Teneo®

Insights

The New Executive Agenda: Six Strategic Cyber Risk and Resilience Trends to Expect in 2027

October 2026



Leading Through Disruption: When the Departure Board Changes

Recently, whilst sitting in an airport waiting for a flight, the departure board quietly changed from "Boarding" to "Delayed."

Nothing dramatic happened. The aircraft was still sitting outside the terminal window. Some passengers glanced up from their phones and a few headed towards the gate desk looking for more information, but there was not much information to give.

That uncertainty changed the nature of the situation. Would passengers miss connections? What would it mean for the aircraft's next journey and crew? At what point should the airline stop waiting for the original plan to recover and put an alternative into action?

For anyone who works in cyber, the parallel is familiar.

When an organisation first detects unusual activity, it rarely has a complete picture. It may know that something is wrong. Systems may have been taken offline or access restricted as a precaution. But the leadership challenge begins before the picture is complete. Clients still need to be served. Employees need to work. Regulators may need to be informed. Communications, legal, operational and financial decisions cannot wait for perfect certainty.

At the airport, the question quickly stops being simply, *why is the aircraft delayed?*

It becomes: *what do we do while we do not yet know?*

The same is true of a cyber incident.

The technical investigation is critical. But resilience is demonstrated by what the organisation can do while that investigation is still under way, i.e. how it keeps critical services moving, establishes reliable facts, makes decisions and adapts as the picture changes.

That is why cyber resilience has become a leadership issue.

This shift is reflected in the UK's cyber landscape. The Financial Conduct Authority (FCA), National Cyber Security Centre (NCSC) and Bank of England continue to reinforce expectations around operational resilience, requiring firms to demonstrate that they can continue operating through disruption. Increasingly, boards are expected not only to approve cyber strategies but to evidence effective oversight, challenge management decisions and understand the risks associated with the changing threat landscape.

Against this backdrop, future cyber and resilience trends may not be defined by technology alone, but by how boards and management lead through disruption, change and uncertainty.

1. Cyber is Now a Leadership Issue

Cyber response is becoming an enterprise leadership discipline, not an IT escalation process.

Many incidents still begin with something technical. What has changed is the range of business decisions that follow across operations, customers, disclosure, transactions, reputation and enterprise value.

As AI systems become more deeply connected to organisational technology and data, the decision environment becomes harder. For leadership teams, the implication is not simply "more AI risk." It is that the speed at which assumptions become unreliable is increasing.

In 2027, we anticipate organisations will increasingly design incident response around enterprise decision-making, not just technical containment. The trend to watch is what executives do when the event is live.

If a significant incident happened tomorrow, would the leadership team know who decides what and on the basis of which facts?

2. Readiness Beats Documentation

Resilience will be judged by rehearsed decision-making under pressure, not by the existence of a plan.

At the airport, nobody appeared to be inventing the response after the delay occurred. Engineers, operations teams and customer-facing staff knew their roles. The event was unexpected. The response was not.

That is perhaps the simplest definition of operational readiness. Resilient organisations do not succeed because they correctly predict every incident. They succeed because they have prepared people to make decisions when a scenario they did not predict occurs and, therefore, to respond effectively.

UK firms in scope of the operational resilience regime were required by 31 March 2025 to remain within impact tolerances for important business services in severe but plausible scenarios. The FCA's 2026 review continues to emphasise testing and remediation. The Digital Operational Resilience Act (DORA) has applied across the EU financial sector since January 2025, embedding Information, Communications and Technology (ICT) risk, testing, incident management and third-party resilience into the operating model.

The next deadline is already visible: from 18 March 2027, new FCA, Prudential Regulation Authority (PRA) and Bank of England rules will standardise reporting of material operational incidents and material third-party arrangements.

Therefore, the differentiator in 2027 will increasingly be decision readiness rather than documentary readiness. A resilience plan that nobody has rehearsed is not so different from a safety card nobody has read.

