enterprise CONNECT

AI Governance: Putting the Horse in Front of the Cart

Melissa Swartz

Independent Consultant

GLOBAL TECH
Empowering the World through Cutting-Edge Technology

mswartz@globaltech.net
www.GlobalTech.net
www.linkedin.com/in/MelissaSwartz

no jitter | Produced by enterprise CONNECT

SCTC SOCIETY OF COMMUNICATIONS TECHNOLOGY CONSULTANTS INTERNATIONAL

BUSINESS COMMUNICATIONS STRATEGIES
An Essential Buyer's Resource

Brian Harrison

Chief Technology Officer

Broward College

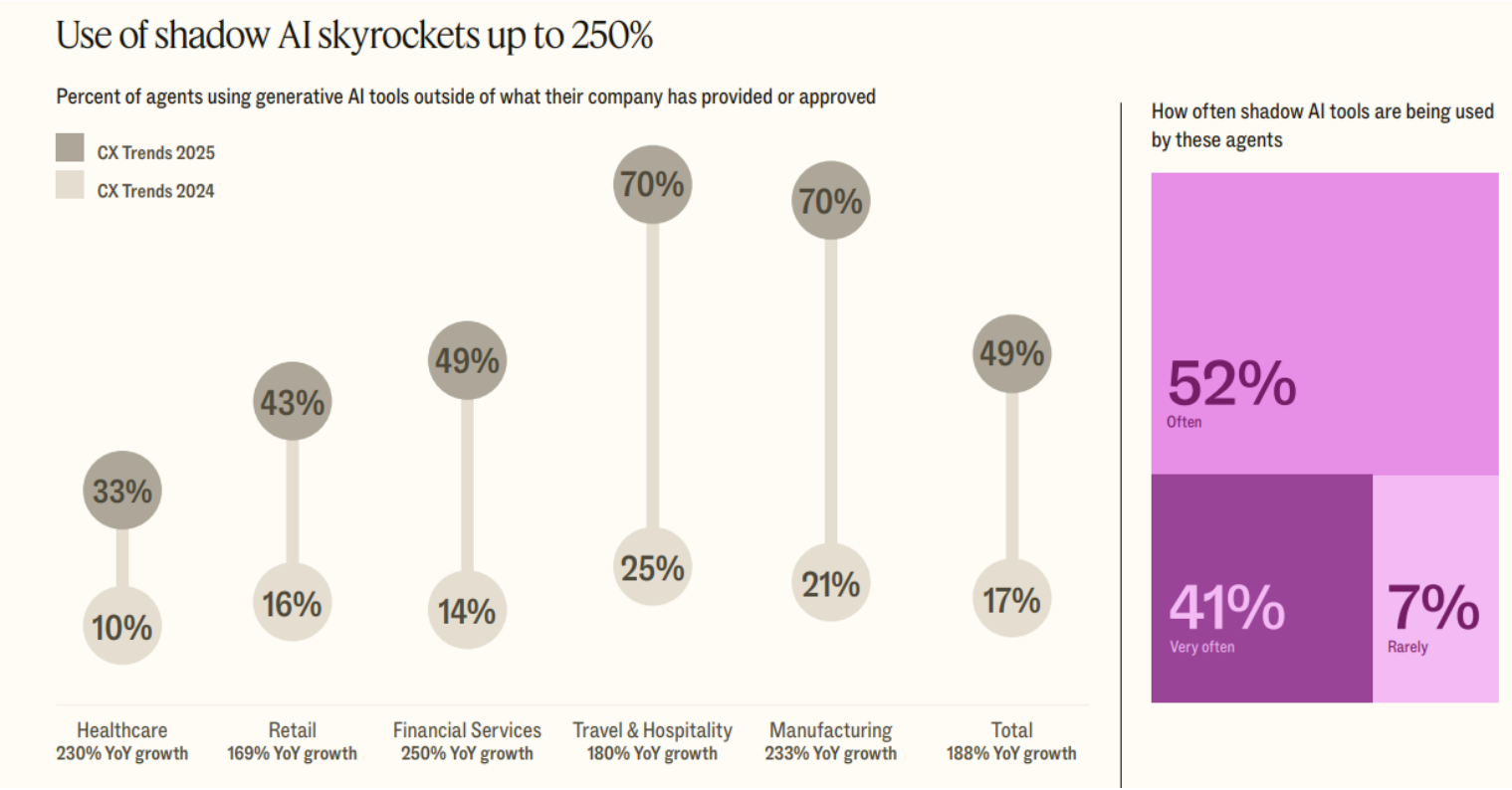
Setting the Stage: The New AI Reality

