Why Every CEO Needs to Understand the Risk of **Shadow AI**

UNIQUS x CRANIUM

Swipe >>

Why Is Shadow AI a Growing Concern?

Imagine a massive data breach: source code, confidential emails, and sensitive documents leaked—all because an employee used an unauthorized AI tool. This is the threat of Shadow AI, where employees or departments adopt artificial intelligence tools without approval or oversight from IT or security teams. While these tools might boost productivity, they can also create serious security risks. For example, Samsung banned AI chatbots like ChatGPT after sensitive data, including source code and meeting minutes, was accidentally shared[1]. Other organizations followed suit, introducing similar restrictions on AI use.

What Are the Risks of Shadow AI?

Security Concerns

- **Unregulated Usage**

A recent survey revealed that over 50% of U.S. employees already use generative AI tools at work without formal approval[2]. Even more troubling, 41% of employees modify or create technology outside IT's knowledge, which Gartner[3] predicts will rise to 75% by 2027.

- **Data Breaches**

After Samsung's data leak, major financial institutions like JPMorgan, Goldman Sachs, and Wells Fargo restricted employee AI use[4]. Amazon also issued warnings about AI misuse[5]. Data not adequately managed or classified—often called "shadow data"—was involved in 35% of breaches, with an average cost of $5.27 million per breach[6].

- **Intellectual Property Theft**

Sensitive data breaches have led to a 26.5% increase in intellectual property theft, causing higher financial losses and risks to market share[7].

[1] https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak
[2] https://www.lakera.ai/blog/shadow-ai
[3] https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024
[4] https://www.bloomberg.com/news/articles/2023-02-24/citigroup-goldman-sachs-join-chatgpt-crackdown-fn-reports?sref=CSMHWBLp
[5] https://timesofindia.indiatimes.com/gadgets-news/amazon-warns-employees-against-using-third-party-ai-tools-for-work/articleshow/108013700.cms
[6] https://www.ibm.com/blog/hidden-risk-shadow-data-ai-higher-costs/
[7] https://www.ibm.com/blog/hidden-risk-shadow-data-ai-higher-costs/

Compliance Risks

- **Regulatory Penalties**

Non-compliance with global AI regulations, such as the EU AI Act[8], can lead to fines as high as €35 million or 7% of global turnover. Countries like the U.S., UAE, and Saudi Arabia are also advancing strict AI governance.

- **Copyright Infringement**

Generative AI tools often rely on copyrighted data during training, leading to legal disputes. For instance, Google's Imagen AI faced accusations of unauthorized use of artists' work[9].

- **Reputation Damage**

Shadow AI increases the risk of data leaks, eroding public trust and damaging an organization's credibility.

Operational Challenges

- **Inefficiencies**

Unauthorized tools disrupt workflows, complicate data governance, and add to IT workloads. They also create vulnerabilities, making organizations more susceptible to cyberattacks.

- **Lack of Oversight**

Without monitoring mechanisms like audit trails or performance checks, ensuring ethical and responsible AI use is nearly impossible. This opens the door to biased outcomes, unethical behavior, and security loopholes.

[8] https://artificialintelligenceact.eu/
[9] https://www.reuters.com/legal/litigation/google-sued-by-us-artists-over-ai-image-generator-2024-04-29/

How to Discover and Manage Shadow AI

Understanding and managing Shadow AI requires a systematic approach:

1. **Strengthening the Three Lines of Defense**
   - Operational Teams: Educate teams on the risks of unauthorized AI use.
   - Risk and Compliance: Ensure tools meet regulatory and organizational standards.
   - Audit: Provide auditors with accurate data to assess exposure and vulnerabilities.

2. **Identifying Threats**
   - Open-Source Models: Evaluate licensing implications for unapproved open-source AI tools.
   - Third-Party Tools: Monitor unauthorized software to avoid unexpected costs and vulnerabilities.

3. **Addressing Security Risks**
   - API and Injection Attacks: Secure Shadow AI tools against malicious inputs and adversarial prompts.
   - Access Control Weaknesses: Implement role-based access control (RBAC) to prevent unauthorized usage.

4. **Mitigating Hidden Costs**
   - Unexpected Expenses: Unauthorized tools may incur subscription fees and increase IT support costs.
   - Technical Debt: Shadow AI creates long-term integration and security challenges.

At a large life sciences organization, the security team actively identified where AI was being used across the enterprise, a challenging task given the multitude of different tools and technologies in use and in development. Across the organization, there were ~70,000 different code repositories, and there was no way to identify where AI was being instantiated quickly. The company has worked with Cranium and its Detect AI feature to tackle this problem and determine where AI was being leveraged, addressing the challenge of Shadow AI.

Steps to Overcome Shadow AI Risks

1. Identification

Use automated tools to inventory all AI tools in use—both approved and unapproved. Detect applications accessing organizational data.

2. Change Assessment

Evaluate Shadow AI's impact on workflows, compliance frameworks, and security protocols. Identify dependencies on third-party tools.

3. Mitigation

- Policy Updates: Clearly define AI approval and usage guidelines.
- Employee Training: Educate teams about the risks and encourage using approved tools.
- Enhanced Security: Strengthen controls like endpoint detection and network segmentation.
- Centralize AI oversight and monitor compliance.

Why Organizations Must Act Now

Managing Shadow AI is not just about compliance but safeguarding your organization's future. Proactively addressing Shadow AI ensures security, regulatory alignment, and operational efficiency, enabling long-term success in an AI-driven world.

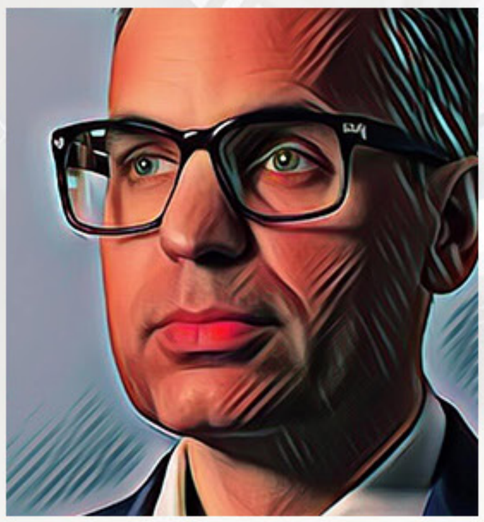
A TEAM THAT
YOU CAN TRUST TO DELIVER

Abhijit Varma
Partner, Tech Consulting
av@uniqus.com

Bharat Chadha
Partner, Tech Consulting
bharatchadha@uniqus.com

Mitushi Pitti
Partner, Tech Consulting
mitushipitti@uniqus.com

Jonathan Dambrot
CEO & Co-Founder
jdambrot@cranium.com



Felix Knoll
COO/CRO & Co-Founder
fknoll@cranium.com

Daniel Christman
Director of AI Programs, Co-Founder
dchristman@cranium.com