# Navigating the dual nature of artificial intelligence in the security sector



Innovative developments in artificial intelligence (AI) continue to spark discussions across various sectors, including the security industry. Recent insights suggest that while AI presents opportunities for growth and differentiation, it also harbours potential pitfalls that companies must navigate with caution.

The discussion arises from a piece published by Security Sales & Integration, where the author highlights the dual nature of AI technology. While it can enhance operations, lead to increased profits, and improve customer service, there are significant risks for those unprepared or overconfident in their approach to integrating AI into their business strategies.

A central theme is the necessity for thorough planning, training, and a clear understanding of AI's capabilities before attempting to market and implement new technologies. The article warns against the temptation to rush into adopting AI solutions based merely on client interest, particularly in high-profile products like AI-enabled cameras or video management systems (VMS). The author stresses the importance of asking essential questions about the technology's functioning and costs, and urges companies to lean on trusted networks for advice.

"Ideally, the provider of that technology must thoroughly do that training," the author states, emphasising that companies cannot rely solely on the technology to educate their personnel. Realistic customer expectations are crucial, as the article underscores the potential for AI to reach only about 90% accuracy, suggesting businesses should "under-promise and over-deliver" when introducing AI applications.

The discussion extends to the impact of AI on the workforce. The implementation of AI can lead to the automation of routine, manual tasks, which may jeopardise jobs for those who resist updating their skills or career paths. The article posits that those who do not actively seek to improve or adapt may find themselves at a disadvantage in an evolving marketplace.

Additionally, the piece highlights the significance of beginning AI initiatives internally, with suggestions for conducting pilot tests before rolling out technology to customers. Engaging innovative clients in dialogues about risks and rewards associated with AI can yield valuable insights and referrals.

The author points out the distinction between contemporary AI applications and the previous wave of excitement surrounding video analytics a decade ago. Although hardware improvements and processing capabilities at the network edge have advanced AI, the article suggests caution regarding "overenthusiastic exposure" to new technology buzzwords.

In its conclusion, the article hints at the potential for deeper concerns surrounding AI in the coming months. The next column is expected to explore the "ugly" aspects, such as the emergence of deepfakes, which raise serious ethical questions about fraud and misinformation.

With the security sector poised at a crossroads of innovation, companies must consider both the promising and precarious aspects of AI integration to effectively navigate this emerging landscape.

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

## References

* <https://www.nucamp.co/blog/coding-bootcamp-cybersecurity-2025-what-role-will-ai-play-in-cybersecurity-in-2025> - This article highlights the transformative impact of AI on cybersecurity, including its role in threat detection and response, which supports the discussion on AI's dual nature in enhancing operations while posing risks.
* <https://www.zdnet.com/article/how-ai-will-transform-cybersecurity-in-2025-and-supercharge-cybercrime/> - This piece explores how AI will transform cybersecurity by enhancing both defensive and offensive capabilities, aligning with the article's theme of AI's potential benefits and pitfalls.
* <https://www.scworld.com/feature/ai-to-change-enterprise-security-and-business-operations-in-2025> - This article discusses the advancements in AI systems and their impact on enterprise security, emphasizing the need for robust AI governance to mitigate risks, which aligns with the importance of thorough planning and understanding AI capabilities.
* <https://www.vacourts.gov/courts/scv/rulesofcourt.pdf> - Although not directly related to AI, this document provides a framework for legal and procedural considerations, which can be relevant when discussing regulatory and legal implications of AI integration in business strategies.
* <https://www.federalregister.gov/documents/2024/04/22/2024-07496/guidance-for-federal-financial-assistance> - This document offers guidance on federal financial assistance, which can be relevant when considering the financial implications and regulatory compliance of AI integration in various sectors.