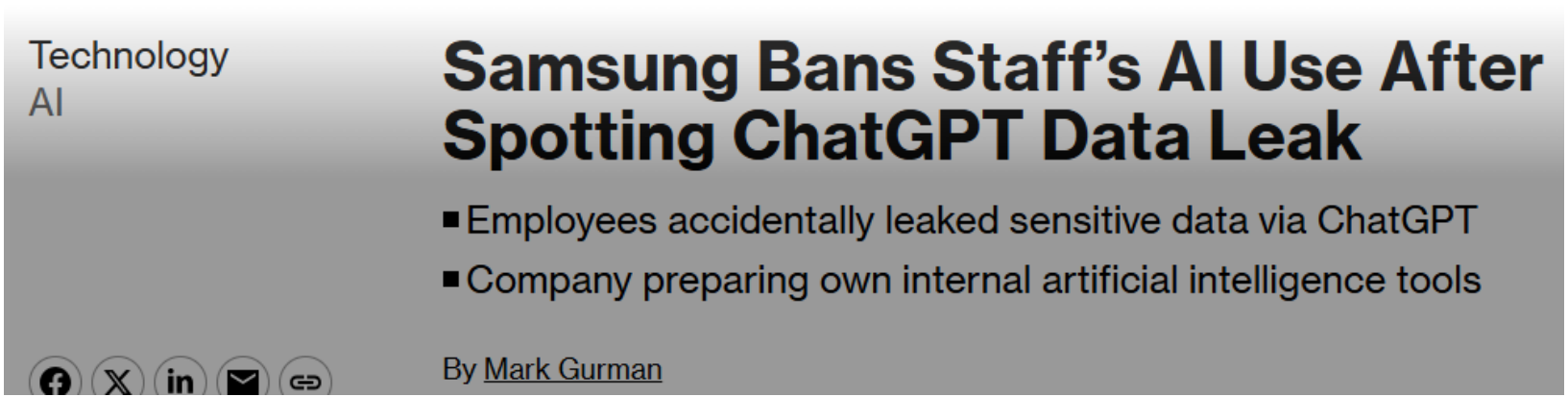
There is quiet AI revolution in your enterprise

Employees are *already* using AI tools, often without oversight

Example: Marketing team using ChatGPT to draft customer communications, potentially exposing sensitive data

Zendesk CX Trends 2025 Report found:





https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak?embedded-checkout=true

Free eBook:

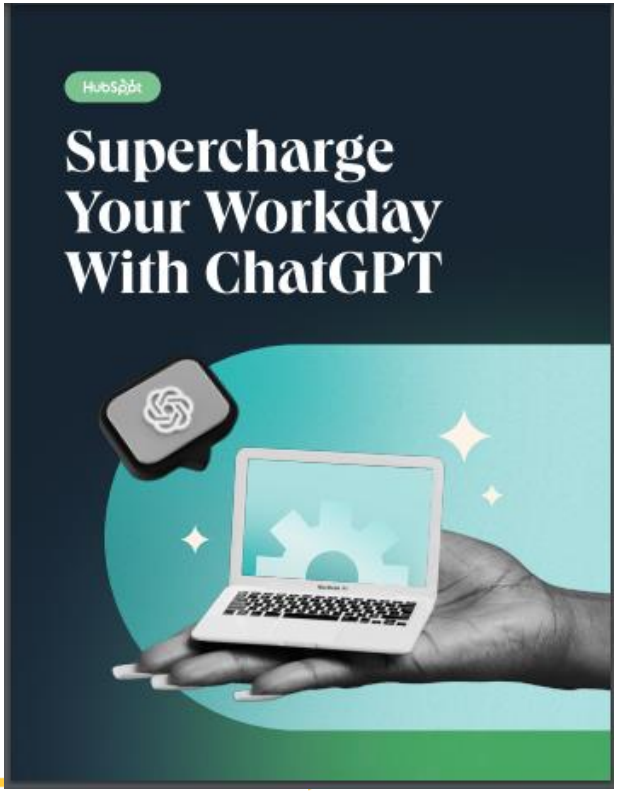


Table of Contents

https://www.hubspot.com/hubfs/%5Bebook%5D%20Supercharge%20Your%20Workday%20with%20ChatGPT.pdf?

