MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

Quarter 1 2026

Cyber-security Trends for 2026

The cyber-security landscape in 2026 will be defined by fast-moving technologies, increasingly complex threat tactics and rising regulatory expectations. UK organisations face mounting pressure to strengthen digital resilience as attackers become more adaptive and resourceful.

The following emerging trends are expected to have the greatest influence:

- **The rise of AI-driven attacks**—Attackers are leveraging AI to automate targeted scams and malware, while defenders increasingly rely on AI-driven detection and response.
- **Escalated ransomware and supply-chain compromises**—Threat actors are expanding into cloud and third-party systems, prompting organisations to reassess vendor dependencies and continuity plans.
- **Greater regulatory scrutiny**—Revised UK requirements via the Cyber Security and Resilience Bill, and EU frameworks such as the Cyber Resilience Act, will heighten expectations around governance, reporting and demonstrable cyber-resilience.
- **Identity as the new perimeter**—With hybrid work and cloud adoption, organisations are accelerating Zero Trust models and strengthening authentication to protect identity-based attack surfaces.
- **Preparation for quantum risk**—Firms are beginning to map cryptographic dependencies and plan for future transitions to quantum-safe encryption.
- **Security culture and resilience**—Organisations are prioritising secure-by-design practices, improved cyber-hygiene and targeted workforce training to reduce human-factor risks.

Organisations that adopt adaptive security models, invest in identity-centric controls and prepare early for regulatory and technological change will be better positioned to manage the rapidly evolving cyber-risk landscape in 2026 and beyond.

Common Reasons Cyber-insurance Claims Are Denied

Cyber-insurance is now a key element of organisational risk management, yet obtaining cover—and having claims approved—can be challenging. Insurers expect clear evidence of cyber-security maturity, strong governance and well-maintained controls. When these elements are missing, applications and claims may be denied.

Denials sometimes stem from inadequate security testing, missed patches or outdated systems that contribute to breaches. Claims may also fail when organisations lack a current, tested incident response plan or when notification delays breach policy conditions. Weak backup and recovery processes, especially when data is incomplete or untested, pose another major barrier.

Supply-chain vulnerabilities are increasingly scrutinised; if a breach originates with a vendor and organisations cannot demonstrate proper oversight, insurers may withhold cover. Outdated technology, limited staff training and non-compliance with requirements such as the UK General Data Protection Regulation also signal insufficient risk management and may lead to claim denial or reduced cover.

Contact us today for additional cyber-security guidance and to review your cover.

Understanding Vendor Email Compromise Risks

Vendor email compromise (VEC) is an increasingly common cyber-threat affecting UK organisations of all sizes. Unlike traditional business email compromise, which often impersonates internal executives, VEC attacks exploit trusted supplier relationships. Criminals pose as legitimate vendors to redirect payments, access sensitive information or disrupt operations—and because these communications appear routine, they are far more difficult to detect.

VEC attacks typically begin when criminals compromise a vendor's mailbox through phishing, credential stuffing or lookalike domains. Once inside, they monitor email traffic—sometimes for weeks—to understand payment schedules, ongoing projects and key decision-makers. Attackers may set email-forwarding rules to collect information without alerting the vendor.

Armed with this insight, attackers send highly tailored messages to customers, often requesting updated bank details or urgent payment of invoices. Because the emails closely match genuine communication patterns, organisations frequently do not realise they have been targeted until funds or data have already been lost.

Several factors make VEC scams particularly effective:

- Routine vendor interactions lower employees' suspicion of payment-related requests.
- Fraudulent emails often come from genuine, compromised accounts, leaving no obvious signs of fakery.
- The timing of the scam aligns with standard payment cycles, thanks to detailed attacker reconnaissance.
- Traditional email filters may not flag these messages, as they often contain no malicious links or attachments.

The result is a sophisticated social-engineering attack that blends seamlessly into normal business processes.

Even legitimate vendor accounts can be hijacked, making fraudulent payment requests hard to spot.

A layered approach is essential for defending against VEC. Key measures include the following:

- Strengthen email authentication with SPF, DKIM and DMARC, pairing them with behavioural monitoring tools that detect unusual communication patterns.
- Verify any vendor requests involving payments or sensitive data—preferably through out-of-band channels such as a confirmed phone call.
- Monitor the security posture of key suppliers and require them to maintain appropriate controls.
- Provide targeted staff training on recognising VEC techniques and the importance of slowing down before actioning unexpected account changes.

Cyber and commercial crime insurance may offer protection against financial losses from fraudulent payment instructions, but cover depends on policy wording. Some policies require evidence of a direct system breach, while others only respond if specific social-engineering or payment-diversion endorsements are in place. An experienced broker can help organisations understand these nuances, address cover gaps and navigate the claims process effectively.

By strengthening vendor oversight, enhancing email security and reviewing insurance arrangements, organisations can improve resilience against the growing threat of VEC.

Contact us today for further guidance on cyber-risk management.