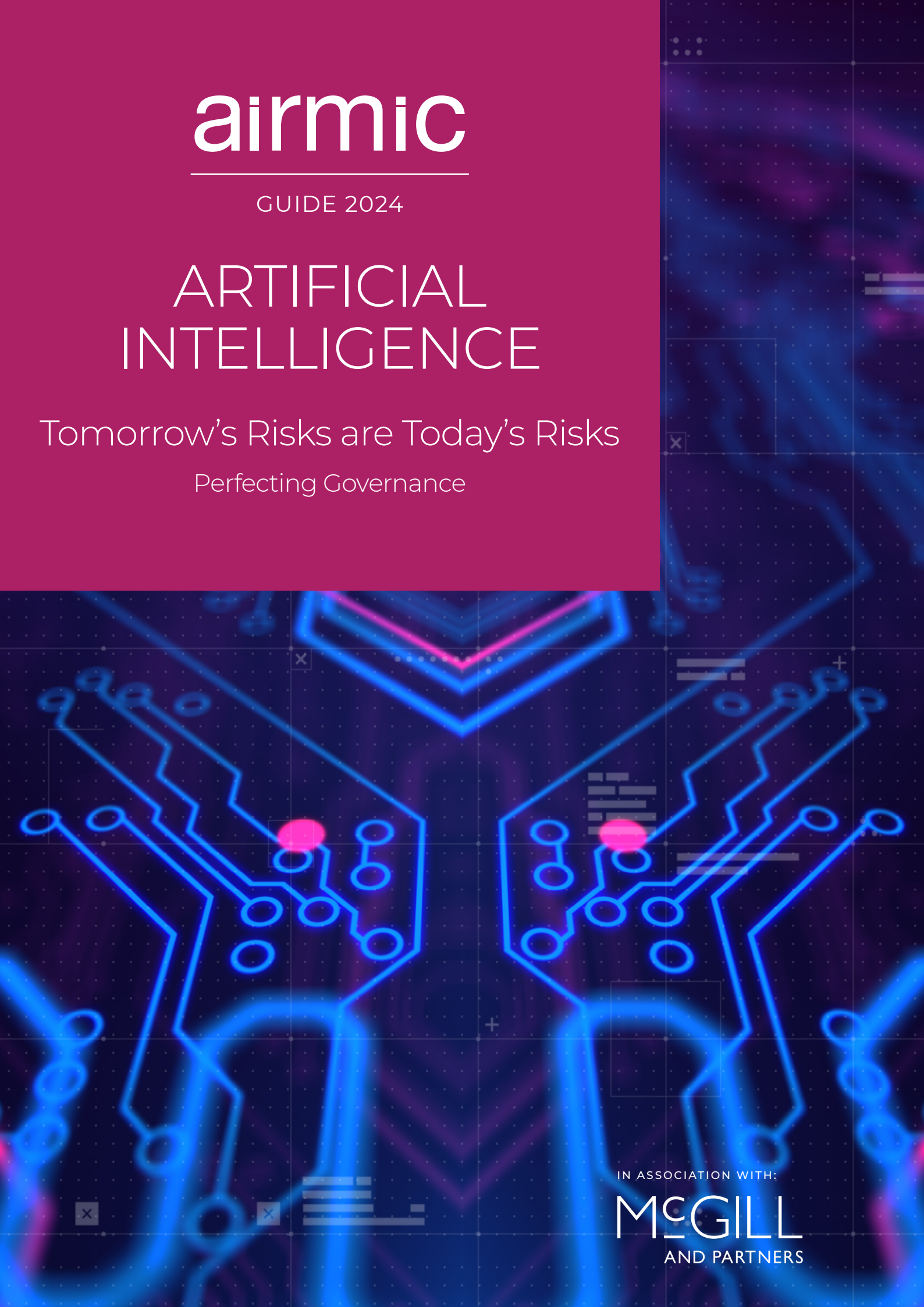
airmic

GUIDE 2024

ARTIFICIAL INTELLIGENCE

Tomorrow's Risks are Today's Risks

Perfecting Governance



IN ASSOCIATION WITH:

McGILL AND PARTNERS

Acknowledgements

Francis Kean joined McGill and Partners in 2020 bringing with him thirty years of experience in the industry. Francis is a Partner within the Financial Lines team. Previously, he was a partner at the law firm Barlow Lyde and Gilbert. Francis has handled a wide variety of financial lines claims for both insurers and clients, and has considerable experience of drafting policies and advising all parties in connection with coverage issues. He is a frequent author and speaker on liability issues affecting boards.

