Connection
we solve IT

DIGITAL WORKSPACE SOLUTIONS

AI and Compliance: What You Need to Know

Table of Contents

Introduction

AI is on almost every business leader's mind, presenting an incredible opportunity to improve productivity—for those who can properly harness its power.

While AI isn't new, the proliferation of AI tools accessible to the average person is. This early access has created a big challenge for organizations that need to protect their data and their customers. How do you establish an AI strategy that encourages experimentation without introducing additional organizational risk?

In this ebook, we'll walk you through the security and compliance risks of AI. We'll also share some practical ways to mitigate these risks through preparation, policies, and technology.

The AI Opportunity and Why You Can't Ignore It

IDC's Worldwide Artificial Intelligence Systems Spending Guide found that enterprise spending on AI is expected to grow at a 26.9% compound annual growth rate (CAGR) through 2027. This far surpasses the 5.7% CAGR for worldwide IT spending expected over the same period. The takeaway is that companies around the globe are going all in on AI investments.

What do these companies stand to gain from their investments? Better insights, increased efficiency, lower overhead, topline growth, and improved customer experiences are just a few of AI's potential benefits. In addition, investments in AI are producing an average return of $3.50 for every dollar invested.[2]

In the past, many companies waited to deploy new technologies until the market was mature. With AI, organizations that wait to invest risk falling behind. That's because AI tools already offer significant benefits to early adopters.

Yet developing and integrating specific AI applications takes time, and even off-the-shelf solutions like ChatGPT need to be trained on an organization's specific data, brand, and methodologies to deliver the most value.

Companies can speed up 20% of tasks without quality loss using today's generation of AI

– Bain & Company[3]

[1] Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

[2] Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

[3] "Technology Report 2023," Bain & Company, https://www.bain.com/globalassets/noindex/2023/bain_report_technology_report_2023.pdf

Potential Risks of Using AI for Business Gains

AI can be an incredible tool, but it's not without its hazards. Part of any good AI strategy is performing risk assessments that pinpoint key areas of concern. Once you've identified these areas, you can mitigate against them as you deploy AI solutions.

Below are common areas of risk each company should consider before using AI:

1) Liability

You've probably read the headlines about AI hallucinations where a large language model (LLM) fabricated unsubstantiated information. If employees use AI outputs without human fact-checking or oversight, your organization could face lawsuits for copyright infringement, libel, slander, and any number of other harms.

Possible mitigations:
Implement checks and balances for AI outputs, such as human fact-checking or legal review. Also, consider using AI solutions that limit your liability. Microsoft, for instance, issued a Copilot Copyright Commitment that says they will defend customers accused of copyright infringement based on Azure OpenAI Service outputs[4]. Assurances like this can significantly limit your exposure. When choosing a vendor, make sure you review the indemnification language and understand what liabilities the vendor will protect you from.

28% of companies are concerned about the liability risks of AI use[5]

---

[4] Brad Smith & Hossein Nowbar, "Microsoft announces new Copilot Copyright Commitment for customers," Microsoft.com, Sep 7, 2023, https://blogs.microsoft.com/on-the-issues/2023/09/07/copilot-copyright-commitment-ai-legal-concerns/

[5] Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

2) Security

Organizations fear losing IP, trade secrets, or sensitive customer information if they train AI tools on company data. While there are still risks with models built and owned in-house, the hazards grow exponentially when companies use software as a service (SaaS) AI solutions. One big risk is that these third-party apps could surface critical data about your business to a competitor or bad actor. Additionally, any data you gather to train AI is a prime target for cybercriminals

Possible mitigations:
Put guardrails in place to limit the information used by AI models to what's necessary to perform the task at hand. Also, limit the use of AI to company functions that don't regularly use IP. For instance, you may decide that teams coding your software can't use third-party AI platforms, because this risks exposing the code of your proprietary products to a LLM training database accessible to others. Lastly, employee education is essential. Even one employee or company agent who feeds your sensitive data to AI can cause a serious breach.

37% of companies are concerned about a security breach related to AI use[6]

3) Reputational Harm

No one wants their company's brand or operations damaged because of a legal action, disgruntled customer, or a security breach related to AI. Some recent AI blunders have exposed potential issues for brands that go beyond the challenges we've already discussed. Examples include AI chatbots that have provided incorrect information to customers and AI recruiting software that discriminated against a particular demographic of applicants[7].

Possible mitigations:
Do your due diligence on as many incident scenarios as possible, thinking through ways to prevent adverse outcomes. Ensure the data your AI is trained on is accurate and lacking bias. Lastly, prepare a crisis communication team who can get ahead of any incidents that may occur.

