasing shiny tools and starts investing where it actually matters.

And operationally? Things break less often. Or when they do, recovery is faster, more controlled, less chaotic.

The uncomfortable truth

You can’t outsource accountability.

You can outsource services. You can bring in consultants. You can invest heavily in technology. But governance stays where it belongs, at the top.

Some boards resist this. It feels too technical. Too detailed. Too far removed from strategy.

But that’s the point.

Cyber risk is already part of your strategy. It affects revenue, reputation, compliance, and continuity. Ignoring it doesn’t simplify things. It just shifts the risk somewhere less visible.

Usually until it’s too late.

A shift worth making

Treat cybersecurity as a governance issue first, a technical issue second.

That doesn’t mean boards need to become security experts. It means they need to ask better questions. Demand clearer answers. And be willing to make informed trade-offs.

Because in the end, strong cybersecurity isn’t built on tools alone.

It’s built on decisions.

And decisions are what governance is all about.