Traditional IT governance isn't enough

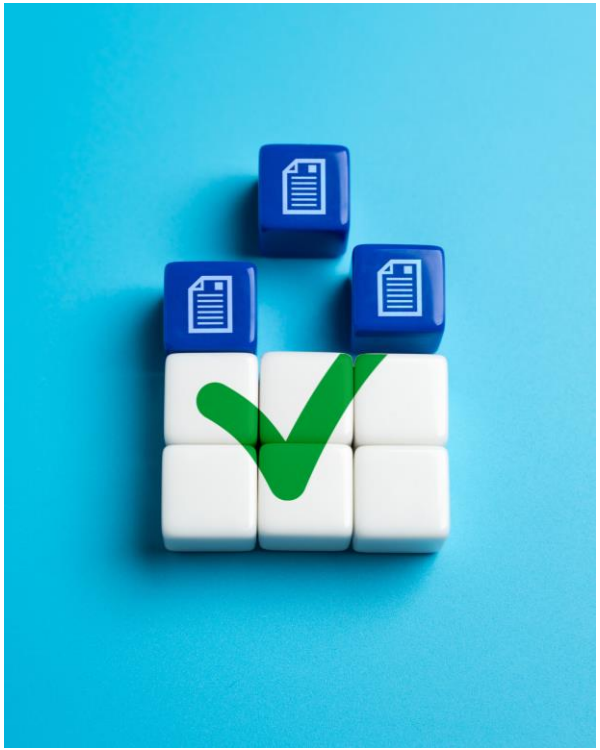
Unique challenges of AI

- **Speed:** AI tools can process and generate enterprise data in seconds
- **Scale:** A single prompt can expose massive amounts of sensitive information
- **Invisible risks:** Data exposure through AI can be subtle and hard to detect
- **Integrations:** AI is becoming embedded in standard productivity tools

Governance: Putting the Horse in front of the Cart

Essential Elements of AI Governance

- Cross Functional Governance
- Data Protection and Privacy
- Tool Authorization Framework
- Employee Education
- Monitoring and Visibility



