The Cost of Silence: Why CFOs Can't Ignore Cyber Risk

value through insight™

CYBER RISK HAS TRAVELLED A LONG WAY FROM THE SERVER ROOM.

It now sits in the places CFOs worry about most: cash flow, customer confidence, continuity, compliance, enterprise value and the ability of the business to keep moving when something goes wrong.

That is why the old separation between “IT risk” and “business risk” no longer works. A serious cyber incident can stop trading, delay production, expose sensitive data, pull leaders into legal and regulatory action, disrupt suppliers and damage trust with customers. It can also create sudden, unplanned cost at exactly the moment the business has the least control.

The real danger is not only the attack itself. It is the quiet confidence around it. The belief that existing insurance cover is enough. That the continuity plan still reflects reality. That suppliers are ready. That the organization could recover inside the same timeframes it modelled a year ago.

Paul Gravatt, ERA Group’s risk and insurance specialist, describes cyber as one of the biggest global threats from a risk and insurance perspective. This is no longer about isolated individuals causing disruption from behind a laptop. Increasingly, cybercrime is organized, politically motivated and highly sophisticated.

That changes the conversation. Cyber is not just a technical problem. It is a financial exposure. And the cost of getting it wrong rarely arrives neatly in one line on a budget.

The Opportunity Inside the Risk

The latest UK Cyber Security Breaches Survey underlines the scale of the issue. In 2025/26, 43% of businesses reported a cyber breach or attack, with phishing alone affecting 38%. In total, the survey estimates that around 612,000 UK businesses identified at least one breach or attack during the year.

That is the uncomfortable backdrop. But this is not only a story about rising threat. It is also a story about timing.

Paul's view is that while the severity and visibility of cyber-attacks have increased, many organizations are also becoming more resilient. In parts of the market, cyber premiums have been moving down, which creates a practical window for businesses to review whether stronger cover, higher limits or wider protection may now be more accessible than before.

For CFOs, that does not mean buying cyber cover in isolation or simply adding another cost line. It means looking at the organization's total cost of risk and asking a better question: could savings in other areas of insurance, supplier cost or operational spend be used to fund stronger cyber resilience?

When people picture cyber risk, they often picture ransomware such as locked systems, frozen screens, halted trading and a demand on the table. That happens, of course. But the more painful cost is often found somewhere else entirely.

It shows up when invoices cannot be raised, orders cannot be processed and customers cannot be served. It appears when production lines stop, stock cannot be replenished, emergency suppliers are brought in at premium rates and leadership teams lose days to legal, regulatory and communications work. Even after systems are restored, the reputational damage can keep running.

This is where the conversation has to move beyond cybersecurity and into business continuity.

Paul makes the point that wider supply chain disruption has changed the recovery picture. Replacing equipment, sourcing building materials or replenishing stock can now take longer than many businesses assume. A recovery plan that looked sensible a year ago may already be out of date. Business interruption insurance needs to be tested against that reality, particularly around indemnity periods and the true length of time a business may need support.

A business may have cover, but is it enough? It may have a recovery plan, but does it still hold up? It may have modelled downtime, but has it modelled the current supply chain? It may assume replacement equipment will arrive in weeks, but what happens if it takes months?

The cost of silence is often hidden in those assumptions.

Cyber Risk Does Not Stay in Its Lane

Azunna Anyanwu, ERA Group consultant in the US, adds an important lens. For CFOs, the cost of cyber risk is not only financial. The financial impact is often the visible result of failures somewhere else: reputation, operations or compliance.

That matters because the damage does not stop once the technical issue is contained.

Reputation risk is one of the hardest areas to price properly, and one of the easiest to underestimate. A breach can damage the organization's brand, public image, stakeholder confidence and customer trust. Those effects can then become very real financial consequences like lost revenue, weaker retention, higher acquisition costs and lower enterprise value.

This has become sharper as ransomware groups increasingly use stolen data as leverage. The threat is not always "pay us or your systems stay down." It can become "pay us or we publish what we found." Azunna describes this as "big shame hunting", where public exposure of sensitive information becomes the pressure tactic, rather than operational disruption alone.

