THE CHARTERED INSTITUTE
OF LOSS ADJUSTERS

Cyber risk predictions for 2026

What UK business leaders need to know

By Suleyman Salih

Written for Marsh and reproduced with permission by the Cyber & Technology SIG
March 2026

Marsh Risk is a business of Marsh (NYSE: MRSH), a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. As specialists in enterprise risk and in cyber, we can help you take an enterprise-wide approach in building your cyber resilience. Together, we identify your risks, and work with you to develop a programme tailored to your circumstances. We inform your approach and decision-making process with our more than 25 years of cyber experience and data-driven insights. By doing so, your path to cyber resilience can be more productive and predictive and your outcomes more efficient and effective. For more information about Marsh Risk, visit marsh.com, or follow us on LinkedIn

MARSH

UK businesses face an increasingly complex and dynamic cybersecurity landscape. For organisations, the stakes have never been higher. Cyber threats are evolving rapidly, driven by advances in artificial intelligence (AI), expanding supply chain vulnerabilities, and the sophistication of collaboration among threat actors. At the same time, regulatory frameworks are tightening, demanding greater cyber resilience and governance.

This article provides an outlook on cybersecurity risks for 2026, highlighting key trends, emerging threats, and critical considerations for cyber insurance. It aims to equip senior professionals with actionable insights to navigate the challenges ahead.

2025 in review: A year of escalating threats and shifting tactics

The past year marked a pivotal moment in the evolution of cyber risk. Cloud intrusions surged significantly, while voice phishing (vishing) attacks doubled, signalling a shift toward more personalised and effective social engineering campaigns. Interactive intrusions, including hands-on-keyboard attacks that require real-time human operation, increased by 27% year-over-year, according to one estimate, underscoring the growing sophistication of adversaries.

Ransomware gangs continued to leak data in 2025. Groups such as Scattered Spider (later known as Scattered Lapsus Hunters) employed multi-pronged extortion tactics, combining distributed denial-of-service (DDoS) attacks with media pressure to maximise their impact.

Artificial intelligence emerged as a double-edged sword. While defenders continue to harness AI for threat detection and response, attackers are increasingly leveraging generative AI to automate social engineering, develop polymorphic malware (malicious software that changes its code each time it replicates), and create synthetic personas for deception (a fake identity using a mix of genuine and fabricated information). We are beginning to see adversaries use AI tools to accelerate reconnaissance and exploit development and post-compromise operations.

Supply chain attacks doubled in frequency in 2025, according to one source, which highlighted how attackers exploit trusted vendor relationships to infiltrate downstream systems.

High-profile attacks on prominent British brands maximised disruption, causing significant impact not only to the organisations themselves but also to third-party individuals and businesses. These incidents received extensive media coverage, in part due to direct engagement by threat actors with media outlets, which helped amplify their impact.

Regulatory momentum accelerated with the announcement of the UK Cyber Security and Resilience Bill, increased adoption of Cyber Essentials certification, and heightened board-level focus on cyber risk governance.

10 cyber threat predictions to watch for in 2026

1) The rise of AI: Enhancing traditional threat actor activities in 2026

AI remains a powerful and immediate influence, reshaping the cyber threat landscape. Contrary to popular belief, AI is not a standalone solution that functions with minimal human involvement. In practice, traditional threat actor methods continue to be effective, and adversaries have little reason to abandon tactics that have proven successful.

However, 2026 is set to mark a shift. Threat actors are expected to increase their use of AI and generative AI to augment traditional attack methodologies rather than replace them. AI accelerates reconnaissance, automates exploit development, and scales social engineering campaigns with unprecedented speed and sophistication.

Phishing campaigns are on course to routinely use AI-generated, contextually aware content that bypasses conventional detection and user training. Deepfake audio and video enabled hyper-realistic impersonations, elevating vishing (voice phishing) and business email compromise (BEC) attacks to new levels of effectiveness.

AI-powered malware - such as PromptFlux, which dynamically rewrites its code during attacks, evading signature-based detection and other security systems that are unable to identify it as malware — will likely continue to be developed. A black market for AI-powered malware tools is expected to emerge in 2026.

Additionally, as AI adoption grows within organisations for productivity, AI agents themselves will be targeted more than ever before. Prompt injection attacks, where adversaries manipulate AI inputs to leak sensitive data or execute malicious commands, pose a growing risk.

2026 will also see the rise of "hallucinated intelligence," where AI fabricates threat data, deliberately misleading security analysts and increasing false positives, thereby draining resources and making it harder to contain real threats efficiently.

2) Advanced threat actors leveraging localisation tactics

Sophisticated threat groups are refining their social engineering by adopting localisation tactics that exploit regional trust and cultural familiarity. This includes the use of local threat actors who speak and behave like employees, reducing suspicion during vishing attacks.

