## THOUGHT LEADER:

**TONY SCRIBNER, CISSP**
*VP - Solution Advisory*
*Bluewave*

Tony Scribner, Bluewave's Vice President of Solution Advisory started with the company in 2024. He has over 35 years of industry experience in infrastructure, managed IT services, software development, telecommunications, and Cybersecurity. Tony also holds the ISC2 CISSP Certification.

Prior to joining Bluewave, he served as Chief Information Security Office and Field CTO of Ntirety, a global Managed Services Provider. Tony's executive leadership experience includes, CTO of a medical startup, Senior Solution Architect at Apparatus and Comsys, and CTO at Kinetic Corporation. He has also held strategic technology positions at GE Aircraft Engines, Litton, Silicon Graphics, and Broadwing/ Cincinnati Bell.

Tony is an alumnus of The University of Cincinnati, and he resides in Louisville, KY with his wife and twin boys.

Bluewave
TECHNOLOGY GROUP


GETTY IMAGES

**How prevalent is shadow AI in corporate enterprises, and what are the key risks it poses?**

Shadow AI, the unauthorized use of AI tools by employees, surged in 2024, with over 65% of enterprises reporting unapproved AI use. Key risks include data breaches from unsecured platforms, compliance violations, and inconsistent responses disrupting operations. To mitigate, businesses should enforce AI governance policies, conduct regular employee training, and deploy approved AI tools. Centralized oversight and real-time monitoring can reduce vulnerabilities, ensuring data security and regulatory compliance while harnessing AI's benefits for innovation.

**How can small businesses protect themselves from cyberattacks, given they may believe they're not targets?**

Small businesses are prime targets, with 43% of cyberattacks in 2024 aimed at them due to weaker defenses. Many falsely assume their size makes them invisible. Protection starts with employee training on phishing and password hygiene, implementing multi-factor authentication, and using affordable security tools like firewalls and VPNs. Regular data backups and incident response plans are critical. Investing in managed security services can bridge resource gaps, ensuring robust protection against ransomware and malware threats.

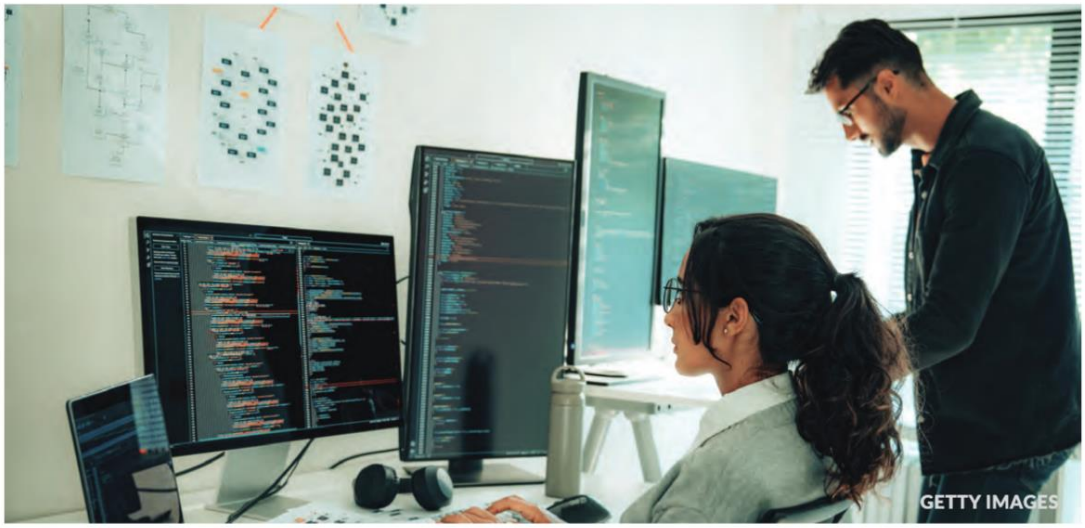
**What role will quantum technology play in cybersecurity for businesses in 2025 and beyond?**

Quantum technology, particularly quantum key distribution (QKD), will enhance cybersecurity by offering unbreakable encryption for data transmission. For the average company, adopting quantum-resistant algorithms when available is practical as quantum computing continues to develop, it will threaten current encryption

standards. IT leaders should prioritize assessing their cryptographic systems and partnering with vendors offering quantum-safe solutions. While full quantum adoption is distant, early preparation ensures long-term data security, protecting intellectual property and customer trust against future quantum-based attacks.

### How can AI-driven cybersecurity tools improve threat detection and response in 2025?

AI-driven cybersecurity tools will revolutionize threat detection in 2025 by leveraging machine learning to analyze vast network data in real-time. These tools identify anomalies, predict attack patterns, and automate responses, reducing detection times by up to 60%. Benefits include fewer false positives, faster incident containment, and reduced IT workload. However, businesses must address AI biases and ensure human oversight to avoid flawed decisions. Regular updates and training data audits are essential to maximize AI's effectiveness in combating sophisticated cyberthreats.


GETTY IMAGES

### What are the emerging cybersecurity challenges posed by IoT proliferation in enterprises?

The explosion of IoT devices in 2024, with enterprises managing thousands of connected endpoints, heightens cybersecurity risks. Each device is a potential vulnerability for malware or unauthorized access. Challenges include weak device authentication and unpatched firmware. Businesses should implement network segmentation, enforce strong access controls, and use AI-driven monitoring to detect anomalies. Regular device audits and vendor partnerships for secure IoT solutions are critical to safeguard operations and customer data against escalating IoT-based attacks in 2025.