Security talking points in 2025

Security predictions for 2025

John Swanson, Global Security Portfolio Lead, Uvance, at Fujitsu

AI Hype Fades: Spotlight on Risk and Practicality

As the enthusiasm surrounding artificial intelligence begins to temper in 2025, I expect the cybersecurity industry to pivot from speculative debates to more tangible use cases. Organizations will move away from treating AI as a universal solution or existential threat. Instead, they will focus on the specific risks and benefits it introduces. This shift will drive the rise of tools designed to identify and mitigate AI-related security vulnerabilities.

Expect to see an increase in prominence for platforms like Cranium, which offer insights into how AI models operate within an organization. These tools will help organizations audit AI systems for potential weaknesses, such as data poisoning, adversarial attacks, or unintended bias that malicious actors can exploit. Additionally, cybersecurity frameworks will evolve to address risks associated with integrating AI into core business processes, ensuring these technologies remain secure, compliant, and ethical.

The emphasis will also shift toward leveraging AI for defensive purposes, such as real-time threat detection and automated response systems. Expect massive growth in the leverage of private AI to exploit the wealth of internal data locked within organizations, such as processes, work instructions and user information. Employees can look forward to querying their internal knowledge base, similar to how Microsoft Copilot allows selected custom data sources such as user profile data to be integrated.

They will also benefit from improved guidance on responding or protecting themselves from cyber-attacks as this capability is integrated into security software, offering features like querying internal work instructions or configuration management databases (CMDBs). However, organizations must ensure these solutions are transparent, explainable, and resilient against manipulation. By focusing on realistic use cases and addressing associated risks, 2025 will mark a turning point in the responsible deployment of AI in cybersecurity.

Digital Twins: The New Frontier of Impersonation Attacks

Deepfake technology is poised to become one of the most significant cybersecurity challenges of 2025. As voice synthesis and video manipulation tools grow more accessible and convincing, cybercriminals will increasingly weaponize these innovations to create malicious digital twins. These hyper-realistic forgeries of individuals' voices, faces and behaviors start to blur the line between reality and fabrication, enabling a surge in impersonation-based attacks.

Such attacks may target organizations through fraudulent requests that appear to come from trusted executives or colleagues, bypassing traditional security measures. On a broader scale, digital twins could be used to spread disinformation, disrupt public trust or manipulate

money markets. The potential for harm extends beyond individual victims, impacting entire industries and eroding confidence in digital communications.

To combat this threat, organizations must adopt proactive measures. These can start with simple changes, such as switching back to a generic voicemail greeting that doesn't reveal personal details – as this helps stop AI-based voice cloning. Safeguarding trust will require vigilance, innovation and collective action in this evolving landscape. We'll see more use of AI-driven tools to detect deepfakes, robust authentication protocols such as multi-factor verification, and awareness campaigns to educate employees and the public. We'll also see a rise in 2025 of GenAI bots designed to trap and slow down the scammers – by tying them up in conversation loops that prevent them from getting through to a human.

Human-Centric Security: Empowering the Weakest Link

As cyber threats grow more sophisticated, organizations will recognize a vital truth: technology alone cannot secure them. It's a conundrum that human intuition is often the first line of defense in cybersecurity. Nevertheless, humans are prime targets for attacks such as phishing, social engineering and insider threats. In 2025, the focus will shift dramatically toward human-centric security. Businesses will increasingly invest in robust training programs that reach beyond annual compliance courses, emphasizing ongoing, interactive, and role-specific education.

These initiatives will aim to cultivate a culture of security awareness where every individual, from executives to contractors, will play an active role in defending against threats. Advanced tools like simulated phishing campaigns and real-time behavioral coaching have already become standard practices – in 2025, expect to see more of what's called "human surface management", underlining that it is essential to provide targeted and relevant training by individual and user groups to complement technical controls. This will also foster even stronger human-technology collaboration.

Furthermore, organizations will adopt metrics to measure the effectiveness of these programs by tying human behavior improvements to overall risk reduction. By empowering employees with the knowledge and skills to identify and mitigate risks, human-centric security strategies will transform the workforce from a vulnerability into a critical line of defense.

John Swanson
Global Security Portfolio Lead, Uvance, at Fujitsu

John has fulfilled many Information Security leadership roles across Public and Private sectors including security programme and capability leadership, consultancy (advisory and delivery), Security Operations Centres and Security Pre-sales functions.

He is responsible for developing Fujitsu's compelling Cybersecurity go to market propositions, which also underpin Fujitsu's wider Applications, Hybrid IT, Digital Workplace and Industry Sector aligned propositions. John focuses on the business aspects of Information Security and how Fujitsu can help clients enhance the strategic and operational maturity of the information security capabilities within their organizations.

