CLEARY GOTTLIEB

AI May Do Wonders for Your Business, But What About Your Risk Profile?

January 17, 2024

Artificial intelligence (AI)[1] was the biggest technology news of 2023. AI continues to revolutionize business in big and small ways, ranging from disrupting entire business models to making basic support functions more efficient. Observers have rightly focused on the plentiful value-creation opportunities this new technology affords. Less attention has been given to the risks AI creates for boards and management teams, which call for sophisticated governance, operational and risk perspectives. This article identifies key areas of risk and offers suggestions for mitigation on the road to realizing the enormous benefits AI promises.

In the last year, advances in generative AI have catalyzed board level discussion of use cases and increased budgets to fund investment and adoption,[2] but for many corporations risk management lags behind and survey data indicate sub-optimal numbers of senior leaders taking ownership of AI risk management.[3] Delays in formalized risk management and senior leadership involvement highlight the extent to which investment outpaces risk mitigation and corporate oversight strategies.

Deepfakes and Public Relations

2024 will see the release of new AI tools giving average usersthe ability to make fake video content that is indistinguishable to the naked eye from the real thing.[4] While some commentators have considered the impact of cheap, numerous and convincing deepfakes on politics, corporations are also potential targets of smear campaigns using deepfakes to mislead – whether by way of embarrassing corporate leaders, discrediting corporate policies or manipulating stock prices through plausible, but inaccurate, videos.

Corporations and public companies, in particular, should conduct table-top exercises or otherwise develop response plans for identifying false content, proving it is not genuine and disseminating a prompt, corrective counter-narrative – all before a deepfake goes viral. Skilled advisors will be needed to navigate these nightmare scenarios, including the increasing use of third-party experts who can credibly distinguish authentic video from AI-generated fakes. Given the obvious public relations implications, it will be important to have a plan to address potential exposure, correct the record, and prepare company leaders for any necessary public statements.

Securing these services ahead of time will be a worthwhile investment if a concerted campaign is launched against a corporation or its leadership team.

Crisis Management

Nefarious AI use by bad actors can create a crisis at a moment's notice, making a sophisticated crisis response plan all the more imperative to successful public relations.

Holistic crisis management frameworks should be adopted and should address the three phrases of a crisis:

- **Pre-Crisis Phase (Prevention and Preparation)**
  - Establish key processes in the event of a crisis and incident reporting trainings for employees.
  - Identify the trusted advisors who will be prepared to give immediate support and counsel in the event that an urgent need arises.
- **During-the-Crisis Phase (Responding to the Crisis)**
  - Focus on key processes surrounding comprehensive internal investigation of the crisis, public and internal communications with relevant stakeholders, monitoring of stakeholder feedback on crisis response efforts, and defense mechanisms to protect against reputational harm, economic harm, and legal liability.
- **Post-Crisis Phase (Learning from the Crisis)**
  - Establish a post-crisis recovery plan, which should evaluate the handling of the crisis and lessons learned, update the crisis response plan, follow up on information requests from relevant stakeholders, identify root causes, and consider whether the incident and its root causes require further investigation and/or external consultation to resolve the root causes and/or mitigate liability and (where possible) future vulnerability or exposure.

For further discussion on crisis response and preparedness, *see* Cleary Gottlieb Global Crisis Management Handbook: Fourth Edition.

Governance and the Expertise Gap

Boards can be liable to shareholders under Delaware law for a failure to adequately oversee corporate activity, including key risks. Ideally, as AI use cases are evaluated by management teams, under board oversight, both rewards and risks associated with oversight and response strategies should be analyzed. Boards should be thorough in documenting their consideration and oversight of these opportunities and the corresponding risks – while latitude is given to companies exercising business judgment in good faith, it can be more challenging to defend decision-making when the paper record does not reflect all of the care taken by the leadership. A board's satisfaction of its oversight obligation under Delaware law could come into question when AI adoption is not met with robust risk mitigation, for example, if employees leverage AI without formalized use policies in place.

Only some board and management teams, particularly outside of the tech sector, currently have meaningful in-house AI expertise or infrastructure.[5] Given the power of AI, employee use can easily become mis-use without well-developed policies and procedures. Additional recruiting and staffing may be needed, though specific requirements for use policies and senior-level AI expertise, whether in the boardroom or in the C-suite, likely will vary with how important AI is to the central business mission and how deeply embedded it is likely to become.

AI Decision-Making: Bias and Error

AI use in decision-making creates omnipresent risks across a business. For example, AI use in hiring processes could lead to claims of discrimination or bias. The idea of "AI bias" is perhaps counter-intuitive, but research has shown bias can stem from the training data, data inputs or the algorithm itself, and can exist despite the diligent efforts of developers due to subconscious cognitive biases.[6] An AI-integrated human resources function therefore can be subject to both regulatory and civil litigation risk. This is not to say that the promise of AI should be avoided in HR functions. Rather, it should be adopted with disciplined risk mitigation in focus at the outset.

