Identity-Based Attacks Lead Cybersecurity Concerns as AI Threats Rise and Zero Trust Adoption Lags

Keeper Security survey reveals a growing disconnect between AI risk readiness and zero trust maturity

LONDON, UNITED KINGDOM, July 4, 2025 /EINPresswire.com/ -- Identity-based attacks have taken centre stage as the top cybersecurity concern for organisations in the coming year, according to a new survey conducted by Keeper Security at Infosecurity Europe 2025. The leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections, found nearly one in four (23%) of cybersecurity professionals cited threats such as phishing, credential stuffing and other identity-targeted tactics as the most likely cause of a major breach – highlighting the growing intersection between AI-powered exploits and insufficient access controls.

The data also exposes a widening gap between zero-trust maturity and AI threat preparedness. Among organisations with a highly effective zero trust implementation, half of respondents said they were fully or partially confident in their ability to manage AI threats. In contrast, organisations with little to no zero-trust controls in place reported significantly lower levels of confidence.

Keeper's survey of 160 cybersecurity professionals at the conference reveals an industry under pressure: identity-driven risks are rising, while organisations grapple with the realities of defending against AI-generated phishing, deepfakes and automated exploits. Despite AI's promise, most professionals aren't confident in their readiness – only 12% said their organisation is fully prepared to handle AI-enhanced attacks, while more than half expressed uncertainty or doubt.

Yet, AI is also seen as a potential solution. Over half of respondents (53%) said AI-driven identity validation and authentication will be the most transformative technology in the next three to five years, surpassing traditional password solutions and quantum-resistant encryption.

While zero trust is widely acknowledged as a strategic imperative, real-world adoption remains slow. Just 18% of respondents reported a highly effective zero trust implementation. Nearly half (44%) said they haven't started implementing zero trust or do not view it as relevant to their organisation. Common roadblocks include budget constraints, executive support and the

complexity of integrating zero-trust frameworks within existing systems. Without these controls, gaps in identity and access management persist – leaving organisations vulnerable to privilege escalation, insider threats and account takeovers.

The survey also shed light on common PAM failures. The most cited mistakes included:

- Failing to enforce Multi-Factor Authentication (MFA) - 43%
- Granting excessive permissions - 35%
- Not revoking access when no longer needed - 34%
- Lack of visibility into privileged accounts - 30%
- Absence of dedicated PAM tools - 37%

These shortcomings are often exacerbated by third-party access risks (35%) and poor auditing practices (30%).

While over half (53%) believe AI risks are overhyped in the media, cybersecurity professionals take a more grounded view. Only 24% believe the industry is overstating the danger, and many acknowledge the very real threat of AI-enhanced attacks – especially when identity security is weak. Among end users, 42% believe AI threats are exaggerated, but a sizable portion (32%) remain undecided, signaling a need for more awareness and education.

“The findings from Infosecurity Europe 2025 reinforce what we see everyday – AI is reshaping the threat landscape, and identity-based attacks are becoming more precise, scalable and damaging,” said Darren Guccione, CEO and Co-founder of Keeper Security. “Organisations that haven’t embraced zero trust and strong privileged access controls are falling behind, both in protection and in confidence.”

###

About Keeper Security

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organisations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organisation against today’s cyber threats at KeeperSecurity.com.

Learn more: KeeperSecurity.com
Follow Keeper:
Facebook

(https://www.facebook.com/keeperplatform/?&utm_medium=press_release&utm_campaign=Communications)
Instagram
(https://www.instagram.com/keepersecurity/?&utm_medium=press_release&utm_campaign=Communications)
LinkedIn (https://www.linkedin.com/company/keeper-security-inc-/?&utm_medium=press_release&utm_campaign=Communications)
X
(https://twitter.com/keepersecurity?&utm_medium=press_release&utm_campaign=Communications)
YouTube (https://www.youtube.com/channel/UCKBCmTYm0iTX-eRuCK_s6qg?&utm_medium=press_release&utm_campaign=Communications)
TikTok
(https://www.tiktok.com/@keepersecurityinc?&utm_medium=press_release&utm_campaign=Communications)

Charley Nash
Eskenzi PR
charley@eskenzipr.com
