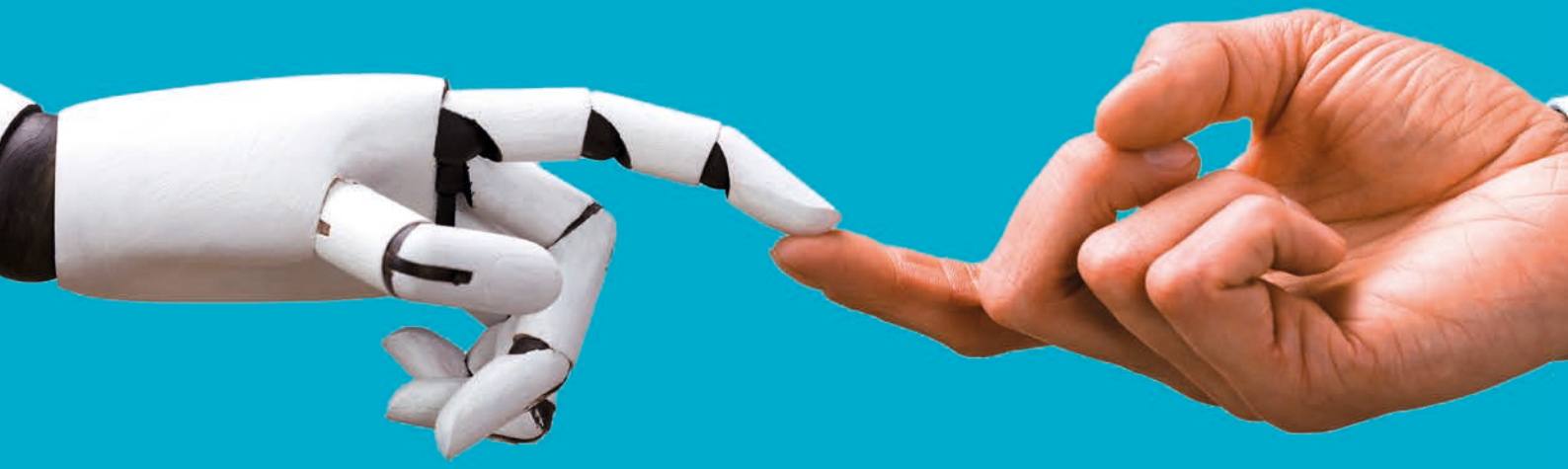
CMS
law·tax·future

Advising the Board on **AI Risk**

Reports looking at the full range of commercial risk



Risk, Resilience and Reputation

Artificial Intelligence

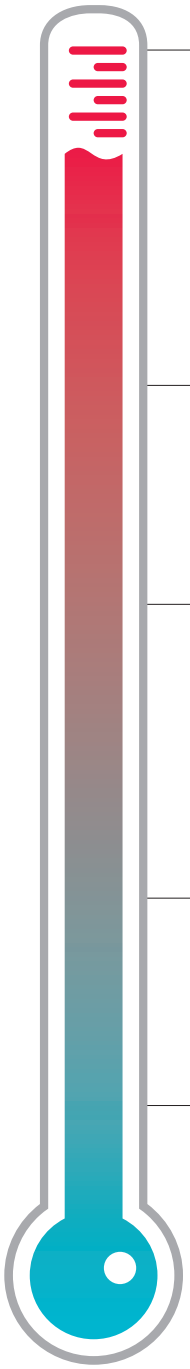
Directors' risk report'

The use of artificial intelligence (AI) can enable businesses to improve efficiency, reduce costs and deliver new products or services. As AI continues to transform industries and contribute more intelligently and efficiently to business activities, boards play a key role in integrating AI into their business and understanding its opportunities and risks.

Increasingly, boards need to weigh up the opportunities AI creates (such as tapping into the value of data) against the risks (such as data breaches) to determine how it is in the best interests of their company to use AI and integrate it into their business.

In this report, we examine the risks and liabilities associated with AI facing boards and directors and how these risks can be mitigated.