23% of companies are concerned about possible damage to their brand reputation caused by AI use[8]

---

[6] Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

[7] Thor Olavsrud, "10 Famous AI Disasters," CIO, April 17, 2024, https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html

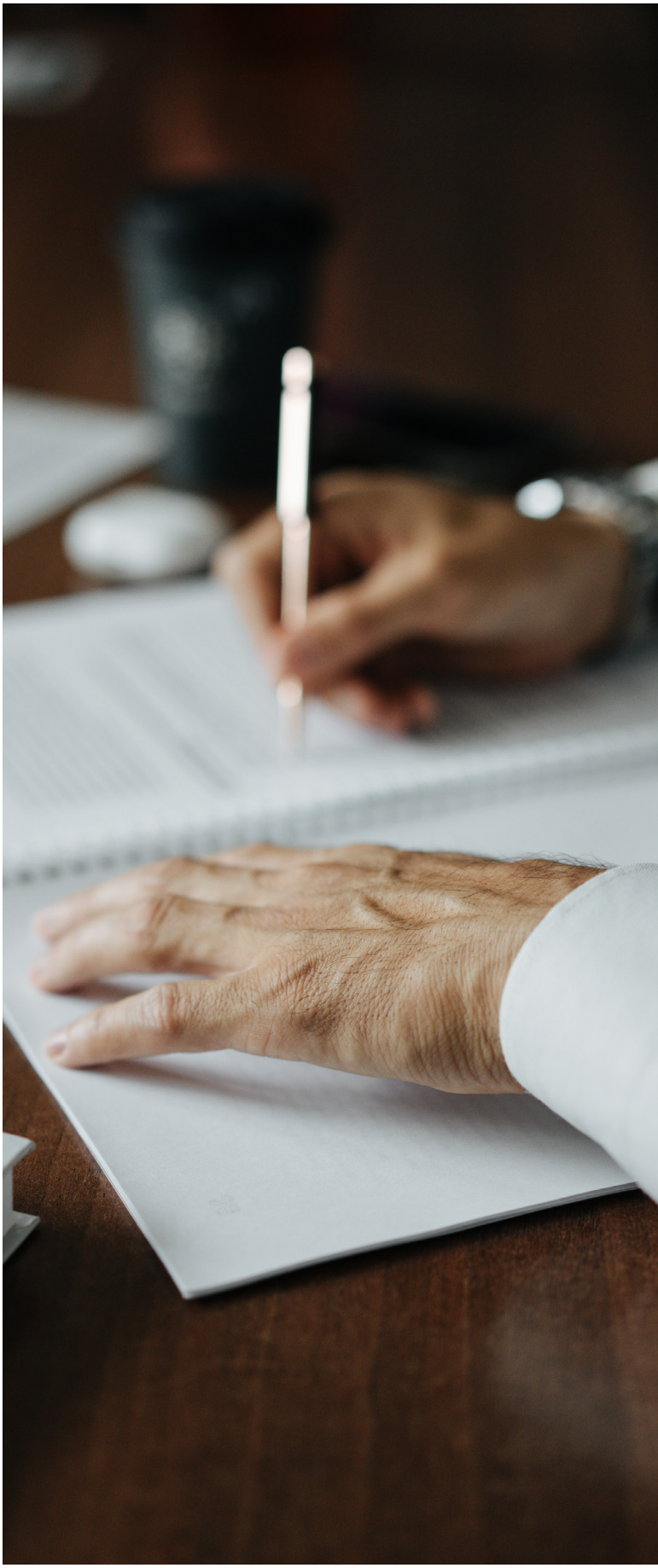
[8]Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

4) Compliance

Legal parameters for responsible AI use are just now being implemented, but many suggested frameworks are not yet binding. However, existing regulations around data handling and consent still apply. Many companies are concerned about the compliance and privacy implications of using sensitive customer data to train AI. Some organizations have updated their terms of service and privacy policies to create opt-in coverage for broader AI-related use cases.

Possible mitigations:
Assess the laws that apply to your industry and business activities. Then evaluate the AI implementations that can comply with regulations versus those that can't and are too risky. Review your terms and policies and those of any third-party AI tools you use. This review will help you ensure transparency and compliance around the use of customer data for AI training.

