ORGANISATIONAL RESILIENCE *in a* world *of* CHANGING priorities

Skills decay is not an L&D issue – it is a resilience vulnerability, explains regular ISJ Contributor and Managing Director of SSR Personnel, Peter French MBE

Across Europe, boards are increasingly reassessing how risk is understood, measured and governed. While cyber-threats continue to escalate in sophistication and frequency, AI is reshaping business operations faster than most regulatory and governance frameworks can adapt.

Geopolitical fragmentation has exposed weaknesses across supply chains, infrastructure resilience, climate change and operational continuity. Simultaneously, the expansion of European regulation, particularly the Network and Information Security Directive 2, Digital Operational Resilience Act, EU AI Act and the Corporate Sustainability Reporting Directive, have all materially increased C-suite accountability – not fully understood in the boardroom.

Upskilling is often framed as a productivity or employability initiative. In security-relevant and high-consequence environments, it is an operational risk control. In an era of sustained disruption through climate change, geopolitical instability, tech acceleration and workforce pressure, organisational resilience is increasingly determined by people rather than physical assets. Training, skills shortages, and rising levels of burnout and stress are often treated as separate workforce challenges.

Together, these factors form a single resilience system – and executives who do not treat human capability as infrastructure increase their exposure to escalating operational and security risks.

Executive impact of AI adoption

AI is expected to remove routine and repetitive tasks. At the same time, executives are themselves facing growing wellbeing pressures, contributing to a rise in fractional and portfolio careers. This is fuelling an in-house skills experience scarcity as managers find themselves without the human tools that would be in a traditional manufacturing process in place to manage their automation.

In this "5.0 edition" of the Industrial Revolution, the crossover and speed of technology application are outpacing most boards, which is leading to resilience threats. Many security leaders who we interviewed in our 2026 trends report quote that their businesses have an AI governance gap. This is directly fuelling operational and reputational risks. Organisations need to prioritise their controls, such as human oversight and acceptable use policies.

New roles that will need funding will include machine trust auditors and AI compliance officers, both of which are operational. With hefty fines a possibility, the issue is no longer whether organisations use AI but can govern it safely. This is creating a new layer of security leadership roles.

From resilience planning to resilience capacity

For decades, resilience strategies have prioritised infrastructure protection, redundancy and continuity planning. While these remain essential, recent failures across critical national infrastructure, defence-adjacent industries, logistics, healthcare and technology reveal a consistent pattern of breakdowns increasingly originating in human systems rather than technical ones.

> **"Across Europe, boards are increasingly reassessing how risk is understood, measured and governed."**

Delayed decision-making, misinterpretation of information, loss of institutional knowledge and coordination failures are common precursors to incidents. These outcomes are rarely attributable to individual failure – they are systemic effects of skills misalignment and sustained cognitive overload.

Resilience, therefore, is no longer a static property of systems. It is a dynamic capability generated by workforce competence, psychological capacity and leadership effectiveness under stress. Skills erosion is a latent vulnerability from a resilience perspective. Capabilities such as systems thinking, threat assessment, ethical judgment and leadership in ambiguity degrade without deliberate reinforcement. When pressure increases, capability gaps surface abruptly.

The World Economic Forum has highlighted that while many roles remain in name, the new skills required within them are evolving ▸

rapidly. This creates a dangerous illusion of preparedness: organisations appear stable on paper but lack the capabilities required when disruption occurs.

Skill shortages as a structural condition

The assumption that skill shortages are cyclical and self-correcting is increasingly unsupported by the evidence. The challenge is not simply labour availability, but the shortage of complex, hybrid capabilities at speed and scale.

Analysis referenced by the UN International Labour Organization (ILO) founded in 1919, historically shows that skills mismatches persist across advanced economies when technology steps up. Demand is rising for individuals who combine technical expertise with judgement, adaptability and communication – capabilities that cannot be rapidly trained or easily automated.

This creates two critical risks: concentration of knowledge in too few individuals and sustained overload of those individuals. Both undermine organisational resilience and increase exposure to burnout-driven attrition. Key pillars of a retention strategy are a workforce wellbeing strategy, skills development, visible progression pathways, mentoring with corporate champions and making good use of the five generations that are in work today.

Effective mitigation lies not only in recruitment but in building workforce capability in depth, ensuring critical skills are distributed, transferable and routinely exercised. The organisation that retains security talent best will combine competitive pay with development, leadership, flexibility, purpose and clear progression.