Risk thermometer



Employees

— If AI algorithms have been trained on incomplete or biased data and these systems are used to make key decisions about employees, these individuals may seek to claim on the grounds of discrimination. Poor implementation and use of AI systems may also demoralise employees and lead to falling standards.

Board

— Association with poor AI governance procedures or claims for AI technology failure or misrepresentation could be a breach of directors' duties and may damage a company's reputation.

Customers

— In addition to data controllers (who decide why and how personal data will be used) processors (who process data on behalf of a controller) can be directly liable for certain data protection breaches. Data processing agreements will seek to allocate liability between customer and supplier. The supply chain may be targeted by malicious actors.

Suppliers/programmers/manufacturers

— Poor AI systems may lead to late payment of invoices for goods and services delivered. Suppliers/programmers/manufacturers may also be implicated in claims for AI failure.

Shareholders

— High profile claims or complaints against the company for the use of an AI system or for data breaches may have a significant negative impact on a company's reputation and in turn lead to diminishing revenue reducing shareholder value.

Covid-19 and AI Risk

During the Covid-19 pandemic, companies across industry sectors have expanded their IT capabilities to facilitate remote working. This has been achieved by increasing capacity across existing IT systems and adopting new technologies to enable them to collaborate and communicate effectively across their teams.

The confidence gained by effective use of IT on such a large scale will encourage many companies to invest further in their IT systems and is likely to accelerate the adoption of AI-based technologies. However, deployment of AI technologies should be approached with the long term needs of the business in mind, even if their initial implementation is directed at alleviating short term pressures.

Implementation of many AI technologies which can improve business efficiencies must be accompanied by a change in working practices to secure the business benefits. Such changes can rarely be implemented effectively without significant thought and forward planning, complemented by the right level of appropriately skilled resources. This takes time to implement and can be counterproductive if advanced too quickly.

Further, many AI systems which operate by machine learning require large quantities of data to reach a point at which they operate effectively, which may require months of live operation. Those systems must be implemented as part of a long-term strategy rather than to meet short term needs.

Whilst a crisis can force changes to business practices which have long term financial benefits and use of technology is strongly associated with improved efficiencies, it is important that careful consideration goes into the adoption of new technologies to ensure that they are right for the long term needs of the business, as well as giving due consideration of the other issues covered in this report.

AI and Risk Management

AI is a game changer for risk management. AI can enhance complicated decision-making processes and help improve a company's supply chains, strategies and risk management models and identify risks. In particular, machine learning, the form of AI where computer algorithms improve over time through their experience of using data, plays an increasingly prominent role in company risk management, for example, enhancing company monitoring and early warning capabilities and providing management teams with unprecedented knowledge. AI technologies such as data analytics, dynamic pricing and personalisation algorithms will eventually become the new standard across traditional industries as consumers' expectations shift towards quicker, easier and more personalised experiences.

Key considerations for boards to mitigate AI risk

Commercial	Tech	Governance	Resourcing	Risk
— Does the board understand the potential impact of AI on the company's business model, culture, strategy and sector? — Which aspects of the business could benefit from increased automation or machine learning?	— Does the company have the computing power and infrastructure to support the use of AI? — How will a "black box" machine learning AI system be audited and kept up to date?	— How will decision making have to change because of AI? — Does the company have an AI ethics committee? — Are the company's data protection policies GDPR compliant? — Is the board up to speed with emerging policies and legislation in respect of AI?	— Does the company have the right people to develop, use and maintain AI? — Does the company have a talent acquisition strategy for recruiting and retaining people with the necessary skillsets to manage and staff AI-related projects?	— How will any AI bias be managed? — How will any intellectual property be protected? — Are there any cyber risks or data privacy issues with the proposed AI? — Is there a process/ policy in place in the event of AI failure? — How will the company gain the trust of stakeholders if it uses AI?

The risks associated with using AI in business

As considered below in more detail, some of the key risks for companies associated with adopting and using AI can be placed into the following categories: legal, cyber-security, ethics and reputation.