29% of companies are concerned about the regulatory risks of using AI[9]



[9] Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

Special Security and Compliance Concerns by Industry

There are risks with AI use for every industry. However, a few highly regulated industries face even greater security concerns. These industries are already prime targets for cybercriminals because they maintain valuable customer data like credit cards, social security numbers, and other confidential information. Let's look at a few of these industries and unpack some of their unique security and compliance concerns.

Healthcare

The healthcare industry's big concern is compliance with The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), which protects patient data and confidentiality.

Potential AI risks:

- Unauthorized exposure of confidential patient information in AI outputs
- Misuse of patient data for AI training
- Bias in AI algorithms that could affect patient access to treatment
- Harm to patients from medical errors caused by AI

Finance

Financial industry laws and regulations require the secure storage of financial records and the protection of cardholder data according to the Payment Card Industry Data Security Standard (PCI DSS).

Potential AI risks:

- Use of third-party AI solutions whose hosting, security, or model training do not meet regulatory requirements
- Exposing financial or protected personal data in AI outputs
- Employees or bad actors prompting AI to ignore a set of financial records to hide crimes

Government and Public Sector

Governments and public sector organizations often house sensitive information and databases. They also oversee elections and their security.

Potential AI risks:

- Election tampering
- Mishandling of sensitive records that leads to privacy violations
- False or misleading information caused by hallucinations
- Bias based on AI training inputs
- Funding constraints that lead to less secure deployments of AI

Technology

Technology companies, particularly those that offer SaaS products, can host sensitive data from multiple customers on their servers.

Potential AI risks:

- Customer data/IP exposure or use to train third-party AI models
- Prompt injection attacks or data poisoning
- Discriminatory bias that exposes companies to legal action from an employee or customer

Only 39% of North American organizations surveyed say they have an AI governance body to oversee responsible AI[12]

[12]Ritu Jyoti and Dave Schubmehl, "The Business Opportunity of AI: How Leading Organizations Around the World Are Using AI to Drive Impact Across Every Industry," November 2023, IDC, https://info.microsoft.com/ww-landing-idc-delivering-real-business-value-from-ai.html

The Role of Employee Education

Communicating AI risks and compliance requirements is crucial for successful deployments of AI. The average enterprise already manages a SaaS portfolio of 342 apps[10]. Now, with AI, IT departments are scrambling to gain control of the rise of AI-related shadow IT applications. These are applications not sanctioned or overseen by IT that can open companies up to multiple unseen security and compliance concerns. In 2023, ChatGPT was the most used shadow IT application[11].

Employee education around AI shouldn't be a one-time event for three reasons:

