Business Professionals Are Half as Concerned as Technical Teams About AI-Driven Threats, Social Links Report Reveals

NEW YORK , NY, UNITED STATES, June 13, 2025 /EINPresswire.com/ -- A new study from Social Links, a leader in open-source intelligence solutions, reveals a gap between business and technical professionals when it comes to recognizing the risks posed by AI-powered cyberattacks. Despite the rapid rise in threat sophistication, business respondents appear significantly less concerned than their tech colleagues. This fact highlights a potential blind spot in organizational preparedness.

The survey gathered insights from 237 professionals (from CEO and Technical C-level to Cybersecurity Specialists and Product Managers) across various industries, including Financial Services, Technology, Manufacturing, Retail, Healthcare, Logistics, Government etc.

The results showed that just 27.8% of business people (professionals in non-technical, business-oriented roles) identified usage of AI to generate fake messages as one of the most relevant cyber threats. In contrast, 53.3% of technical professionals flagged it as a top concern—nearly double the level of alarm. A similar pattern emerged around deepfake technology: 46.7% of technical staff expressed concern, compared to just 27.8% of business respondents.

This gap underscores a critical vulnerability in organizational security: business professionals, who often make prime targets for sophisticated AI-driven social engineering and deepfake schemes, show notably lower levels of concern or awareness about these threats.

At the same time, the most vulnerable departments for cyber threats identified by respondents were Finance and Accounting (24.1%), IT and Development (21.5%), HR and Recruitment (15.2%), and Sales and Account Management (13.9%).

“This is no longer a question of ‘if’—AI-powered threats are already here and evolving quickly,” says Ivan Shkvarun, CEO of Social Links. “We’re seeing a clear gap between those building defenses and those most likely to be targeted. Bridging that gap requires not just better technical tools, but broader awareness and education across all levels of an organization.”

Key Insights from the Research:

Traditional vs. AI-Driven Threats: While phishing and email fraud remain the most cited threats

(69.6%), followed by malware/ransomware (49.4%), AI-driven attacks are gaining ground. 39.2% of respondents identified the use of AI to craft fake messages and campaigns as a major concern, and 32.9% pointed to deepfakes and synthetic identities—confirming that generative technologies are now a recognized part of the corporate threat landscape.

“Traditional threats like phishing and malware still dominate the charts. But what we’re seeing now is that AI isn’t replacing these risks, it’s supercharging them, turning generic scams into tailored operations—fast, cheap, and more convincing. That’s the real shift: automation and personalization at scale,” explains Ivan.

Employee Footprint Risk: 60.8% of respondents report that employees use corporate accounts for personal purposes—such as posting on forums, engaging on social media, or updating public profiles. 59.5% also link publicly available employee data (e.g., LinkedIn bios, activities in forums and blogs) to real cyber incidents, identifying it as a recurring entry point for attacks.

Unregulated AI Adoption: Over 82% of companies let employees use AI tools at work, yet only 36.7% have a formal policy that controls how those tools are used. This gap fuels “Shadow AI”—the unsanctioned adoption of chatbots, code assistants, or other AI services without IT oversight, which can leak sensitive data and create hidden security and compliance risks.

“You can’t really stop people from using work accounts or data when they’re active online. The same goes for AI tools: people will use them to save time or get help with tasks, whether there’s a policy or not. But all this activity leaves digital traces. And those traces can make it easier for scammers to find and target employees. What actually helps is teaching people how to spot the risks and giving them the right tools to stay safe, instead of just saying ‘don’t do it,’” explains Ivan.

The research emphasizes that effective cybersecurity in the AI era requires a holistic approach that extends beyond technical controls to include comprehensive human-centric security programs. Employee training on safe AI use was overwhelmingly perceived by survey respondents as the most effective mitigation measure for "Shadow AI" (72.2%), followed by the development of internal policies (46.8%).

Social Links is committed to addressing these evolving challenges and has recently launched the Darkside AI initiative, aimed at further exploring and mitigating the risks posed by advanced AI-driven threats.

About Social Links:
Social Links is a global provider of open-source intelligence (OSINT) solutions, recognized as an industry leader by Frost & Sullivan. Headquartered in the United States, the company also has an office in the Netherlands. Social Links brings together data from over 500 open sources covering social media, messengers, blockchains, and the Dark Web, enabling users to visualize and

analyze a comprehensive informational picture and streamline investigations. Its solutions support essential processes across various sectors including law enforcement, national security, cybersecurity, due diligence, banking, and more. Companies from the S&P 500 and public organizations in over 80 countries rely on Social Links products every day.

Contacts:
Email: sociallinks@perform.it.com
Website: https://sociallinks.io/

Social Links Press Office
PER:FORM
email us here
Visit us on social media:
Other
