AI Has Changed the Cybersecurity Threat Landscape for SMBs, Warns Eclipse Networks

Atlanta-Based IT Leader Urges SMBs to Audit Infrastructure and Establish AI Governance Before Adopting New AI Platforms

AI cybersecurity threats are on the rise

ATLANTA, GA, UNITED STATES, June 2, 2026 /EINPresswire.com/ -- Eclipse Networks, Atlanta's oldest managed IT and cybersecurity provider serving small and mid-sized businesses, today issued an urgent advisory for business leaders navigating the rapidly evolving threat of artificial intelligence in cybersecurity. As organizations rush to adopt AI tools and platforms, Eclipse Networks is calling attention to two converging risks that are leaving SMBs dangerously exposed: the use of AI by cybercriminals to conduct more sophisticated attacks, and the uncontrolled use of AI by employees inside organizations that have not yet established governance frameworks.

> If your infrastructure hasn't been audited and your team hasn't been trained, you're adding risk faster than you're adding capability."
>
> *Steve Ryerse*

AI-driven cyber threats are accelerating faster than most organizations are prepared to address. According to a 2025 Vistage CEO survey, nearly a quarter of SMBs experienced a cybersecurity incident last year, yet 16% of small and mid-sized businesses still don't have any formal cyber strategy in place.

"We used to tell clients that biometrics were one of the strongest forms of authentication available. That is still true when it's part of a layered strategy. What's changed is that no single factor is enough anymore," said Steve Ryerse, Co-Founder of Eclipse Networks. "The businesses we're most concerned about right now are the ones rushing to adopt AI platforms before they've done the foundational work. If your infrastructure hasn't been audited and your team hasn't been trained,

you're adding risk faster than you're adding capability."

Eclipse Networks is highlighting three specific threat vectors that are fundamentally altering the cybersecurity posture of small and mid-sized businesses.

Fingerprint scanners, facial recognition, and voice verification — long considered stronger alternatives to passwords — are increasingly vulnerable to AI-powered spoofing. Security researchers have demonstrated that fingerprint patterns can be reconstructed from high-resolution photos taken from several meters away, using machine learning models to enhance partial prints into usable replicas. Biometric spoof attempts surged 230% year-over-year, fueled in part by generative AI tools now available for under $20.

A public LinkedIn headshot or a photo from a company event can now serve as source material for a biometric spoofing attack. Biometrics remain a valuable layer of defense, but must be combined with additional controls.

Generative AI has eliminated many of the telltale signs that once made phishing attempts identifiable. Attackers can now craft personalized messages using details pulled from public sources — social media, company websites, press releases, and LinkedIn activity — producing communications that are nearly indistinguishable from legitimate correspondence.

Beyond email, AI-generated voice and video are being used to impersonate executives in real time. Deepfake audio has been used to authorize fraudulent wire transfers. Fake video calls have been used to extract credentials from employees who believed they were speaking with a trusted colleague or manager.

The scale of the problem is significant. AI-assisted attacks increased 72% over the last two years, and phishing incidents surged 1,265% due to the proliferation of generative tools, according to research from TotalAssure. According to Pindrop's 2025 Voice Intelligence & Security Report — based on analysis of over 1.2 billion calls — deepfake fraud attempts rose by more than 1,300% in 2024, jumping from an average of one per month to seven per day. The average cost of a deepfake attack for a business now exceeds $500,000 per incident. The average cost of an AI-powered breach overall is $5.72 million.

While external threats dominate the headlines, Eclipse Networks is drawing equal attention to the risk posed by unsanctioned AI use inside organizations — a phenomenon known as shadow AI.

According to IBM's 2025 Cost of Data Breach Report, one in five organizations has already experienced a breach linked to unsanctioned AI use. Employees using unauthorized AI tools are rarely acting with harmful intent. They are attempting to work more efficiently. The risk arises from the gap between individual intent and organizational oversight — a gap that most SMBs have not yet addressed.

Organizations with high levels of shadow AI exposure experience average breach costs of $4.63 million, representing a $670,000 premium over those with low or no shadow AI activity, according to IBM's findings.

Eclipse Networks is urging business leaders to treat AI adoption as both an operational and a security decision. Before deploying AI platforms or agents across an organization, the company recommends a structured assessment that addresses the following questions:

- Where is sensitive data stored, and who currently has access to it?
- Which AI tools are already in use by employees, with or without IT approval?
- Do existing security controls extend to AI-connected systems and integrations?
- Have employees received training on appropriate AI use and data handling policies?
- Is there a documented governance framework covering AI adoption and acceptable use?

Eclipse Networks provides cybersecurity risk assessments, infrastructure audits, and AI governance consulting as part of its managed IT services offering. The company works with organizations across healthcare, construction, legal services, and professional services to build security postures that are practical, well-documented, and aligned with how the business actually operates.

About Eclipse Networks

Eclipse Networks is a people-first managed IT and cybersecurity provider serving small and mid-sized businesses across the Southeast. Founded in 1989 and headquartered in Atlanta, Georgia, Eclipse Networks provides managed IT services, cybersecurity and incident response, cloud infrastructure, backup and data protection, disaster recovery, and VoIP solutions. The company operates its own Private Cloud Data Center and delivers enterprise-grade technology with a local, relationship-driven approach. Eclipse Networks is guided by the principle that technology should be clear, secure, and aligned with the goals of the businesses it supports. For more information, visit www.eclipse-networks.com or call (770) 399-9099.

Aly Lee
Eclipse Networks
+1 770-399-9099
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.