Legal Risk

Claims arising out of the use of AI

At present, there is little legislation governing AI in the UK, other than for autonomous vehicles and data protection, and no specific legal framework for the regulation of the development, use or failure of AI. Nevertheless, boards must be aware of the risk of potential claims under existing law as set out below.

- **Negligence claims –** Redress for victims who have suffered damage as a result of AI failure would most likely be sought under the tort of negligence, where the claimant would need to establish that the defendant company owed a duty of care, breached that duty and that the breach caused injury to the claimant. Liability for negligence would lie with the person/s or entity/ies who might have foreseen the AI product being used as it was. This may include board members.
- **Product liability / breach of contract claims –** Claims may also be brought against a company for failing to ensure that a product that causes harm to users was free from defects or for breach of contract.
- **Misrepresentation claims –** If AI is used to generate reports, such as financial statements which feed into a prospectus or disclosure document for the company, directors may be held personally liable for misrepresentations or inaccuracies in those reports. Companies therefore need to have systems in place to check the results produced by AI.
- **Competition claims –** If AI is used to recommend transactions in price sensitive securities, or to set prices of goods or services the company sells, the board needs to make sure that the AI is not relying upon inside information or causing the company to co-ordinate its prices with competitors in an anti-competitive manner.

Liability for directors under the Companies Act 2006

- **Duty to promote the success of the company – s.172 –** Directors may be in breach of their legal duty to promote the success of the company and act for the benefit of its members as a whole if, for example, decisions are made that allow the company to become too dependent on AI and managers or boards are unable to take control when an AI system fails to perform. This may cause misleading information to be produced which, if relied upon by directors, may lead to decisions that are not in the company's best interests.
- **Duty to exercise reasonable care, skill and diligence – s.174 –** When working with AI, directors must consider their duty to act with reasonable care, skill and diligence in relation to AI and act diligently, keep themselves informed about the company's affairs and join with their co-directors in supervising and controlling any decisions on AI.

  For example, a director may be in breach of this duty where s/he leaves decision making to algorithms without understanding the basis on which the AI is making recommendations, or where a director relies blindly on recommendations or decisions taken by AI.

Liability for data breaches (GDPR)

The use of AI to handle and evaluate vast quantities of unstructured data is enormously helpful to companies, for example, to enhance decision making capabilities. However, boards must build a comprehensive data management strategy and be aware of the risks involved in storing and processing data, in particular personal data, to avoid being liable for significant penalties under the EU's General Data Protection Regulation 2016/679 and the UK's Data Protection Act 2018. **Please see our Advising the Board on Data Risk Report for more detail here.**

The type and complexity of the AI systems involved in making solely automated decisions will affect the nature and severity of the risk to people's data protection rights and will raise different considerations, as well as compliance and risk management challenges. The GDPR requires that companies implement suitable safeguards when using solely automated systems that make decisions with significant impacts on data subjects. For example, where automated systems make recruitment decisions, data subjects should have the right to express their point of view, obtain human intervention and contest the decision made about them. The ICO has made clear that these safeguards cannot be token gestures.

Cyber-Security risk

Cyber criminals who want to steal confidential information about a company or personal data are increasingly likely to target AI systems. Directors who fail to implement adequate cyber-security measures, which leads to an AI system being vulnerable to hackers causing damage to the business, may be implicated in investigations and/or legal claims for a breach of their duties to the company.

With cyber-attacks on the rise and the use of AI becoming more complex, with increased connectivity and the storage and processing of vast quantities of data, the need for companies to invest in cyber-security, including fraud detection, has never been more critical.

Equally, AI can be part of the solution – as cognitive fraud detection systems continue to learn, they will be able to detect more complex fraud and boards should consider the use of such AI models in their cyber-security strategy.

Ethics – AI Bias and Discrimination

How AI technology is used depends on the information on which it is trained and how it is trained. Machine learning algorithms identify patterns in data and codify them in predictions, rules and decisions. If those patterns reflect some existing bias, the algorithms are likely to amplify that bias and may produce outcomes that reinforce existing patterns of discrimination. Where there are programming errors in the AI, algorithms may not perform as expected and may deliver misleading results that have serious consequences.

