For the Attention of the Board

Information directors need to know

Questions directors need to ask

With expert perspective from DRD PARTNERSHIP

AI at the Helm: Boardroom Enquiries for Smart Integration and Strategic Success

Mishcon de Reya

Artificial intelligence (AI) is no longer a buzzword whispered in tech circles - it is now the hot topic for business leaders.

A 2023 McKinsey survey of organisations around the world revealed that 40% of respondents plan to ramp up their AI investment. Embedding AI at speed could, however, risk a devaluation of core intellectual property assets, discrimination claims resulting from algorithmic biases, and a reputational fall-out from inaccurate outputs.

This difficulty is compounded by a shifting regulatory landscape, as well as the need to be vigilant against the external threats posed by fraudsters' increasing use of AI to compromise business integrity and information security. Offering a compass to board directors as they navigate this technology's disruptive potential, this briefing note sets out the key questions to ask when deciding upon incorporating AI into their companies' work processes and highlights common AI-based activities that could be fraudulent.

Questions directors need to ask of their team

Integrating AI within your business operations: should you press the green button?
Evaluating the legal, ethical, and organisational implications of rolling out AI within your company can, understandably, sound daunting. The following questions will help steer the Board to a considered approach:

- What is the end goal of the AI in question, and what kind of data will it handle? How sensitive is that data?
- What is the benefit of introducing the technology and are there any risks exposed as a result? Can these be mitigated?
- Is the AI under consideration simply one of many tools to accomplish a specific task, or will it constitute the core of your company's operations? In the latter case, will it be easily to separate the AI-driven elements from the remainder of your business's activities?
- If the AI in question were to be removed shortly after implementation, what would the impact be? In other words, how integral is it to your organisation?
- Are the specific use cases of the AI in question regulated? Are there any sector-specific regulations or guidelines to consider as well? Do they prevent you from using the technology to achieve the end goal?
- Are there any cultural or societal impacts of using the AI? Are there any impacts on the rights and freedoms of individuals, groups or the environment? Can these be balanced?
- Do you have appropriate insurance coverage in place for those use cases?
- Does your business have the resources (in terms of technology, infrastructure, staffing, talent pool, and learning culture) to ensure effective and responsible implementation of the AI in question?

Once the Board have considered these issues, it will be in much better position to evaluate whether the commercial benefits of the AI system in question are likely to outweigh the risks. The next section of this briefing sets out practical ways of mitigating these.

How to manage the risks of implementing AI

- **Craft an AI strategy.** A high-level AI strategy and governance procedure is key to adopting a consistent approach to AI technologies. The core principles outlined in the UK government's 2023 AI white paper – including safety, transparency, fairness, accountability, and redress – offer an excellent starting point. It is also worth monitoring whether other businesses in your sector adopt particular international standards for the management of AI, such as the recently published ISO/IEC 42001(which we have summarised here). You can refer to our Artificial Intelligence and Machine Learning resources, available here, for further guidance.
- **Assemble an advisory team.** It is worthwhile appointing at least one director to spearhead AI issues within the company. Depending on your company's size, you may wish to consider establishing an internal AI committee. If your staffing resources do not allow for this, now would be a good time to engage external advisers so that you have a trusted point of contact.
- **Maintain an audit trail of risk assessments and due diligence.** With a high-level AI strategy in place, develop specific policies and procedures to address more use-case-specific risks arising from the AI in question. This will also be invaluable in flushing out any legal, ethical, or technological concerns when you negotiate with AI vendors, and will help your business to demonstrate compliance and accountability.
- **Plug any gaps with contractual commitments.** If, as part of your risk assessments, it becomes clear that your favoured AI system supplier cannot address all your concerns or responsibilities (be they legal, ethical, or commercial), you should require additional contractual commitments from them to mitigate your company's risk. This might include, for example, seeking assurances on the provenance and legality of the data used to train the AI system and obtaining a clear commitment to 'explainability', so that you have the right tools and frameworks to understand and interpret the predictions made by the AI system in question. Where suitable, you may want to seek such reassurance by way of an indemnity.
- **Keep humans in the loop.** Ensuring appropriate human oversight of AI systems is vital for mitigating the risks of inaccuracy and bias and for identifying critical divergences between AI-powered decisions and human choices. This will also help to achieve legal and regulatory compliance, since developing AI laws are likely to mandate human intervention (and certain existing legislation, like the GDPR, already requires this in respect of automated decision making and the profiling of individuals). Humans will also be important for effecting quality control measures to mitigate the risk of deviation caused by bad data.
- **Strive for continuous improvement.** To ensure the risk management strategy is fit for purpose, it needs to evolve with the technology. Therefore, introducing regular review points and continuously striving to identify and mitigate the effect of new risks will be important. The technology is not static, therefore applying static, infrequent review periods is unlikely to be effective. Introducing trigger points at various stages in the technology's lifecycle and in response to key events, in addition to regular static reviews will be beneficial for achieving this.

