# Artificial intelligence reshapes business security amid evolving threats



The ongoing integration of artificial intelligence (AI) automation within business operations is reshaping industries across the globe, presenting both opportunities and challenges. In light of the complexities introduced by the convergence of digital and physical realms, a recent webinar titled "Shaping the Cyber-Physical Future: Trends, Challenges, and Opportunities for 2025" offered insights from industry experts on key trends and security concerns shaping the future landscape.

Organised by Claro Enterprise Solutions, the webinar featured prominent speakers including Allison J. Taylor, the founder and CEO of Thought Marketing LLC. Taylor discussed emerging trends and strategies for businesses eager to enhance their security measures in the face of evolving cyber threats. Cesar Salazar, the Chief Operating Officer of Claro Enterprise Solutions, focused on innovative technologies driving business advancement and highlighted the critical importance of cyber-physical convergence using adaptive security operations.

The core of the discussion revolved around the anticipated impact of technological waves, notably the "AI wave" projected to define the period from 2025 onwards. Taylor highlighted how such technological advancements necessitate a strategic approach, with businesses expected to identify actionable ways to leverage AI for operational efficiency and competitive advantage.

Salazar elaborated on the evolution of technological adoption, tracing a pathway from early internet iterations through to the current AI landscape. He explained that initial excitement surrounding new technologies often gives way to a period of careful refinement, where businesses learn to maximise value from these tools. Today, organisations are navigating a tech ecosystem that encompasses cloud computing, blockchain, and increasingly sophisticated AI applications.

Against this backdrop, the rise of hyperconnectivity poses intensified security challenges. Businesses are increasingly relying on cloud-based platforms and collaborative tools, which, while enhancing productivity, also create expansive environments that broaden the potential for security threats—an observation echoed by Check Point Research, which noted a 30% increase in threat volume from 2023 to 2024. The convergence of cyber and physical security environments is now seen as crucial, as threats emerge not only from digital avenues but also from physical vulnerabilities.

Salazar outlined four key trends affecting the security landscape: an expanded scope for potential threats due to hyperconnectivity, the rising frequency of attacks, an increase in external influences from geopolitical tensions and compromised security, and the evolution from purely cyber threats to complex cyber-physical threats.

In anticipation of these challenges, the webinar identified five paramount priorities for organisations to address by 2025. These include fostering continual human-AI collaboration, enhancing data privacy measures, strengthening supply chain resilience, ensuring proactive threat detection, and preparing for the future of cyber-physical security.

One critical element discussed was the necessity for businesses to assess their current IT stances—whether they are operating in "Survival Mode," "Smart Mode," or "Leadership Mode." This assessment is pivotal for informing appropriate cybersecurity roadmaps for the future.

Claro Enterprise Solutions provided attendees insight into essential safeguards for managing cyber-physical security. These include regular cyber-physical asset discovery, the adoption of zero trust security models, rigorous security monitoring, enhanced investment in user training, and governance frameworks to tackle compliance risk.

Challenges such as resource constraints and the complexity of integrating disparate systems were also acknowledged, highlighting the need for organisations to adopt a holistic approach that effectively amalgamates cyber and physical security measures.

In closing, Claro Enterprise Solutions articulated their vision for a fully integrated defence system that marries cyber and physical security through real-time data monitoring and response systems, utilising advanced technologies such as AI and IoT. This progressive approach is geared towards building resilience within organisations as they navigate the multifaceted challenges this new cyber-physical era presents.

The insights shared during the webinar serve as a comprehensive guide for businesses preparing to face the realities of a rapidly evolving technological landscape while ensuring robust security measures remain a top priority.

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

## References

* <https://calvettiferguson.com/ai-automation-trends-2024/> - This article supports the claim that AI and automation are transforming business operations by streamlining complex processes, improving efficiency, and driving strategic breakthroughs.
* <https://www.rapidinnovation.io/post/how-ai-is-transforming-business-automation-in-2024> - This source corroborates the idea that AI is revolutionizing business automation by enhancing efficiency, reducing operational costs, and improving decision-making through technologies like machine learning and natural language processing.
* <https://hellodarwin.com/blog/automate-business-ai> - This article explains how AI automation is transforming business operations by automating repetitive tasks, enhancing customer service, and making smarter decisions through advanced analytics and process optimization.
* <https://www.avvale.com/newsroom/the-impact-of-ai-on-business-operations> - This source highlights the impact of AI on business operations, including process automation, advanced data analytics, customer experience personalization, and security and risk management, all of which are crucial in the evolving business landscape.
* <https://leapzonestrategies.com/2024/09/ai-automation-transform-your-business-operation/> - This article discusses how AI automation can boost business productivity, cut costs, and provide a competitive edge by automating complex tasks, improving decision-making, and enhancing compliance and risk management.
* <https://calvettiferguson.com/ai-automation-trends-2024/> - This source supports the necessity for businesses to manage associated AI risks by establishing ethical frameworks and governance models to ensure responsible use of AI.
* <https://www.rapidinnovation.io/post/how-ai-is-transforming-business-automation-in-2024> - This article emphasizes the role of AI in optimizing logistics and supply chain management, which is a key aspect of navigating the complexities of cyber-physical convergence.
* <https://hellodarwin.com/blog/automate-business-ai> - This source explains how AI-driven automation can integrate with various business systems, ensuring that all decisions are informed by comprehensive, real-time data, which is essential for proactive threat detection and cyber-physical security.
* <https://www.avvale.com/newsroom/the-impact-of-ai-on-business-operations> - This article highlights the importance of AI in enhancing customer experience through personalization and in managing security and risk, which aligns with the webinar's focus on cyber-physical security challenges.
* <https://leapzonestrategies.com/2024/09/ai-automation-transform-your-business-operation/> - This source supports the idea that adopting AI automation requires a holistic approach to effectively amalgamate cyber and physical security measures, addressing challenges such as resource constraints and system complexity.
* <https://www.rapidinnovation.io/post/how-ai-is-transforming-business-automation-in-2024> - This article discusses the future of work where human and AI collaboration is increasing, which is relevant to the webinar's emphasis on fostering continual human-AI collaboration by 2025.
* <https://thehackernews.com/2024/11/protecting-tomorrows-world-shaping.html> - Please view link - unable to able to access data