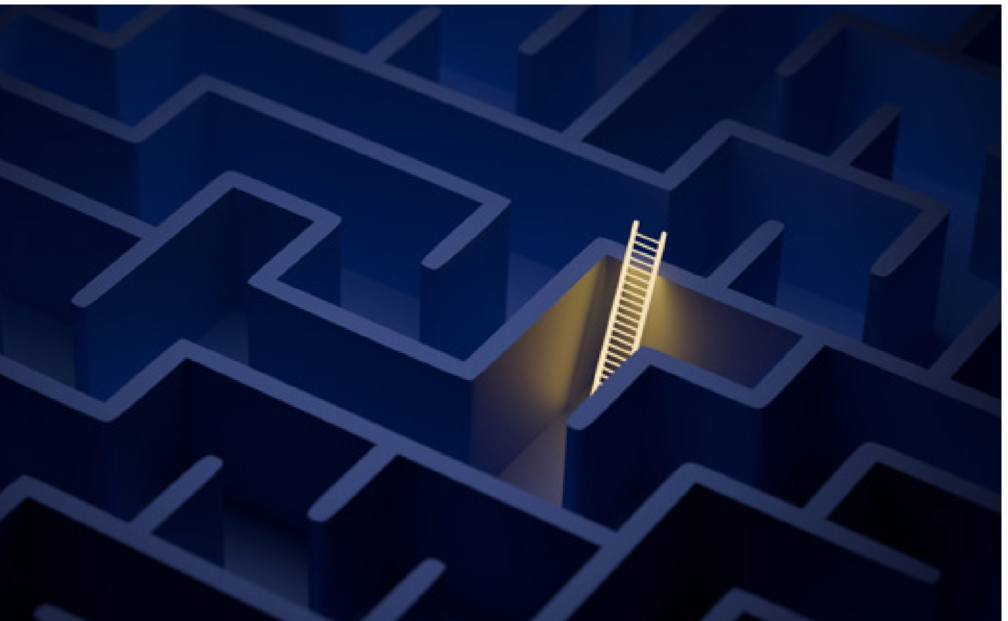
Statista estimated that online authentication and third-party costs for cybersecurity vendors in 2025 reached €49b. By the year 2030, factoring in the cost of online resilience, AI defence, managing unauthorised images, cyber-threats and predicted costs increase to nearly €100b. Managing procurement, performance and return on investment becomes even more important.

> **“Human capability remains largely invisible in traditional assurance frameworks.”**

The question we need to ask is where the CFO can make savings to pay for business-critical services that might quadruple over five years. There are no corners to be cut, but some outsourcing will be required to benefit from pooled security knowledge for many private and public bodies.

Making people visible in resilience assurance

Human capability remains largely invisible in traditional assurance frameworks. Where physical and digital assets are measured precisely, workforce fragility is assumed and goes unmeasured.



Forward-looking organisations are beginning to track time-to-competence for critical roles, seeking skill redundancy, burnout risk indicators and leadership performance measurement under simulated stress. These metrics provide foresight, enabling intervention before human capability gaps become incidents. Human capability metrics are likely to become standard components of resilience assurance alongside cyber-maturity and third-party security. Tracking these capabilities requires a combination of behavioural, operational and strategic indicators.

The most valuable professionals in the market are no longer defined solely by operational expertise or technical capability. Increasingly, organisations seek leaders capable of integrating physical security, cyber-resilience, intelligence, crisis management, governance and strategic communication into a unified enterprise resilience model. As a result, compensation growth remains strongest among executives able to bridge operational, technical, commercial and regulatory disciplines.

At the same time, the broader European compensation environment has entered a more disciplined phase following the inflation-driven salary acceleration experienced between 2022-2024. Negotiated wage growth across the Euro area moderated during 2025 and is expected to continue easing into 2026 as the military action spike in inflation pressures stabilise, and economic growth softens (European Central Bank).

The UN defines the continent of Europe as 44 countries and a population of 743 million people, of which 350 million people are working. Due to data reliability, our focus is within the EU and UK, which we refer to as Europe, with a working population of 200 million. There is a range of labour costs from €12-€57, which has increased nearshoring arrangements, which is causing disproportional wage growth in countries such as Poland, Portugal, Romania and the Baltic states.

Disruption is now a permanent operating condition. Organisations cannot eliminate uncertainty, but they can determine how effectively they respond to it. ■