Lowenstein Sandler

Client Alert

Data, Privacy & Cybersecurity

February 18, 2025

Top AI Risks General Counsels Should Address

By Diane Moss, Ken Fishkin CISSP, CIPP/US, CIPM, CIPT, and Judith G. Rubin CIPP/US/E, CIPT

Considering the rapid development and deployment of artificial intelligence (AI) in a wide array of applications and business sectors, it can be a daunting task for a company's General Counsel (GC) to keep pace in identifying and managing associated risks. The following overview of the major legal, compliance, and cybersecurity risks is intended to help you understand which AI-related risks a GC may typically face and how to minimize them.

A company will typically be confronted with AI risks in the following contexts, which we will address in more detail below.

1. Identifying and Understanding AI: A tool may contain AI features without the user being aware of it, a vendor may be using AI without the knowledge of its customers, and a company's understanding of the scope or functions of an AI tool may be incorrect.
2. Allowing and Limiting the Use of AI: Employees may be using AI without authorization, and AI tools may be used in a way that exceeds what they were meant or approved for.
3. Data Quality, Rights, and Confidentiality: The quality of the underlying data (including the right to use such data) is of particular importance in the context of AI and machine learning. Moreover, AI tools may not meet confidentiality and privacy requirements.
4. Cybersecurity Risk Management: The use of AI by threat actors can lead to more sophisticated attacks, and integrations with third-party tools can make a company more vulnerable.
5. Evolving Legal and Regulatory Landscape: Laws, regulations, and best practices are still adapting to the new technology, and legal and contractual obligations are not always clear and predictable.
6. Data Governance and Accountability: Lack of clear responsibilities and expectations means that a company will not be sufficiently prepared for the risks associated with the new technology. Regulators, business partners, and customers, on the other hand, are paying more attention to these issues.

1. Identifying and Understanding AI

Companies are always adding new features to their services, but in the case of AI, third parties may be slipping new AI features into their products without notifying users about this fact and the associated risks it might cause. It is thus advisable to carefully vet the vendors of such software, understand the tool's terms of use, and routinely review any feature release notes to identify new or modified AI use cases.

2. Allowing and Limiting the Use of AI

Shadow IT: When employees feel the ability to do their work is hampered by existing policies or tools, they will often develop workarounds to make them more efficient, even though they may be bypassing security protocols. By accessing public AI tools and inputting private or confidential information into them, they could be causing a security breach for the company. Companies should implement a workflow with the procurement department to ensure that due diligence is performed before any tools or services are purchased.

Access Control: Implementing the proper access controls for an AI system is critical for three reasons: security, integrity, and privacy. If access controls are not designed and tested adequately, there is a risk that the data could be accessed by an unauthorized user, which would allow them to either steal the data or tamper with it on purpose or accidentally. Companies should perform regular access reviews to ensure that only the necessary people have access to AI tools, and that their permissions are limited to what is needed to perform their jobs. Too often, employees are given more access than needed.

3. Data Quality, Rights, and Confidentiality

Companies usually use AI tools to boost efficiency, streamline internal workflow processes, or facilitate the provision of services to customers. By deploying tools that were trained on high-quality data, companies can realize these advantages and mitigate the risk of business disruptions, fines, and reputational harm associated with the use of output that is illegal, inaccurate, infringing, or biased. Consider implementing the following best practices:

- Use models trained on accurate, complete, relevant, and representative data.
- Assume that biases will exist, and proactively address any concerns that are relevant to the use case.
- Understand that as potentially helpful as the tool may be with respect to business operations, outputs are only as reliable as the training material and may contain errors or perpetuate biases and discriminatory practices.
- To mitigate these risks:
    - Confirm the source of training data and the vendor's practices to ensure data quality during the diligence process to vet a tool.
    - Seek the inclusion of representations and warranties from the vendor to decrease exposure for inaccuracies and biases.
    - Incorporate the obligation for human review of output to confirm that the material is accurate and reliable as part of your company's responsible AI business practices. Human involvement is critical as machines can make mistakes, even if quality training data was used.

4. Cybersecurity Risk Management

Vendor Management: Performing sufficient due diligence on third parties that offer AI solutions is imperative since a company is responsible for the data it manages. Companies should require that a vendor does not add features that might increase risks without giving adequate notice. At a minimum, ask the following basic questions:

- In what geographic location(s) is the vendor's data stored?
- Can the vendor's data be used for training purposes?
- Does the vendor have adequate cyber insurance?
- Does the vendor have a SOC2 Type 2 report or ISO 27001 certification?
- What third parties does the vendor utilize?

Companies should also consider regularly reviewing existing vendor contracts to ensure that they still meet required cybersecurity and confidentiality obligations.

Employee Training: Most data breaches currently involve the human element. AI has made cyberattacks easier to execute and more convincing than ever. All employees should thus undergo cybersecurity training during their onboarding process and regularly thereafter. Such training should cover potential threats like phishing scams and social engineering tactics, malware protection, how to prevent attacks, and how to handle any security incidents that may occur.