To mitigate the risk of AI bias, for example in board decision-making or appraisals, boards should ensure that a record of all data which has been input is kept and that the data used is as diverse as possible and free from any discrimination such as prejudices, biases and societal injustices. If they do not, directors may be at risk of discrimination claims (for example, under the Human Rights Act 1998).

Reputation Risk

Any AI system that demonstrates bias, is predisposed to errors, is hacked or used for unethical purposes poses significant reputational risks to the company that owns it. To build trust, boards need to be transparent about the AI's decision making process and how the AI system reaches its conclusions. If grave or frequent mistakes are identified, boards will need to take immediate steps to understand and rectify the underlying issues and, if necessary, suspend the use of the automated system to avoid reputational damage.

Insurance Risk

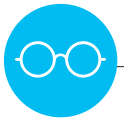
One very real risk for companies is if inadequate insurance is taken out against the risks arising from the company's use of AI. If the company suffers loss due to a failure in AI adopted by the company and it does not have adequate insurance, this may lead to claims against the companies and in these circumstances directors may be found liable for breach of their duties for failing to arrange adequate insurance coverage. Certain insurance policies are available to cover the technology risks involved in the adoption and use of AI, for example:

— product liability insurance in respect of customer products which make use of AI;
— cyber-insurance to cover loss of data in the event of a cyber-attack;
— Directors and Officers (D&O) / management liability insurance to cover general risks, such as breach of directors' duties, employment claims and tortious claims.

Boards will need to consider what type of insurance is available to protect against liabilities which may arise from their use of AI technology and review carefully the definition of an insurable incident in proposed policies to ensure the particular type of loss is covered. Third party liability will also become more complicated, if, for example, directors cannot show that they took reasonable security measures to prevent a cyber-attack happening.

Summary: practical risk management

AI presents huge opportunities for companies – if the risks of using AI technology are well managed. The board has a key role to play in managing these risks and understanding the potential impact of AI on the company's business model, culture, strategy and sector. Successful management is likely to be the difference between successful AI implementation and its failure.



1. Liability

a. Ensure there are clear agreements in place with programmers, designers, experts, manufacturers and customers clearly outlining the scope of liability in the event of AI failure.

b. Ensure that there are clear mechanisms in place:
   i. to prevent the company becoming too reliant on AI;
   ii. for the board to gain back control from an AI system;
   iii. for the board to check any statements made in reports produced by AI.

c. Data management:
   i. ensure that a comprehensive data management strategy is in place for storing and processing data;
   ii. ensure that the company's data protection policies are GDPR compliant, clear on how data collected by AI will be used and employ a Data Protection Officer if appropriate;
   iii. ensure that safeguards are in place for a human review of AI decisions which impact data subjects.

2. Cyber-security

a. Invest in robust cyber-security systems, for example, using AI models such as cognitive fraud detection systems.

3. Ethics and Reputation

a. Ensure that there are clear mechanisms in place to train AI systems without algorithmic bias and use a complete and diverse set of data free from discrimination.

b. Set up and use a diverse AI ethics committee.

c. Keep a record of all data inputted into the AI machine.

4. Insurance

a. Ensure adequate insurance is taken out to protect against the claims which may arise from the use of the AI systems such as product liability, cyber and/or D&O insurance.

b. Carefully check the definition of an insurable incident under proposed policies.

5. Resource

a. Ensure the company has the computing power and infrastructure to support the use of AI as well as the talent with the necessary skillsets to manage AI-related projects.

6. Governance

a. Ensure that the company keeps up to speed with emerging policies and legislation in respect of AI.

Authors

Lee Gluyas
Partner
T +44 20 7524 6283
E lee.gluyas@cms-cmno.com

Colin Hutton
Partner
T +44 131 200 7517
E colin.hutton@cms-cmno.com

Stefanie Day
Associate
T +44 20 7524 6123
E stefanie.day@cms-cmno.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

2001-0120099-9