

MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

Q4 2026

How Agentic AI Is Changing the Cyber-threat Landscape

Agentic artificial intelligence (AI) is changing cyber-threats by enabling systems to plan, act and adapt with minimal human oversight. Unlike generative AI, which responds to prompts, agentic AI can independently scan networks, identify vulnerabilities, write malicious code and retry unsuccessful approaches. This could make attacks faster, more persistent and harder to detect.

Cyber-criminals may use agentic AI to move laterally through networks, escalate privileges and locate valuable data. This technology can also gather information from social media and public records to create highly personalised phishing messages, business email compromise scams and deepfake impersonations at scale. Attackers may even poison an AI agent's memory, causing it to make harmful decisions later, or deploy several agents simultaneously to overwhelm an organisation's defences.

To manage these emerging risks, organisations should:

- Segment networks and apply zero-trust principles to restrict movement and access.
- Use behaviour- and anomaly-based endpoint monitoring alongside traditional antivirus tools.
- Audit the permissions granted to internal AI tools regularly and limit access to what each agent needs.
- Update incident response plans and exercises to reflect the speed of AI-enabled attacks.
- Review cyber-insurance policies with a trusted insurance professional, such as a broker, to clarify how AI-related incidents, compromised tools and autonomous activity are treated.

As agentic AI develops, organisations must strengthen their associated governance measures and controls so they can detect, contain and respond to increasingly automated cyber-attacks.

The Value of Using a Virtual Private Network

A virtual private network (VPN) encrypts internet traffic between a device and a remote server. For employers with remote or travelling staff, it can help protect corporate systems and information, particularly when workers connect to a public or otherwise untrustworthy Wi-Fi network.

A properly managed VPN can secure access to company files, emails, applications and internal systems. It may also reduce exposure to network eavesdropping and certain account compromise attempts and support compliance with applicable data protection requirements.

Employers should establish clear rules requiring workers to use the approved VPN whenever they are outside the corporate network, access sensitive systems or connect through public Wi-Fi. Where possible, devices should connect automatically. VPN access should also require multifactor authentication (MFA), and employees should know how to promptly report connection problems or suspicious network activity.

However, a VPN is only one layer of protection. It cannot prevent phishing, protect credentials that have already been compromised or remove malware from an infected device. Employers should therefore combine VPN use with secure configuration, endpoint protection, access controls, patch management and regular staff training. They should also monitor access logs and remove accounts that are no longer required. Contact us today for additional cyber-security guidance.

What Security Debt Means for Cyber-Risk

As organisations adopt new technologies and modernise their operations, cyber-security safeguards can fall behind. Unpatched software, outdated systems, excessive user privileges, overlooked training and unapproved tools can create unresolved weaknesses known collectively as security debt.

Security debt is broader than vulnerability debt, which generally concerns technical flaws. It includes gaps across an organisation's people, processes and technology, such as weak governance, unsupported systems, forgotten cloud resources and poor access controls. As these issues accumulate, organisations may face a greater risk of data breaches, operational disruption, regulatory penalties and reputational damage.

Security debt rarely stems from a single major failure. It builds through postponed fixes, outdated technology and weak oversight, gradually increasing both the likelihood of a cyber-incident and the cost of recovery.

Security debt can result from intentional trade-offs, such as delaying patches to avoid disruption, skipping code reviews to meet deadlines or postponing security improvements due to competing priorities. It can also arise unintentionally as technology develops faster than oversight. Examples include expired digital certificates, unused open ports, shadow IT and privileged accounts that are not regularly reviewed.

Cloud adoption, AI tools, third-party suppliers, mergers and system migrations can add further complexity. Over time, unresolved weaknesses can become more difficult and expensive to address while expanding an organisation's attack surface. Cyber-criminals are also using automation to identify and exploit vulnerabilities more quickly, leaving organisations with less time to correct them.

Accumulating security debt may also affect cyber-insurance. Applications commonly ask about controls such as patch management, MFA, endpoint detection and vulnerability management. Organisations should ensure this information remains accurate, as material inaccuracies could affect cover. Some policies may also require specified controls to be maintained throughout the policy period. Organisations should review their policy wording with insurance experts to understand how these requirements apply.

To manage security debt, organisations should consider the following:

- Maintain an inventory of systems, applications, devices, cloud resources and third-party connections.
- Continuously scan for vulnerabilities and document remediation work.
- Prioritise weaknesses affecting critical systems, sensitive data or essential operations.
- Replace unsupported technology where feasible.
- Report security debt to senior leaders.
- Track critical vulnerabilities, unsupported assets and remediation times.

Although some security debt may be unavoidable, allowing it to accumulate can increase the likelihood, severity and cost of cyber-incidents. A risk-based approach can help organisations address the most serious weaknesses while keeping their security controls, exposures and insurance cover aligned.

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

Contains public sector information published by the ICO and NCSC and licensed under the Open Government Licence v3.0.
The content of this publication is of general interest and is not intended to apply to specific circumstances or jurisdiction. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice from their own legal counsel. Further, the law may have changed since first publication and the reader is cautioned accordingly.
© 2026 Zywave, Inc. All rights reserved.