Phishing kits now include built-in localisation dictionaries and control centres to rapidly generate convincing fake pages and communications tailored to specific geographies and languages. This approach significantly increases conversion rates compared to generic campaigns by appealing directly to local customs, language nuances, and trusted brands.

Advanced voice cloning and video deepfakes enable attackers to impersonate local executives or authorities convincingly, bypassing traditional text-based security awareness training. Localisation will no longer be an optional add-on but a core feature of modern cybercrime, enabling threat actors to conduct highly targeted, multi-jurisdictional campaigns with greater success. More organisations are expected to fall victim to localisation social engineering tactics in 2026.

3) Targeted attacks and newsworthy events: The looming risk to British brands and critical infrastructure

2025 witnessed numerous high-profile cyberattacks on major British brands, resulting in severe consequences. Looking ahead, 2026 is expected to bring an escalation in high-impact, headline-grabbing attacks targeting British brands and critical infrastructure. Groups like Scattered Lapsus Hunters continue their "big game hunting" ransomware campaigns, combining sophisticated social engineering and technical exploits with media pressure and DDoS attacks to maximise disruption. Unlike traditional threat actors, these groups appear to be motivated more by notoriety than by financial gain.

Alongside notoriety-driven groups, nation state-sponsored threat actors will continue to pose a significant risk of cyberattacks that could lead to critical infrastructure failures, such as power outages, disruptions to banking payment systems, or paralysis of NHS operations. The heightened risk is reflected in the UK government's Cyber Security and Resilience Bill, which mandates stronger defences and comprehensive incident response planning across key sectors including healthcare, energy, transport, and digital infrastructure.

Such an event would have profound societal and economic consequences, underscoring the need for robust cyber resilience and cross-sector collaboration.

4) The expanding attack surface and supply chains

In 2026, businesses will continue to drive productivity by expanding their supply chains. However, this growth broadens the attack surface, increasing cyber risks such as cloud misconfigurations, stolen credentials, and vulnerabilities in network edge devices like VPNs and firewalls, which remain key entry points for threat actors seeking initial access to networks.

Threat actors are exploiting the expanded network infrastructure to their advantage by bypassing advanced endpoint detection and response (EDR) systems. They achieve this by compromising components that typically fall outside EDR monitoring, such as hypervisors and even webcams, allowing them to evade detection, maintain persistent access, and successfully deploy ransomware.

Threat actors will increasingly target vendors and service providers to gain access to downstream organisations. More than 70% of organisations experienced at least one material third-party cyber incident in the past year, according to a Marsh report, a statistic that is unsurprising given that many UK businesses overestimate their visibility and control over supply chain security.

Industries heavily reliant on major vendors experienced a significant number of data breaches in 2025. This trend is expected to persist, allowing attackers to extort multiple organisations through a single supplier breach.

Emerging threats include source code attacks, threat actors are increasingly likely to inject malicious code into source code, often via open-source packages. This creates new vulnerabilities, one example being the recent Shai-Hulud attack, which infected hundreds of packages in the NPM (Node Package Manager) registry. One example of such an injection is a vulnerability that permits any input entered into the password field during login to be accepted, effectively bypassing authentication controls. Organisations must now audit the open-source code integrated into their environments and software to identify these emerging threats.

The Cyber Security and Resilience Bill is set to formalise supply chain accountability, requiring systematic third-party risk assessments, contractual security obligations, continuous monitoring, and employee training.

5) The insider threat: A growing and sophisticated risk

Insider threats are set to rise in frequency and complexity. Collusive insider-external actor attacks, where insiders actively collaborate with cybercriminals, pose significant risks.

Threat actors actively gather intelligence on disgruntled employees with critical system access, offering high rewards to "leave the door unlocked."

Insiders can use generative AI tools to mask their identities, automate tasks, and evade detection, thereby complicating traditional security controls.

Nation-state actors will continue their efforts to recruit insiders for espionage and fraud, further elevating the threat.

6) Evolving extortion tactics

The rate of ransom payments, according to one estimate, fell to an all-time low of 23% in the third quarter of 2025. As organisations become less likely to pay ransoms through encryption alone, cybercriminals are adapting by employing more aggressive extortion strategies.

Double and multi-extortion, in which attackers encrypt systems, steal data, threaten public disclosure, and launch DDoS attacks, are now commonplace and are expected to continue in 2026.

In 2026, we may witness a surge in physical threat extortion tactics directed at organisations hit by cyberattacks, including bounties on senior leaders and threats to damage property, designed to further pressure them into making a payment. Marsh has been involved in client cyber claims where threat actors have employed these tactics.

7) Higher risk of system failures and operational errors

System failures and operational errors differ from cyberattacks; they are often unintentional, caused by faulty updates, misconfigurations, or human error.