Expert perspective : AI regulation – pinning down specifics

Michael Rose, Senior Associate, DRD Partnership

The AI Safety Summit in November 2023 was something of a political coup for the Prime Minister. Industry heavyweights, senior politicians and world-leading experts ensured the UK avoided the embarrassment of a room devoid of real decision makers. While positive progress was made towards reaching an international consensus on how AI might be governed, we are still a long way off a codified, international set of rules and principles akin to the Paris Climate Treaty or the Convention on International Civil Aviation.
So, if you are sitting in the boardroom of a multinational company considering a rollout of AI technology across your organisation, which rules matter to you? Unfortunately, until a globally agreed set of guidelines are in place, likely to be many years off, those in charge will need to look market-by-market and the picture emerging is not one of uniformity or close alignment.

The EU, for example, is proudly trumpeting the codified set of rules soon to be forthcoming in its AI Act, despite some internal opposition, most notably from President Macron. Across the Atlantic, President Biden has issued a range of executive orders aimed at achieving a balance between promoting innovation and education, while enhancing cyber-security. The UK government, meanwhile, has adopted a more reactive approach, preferring to 'wait and see' how the technology develops and mandating existing regulators to produce AI rules specific to their sectors.
Nobody yet knows for certain which path will prove most effective. Clear 'rules of the game', as per the EU approach, can provide businesses using AI with clarity. Alternatively, the UK's more laissez-faire structure may allow for an ability to quickly adapt to a technology advancing at breakneck speed.

However, in the here and now, what should board directors take into account? First, it is vital to identify which regulators have authority over their businesses' operations. In the UK, for example, this will involve multiple authorities. Next, gather evidence and data to highlight how your operations are not only compliant, but harnessing the positive potential of AI to achieve better outcomes. Finally, marshal your arguments into a clear, persuasive, and concise narrative.

In parallel, boards should consider some key 'watchouts' in their approach (for example, stipulating that staff are not to input confidential data into generative AI bots). Further practical tips are provided at the end of this briefing.
Once all this has been achieved, a proactive board seeking to get ahead of the game will begin engaging directly with relevant regulators and stakeholders. Establishing a clear line of communication, backed-up by positive, proactive demonstrations of the company's actions on AI, will ensure regulators better understand a company's motives, actions, and operations ahead of challenges arising and scrutiny being applied. This approach will ensure boards can keep up the pace and stay ahead of the AI game.

What should the strategy cover? Important considerations

Regulatory requirements

As discussed in the 'Expert Opinion', the global race to regulate AI is intensifying. 2023 concluded with the EU's three main institutions having reached a provisional agreement on the text of the EU Artificial Intelligence Act. Once this is formally adopted and becomes law (which we expect to occur in early 2024), it will place an outright ban on AI tools deemed to carry unacceptable risks (for example, those used to classify individuals based on their social behaviour or personal characteristics) and will strictly regulate 'high-risk' AI (as might be found, for example, in systems that determine access and eligibility to public services and benefits). Brexit notwithstanding, UK businesses with global operations cannot afford to ignore this legislation, since it will apply to any organisation implementing AI systems in the EU, serving EU-based users, or utilising AI outputs within the EU. The proposed penalties for non-compliance are staggering: up to 7% of global revenue or €35 million. Given the global trend towards greater governance, it would be unwise to overlook this legislative landscape and risk incurring financial penalties. In addition, your business may already have various existing regulatory obligations to consider if it operates in a sector such as healthcare, finance, or transportation.

Intellectual Property (IP)

Permitting your staff to use publicly available AI tools such as ChatGPT could inadvertently expose your business's valuable IP and confidential trade secrets to competitors, especially if they are incorporated into the data used to train AI models. Even using non-public tools with walled gardens, whilst more secure, is not without risk. Outputs generated by AI may also infringe third parties' IP, leaving your business open to legal action if it makes use of them without first considering the risk of infringement. With proceedings already underway around the world against major AI vendors (including OpenAI, Meta, Microsoft, Midjourney and StabilityAI) for allegedly having unlawfully trained their foundation models on copyright-protected content, your company could be next in the firing line of litigation if, without having taken sufficient precautions, it builds its core operations on those foundation models. Our guide on Generative AI and IP sets out how to navigate both the opportunities and risks, together with practical steps to mitigate infringement risks.

Hallucinations

Generative AI is known for 'hallucinating' (creating inaccurate information). Since this can impact customer interactions, internal decision-making, and even high-level business strategy, over-reliance on these technologies without further scrutiny or verification could result in reputational damage and claims for misrepresentation or professional negligence. It could also attract financial penalties if hallucinations result in inaccurate datasets comprising personally identifiable information, given that accuracy is a core data protection principle.

Bias and discrimination

While powerful, AI systems are not immune to bias and discrimination. Since they learn from data, if that data contains discriminatory biases, then AI-powered outcomes can perpetuate and even amplify them. If unaddressed, this could result in legal repercussions by way of breaches of equality legislation, as well as a commercial fallout resulting from a loss of trust. See our Guide on AI in the Workplace for further information.

