# Businesses in the UK unprepared for generative AI cybersecurity threats



Research conducted by Ivanti has revealed that a significant number of businesses in the UK are unprepared to deal with the threats posed by generative AI (GenAI), with one in four lacking a documented strategy to address these risks. This finding raises concerns about the corporate approach to cybersecurity, with parallels drawn to workplace health and safety protocols that are typically more stringent.

The rapid advancement of GenAI technology has seemingly left many security teams struggling to keep pace. While 47% of security professionals in the UK perceive GenAI as beneficial for cybersecurity, this positive outlook is accompanied by a notable lack of readiness to counteract potential threats. Alarmingly, nearly half (49%) of UK IT and security experts expect phishing attacks to increase due to GenAI capabilities, yet there is a disconnect between this concern and proactive measures taken to mitigate such risks.

David Shepherd, Senior Vice President EMEA for Ivanti, commented on the dispersal of critical security data, noting that 72% of organisations report their IT and security information is siloed across various systems. This fragmentation complicates security efforts and poses a threat to response efficiency, with 63% of organisations indicating that these barriers slow down their ability to act against security threats effectively.

Security teams increasingly recognise human error as a vulnerability. In response, 57% have implemented anti-phishing training as a primary defence mechanism against sophisticated social-engineering attacks, making it the most widely adopted protective measure against threats driven by AI. However, Shepherd cautions that sturdy employee training alone is insufficient, characterising the reliance on basic training as a response to modern threats akin to using outdated tools in the face of current dangers.

As GenAI expands its capabilities, new vulnerabilities emerge, often more rapidly than traditional security methods can adapt. This has necessitated a re-evaluation of security strategies, advocating for a more integrated approach to exposure management. Key recommendations for security teams include:

**Continuous Monitoring and Assessment**: Traditional periodic assessments cannot keep pace with AI-driven threats. Real-time visibility into the entire attack surface is required to identify and respond to threats dynamically.

**Breaking Down Data Silos**: Efficient security responses are hampered by fragmented data systems. Unified visibility is a critical requirement when confronting intricate AI-driven threats, and organisations must prioritise overcoming these silos.

**Evolving Training Protocols**: While security awareness training is vital, it cannot constitute the only line of defence. Organisations should supplement human awareness with advanced detection and response mechanisms to combat increasingly sophisticated threats.

**Data-Driven Security Responses**: Relying solely on intuition and experience may no longer suffice. Comprehensive data visibility is needed to recognise patterns and anomalies that indicate emerging threats, reinforcing the necessity of dismantling data silos.

The research suggests that organisations cannot afford to adopt a passive ‘wait-and-see’ approach regarding GenAI security risks. As GenAI continues to develop and reshape the cybersecurity landscape, it is imperative that businesses act swiftly to implement documented strategies, enhance visibility across security frameworks, and elevate their threat detection capabilities.

In summary, the call for a comprehensive, proactive security response to the challenges posed by generative AI is pressing. Organisations that delay implementing effective security measures risk falling behind, facing increased vulnerability as GenAI technologies continue to evolve and become more sophisticated. The time for action is immediate, as waiting could entail significant repercussions in the event of a serious security breach.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://itbrief.co.uk/story/ivanti-report-highlights-risks-of-genai-in-cybersecurity> - This article supports the claim that many UK businesses lack a documented strategy to address GenAI risks and highlights the increased threat of phishing attacks due to GenAI capabilities.
* <https://www.ivanti.com/company/press-releases/2024/ivanti-research-finds-phishing-tops-list-of-growing-cyber-threats-fueled-by-genai> - This press release corroborates the finding that phishing is a top threat increasing in severity due to GenAI and emphasizes the need for effective anti-phishing training.
* <https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report> - This report supports the recommendation for a multilayered approach to AI-powered threats, including combining human expertise with AI tools and addressing data silos.
* <https://www.noahwire.com> - This source is mentioned as the original article's source but does not provide specific corroborative information without direct access to the article.
* <https://www.virginia.gov/agencies/supreme-court-of-virginia/rules-of-supreme-court-of-virginia> - This URL does not directly support the claims about GenAI and cybersecurity but provides general legal context.