THE EVOLVING CYBER SECURITY LANDSCAPE

DECEMBER 2025

Weil

Organisations across the UK, European Economic Area (EEA) and the US are experiencing a sharp escalation in both the frequency and impact of cyber incidents. Threat actors are moving faster, operating more strategically, and targeting vulnerabilities deep within supply chains and critical infrastructure. At the same time, regulatory expectations and insurance requirements are tightening, making cyber resilience a central operational and governance priority. The landscape is becoming more complex, and those who understand these emerging dynamics will be best placed to navigate what comes next.

KEY TRENDS

Over the past year, organisations have seen a pronounced rise in high-impact incidents driven by three dominant forces: (1) the rapid adoption of AI, (2) increased geopolitical instability, and (3) expanding supply chain vulnerabilities. AI now sits at the centre of both attack and defence strategies, with threat actors using AI to accelerate phishing, automate reconnaissance, manipulate audio and video for impersonation, and exploit vulnerabilities at unprecedented speed. Meanwhile, defensive AI is enhancing detection, automating incident responses, and reducing dependencies on human monitoring, widening the gap between prepared and unprepared businesses.

Geopolitical tensions have also fuelled a surge in hacktivism and politically-motivated attacks, while supply chain weaknesses remain one of the most common root causes of exposure. From retail to aviation to manufacturing, the most disruptive incidents this year have stemmed not from core infrastructure failures, but from vulnerabilities in vendors, service providers, and third-party technologies. Attackers are spending longer inside environments, moving quietly and deliberately, and exploiting the “human layer” through increasingly sophisticated social engineering. Collectively, these trends demonstrate that cyber risk now sits at the heart of operational resilience.

Further the rapid expansion of data centres and the growing reliance on outsourced infrastructure introduced additional layers of risk. As capacity increases to meet the demands of AI, cloud acceleration and digital transformation, so too does the attack surface. Concentrated dependencies, shared environments, and complex interconnections between operators and tenants mean that a single point of failure can trigger widespread disruption. Ensuring resilience across these critical facilities is becoming an essential priority for both providers and the organisations that depend on them.

CYBER INSURANCE

The cyber insurance market is undergoing rapid and fundamental change. Premiums continue to rise, policy wording is tightening, and exclusions (especially around human error, outdated or unpatched systems, or unimplemented security recommendations) are becoming far more prominent. Insurers now place significant emphasis on demonstrable resilience: verified technical controls, mature incident response plans, and clear reporting frameworks. At the same time, layered insurance strategies and specialist panel-based support have proven essential during in helping organisations navigate high-impact incidents and manage their financial and operational exposure.

LEGISLATIVE LANDSCAPE

Regulations across the UK, EEA, and US are becoming more complex and increasingly intertwined. In Europe, overlapping frameworks governing cyber security, AI, and data resilience have prompted concerns about regulatory friction. In the UK, the forthcoming Cyber Security and Resilience Bill proposes broader mandatory incident reporting and expanded categories of reportable attacks. In the US, organisations must navigate a complex mix of federal, state and sector-specific rules, including accelerated disclosure requirements for public companies. As these frameworks continue to evolve, organisations will need a clear, integrated approach to compliance to ensure they can meet expectations confidentiality and avoid fragmented or reactive governance. This is because the common threads are clear that scrutiny is increasing with broader and faster reporting expectations, and heightened accountability after an incident.

CONCLUSION

Several themes emerge consistently across the evolving landscape: (1) supply chain dependencies are a major driver of critical incidents, making robust vendor oversight essential, (2) the human layer continues to create exploitable gaps, underscoring the importance of strong identity controls and phishing resistance, and a heightened need to increase employee awareness and training, (3) early detection is crucial as threat actors operate more quietly and remain undetected for longer, and (4) operational resilience must become a core business priority with business continuity plans being regularly tested, clearly defined and understood across the different key teams. Organisations that rigorously test their readiness, strengthen vendor oversight, and embed resilience practices into day-to-day operations will be far better prepared to withstand a cyber attack.

FOR MORE INFORMATION

If you would like more information about the topic raised in this briefing, please speak to your regular contact at Weil or to the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

CLAUDIA SOUSA

+44 20 7903 1697
claudia.sousa@weil.com

WEIL.COM

Weil