Data privacy

Careful navigation of data protection risks is vital if personally identifiable information is to be entered into any AI system you are considering, particularly given the hefty fines that could be imposed for privacy breaches by both the UK's data protection watchdog, the Information Commissioner's Office, and its foreign counterparts. Potential pitfalls include undertaking automated decision-making that could impact individuals (for example, in a recruitment context) without being upfront about this or without incorporating human oversight into the process. AI's propensity to accumulate large volumes of data to improve its outputs could also infringe the fundamental principle of retaining personally identifiable information only for as so long as it is needed.

Product liability and negligence

AI's autonomy and unpredictability may result in unintended safety risks. The quality of data inputs directly affects the performance of AI algorithms, with poor data increasing the risk of malfunctions. As they frequently depend on external platforms, AI systems are additionally susceptible to cyberattacks. The multiple actors involved in the design and deployment of a malfunctioning AI system would likely complicate the attribution of liability in the event of a safety or negligence case, potentially leading to time-consuming and costly litigation.

Reputational risk

Recent headline-grabbing cases underscore the reputational damage inflicted by AI failures. If an AI system behaves unexpectedly or produces unfair results, public trust can be eroded and your company's brand tarnished (and its value consequently decreased). In an era where customers increasingly value ethical conduct, the reputational fallout from getting AI implementation wrong could be catastrophic.

But remember…

These challenges, while significant, also offer a unique advantage. By taking active steps to address these risks (see our tips on page 10 for suggestions), your business will be able to showcase its commitment to responsible AI practices, turning compliance into a competitive differentiator.

Expert perspective : AI Fraud

Elizabeth Metliss, Managing Associate, Mishcon de Reya
T: 020 3321 7472
E: elizabeth.metliss@mishcon.com

As discussed elsewhere in this briefing, your use of AI tools can present certain risks that need to be managed. It is also important to consider who else may be using AI when interacting with your business and the threats that this can cause. In particular, fraudsters are increasingly using AI to carry out fraudulent activity. Businesses need to be proactive in understanding what they should be looking out for.

Fraudsters are using some of the following techniques:

1. **Manipulated chatbots:** It has recently been reported that a ChatGPT feature allows users to build their own customised AI assistants[1]. These can be used to craft convincing emails, texts and social media posts which can encourage innocent recipients to click on malicious links or download suspicious files and also provide personal information or make payments.
2. **Voice cloning:** AI technology can be used to clone voices[2], and then use this to impersonate credible business partners or impersonate people within your business when communicating with, for example, customers/clients or banks.
3. **Deepfakes:** This is when AI is used to create photographs or videos that include the exact same voice, gestures and facial expressions of another person. These can be used, for example, to impersonate people in your business and seek to divert client/customer money.

Responsible AI developers will be looking to investigate where AI tools are being abused in this way and attempt to crack down on some of this activity. At the same time, scams using AI tools will unfortunately only get more sophisticated.

In the meantime, what can your business to do try and protect itself?

1. Make sure all personnel are aware of the need to look out for any requests or content that may appear unusual or outside of what would be expected from normal business activity.
2. Ensure that you have a particular house style for communications, or if you upload videos on to your website, ensure that it is distinctive (for example, with background noises or music) to make it harder for fraudsters to impersonate exactly.
3. Use AI! AI tools are available which help detect anomalies, for examples in language or speech, in the case of a cloned voice recording or a deepfake, and also in transactions or email interactions, if there has been irregular communications or movement of money. This can alert your business to any potential unauthorised activity, or if an employee has fallen victim to a scam.

[1] ChatGPT tool could be abused by scammers and hackers - BBC News
[2] BBC One - The One Show - AI Voice Scams

Summary

Practical risk management tips

Craft an AI strategy.
A high-level AI strategy and governance procedure will be important in adopting a consistent approach to AI technologies.

Assemble an advisory team.
At least one individual should be responsible for responding to and managing AI issues within your organisation. External advisors should be considered where resources are not available internally.

Maintain an audit trail of risk assessments and due diligence.
To accompany your AI strategy, in order to demonstrate compliance and responsible use, policies and procedures should be implemented and updated to address the risks posed by the AI technologies you intend to deploy.

Plug gaps with contractual commitments.
Use your contracting process to address concerns that your intended AI supplier is unable to meet, thus enabling you to mitigate your risks and obtain assurances around key issues, such as lawful use of training data.

Keep humans in the loop.
Human oversight of the technology will be vital for ensuring compliance with incoming laws and regulations. This will also mitigate risk of inaccuracy or bias.

Strive for continuous improvement.
Once implemented, obligations regarding monitoring and assessing risk of the technology are not fulfilled. Regular risk assessments, policy reviews and reviews will be necessary.

Contact

Ashley Williams
Partner
T: 020 7382 8038
E: ashley.williams@mishcon.com

Raj Shah
Managing Associate
T: 020 3321 6755
E: raj.shah@mishcon.com

Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

Mishcon de Reya

It's business. But it's personal.