DAFITC 2026 · ACCELERATING THE DIGITAL EDGE

Shadow AI in the Agency

The Data Behind the Problem, and What to Do About It

Dr. Kenley Hall Obas, Ed.D.
Artificial Intelligence Researcher
Alabama State University

Ahmad Austin
Cybersecurity Executive & Author
Founder & CEO, Cy3 Security

Montgomery, AL · August 24-26, 2026

1 in 5

breached organizations were compromised through shadow AI: unsanctioned AI tools employees adopted without security sign-off.

+$670K

added to the average breach cost when shadow AI was involved at high levels

65%

of shadow AI breaches exposed customer PII, vs. 53% global average

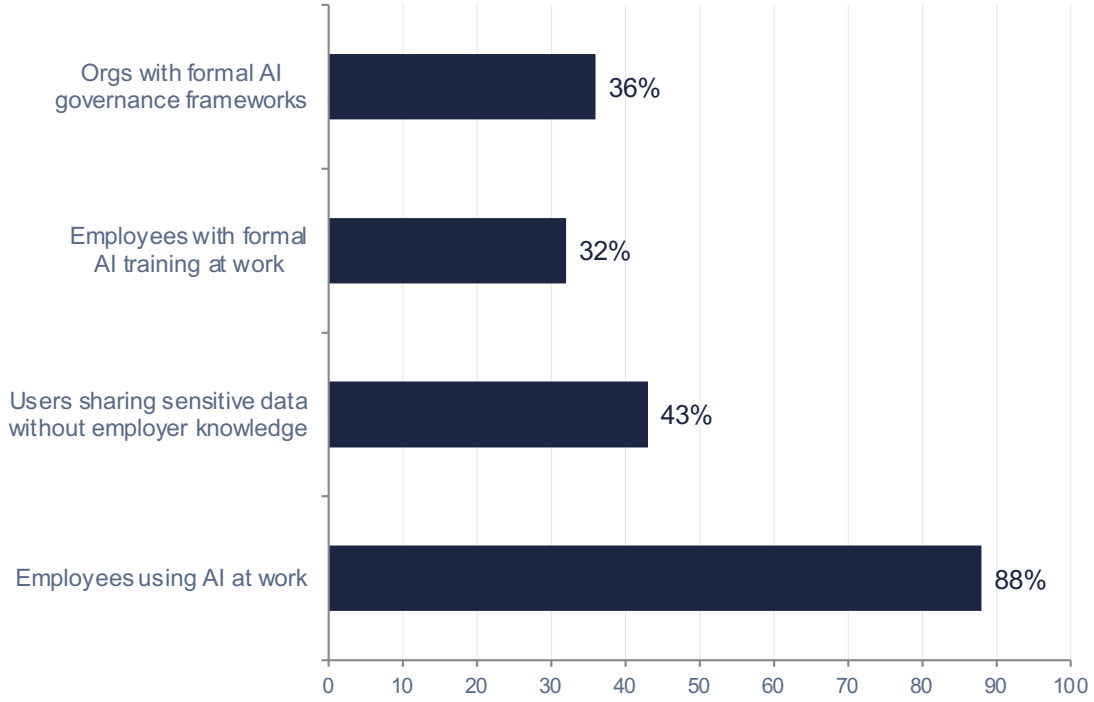
97%

of AI-breached organizations lacked proper AI access controls

Source: IBM Cost of a Data Breach Report 2025

THE SCALE OF THE PROBLEM

Your Workforce Is Already Using AI



The Gap Is the Risk

Adoption is near-universal. Training and governance are not. That distance between use and oversight is exactly where shadow AI incidents happen.

Sources: SQ Magazine Shadow AI Usage Statistics 2026; National Cybersecurity Alliance / CybSafe "Oh, Behave!" Report 2025-26

IT HAS ALREADY HAPPENED

Case in Point: Samsung, 2023

Within 20 days of permitting ChatGPT use, Samsung's semiconductor division logged three separate leaks of confidential material, each by an employee just trying to work faster.

1

The Debug Request

An engineer pasted proprietary source code into ChatGPT to check it for errors.

2

The Optimization Ask

Another employee uploaded defect-detection code, seeking optimization suggestions.

3

The Meeting Notes

A recorded internal meeting was transcribed and fed to the tool to generate minutes.

The result: a company-wide generative AI ban within a month. Prohibition became the fallback because governance wasn't ready. Don't let that be your only option.

Sources: Forbes (May 2023); Bloomberg reporting; AI Incident Database #768

WHY SHADOW AI BREACHES COST MORE

Invisible Tools, Slower Detection, Wider Exposure



Longer Detection

Shadow AI incidents took longer to identify and contain than the global average. Unsanctioned use doesn't trigger traditional alerts. It blends into normal web traffic.



More Sensitive Data

These breaches disproportionately exposed customer PII (65% vs. 53% average) and intellectual property (40% vs. 33% average).



Multi-Environment Spread

62% of shadow AI breaches involved data stored across multiple environments. One unmonitored tool can create organization-wide exposure.