5. Evolving Legal and Regulatory Landscape

Rapid development of laws and lack of harmonization – both globally and within the U.S. – are two of the most challenging aspects of AI regulation. Various parts of the world have adopted varying approaches to AI governance and thus created a patchwork of laws that can be difficult to navigate.

In the U.S., regulation of AI at the federal level has been limited. Several agencies including the CFPB, FTC, and SEC have all issued rules and guidance regarding the use of AI or technologies of which AI is included, and have focused generally on AI adoption that is transparent and conspicuous. Guidance was also issued by the National Institute of Standards and Technology. Much more regulatory progress has been made on the state level, where several states have enacted AI-related legislation, and many more bills have been proposed. The proposed and enacted bills vary widely in scope and obligations. Utah's Artificial Intelligence Policy Act, for example, requires disclosure when using AI tools with customers. California recently enacted two AI laws that will take effect in January 2026 and require developers to be transparent about AI training data and offer AI detection watermarking tools. And the new Colorado AI law, which becomes effective in February 2026, requires developers and deployers of "high-risk artificial intelligence systems" to protect consumers from risks of algorithmic discrimination.

Internationally, countries are approaching AI governance variously via voluntary guidelines and standards, use-specific or comprehensive legislation, and national AI strategies. To mention just a few of these developments: In Europe, the European Union's (EU) Artificial Intelligence Act became effective in August 2024. It has extraterritorial scope and applies to AI systems placed on the EU market or used in the EU by or on behalf of companies located throughout the world. China has adopted multiple laws focusing on the use (as opposed to the development and deployment) of AI. Canada's proposed Artificial Intelligence and Data Act aims to protect Canadians from high-risk systems and ensure the development of responsible AI. Singapore, on the other hand, is taking a sectoral approach and lets the respective authorities publish regulations and guidelines.

While one can observe some common patterns, there is no standard approach to AI regulation, and we can expect that the legal landscape will further evolve as AI technology advances. Businesses are thus advised to stay informed about new developments and be prepared to adapt to new rules.

6. Data Governance and Accountability

Accountability may be the ultimate risk mitigator because being "accountable" requires deployers to be knowledgeable about the multifaceted complexities of AI and encourages cross-teaming with colleagues in different verticals such as privacy, IT, security, and data governance to address its risks.

The prospect of building an effective AI governance program may seem daunting but is not as hard as you think. Even for businesses that do not have the necessary financial and organizational resources to adequately protect their IT infrastructure from common cyber threats or ensure that their AI tools are well protected can implement an AI usage policy as an effective and low-cost way to communicate use restrictions to employees.

Companies that require a robust program can start building such a program by doing the following:

- Identify existing policies, such as confidentiality, privacy, and data compliance policies, that can be leveraged in the context of AI. The principles governing these areas dovetail nicely with the pillars of AI governance (data security, privacy, quality, transparency, contestability, and redress).
- Identify colleagues who have the level of expertise and authority to assess and approve the risk associated with the in-house use of AI tools. Staff members in IT, information security, and privacy can offer valuable assistance in tool diligence and help confirm if tools are safe or appropriate for the respective use case.
- Establish a process and protocol for tool vetting and approval. Along with vendor diligence, make sure your employees know not to download AI applications without prior approval in accordance with the company's established process. To streamline the approval process, it can be helpful to establish a preapproved list of AI tools and associated permitted and prohibited use cases. Applications are not universally acceptable in all use cases and may present larger risks outside the context of the intended use.
- Train your employees in the processes and guidelines. A well-articulated framework is particularly important for its effectiveness. Users must understand the processes and use limitations of applications.
- Establish AI output review protocols to ensure human oversight.

- Establish monitoring and oversight responsibility for the use of AI tools and the laws and regulations that apply to them.
- Work with senior management to establish AI incident response plans and risk management strategies to prepare for situations of misuse or errors related to the use of an AI application.
- Stay current on evolving and emerging AI laws and regulations and related accountability requirements, and maintain an agile framework that is built to adapt.

As a GC of a company that deploys AI tools, AI accountability means that you can answer "yes" to the question "Do we have a defensible AI governance process in place that addresses the tool's life cycle with the company?"

Conclusion

Over the past few years, ChatGPT and other AI tools have taken the world by storm. As a result, GCs must quickly adapt to the changing business landscape and update their AI risk assessments accordingly. Understanding the top AI risk factors, such as access rights, data governance, cybersecurity risk management, data quality management, and the legal and regulatory landscape, is essential to providing GCs with a starting point for developing adequate policies and procedures so their employees can use AI responsibly. Once these policies and procedures are finalized and enforced, GCs should have the necessary guardrails in place to provide their company, clients, and customers with adequate cybersecurity, integrity, and privacy protections.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

DIANE MOSS
Counsel
T: 973.597.2448
dmoss@lowenstein.com

KEN FISHKIN, CISSP, CIPP/US, CIPM, CIPT
Senior Manager of Information Security
T: 973.422.6748
kfishkin@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com