# AI adoption demands strong safeguards, warns CyberHoot



Artificial intelligence is fast becoming a central part of business operations, offering dramatic productivity gains but also posing major security and compliance risks if deployed without care.

CyberHoot has outlined five rules for safe AI adoption, warning that treating AI like an over-eager intern—full of potential but inexperienced—requires oversight and boundaries. Its guidance stresses understanding data risks, choosing trusted vendors, enforcing access controls, maintaining human oversight and training staff.

Data protection is paramount. Sensitive information such as customer records, financial data and intellectual property should never be input into public AI tools, the firm advises. PwC notes that nearly half of business executives now prioritise data security in cybersecurity budgets, highlighting the importance of high-quality training data and governance frameworks.

The risks are underlined by a TechRadar survey showing that while 98 per cent of firms plan to expand AI use, 96 per cent also see AI tools as security threats. Weak visibility into AI access can lead to unauthorised actions, making robust identity and access management essential.

Human oversight remains critical. AI systems can hallucinate, producing inaccurate or biased outputs. Reuters has reported cases such as Amazon’s abandoned recruitment algorithm, which discriminated against women. CyberHoot stresses that businesses must validate AI outputs and ensure compliance with ethical and regulatory standards.

Training employees is another cornerstone. With “shadow AI” tools proliferating outside IT oversight, ongoing education on security and ethics is seen as essential. Axios has argued that managing rather than banning such tools is the most effective way to contain risks.

Legal and regulatory concerns are also growing. Issues range from GDPR compliance and intellectual property disputes to reputational risks from flawed AI outputs. Regulators are responding: the New York State Department of Financial Services has issued AI-specific cybersecurity guidance for banks, requiring stronger data governance and third-party vetting.

The message is clear: AI can be a transformative business asset, but only if accompanied by rigorous safeguards. Embedding responsible governance into AI deployment, CyberHoot argues, will allow firms to harness its benefits while avoiding costly missteps.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://cyberhoot.com/blog/safe-ai-adoption-five-rules-every-business-must-follow/> - Please view link - unable to able to access data
2. <https://www.pwc.com/us/en/tech-effect/cybersecurity/securing-data-behind-ai.html> - This article discusses the heightened data risks associated with AI adoption, emphasizing the need for organizations to train AI models on high-quality data and implement robust governance and security controls. It highlights the importance of data protection and trust, noting that 48% of business executives rank data protection as their top cyber investment priority. The piece also outlines key data risks, including data quality, protection, compliance, and exposure, and offers strategies to mitigate these risks, such as improving compliance and governance controls for AI workflows and reducing data exposure and access sprawl.
3. <https://www.techradar.com/computing/artificial-intelligence/love-and-hate-tech-pros-overwhelmingly-like-ai-agents-but-view-them-as-a-growing-security-risk> - A recent survey reveals that while 98% of organizations plan to expand their use of AI agents within the next year, 96% view them as growing security threats. The research highlights that AI agents are increasingly integrated into sensitive areas such as legal, financial, and supply chain systems, yet only 54% of professionals have full visibility into the data these agents can access. Alarmingly, 80% of companies reported unintended actions by AI agents, including unauthorized access, sharing inappropriate data, and downloading sensitive content. The article underscores the urgency for more robust identity security strategies as enterprises integrate AI agents into core operations.
4. <https://www.reuters.com/sustainability/society-equity/comment-business-leaders-risk-sleepwalking-towards-ai-misuse-2024-11-19/> - This commentary raises concerns about businesses adopting AI tools without sufficient oversight and transparency. It references a past incident where Amazon's AI recruitment tool favored male candidates due to biased training data, highlighting existing issues with AI implementation. Despite the potential productivity benefits of generative AI, the lack of clear guidelines and disclosures regarding its usage poses significant risks, including discrimination and legal ramifications. The article emphasizes the need for businesses to adopt responsible AI governance frameworks to mitigate ethical issues and adhere to regulatory standards.
5. <https://www.techradar.com/pro/ai-in-the-workplace-the-legal-risks-businesses-cant-afford-to-ignore> - As businesses increasingly adopt AI tools, they face significant legal risks if proper safeguards are not in place. Key concerns include data protection under GDPR, especially around the use of AI for employee monitoring and decision-making, data scraping to train AI models, and copyright infringement risks via generative AI tools. The unreliable nature of AI outputs, or 'hallucinations,' also poses reputational and legal threats if false data is published or used in decision-making. The article advises companies to establish robust AI governance frameworks, enforce training and policies, and conduct Data Protection Impact Assessments to navigate the complex legal landscape of AI adoption.
6. <https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec> - This newsletter covers key cybersecurity topics, including the rise of 'shadow AI,' where unauthorized AI tools are used by employees, potentially risking data security. IT teams are focusing on governing AI use rather than banning tools outright. A significant concern is China's DeepSeek AI tool, which has been banned by the Pentagon and U.S. Navy over security issues. Cybersecurity vendors are developing solutions to monitor and mitigate risks associated with shadow AI. The article emphasizes the evolving landscape and the importance of governance in maintaining security in an AI-driven environment.
7. <https://www.reuters.com/legal/legalindustry/new-york-department-financial-services-provides-ai-cybersecurity-guidance-what-2024-11-15/> - The New York State Department of Financial Services (DFS) issued guidance for financial institutions on mitigating cybersecurity risks from artificial intelligence (AI). This guidance advises updating risk assessments annually to address AI threats such as deepfakes, maintaining and testing response plans, and ensuring leadership oversight on AI risks. It mandates policies for vetting third-party service providers, securing access controls using multi-factor authentication by November 2025, and implementing data governance procedures. The guidance emphasizes re-evaluating and reassessing cybersecurity controls and risk assessments as AI evolves to ensure compliance and address vulnerabilities.