# AI's impact on cyber insurance and evolving business risks



Recent discussions surrounding artificial intelligence (AI) and its integration into business practices have shed light on significant trends in cyber insurance, particularly regarding the challenges and changes occurring in coverage. In a recent episode of "AI Talk," hosted by Juliana Neelbauer, Ralph Pasquariello, a Senior Partner and cyber liability specialist at The Tech Collective, elaborated on these pressing issues.

The conversation between Neelbauer and Pasquariello delved into how AI influences social engineering tactics, an increasingly prevalent cybersecurity threat. Social engineering, which often exploits human psychology to gain confidential information, has seen adaptations through AI technologies, raising the stakes for organisations that may fall victim to sophisticated scams.

Within the dialogue, Pasquariello emphasised the transformative nature of AI in evaluating and enhancing cybersecurity measures, notably through the implementation of two-factor authentication. He highlighted the critical role such technology plays in fortifying systems against potential breaches, reflecting a broader trend of businesses seeking to bolster their digital security infrastructure as a direct response to rising cyber threats.

Furthermore, Pasquariello introduced a new initiative aimed at supporting executive teams in 12 states to effectively assess and select cyber insurance policies suitable for their specific needs. This initiative underscores the shifting landscape of cyber insurance, which is evolving rapidly in response to increasing claims and the complexities introduced by digital advancements.

Emerging technologies, such as AI, are not only reshaping the cybersecurity landscape but also influencing the frameworks of coverage and liability within the insurance sector. As companies grapple with the implications of these advancements, industry forecasts suggest that businesses will need to adapt quickly to ensure they are adequately protected against the evolving risks associated with cyber threats.

Pasquariello's insights provide a glimpse into a critical intersection of technology and insurance, where swift action is essential for businesses looking to safeguard their assets amidst growing uncertainties in the digital realm. The evolving nature of cyber insurance is indicative of a larger trend in which businesses must continually reassess their risk exposure and adapt to new technological realities.

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

## Bibliography

1. <https://www.vikingcloud.com/blog/cybersecurity-2025-lessons-learned-expected-trends> - This article supports the trend of evolving cyber insurance policies and the need for stricter controls and robust incident response plans in response to increasing ransomware attacks.
2. <https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks> - This source corroborates how AI is influencing social engineering tactics, making them more sophisticated and effective, and highlights the challenges this poses for cybersecurity.
3. <https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks> - It explains the role of AI in detection evasion, hyper-personalized phishing, and emotional manipulation, all of which are critical aspects of modern social engineering attacks.
4. <https://www.ntiva.com/blog/ai-social-engineering-attacks> - This article details how AI-powered social engineering attacks work, including data collection, AI model training, and the creation of convincing fake content like deepfake videos and voice clones.
5. <https://www.ntiva.com/blog/ai-social-engineering-attacks> - It also discusses the examples of AI-powered traditional social engineering tactics such as phishing, spear phishing, and deepfake videos.
6. <https://www.vikingcloud.com/blog/cybersecurity-2025-lessons-learned-expected-trends> - This source supports the importance of implementing robust cybersecurity measures, including two-factor authentication, to fortify systems against potential breaches.
7. <https://www.wisedocs.ai/blogs/ai-trends-in-2025-for-the-insurance-legal-and-medical-space> - This article highlights the evolving landscape of cyber insurance and the increasing role of AI in the claims industry, including AI-driven customer interactions and process optimization.
8. <https://www.wisedocs.ai/blogs/ai-trends-in-2025-for-the-insurance-legal-and-medical-space> - It discusses the medical industry's need to shore up cybersecurity, including stronger login protocols and greater human oversight when training AI models.
9. <https://www.vikingcloud.com/blog/cybersecurity-2025-lessons-learned-expected-trends> - This source mentions the emergence of AI governance and secure AI models, which is crucial for maintaining model integrity and preventing data poisoning or model theft.
10. <https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks> - It emphasizes how AI amplifies social engineering threats, making businesses' attack surfaces larger and more complex.
11. <https://www.wisedocs.ai/blogs/ai-trends-in-2025-for-the-insurance-legal-and-medical-space> - This article predicts that AI will be central to the strategy of nearly half of global companies in 2025, including those in the insurance sector, highlighting the need for swift adaptation to new technological realities.
12. <https://www.jdsupra.com/legalnews/ai-talk-with-juliana-neelbauer-episode-25779/> - Please view link - unable to able to access data