# Cyber Risks & Liabilities




## How Agentic AI Is Changing the Cyberthreat Landscape

Agentic artificial intelligence (AI) is changing the cyberthreat landscape by enabling systems to plan, act and adapt with minimal human oversight. Unlike generative AI, which primarily responds to user prompts, agentic AI consists of autonomous, interconnected components, often called AI agents, that work together to complete tasks independently. Rather than waiting for instructions, agentic systems can autonomously scan networks, identify vulnerabilities, write and test malicious code and access or exfiltrate data. They can also retain memory between sessions, allowing them to build on actions, observe outcomes and retry approaches until they meet their objectives. As a result, cyberattacks may become more persistent and difficult to detect.

Cybercriminals are already putting agentic AI to work in several ways. It can independently map a network, identify critical assets and escalate privileges to move laterally across systems, often within minutes. CrowdStrike's 2026 Global Threat Report found the average time between initial access and first lateral movement fell to 29 minutes in 2025, with the fastest observed case just 27 seconds. Agentic AI can also harvest data from social media and public records to build highly targeted phishing and social engineering campaigns, refining its approach in real time based on what succeeds and increasing the risk of business email compromise and deepfake impersonation. Attackers can also deploy multiple agents simultaneously, increasing the volume and speed of attacks to the point where they can overwhelm defenses and make threats harder to detect.

To reduce the risks associated with agentic AI, organizations should consider the following measures:

- **Microsegment networks**. Divide networks into smaller, isolated zones with their own security rules to limit lateral movement, and adopt a zero-trust approach that continuously verifies access rather than assuming trust based on network location.

- **Switch to behavior-based endpoint detection**. Implement behavior- and anomaly-based monitoring to help identify unusual activity and detect previously unknown AI-enabled threats.
- **Audit permissions on internal AI tools**. Regularly review the permissions granted to AI tools and agents, limiting access to only the systems and data necessary for their intended functions.
- **Update incident response plans for AI-driven threats**. Review and test incident response plans to account for the speed and autonomy of AI-driven attacks.
- **Review cyber insurance coverage**. Work with a broker to clarify how cyber insurance policies respond to AIenabled attacks and incidents involving AI tools.

Contact us today for more guidance on defending against evolving cyberthreats.

---

## Common Cyberthreats Facing Remote and Hybrid Workers

When employees work from home or on the move, they may rely on unsecured networks, personal devices or outdated software. A single mistake can open the door to cybercriminals, leading to costly data breaches, regulatory penalties, operational disruptions and reputational harm.

Some of the most common threats include phishing attacks, which remain an ongoing concern because remote employees depend heavily on email and messaging platforms. A related threat, business email compromise, can exploit the reduced face-to-face contact associated with remote work, with attackers impersonating executives or suppliers to pressure employees into transferring funds or disclosing sensitive information. Password practices present another risk. Remote workers often juggle logins across multiple cloud-based services and may reuse passwords between them. Attackers can exploit credentials stolen in earlier, unrelated breaches to access company accounts, a technique known as credential stuffing. Employees using personal or less-secure devices may also be more vulnerable to ransomware, which encrypts files and can disrupt operations until a ransom is paid.

To reduce these risks, employers should use a combination of technical and organizational measures, including encrypting internet traffic with VPNs, enabling multifactor authentication for all accounts and providing companymanaged devices with standardized security settings. Clear remote work policies, ongoing cyber awareness training and prompt installation of security updates can further strengthen cybersecurity.

Contact us today to learn more about protecting remote and hybrid workers from cyber threats.

---

## Understanding Security Debt

As organizations adopt new technologies and modernize operations, cybersecurity safeguards can fall behind. Unpatched software, outdated systems, excessive user privileges, inadequate training and unauthorized tools can create unresolved weaknesses collectively known as security debt. Security debt extends beyond technical vulnerabilities. It includes gaps across people, processes and technology, such as weak governance, unsupported systems, forgotten cloud resources and poor access controls.

**Security debt rarely stems from a single point of 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.**

Some security debt stems from deliberate trade-offs, such as delaying patches to avoid disruption, skipping code reviews to meet deadlines or postponing security improvements due to competing priorities. Other forms accumulate unintentionally as technology evolves faster than oversight can keep pace. Common examples include

expired digital certificates, unused open ports, unvetted AI tools and privileged accounts that are not regularly reviewed.

Over time, unresolved weaknesses may become more difficult and costly to address, thereby expanding an organization's attack surface. To help manage this exposure, organizations should:

- Maintain an inventory of systems, applications, devices, cloud resources and third-party connections, with particular attention to retired-but-active systems, forgotten assets and shadow IT.
- Continuously scan for vulnerabilities, apply threat intelligence to spot emerging risks, and track remediation efforts.
- Prioritize weaknesses affecting critical systems, sensitive data, essential operations or regulatory compliance.
- Replace unsupported technology where feasible, and govern security debt from the top with executive-level reporting.
- Track key metrics, such as critical vulnerabilities, the percentage of assets past end-of-life and remediation timelines.

While 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 organizations prioritize the most significant weaknesses.

Contact us today for additional guidance on cyber risk management.

---

This Cyber Risks & Liabilities newsletter is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2026 Zywave, Inc. All rights reserved.