Hilco Global
Asset Smarter

SMARTER PERSPECTIVE: ARTIFICIAL INTELLIGENCE

Managing Shadow AI Risk: A Strategic Approach for Organizations

By Bob Olsen, MBA, MS, CISSP, CCSP

October 2025 The rapid adoption of artificial intelligence across organizations has introduced a new category of cybersecurity risk that extends far beyond traditional shadow IT concerns. Shadow AI - the unauthorized deployment and use of AI-powered tools and capabilities within organizations - presents unique challenges that require specialized governance frameworks and risk management strategies.

The Dual Nature of Shadow AI Exposure

Organizations must contend with two distinct manifestations of shadow AI risk. The first involves employees independently adopting external AI platforms and services without organizational oversight or approval. These tools range from popular generative AI chatbots to specialized automation platforms that employees discover and implement to enhance their productivity or solve specific business challenges.

The second category presents a more subtle but equally significant risk: AI capabilities that activate automatically within previously approved enterprise applications. When established software vendors integrate AI features into their platforms - often enabled by default - organizations find themselves managing AI risks they never explicitly accepted, evaluated or even considered. Companies on average have 67 different GenAI tools running across their systems, yet 90% lack proper licensing or approval.[1] Additionally, on average, 65% of employees use ChatGPT on the free tier where data can be used to train models and potentially lead to corporate information leakage.[2]

Understanding the Risk Landscape

The financial implications of unmanaged AI adoption are substantial. Organizations experiencing security incidents related to unauthorized AI usage can expect significantly higher remediation costs and longer recovery times compared to traditional data breaches. The complexity of these incidents stems from the difficulty in tracing data flows through AI systems, understanding what information was processed, and determining potential exposure scope.

Beyond immediate financial impact, shadow AI creates persistent compliance challenges. Regulatory frameworks struggle to keep pace with AI advancement, leaving organizations in uncertain territory regarding their obligations when employees use AI tools to process regulated data. This uncertainty is particularly acute in healthcare, financial services, and other heavily regulated industries where data handling requirements are stringent. These challenges and risks will grow over time unless organizations take proactive steps to address these issues going forward.

Establishing Comprehensive Visibility

Effective shadow AI risk management begins with understanding the current state of AI adoption across the organization. Traditional IT discovery methods prove insufficient for identifying AI usage patterns, as many AI interactions occur through web interfaces, mobile applications, or embedded features within existing software platforms.

Organizations need specialized monitoring capabilities that can identify AI-related network traffic, detect when employees are uploading data to external AI services, and track the activation of AI features within approved applications. This visibility must extend beyond technical detection to include user behavior analysis and regular assessments of employee AI adoption patterns. This specialized monitoring will help organizations better understand their unique risks, inform their governance program and ensure they are implementing controls that are impactful and effective.

Developing Adaptive Governance Frameworks

Traditional IT governance models require significant adaptation to address AI-specific risks. Effective AI governance frameworks must balance innovation enablement with risk mitigation, recognizing that overly restrictive policies often drive further shadow adoption rather than compliance.

Successful governance approaches establish clear criteria for evaluating AI tools and services, create streamlined approval processes for legitimate AI needs, and provide transparent communication about approved alternatives. These frameworks must be dynamic, capable of adapting quickly as new AI capabilities emerge and organizational needs evolve.

Building Organizational AI Literacy

The human element remains the most critical factor in shadow AI risk management. Employees often adopt unauthorized AI tools not out of malicious intent but resulting from genuine business needs combined with insufficient awareness of associated risks. Organizations must invest in comprehensive AI literacy programs that help employees understand both the benefits and risks of AI adoption.

Effective education programs address practical scenarios employees encounter daily, provide clear guidance on approved AI usage, and establish accessible channels for requesting new AI capabilities. This education must be ongoing, as the AI landscape evolves rapidly and new risk scenarios emerge regularly.

Creating Secure AI Adoption Pathways

Rather than focusing solely on restriction, organizations should establish clear and reasonable pathways for secure AI adoption. This includes maintaining catalogs of approved AI tools, providing guidance on safe usage practices, and creating processes for evaluating new AI requests quickly and fairly.

Organizations should also implement technical safeguards that enable AI usage while maintaining security and compliance. This might include deploying AI gateways that filter sensitive data, implementing data loss prevention controls specifically designed for AI interactions, or establishing secure AI sandboxes for experimentation. It is also critically important to ensure that the vendor risk management program adequately addresses new functionality and the associated risks that are inherent in previously approved applications such as Adobe.

Governance Monitoring and Continuous Improvement

Shadow AI risk management requires continuous governance monitoring and iterative improvement. Organizations must regularly assess the effectiveness of their governance frameworks, update policies based on emerging threats and regulatory guidance, and adjust their approach based on employee feedback and business needs.

This includes establishing metrics for measuring shadow AI risk, tracking compliance with AI governance policies, and evaluating the business impact of AI adoption initiatives. Regular risk assessments should examine both technical vulnerabilities and organizational processes to identify areas for improvement.

Conclusion

Managing shadow AI risk requires a fundamental shift from reactive policy enforcement to proactive risk management. Organizations that successfully navigate this challenge will create frameworks that protect against AI-related risks while empowering employees to leverage AI capabilities safely and effectively. This balanced approach recognizes that AI adoption is inevitable and focuses on ensuring it occurs within appropriate risk boundaries rather than attempting to prevent it entirely.

Shadow AI should not become an organizational blind spot. Organizations are encouraged to conduct comprehensive assessments of current AI usage—including both sanctioned and unsanctioned applications—to accurately determine risk exposure. Developing clear AI governance policies and offering approved, productivity-focused alternatives can help maintain security and compliance while still supporting employee needs. Taking prompt action is important, as gaps in AI governance increase the likelihood of data breaches, compliance violations, and operational disruptions that proactive risk management could have prevented.

Sources:

[1,2] *Axios*

BOB OLSEN, MBA, MS, CISSP, CCSP
MANAGING DIRECTOR/COO
GLOBAL CYBER ADVISORS
PROFESSIONAL SERVICES

Bob can be reached directly at rolsen@hilcoglobal.com.