3. Cyber Belongs Inside Every Deal

Cyber risk should be treated as a deal-value and execution issue from diligence through separation or integration.

Now imagine that the disruption affecting the aircraft cannot be resolved quickly. The airline cannot simply suspend all operations. It needs to consider alternatives and mitigations while it works out what to do next. Passengers still need to reach their destinations. Crews are scheduled elsewhere. People require updates. Resources have to be reprioritised across the wider network.

The plan has changed. The operation continues.

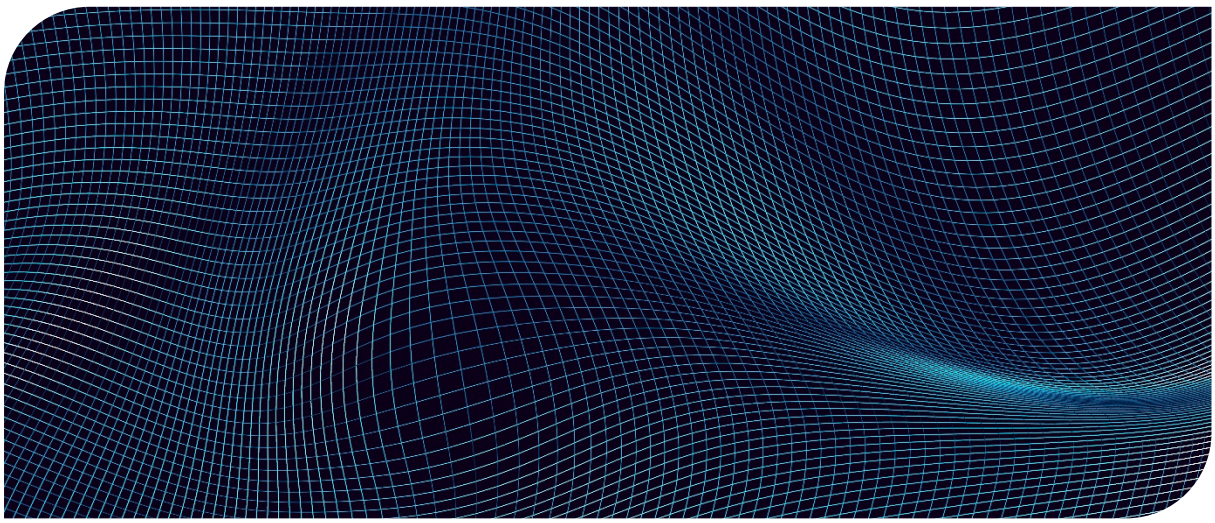
That is much closer to acquisitions, divestitures and restructurings, where there are changes to ownership, systems, suppliers, people and access rights while the business keeps running. Cyber risk is also moving with those dependencies.

In practice, that can mean testing whether a target has unmanaged privileged accounts before signing; determining whether a carved-out business can operate securely on Day One without the seller's identity or security tooling; or preserving monitoring and incident-response capability while a restructuring changes suppliers and teams.

UK investment-security guidance encourages a security-minded approach from the start of investment activity, including cyber protections and due diligence.

Like rerouting passengers across an airline network, a change in one area can create an unexpected dependency somewhere else. In 2027, cyber resilience may increasingly be treated as part of transaction and restructuring execution itself through protecting value, maintaining continuity and understanding which risks are being inherited, separated or created by the deal.

The deals remembered for the wrong reasons are often those where something assumed to be protected turns out not to be.



4. Transformation Is a Resilience Opportunity

Transformation should be used to design out accumulated cyber risk rather than migrate it into the next operating model.

Where restructuring is change forced on a business, transformation is change a business chooses and that difference is the opportunity. A delayed flight may force the airline to rethink its plan, but the objective doesn't change, which is to get passengers to their destination. Transformation gives organisations a similar chance to reconsider how they reach theirs, on their own terms.

The PRA has noted that multi-year digital transformation programmes can introduce execution and concentration risks that require proactive board oversight.