Similarly, the mere allegation of faulty operational AI use in decision-making creates additional public image risk. For example, in November 2023, UnitedHealth was subject to a lawsuit claiming that its use of AI in evaluating elderly patients' qualifications for medical coverage led to a high number of errant recommendations. Regardless of the merits of the suit, the application of AI to a commonplace customer-facing business process risks public scrutiny and doubt.

Beyond public image risk, bias and error can result in significant legal and enforcement risk, particularly for highly regulated industries that are subject to consumer protection laws. For example, while noting the benefits and efficiencies of well-managed AI tools, both the Federal Reserve[7] and the Consumer Financial Protection Bureau[8] have recently warned banks and lenders about potential bias in AI that could lead to violations of fair lending, fair housing and equal opportunity laws. Similarly, the SEC has proposed substantive rules related to the use of (and potential conflicts of interest) associated with using predictive data analytics in connection with products and services offered by investment advisers and broker-dealers.[9] Other retail industries may be similarly affected, and boards in these industries should be especially cognizant of training, testing, data management and monitoring.

Regulatory

Regulation of AI is in its infancy and likely to evolve dramatically in the coming years. On October 30, 2023, the Biden Administration issued a landmark Executive Order nearly one year after publication of the Biden Administration's AI Bill of Rights. The Executive Order directs a number of federal departments and agencies to establish new standards for AI safety and security and lays the foundation for protecting various rights.[10] SEC Chairman Gary Gensler did not mince words in a recent interview with the Financial Times when he called a financial crisis within the next decade “nearly unavoidable” without “swift intervention” to regulate AI.[11] Local level regulation also is likely to expand, as illustrated by New York City’s recent law requiring independent bias audits for employers using AI in hiring processes, designed to combat the exact scenario described above.[12]

Cybersecurity

Regardless of a company’s particular interest in AI adoption, contemporary cybersecurity best practices will have to evolve and adapt. For example, voice approvals for wire transfers lose their efficacy when AI can convincingly simulate voices and be used to hold conversations or appear on video conferences. AI-enabled hacking also may require more sophisticated cryptography to keep passwords, IP and other sensitive data secure. AI is a new and very powerful tool in a cybercriminal’s toolbox. Corporate leaders should prioritize cybersecurity investment and develop, or outsource AI defense mechanisms to protect their systems.

Data Analytics

The efficiencies that AI adoption promises also create a risk of over-reliance that could be irreversible if the integration is not measured and strategic.

- **Knowledge Gap** – AI-related workforce reductions or innovations associated with AI could create a situation where few employees know how a particular process works.

- **Misinformation Reliance** – AI may generate or glean facts that result in patently false outputs known as “hallucinations,” as exemplified by several recent high-profile instances of AI from major developers making incorrect claims during public demonstrations. AI-generated data with errors as a result of hallucinations could pollute otherwise accurate data without being noticed. This risk may compound over time as AI-generated data is used to train other AIs.

- **Decision-Making** – Reliance on generative AI without understanding its limitations could result in faulty decisions that would not be made under normal circumstances.

- **Third-Party Reliance** – Corporations that are not developing AI capabilities wholly in-house are subject to the risks posed by relying on a third-party provider. Leaders should be cautious in the event the relationship sours.

To counteract AI reliance risk, corporations should maintain highly skilled workers who mitigate knowledge gaps and monitor for statistical flaws. Highly skilled employees should be central to AI integration. AI should be a partner to subject-matter experts and data analysts, not a replacement.

M&A

The AI revolution will shift the M&A calculus for corporate leaders. The due diligence process is the traditional tool for surfacing operational and financial risks. But what happens when a target is in the AI business or has integrated AI into its business? How were the AI tools trained? Were appropriate permissions secured? Is the company dependent on certain AI tools in way that presents risk following the transaction? Is AI being used ethically and responsibly?

Sophisticated expertized diligence is required to fully understand the particularized risks an acquisition of an AI-integrated business poses to the acquirer. AI-related transactional expertise will be needed across various disciplines, such as regulatory, intellectual property, consumer protection, antitrust and privacy. As AI adoption progresses, corporate leaders should think of AI risk early and often during the M&A process and engage advisors with the requisite expertise to adequately examine the risks.

Regulated Financial Services

In the financial services industry, AI offers significant promise over a wide range of financial functions from payment processing and transaction speed to fraud detection and regulatory compliance monitoring. At the same time, gaps or weaknesses in addressing and managing risks can have calamitous results for individual institutions and, through contagion, for the financial system generally.

The U.S. Financial Stability Oversight Council (FSOC) – a committee comprised of the Treasury, SEC, CFTC, Federal Reserve, OCC, FDIC, CFPB, NCUA, FHA and members from state banking and insurance agencies – recently identified use of AI for the first time as a potential vulnerability to the financial system if not monitored and managed appropriately.[13] FSOC urged its member regulators and their regulated institutions to:

- Develop design testing and controls for AI;
- Monitor the quality and applicability of both data input to, and information output from, AI;
- Apply existing regulations and guidance about financial institution use of technology to AI, while developing new policies and controls for use of AI;
- Build expertise and capacity; and
- Monitor AI innovation and development, as well as emerging risks.