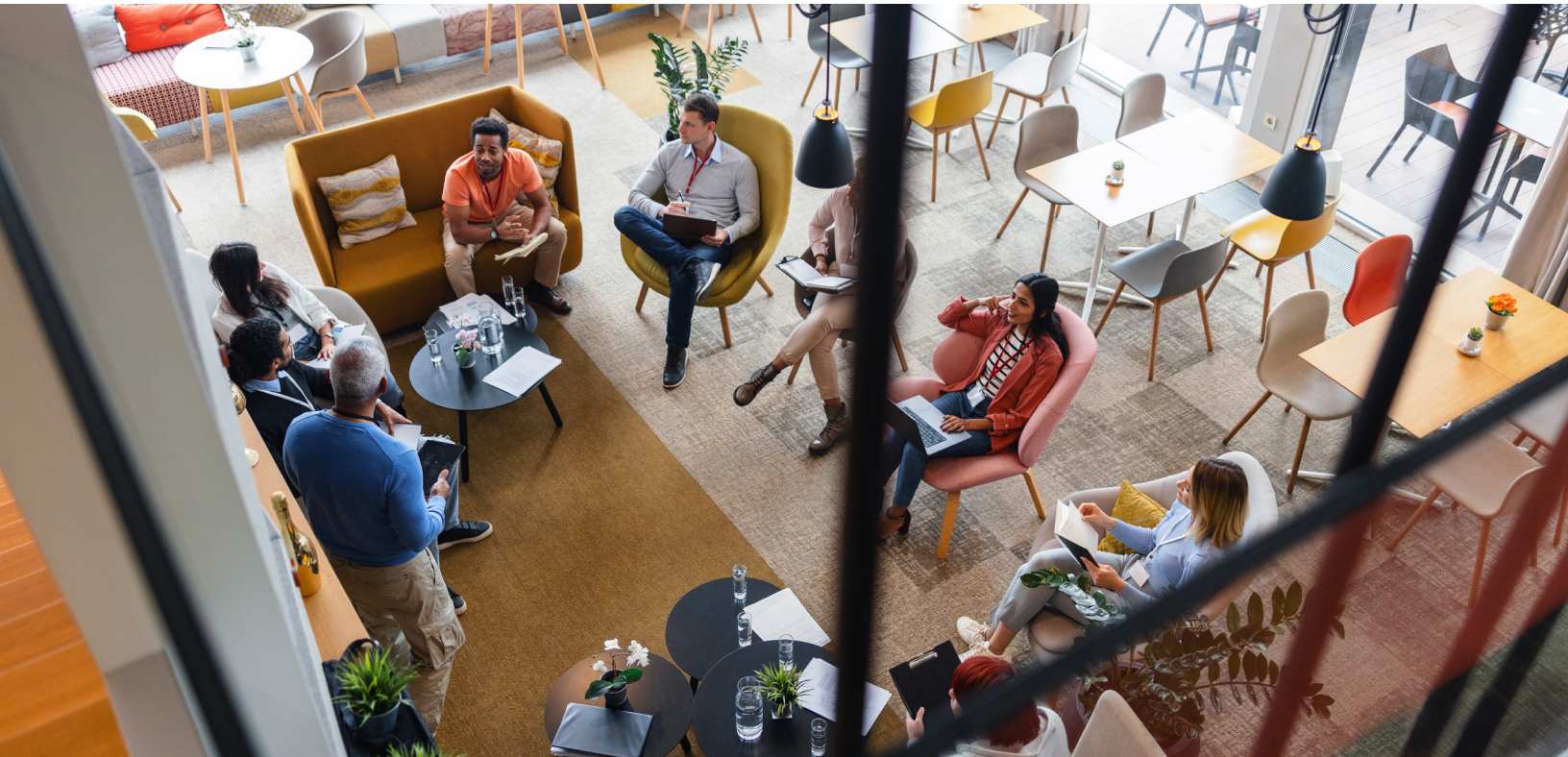
1. **Models and tools are changing quickly.** A regular cadence of AI education can keep employees current with rapidly changing technology, regulations, and company policies.
2. **Repetition is vital to human memory.** Research has shown that repetition is an effective way to move a fact or skill from short-term to long-term memory. Frequent education can strengthen an employee's proficiency in AI use.
3. **Your organization is not static.** Employees come and go over time, so it's important to keep everyone on the same page regarding AI and its use within the organization.

In combination with education, tools such as cloud app security brokers can help you whitelist the AI applications you've approved and block those you don't want employees to use. These added guardrails can help prevent intentional or unintentional misuse of AI applications.

---

[10] "2024 State of SaaS Growth," Productiv, https://productiv.com/state-of-saas/2024-saas-trends-growth/

[11] "2024 State of SaaS Usage," Productiv, https://productiv.com/state-of-saas/2024-saas-trends-usage/



AI Devices as Enablers of AI-Powered Security

In the past decade, companies have moved from on-premises hosting to cloud hosting at a rapid pace. With the proliferation of SaaS applications, much of the work employees now do in their jobs happens in a cloud environment rather than on their devices.

There are definite advantages to the cloud, like scalability and cost. However, depending on the setup, hosting in the cloud can expose companies to increased cybersecurity risks.

C-suite leaders are increasingly concerned about security as AI becomes more prevalent. One way to mitigate the risks is with next-gen AI PCs and smartphones. Engineered from the ground up to support on-device AI processing, these devices shift work from the cloud back to the device.

Next-gen AI devices are a much more efficient way to run AI applications. They save on cloud usage because AI processes require significant resources. They're also faster, with better battery life due to the addition of a Neural Processing Unit (NPU) along with the traditional CPU and GPU.

To show the scope how quickly the industry is moving, IDC expects 170 million next-gen smartphones to ship in 2024. This figure represents 15% of all smartphone shipments for the year.

[13]"The Future of Next-Gen AI Smartphones," IDC, February 19, 2024, https://blogs.idc.com/2024/02/19/the-future-of-next-gen-ai-smartphones/

How Connection Can Help

Connection is here to partner with you on your AI journey. We offer consulting on AI best practices, along with both customized and off-the-shelf AI solutions.

Our Microsoft 365 Copilot Technical Readiness Assessment helps prepare your organization's data for use with Copilot, Microsoft's new productivity-enhancing AI tool. To learn more, read our Readiness Assessment solutions brief.

Explore Our Resources
Digital Workspace
Artificial Intelligence
Microsoft Copilot

Reach out to one of our Connection experts today:

Contact Us
1.800.998.0067