Cross-functional Governance Model

The AI Governance Council

CIO: Technical oversight

CISO: Security guidance

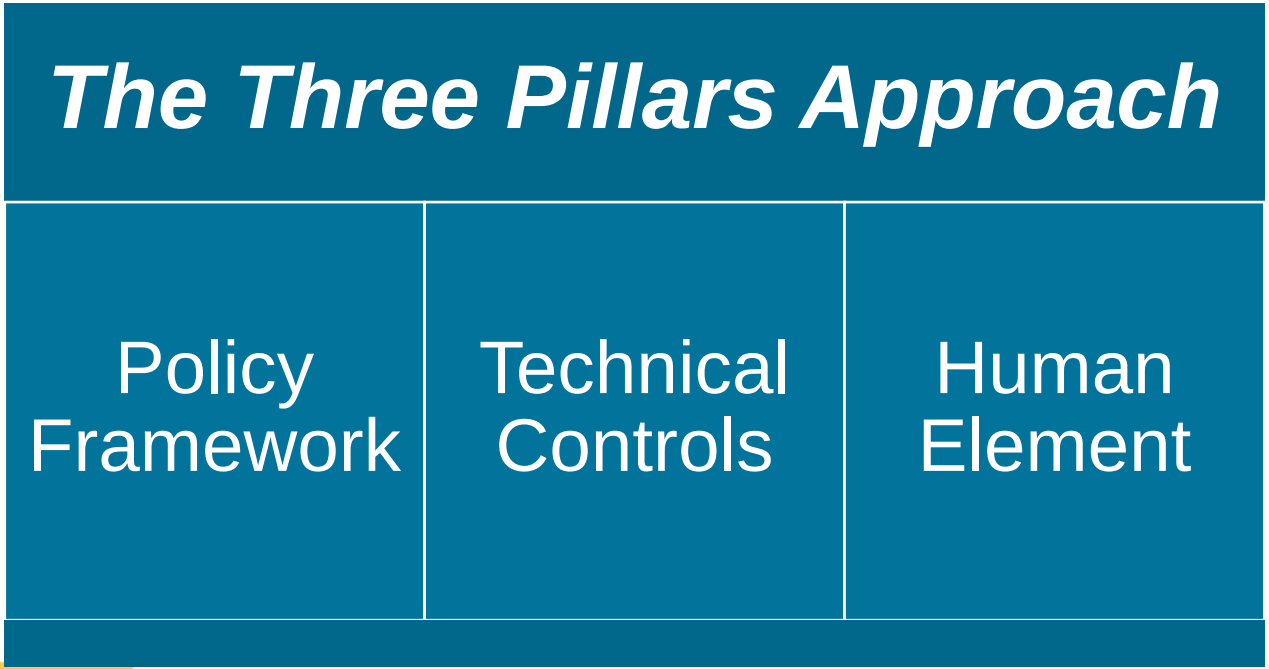
Legal: Compliance verification

Privacy Officer: Data protection

Business Units: Use case validation

HR: Employment Policy

Building Your AI Governance Program



Policy Framework

Clear guidelines for AI usage

- Acceptable Use Policy for AI tools
- Data Classification Guidelines
- AI Tool Selection Criteria
- Incident Response Procedures

Decision rights and accountability

Consequences for non-compliance

Data Protection and Privacy

Creating clear boundaries for AI data usage

The Classification Framework:

1. **Public Data: Safe for AI experimentation**
2. **Internal Data: Requires approved AI tools**
3. **Sensitive Data: Restricted AI usage**
4. **Critical Data: No AI exposure allowed**

Tool Authorization Framework

The AI AppStore Approach:

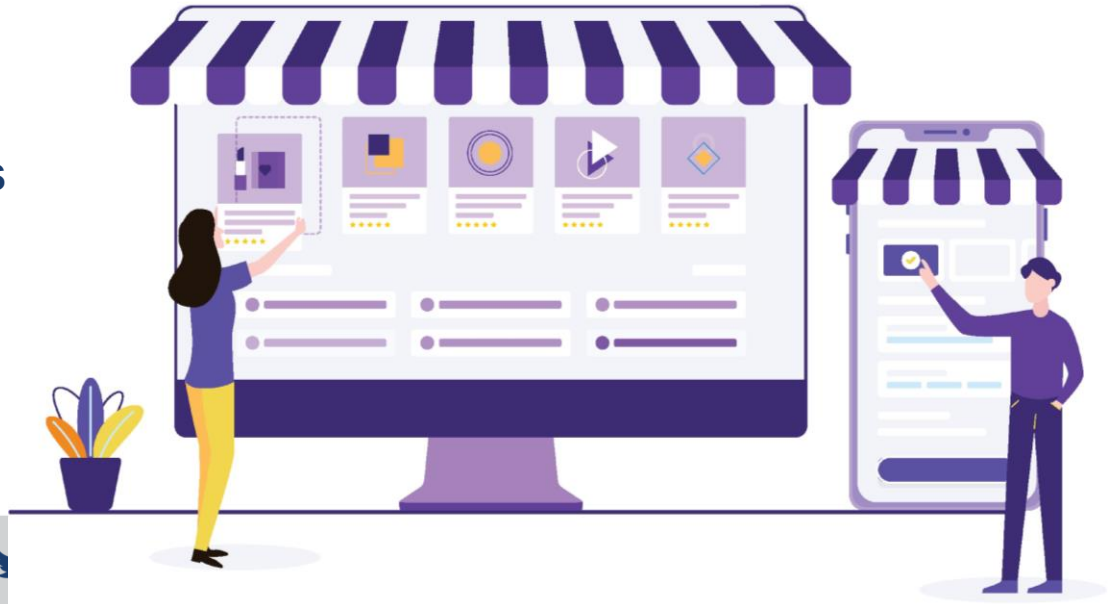
Create an internal marketplace of approved AI tools, each vetted for:

- Data handling practices

- Security controls

- Compliance certifications

- Integration capabilities



Tool Evaluation Matrix Sample

Criteria	Required	Desired
SOC2 Compliance		
API Controls		
Audit Logging		
SSO Integration		
Protected Mode		
Unbiased		
Transparency/Explainability		

Human Element: Employee Education

- Training and awareness programs
- Change management strategies
- Building a responsible AI culture

Monitoring and Visibility

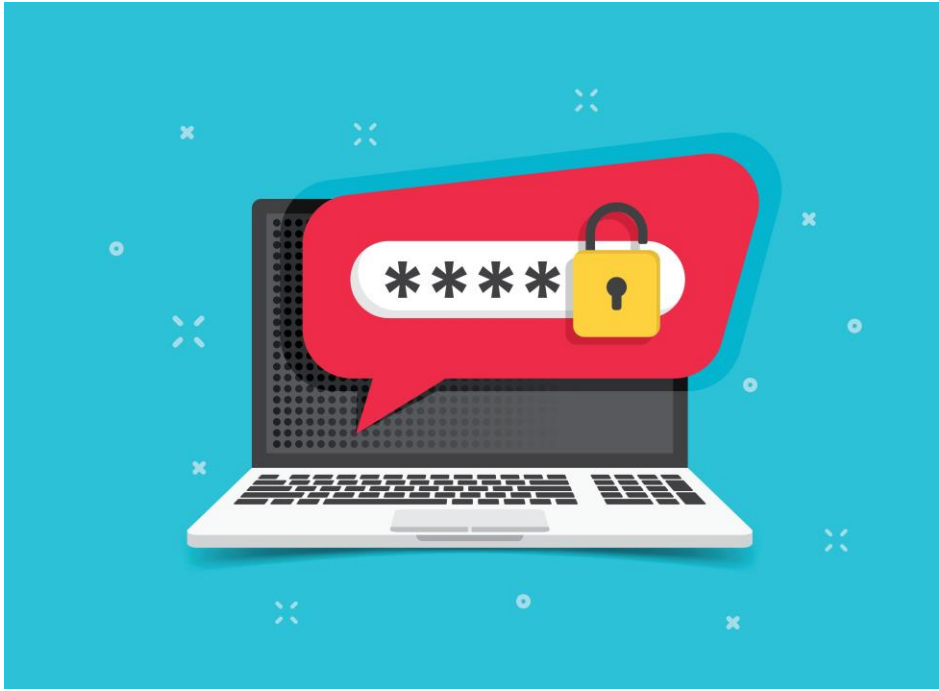
Balance between security and productivity

Technical Implementation:

- **Applications that scan for existing AI in use**
- **API gateways that scan for sensitive data patterns**
- **DLP systems configured for AI-specific scenarios**
- **Automated data classification tools**

Technical Controls

- Authentication and authorization
- Data protection mechanisms
- Usage and adoption monitoring
  - Monitor AI performance
  - Track compliance
  - Evaluate impact
- Manage
  - Implement controls
  - Respond to incidents
  - Optimize processes



Implementation Roadmap

Long Term (180+ Days)
- Advanced analytics + monitoring
- AI risk dashboard
- Culture transformation

Medium Term (90+ Days)
- Deploy technical controls and basic monitoring
- Tool evaluation
- Launch training program
- Draft initial policies

Quick Wins (30+ Days)
- Establish governance committee
- Conduct AI tool inventory
- Identify AI Use Cases

Guidelines and Frameworks
References for AI Governance

NIST AI Risk Management Framework (AI RMF 1.0) January 2023
Comprehensive guidance for managing AI risks in organizations
https://www.nist.gov/itl/ai-risk-management-framework

ISO/IEC 42001 Published: 2023
Artificial intelligence management systems requirements
Implementation Guide: Available through ISO

EU AI Act Framework (Final Version) December 2023
Global standard for AI regulation
Compliance Requirements: Risk-based approach to AI governance

Your Turn!