Shadow AI has displaced the security skills shortage as one of the top three costliest breach factors tracked by IBM.

Source: IBM Cost of a Data Breach Report 2025

THE HUMAN LAYER

This Is a Behavior Problem, Not a Malice Problem

60%	of employees say they will use shadow AI anyway if it helps them meet a deadline. Productivity pressure beats policy when the two collide.
56%	of workers say they lack clear guidance on AI usage policies. Most shadow use starts in a guidance vacuum, not an act of defiance.
47%	access AI through personal or unmanaged accounts, completely bypassing whatever enterprise controls do exist.
40%	fewer security incidents reported by organizations that run AI training programs. Behavior change works when you invest in it.

Sources: SQ Magazine Shadow AI Usage Statistics 2026 (compilation of enterprise survey data)

THE GOVERNANCE VACUUM

Why Existing Frameworks Don't Cover This

- Acceptable Use Policies written pre-2022 rarely contemplate generative AI at all.
- CMMC and NIST 800-171 controls govern systems of record, not transient AI interactions.
- Employees experience AI as a conversation, not a data transfer. Training hasn't caught up to that mental model.
- Only 29% of companies regularly audit AI usage across teams; most have no visibility at all.
- 44% of organizations are still developing AI policies that have not yet been implemented.

The policy gap isn't laziness, it's a category problem. Organizations are governing a new behavior class with frameworks built for a different era.

Sources: SQ Magazine 2026; Foley & Lardner, "Shadow AI in the Workplace" (April 2026)

THE GOVERNANCE MODEL

What Good Governance Looks Like

01

Inventory Before Policy

Survey employees, analyze network traffic, review extension installs. You can't govern what you haven't identified.

02

Tiered Approval

Fast-track low-risk tools so employees have a sanctioned path instead of going around it.

03

Provision Alternatives

Providing approved alternatives measurably reduces unauthorized use. Prohibition without provision fails.

04

Reframe Training

Teach AI input in the same terms staff already use for file sharing and email classification.

05

Monitor, Don't Surveil

Network-level detection and DLP rules for AI endpoints, without driving use further underground.

06

Build the IR Playbook

Most organizations have no response plan for “CUI pasted into a consumer AI tool.” Build one now.

START THIS WEEK

Five Moves You Can Make Right Now

1. **Get visibility first** Use SaaS discovery, browser extension audits, and endpoint logs to surface AI use already happening.
2. **Skip the blanket ban** Bans push usage underground into less visible tools. Enable safe use with clear data rules instead.
3. **Borrow from shadow IT** Enablement plus guardrails beat lockdowns: lightweight approvals and secure internal alternatives.
4. **Set role-based allowances** Developers, marketing, and HR don't need the same access. Match permissions to team function.
5. **Stand up an intake process** A simple, promoted request form keeps new tools visible. Reassess approvals every 6 to 12 months.

890%

surge in GenAI traffic across enterprises in 2024

66

GenAI apps in use at the average organization, about 10% of them high risk

2.5X

increase in GenAI-related data loss prevention incidents, now 14% of all DLP events

Source: Palo Alto Networks, "What Is Shadow AI?" (Cyberpedia) and The State of Generative AI 2025

TAKEAWAYS

Three Things to Do in the Next 30 Days



Survey

Run an anonymous, no-consequence inventory of current AI tool use across your organization.



Audit Your AUP

Pull your current Acceptable Use Policy and identify the AI gap in writing.



Provision One Alternative

Identify a single sanctioned AI tool you can offer in place of the consumer tools already in use.

REFERENCES

Sources & Further Reading

- **IBM Cost of a Data Breach Report 2025**
  Primary source for breach frequency (20%), added cost (+$670K), PII/IP exposure rates, and multi-environment findings.

- **Palo Alto Networks, "What Is Shadow AI?" (Cyberpedia) and The State of Generative AI 2025**
  Five-step protection framework, GenAI traffic growth (890%), average app counts, and DLP incident trends.

- **National Cybersecurity Alliance & CybSafe, "Oh, Behave!" Annual Report 2025-26**
  Survey finding that 43% of AI users have shared sensitive company information with AI tools without employer knowledge.

- **Foley & Lardner LLP, "For Your Eyes Only? Not Quite: Shadow AI in the Workplace" (April 2026)**
  Legal perspective on governance, visibility, and integrating AI oversight into existing compliance programs.

- **SQ Magazine, "Shadow AI Usage Statistics 2026"**
  Compilation of workforce adoption, training, and policy statistics across enterprise surveys.

- **Samsung / ChatGPT incident reporting (Forbes, Bloomberg, May 2023; AI Incident Database #768)**
  Documented real-world shadow AI data leakage incidents and the resulting company-wide generative AI ban.

Statistics cited reflect published survey and incident research as of mid-2026. Verify current figures before reuse.

Questions & Discussion

The data says shadow AI is already inside your organization. The only question is whether governance gets there before the incident does.

Dr. Kenley Hall Obas, Ed.D.
Kindred Technology Group

Ahmad Austin
Cy3 Security