The 2027 timing matters because when businesses are already redesigning operating models, technology platforms and supplier relationships, they have an opportunity to address risks that have built up over years as well as the new risks created by emerging technologies.

The point isn't predicting exactly when that risk materialises. It's not building tomorrow's organisation entirely on yesterday's assumptions. It is about securing the future, not just fixing today.

It is about understanding that every transformation programme leaves behind an organisation that is either more resilient or more fragile than the one it started with. Rarely does it leave things unchanged.

5. Forensics Is Now Executive Intelligence

The value of forensics is increasingly the speed at which it turns uncertainty into decision-grade facts.

Eventually, someone needs to determine what caused the original aircraft fault. Was it a one-off issue? Does a component need replacing? Is there a wider problem affecting other aircraft? The answers shape every decision that follows.

The same logic applies to cyber incidents and corporate investigations. During a major incident, executives rarely lack information. They lack reliable information and that matters when deciding whether to isolate systems, notify regulators, communicate with customers or restore operations.

The National Institute of Standards and Technology (NIST)'s 2025 incident-response standard reflects this shift by integrating incident response across cybersecurity risk management rather than treating it as a stand-alone technical activity. The UK's 2027 operational-incident reporting regime will further increase the premium on timely, consistent facts about impact and recovery.

Indeed, disruptive technologies like AI can help analysts search evidence faster, but speed must not come at the expense of provenance. In regulatory, board or legal contexts, findings should still be traceable and open to human challenge.

In 2027, the organisations that move quickly from assumptions to facts are likely to be better positioned to make decisions about containment, disclosure, client communications, litigation, insurance, remediation and recovery.

Resilience is not about having perfect evidence. It is about having evidence that remains credible when tested under pressure.

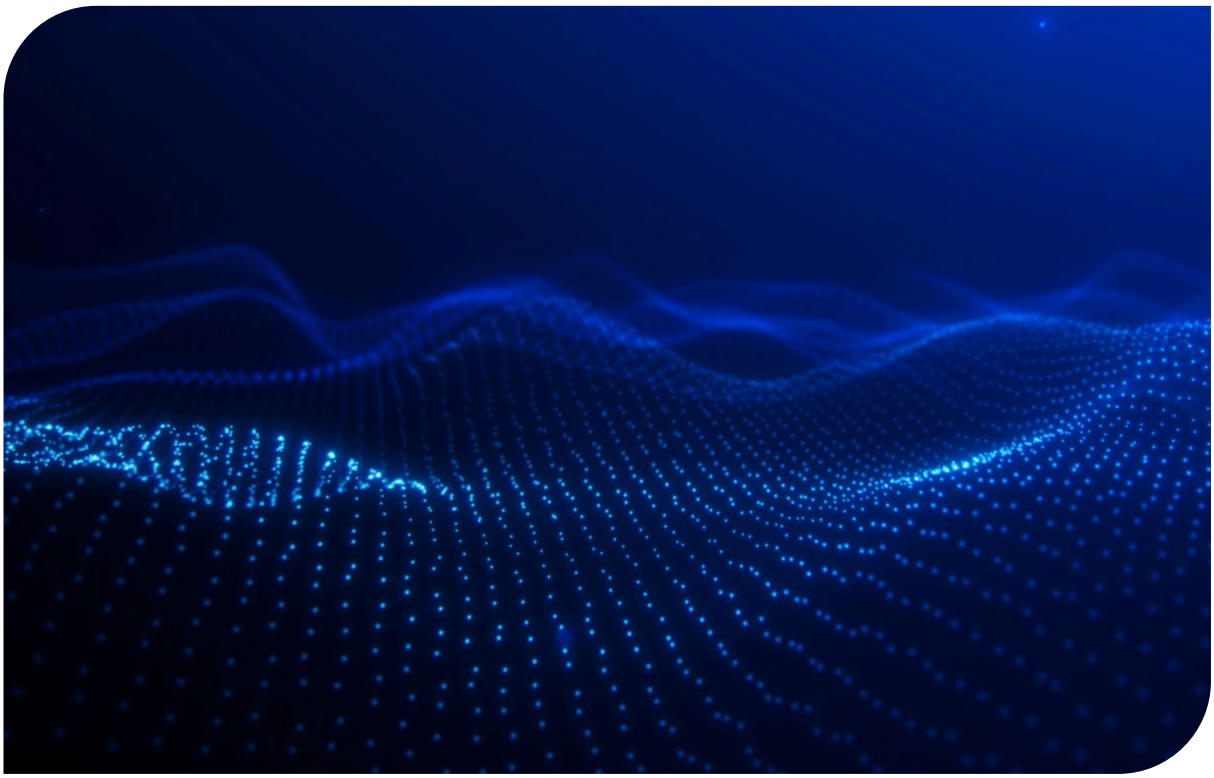
6. Governance Is the Real Differentiator