With the likelihood of even more exploitable vulnerabilities being identified in 2026 than ever before, IT and cybersecurity administrators will need to patch more frequently as updates are pushed out by vendors. Additionally, the continued acceleration of cloud and SaaS adoption, along with rapid investment in new technologies like agentic AI, further increases the risk of system failures and operational errors. Vibe coding — AI-assisted rapid code generation — is a fast-growing trend that could also introduce significant risk of system failures, alongside insecure code and vulnerabilities.

Major providers experienced significant outages in 2025, disrupting critical services and platforms. UK businesses must prioritise critical system mapping and resilience planning to prevent cascading disruptions from such failures.

8) The regulatory landscape

The UK's regulatory environment is undergoing transformation. The Cyber Security and Resilience Bill, expected to be enacted in 2026, expands the scope of regulation to include managed service providers (MSPs), data centres, and critical suppliers, imposing stringent security and supply chain duties. Furthermore, Cyber Essentials certification is set to become a de facto requirement in supply chains.

Boards are under increasing pressure to prioritise cyber risk governance, with formal reporting, senior ownership, and integration of cyber strategy into overall business strategy mandated by the Cyber Governance Code of Practice.

Globally, AI security regulations remain fragmented, with the UK striking a balance between innovation and security, while the EU enforces stricter compliance through the AI Act.

UK businesses must navigate this complex landscape carefully to ensure compliance and avoid penalties.

UK government ministers recently urged business leaders, including all FTSE 350 CEOs, to act decisively to protect their organisations and the UK economy from cyberattacks. They stressed the importance of having a robust cyber incident response plan, stating: "In this increasingly hostile landscape, organisations recover better from incidents when they have planned for the worst and rehearsed their business continuity and recovery."

2026 will likely see further advancements in government regulations and recommendations, alongside the introduction of government-backed schemes that actively promote education and awareness of cyber threats to UK organisations.

9) US class action lawsuits: Cross-border legal risks for UK businesses

UK companies with US customers face growing litigation risk due to surging US data breach class action lawsuits and state privacy laws.

The fragmented US regulatory landscape, including the California Invasion of Privacy Act (CIPA), the Telephone Consumer Protection Act (TCPA), the Americans with Disabilities Act (ADA), and new laws in Indiana, Kentucky, and Rhode Island, increases compliance complexity.

Heightened enforcement, alongside emerging "non-attack" claims related to routine data processing, is driving a surge in class actions expected to continue into 2026.

10) The evolution of cybersecurity operations and workforce transformation

Cybersecurity operations will continue to evolve. The traditional divide between IT and security teams is blurring, with 2026 poised to see increased adoption of integrated digital operations centres (DOCs), which consolidate infrastructure, security, compliance, and user experience under unified leadership, often led by chief trust officers.

Managed service providers (MSPs) will increasingly co-manage security alongside internal teams, leveraging vertical specialisation for sectors like healthcare, finance, and retail. This hybrid model enhances organisational resilience, lowers cost barriers, and helps address ongoing talent shortages.

Automation, AI-driven security orchestration, and agentic AI will empower security operations centres (SOCs) to detect and respond more quickly, reducing alert fatigue and enhancing threat hunting.

Investment in workforce training, certification, and cross-functional collaboration will be crucial to maintaining a skilled and agile cybersecurity workforce in 2026.

A note on cyber insurance for UK businesses in 2026

Cyber insurance in the UK remains highly competitive, driven by rising demand from organisations and expanded capacity among insurers. This soft market environment is expected to persist, helping to keep premiums relatively low.

It is essential for organisations to thoroughly understand their cyber risk exposure, particularly the elements typically covered by cyber insurance policies and how these align with the evolving cyber threat landscape. There has never been a better time to review and enhance coverage.

Preparing for a complex and evolving cyber future

As always, the cybersecurity industry and cybercriminal networks are continuously adapting their tactics in this fast-paced, ever-evolving cat-and-mouse game. Prioritisation through senior executive and board involvement, combined with thorough risk analysis and appropriate budgeting, is essential to staying at least one step ahead of emerging threats.

The cybersecurity threat landscape in 2026 will be defined by rapid technological change, expanding attack surfaces, and evolving adversary tactics and collaborations. AI-powered attacks, supply chain vulnerabilities, and insider threats will challenge traditional defences.

UK regulatory frameworks will continue to evolve, placing greater responsibility on boards and organisations to embed cyber resilience into their core strategies.

Incident response planning and tabletop exercises remain top controls, demonstrating that preparation drives positive security behaviours and stronger controls.

Success in 2026 will depend on embracing innovation, fostering collaboration across internal and external partners, and maintaining vigilant governance to protect against an increasingly sophisticated and relentless cyber threat environment.