Boards of financial institutions should ensure that management is providing information about the institution's efforts for both employing AI in everyday business and controlling its risks. External advisory resources and internal dedicated resources can enhance the board's understanding of the benefits and risks of AI. Furthermore, regulators are likely to inquire about, and examine controls for, the use of AI.[14] Therefore, boards and management should ensure they have undertaken appropriate enterprise-wide diligence and adopted policies, and coherent and consistent internal and external messages, regarding AI's use.

Key Takeaways

–

AI is rich in promise but should be adopted with risk mitigation in mind to maximize value and minimize unforeseen liability.

- Senior leaders should be involved in AI adoption, and boards should be involved in its oversight, as it poses key risks in addition to great benefits.
- AI should not replace subject matter experts, but instead should be integrated with their roles to protect against over-reliance risks.
- Corporations that are not adopting AI still face risks associated with the AI revolution and should prioritize mitigating this new type of risk in all its various aspects.

---

[1] In referring to AI, this article is focused on the recent developments in generative AI and large language models.

[2] According to the latest annual McKinsey Global Survey, 28% of respondents reporting AI adoption at their organizations have generative AI use on their board's agenda and a third of all respondents are using generative AI regularly in at least one business function. *See* McKinsey & Company "The State of AI in 2023: Generative AI's breakout year" (August 1, 2023), available here. Additionally, AI investment took center stage in budget reviews. 47% of technology officers across a variety of industries said that AI is their number one budget item over the next year, more than double the second-biggest, which is cloud-computing, according to the CNBC Technology Executive Council bi-annual survey from June 2023. *See* CNBC "A.I. is now the biggest spend for nearly 50% of top tech executives across the economy: CNBC survey" (June 23, 2023), available here.

[3] KPMG surveyed 225 U.S. executives across industries in organizations with $1 billion or more in revenue in March 2023 on their views of generative AI with an updated survey of the same population in June 2023. 66% of respondents do not have a formalized AI risk management function, and do not expect to have one for periods ranging between one and four years. Although 44% of C-suite executives responded that they were directly involved in establishing new AI processes, only 33% were responsible for developing and/or implementing governance to mitigate AI risk and only 23% were responsible for review of AI risks themselves. *See* KMPG "Responsible AI and the challenge of AI risk" (2023) available here.

[4] Axios "Behind the Curtain: What AI architects fear most (in 2024)" (November 8, 2023), available here.

[5] In a KPMG study, 53% of respondents cited a lack of appropriately skilled resources as the leading factor limiting their ability to review AI-related risks. *See* KMPG "Responsible AI and the challenge of AI risk" (2023) available here. In McKinsey's survey, just 21% of adopters said their organizations have established policies governing employees' use of AI. *See* McKinsey & Company "The State of AI in 2023: Generative AI's breakout year" (August 1, 2023), available here. At present, 68% of executives surveyed by Deloitte reported a moderate-to-extreme AI skills gap. *See* Deloitte Center for Technology, Media & Telecommunications "Talent and workforce effects in the age of AI: Insights from Deloitte's State of AI in the Enterprise, 2nd Edition survey" available here.

[6] IBM "Shedding light on AI bias with real world examples" (October 16, 2023), available here.

[7] *See, e.g.,* Michael S. Barr, Vice Chair for Supervision, Board of Governors of the Federal Reserve System, *Furthering the Vision of the Fair Housing Act,* Speech at "Fair Housing at 55—Advancing a Blueprint for Equity", National Fair Housing Alliance 2023 National Conference, Washington, D.C. (July 18, 2023), available here.

[8] *See, e.g.,* CFPB "CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence"(September 19, 2023), available here.

[9] *See* SEC Press Release "SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers" (July 26, 2023), available here.

[10] For further discussion of the Biden Executive Order, *see* our November alert memo available here.

[11] Financial Times "Gary Gensler urges regulators to tame AI risks to financial stability" (October 15, 2023), available here.

[12] *See* NYC Local law 144 FAQs, available here.

[13] FSOC "Annual Report 2023" (December 14, 2023), available here.

[14] *See, e.g.,* Christopher J. Waller, Governor, Board of Governors of the Federal Reserve System,"Innovation and the Future of Finance"Speech at Cryptocurrency and the Future of Global Finance, Sarasota, Florida (April 20, 2023), available here; OCC, Federal Reserve, FDIC, CFPB, NCUA, "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning" 86 Fed. Reg. 16837 (March 31, 2021), available here.

CLEARY LAWYERS INVOLVED

David Lopez
New York
Adam Fleisher
New York
Daniel Ilan
New York
Benet J. O'Reilly
Bay Area
James R. Burns
Washington, D.C.

Hugh C. Conroy, Jr.
New York
Lina Bensman
New York
Synne D. Chapman
New York
Marcus Holtzman
New York

SEE MORE

VIEW OTHER PUBLICATIONS

Artificial Intelligence

Attorney Advertising.