Governance determines whether cyber risk is understood, owned, assured and connected to enterprise risk before a crisis begins.

Passengers do not expect an airline's CEO to repair an aircraft. Nor should boards become cybersecurity engineers. They have a critical role in ensuring that the organisation understands its critical dependencies, sets risk appetite, challenges management and has credible assurance that resilience measures work.

This is distinct from leading an incident. It is the system of accountability that exists before an incident. NIST Cybersecurity Framework (CSF) 2.0 added "Govern" as a sixth core function, explicitly positioning cyber as enterprise risk, while the UK Cyber Governance Code of Practice sets out board actions across risk management, strategy, people, incident response and assurance.

In 2027, organisational resilience will increasingly depend on boards understanding what matters most, how much disruption the business can tolerate and whether they have the evidence to demonstrate their ability to adapt under uncertainty.



The CEO Agenda for 2027

The departure board mattered because it did not simply describe a technical fault. It changed the journey.

Organisations will increasingly be judged in the same way. Disruption cannot always be prevented, but stakeholders expect an organisation to know what is critical, establish the facts quickly and make credible decisions when circumstances change.

For CEOs and boards, three questions should frame the 2027 agenda:

- If a major cyber event began tomorrow, are our decision rights, escalation paths and communications sufficiently rehearsed to operate before the facts are complete?
- Across our deals and transformation programmes, where are we creating, inheriting or concentrating cyber and resilience risk?
- What evidence gives the leadership confidence that our critical services can remain within tolerable disruption levels, including when a key technology or third party fails?

This is where Teneo's multidisciplinary model matters.

A cyber incident may begin as a technical event, but its consequences can extend across operations, regulation, reputation, transactions, restructuring and enterprise value. Teneo connects those dimensions, helping leaders establish decision-grade evidence, protect value through transactions and change and convert lessons into a more resilient organisation.

The departure board will change again. But these defining questions can help leadership understand their tolerance levels under uncertainty, protect what matters and keep the organisation moving towards its destination.

Teneo's Cyber Team

Authored by Sabika Ishaq, with support from Teneo's Cyber team.



Serdar Cabuk
Senior Managing Director



Sabika Ishaq
Director



Micheal Conway
Director



Lara Pace
Associate Director

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance and ESG.

The firm has more than 1,800 employees located in 50+ offices around the world.

teneo.com

© 2026 Teneo. All rights reserved. This material was produced by Teneo for use solely by the recipient. This communication is intended as general background research and is not intended to constitute advice on any commercial investment or trade matter or issue and should not be relied upon for such purposes. The views expressed here represent opinions as of this date and are subject to change without notice. The information has been obtained from sources believed to be reliable but no guarantees can be given as to its accuracy, completeness or reliability. AI-enabled tools may have been used in the preparation of this report to assist with data analysis, content structuring, and editorial refinement. Where used these tools did not operate autonomously and did not replace expert judgment. All outputs were reviewed, validated, and finalized by the report authors, who retain full accountability for the accuracy and integrity of the work. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or otherwise, without the prior consent of Teneo.