Operational risk can be quieter, but just as damaging. It is the failed process, the unavailable system, the compromised email account, the partner issue that suddenly becomes your issue. Business Email Compromise and misdirected vendor payments are good examples because they do not always look dramatic from the outside. A payment is sent to the wrong place, a supplier process fails, money leaves the business, and the impact is painfully real.

The supply chain point matters too. A business does not need to be the direct target to feel the cost of a cyber incident. If a key supplier, logistics partner, technology provider or outsourced process is compromised, the disruption can land quickly on your own revenue, service delivery, workforce productivity and customer commitments.

Then comes compliance. Cyber incidents can trigger legal duties, regulatory scrutiny, contractual obligations and sector-specific standards. Failure here can create unplanned liabilities, legal expenses, settlement costs and, in regulated industries, the loss of future business opportunities.

For US organizations, that governance angle is becoming harder to ignore. Public companies are operating under SEC cybersecurity disclosure rules that require material cybersecurity incidents to be disclosed on Form 8-K within four business days of determining materiality, alongside annual disclosure on cyber risk management, strategy and governance.

The financial exposure is also stark. The FBI's Internet Crime Complaint Center received 859,532 complaints in 2024, with reported losses topping $16.6 billion.

What CFOs Should Be Asking Now

The right cyber conversation does not start with software. It starts with exposure.

A CFO does not need to know every technical detail of the cyber environment, but they do need to understand what a serious incident would do to the business financially, operationally and commercially.

What would happen if systems were unavailable for a week? Which revenue streams would stop first? Could invoices still be raised? Could payroll still run? Which suppliers would become critical immediately? Would insurance respond in the way the business expects? Are indemnity periods long enough? Are cyber limits realistic? Is the organization exposed through a third party? Has anyone tested the assumptions sitting behind the recovery plan?

Those questions are not designed to create panic but to create visibility.

Visibility gives CFOs choices. It allows them to challenge cover, review suppliers, improve continuity plans, strengthen contractual protection and decide where investment is genuinely needed. It also allows them to look across the wider cost base and identify where savings could fund better resilience without simply adding more cost to the business.

How ERA Group Can Help

ERA Group helps organizations look at cyber risk through a commercial lens.

We do not replace internal IT teams, CISOs or technical cyber specialists. That is not the role. Our work sits alongside them, helping CFOs and leadership teams understand the financial, operational, insurance and supplier-side implications of cyber risk.

That can mean reviewing cyber insurance and the total cost of risk, benchmarking the market, testing limits and exclusions, and identifying whether savings in other insurance lines could be used to strengthen cyber protection.

It can also mean looking at business interruption cover and continuity planning together, rather than treating them as separate exercises. If recovery timelines have changed because of supply chain pressure, equipment availability, supplier dependency or operational complexity, the insurance programme needs to reflect that.

On the technology side, ERA can help organizations understand where cloud and IT spend is going, whether billing is structured effectively, and where costs may be optimized without compromising resilience.

Supplier and contract review is another critical part of the picture. Cyber risk often travels through third parties, so it is important to understand which suppliers are critical, what responsibilities sit in the contract, whether service levels are clear, and whether cost increases or risk transfer arrangements are reasonable.

The goal is not to frighten businesses into spending more. It is to help them spend better.

ERA helps clients find value across their cost base so they can strengthen resilience without treating cyber as just another unavoidable cost.

Let's Talk

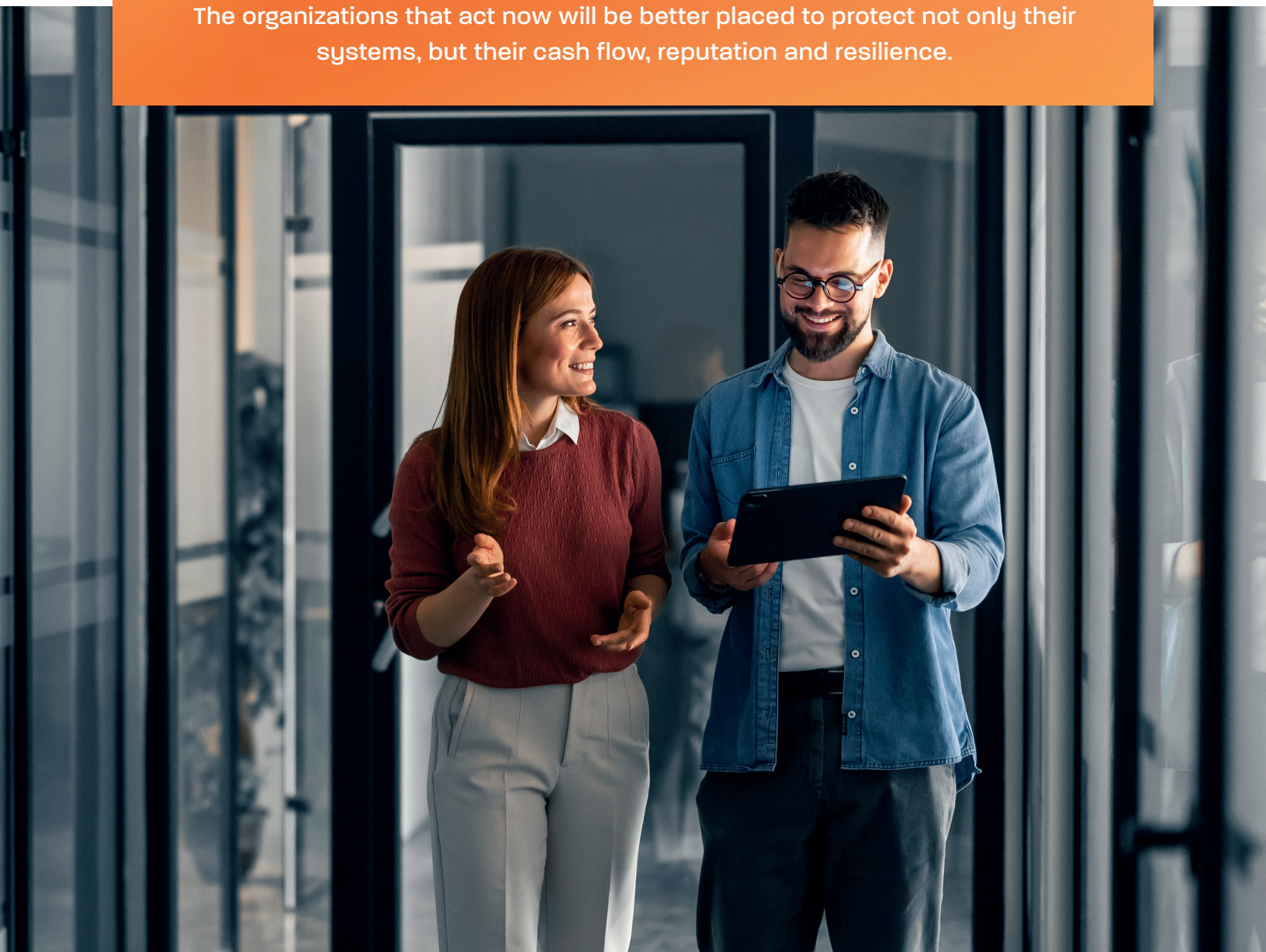
Cyber risk is not going away. It is becoming more sophisticated, more connected to supply chains and more visible to regulators, insurers, customers and investors.

For CFOs, the danger is not just that something happens. The greater risk is discovering too late that the business did not understand the cost of what could happen.

The cover was too narrow. The indemnity period was too short. The supplier exposure was greater than expected. The cloud environment was more complex than anyone realized.

The cost of silence is already sitting in risk registers, insurance schedules, supplier contracts, cloud bills, payment processes and continuity plans.

The organizations that act now will be better placed to protect not only their systems, but their cash flow, reputation and resilience.



Want to know more?
eragroup.com

value through insight™