Jack Elliott-Frey is a Partner in McGill and Partners Financial Lines team, specialising in cyber placements. Jack has worked in the cyber market for almost 10 years, having spent the majority of his career at Aon in London, working on complex multinational cyber placements for some of the world's largest corporations. Jack began his career at a small wholesale broker in London specialising in US wholesale cyber business, before joining the large complex cyber risk team at Aon. His experience includes building and placing large multinational cyber programmes for a range of organisations, from professional services through to auto manufacturers.

McGill and Partners is a global boutique specialist (re)insurance broker focused on large clients and/or those with complex and/or challenging needs. Launched in 2019, the firm has significant backing from funds affiliated with Warburg Pincus, a leading global private equity firm. McGill and Partners is headquartered in London with offices in Bermuda, the US, Ireland, Australia, Switzerland, and Germany.

www.mcgill partners.com

McGILL
AND PARTNERS

About Airmic

Airmic is the leading UK and Ireland association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 1,900 individual members. Individual members are from all sectors and include company secretaries, finance directors, and internal auditors, as well as risk and insurance professionals. Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com

airmic

CONTENTS

01 Introduction

The first digital computers were invented around eight decades ago. Ten years ago, no machine could reliably provide language or image recognition at a human level. Advances in artificial intelligence (AI) have made it possible to use machines in a wide range of domains. Today, the use of AI is growing rapidly and changing whole sectors, with the potential to drive economic growth and transform lives. It can, however, cause damage and harm to organisations as well as to wider society, so it has to be understood and managed by all organisations.

When ChatGPT launched in late 2022, it fired up the world to the transformative potential of AI. The technology underpinning the powerful chatbot was one of the biggest step changes in the history of AI. Rather than analysing or classifying existing data, generative AI was able to create something new, including text, images, audio, and synthetic data. Across business, science, and society, it will enable new human creativity and productivity.

In a survey by the National Association of Corporate Directors (NACD) in the US, 95 percent of directors acknowledged that AI will have a significant future impact on their businesses, but only 28 percent of them said that AI is a regular feature in their board's discussions.

Fast forward to March 2024. Airmic members were polled on whether the topic of AI is now on their board's current agenda – 78% of respondents said that it is.

AI has been flagged as an emerging risk for some time by Airmic member organisations – boards are discussing AI risk frameworks and risk assessments. Where initiatives around generative AI (GenAI) originate at the top, organisations are seeing clear benefits from that strategic leadership. However, boards need to be confident and informed about the outcomes of AI decisions that can affect the lives and wellbeing of people in wide-ranging ways. And when asked specifically about the risks of adopting GenAI, few respondents said that their company is mitigating the most commonly cited risk with GenAI of 'inaccuracy'. Respondents cite inaccuracy more frequently than cybersecurity and regulatory compliance, which were the most common risks from AI cited in previous surveys.

A 2022 survey by The Institute of Directors revealed that 80% of boards did not have a process in place to audit their use of artificial intelligence and that over 86% of businesses already use some form of AI without the board being aware of this. This research reveals a gap between board governance and the use of AI in their business.

01 INTRODUCTION

01 Introduction

The vast majority of organisations rely on digital technologies to conduct their business. As digital acceleration gathers pace, and the digital economy grows, so do the risks posed by cybercrime. This remains the top principal risk to many businesses. As a response, the Government is working to improve cyber resilience across the UK economy to ensure organisations have the tools and support to protect themselves against cyber threats. The proposed Cyber Governance Code of Practice is aimed at helping organisations to manage the cyber risks they face. The Code will set out the critical governance areas directors need to tackle in order to protect their organisations.

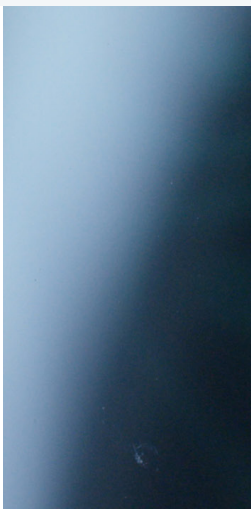
The FRC has distilled the strategic essence of the Code into the form of principles, which are supported by detailed guidance published separately. The guidance is not part of the Code, but a collection of information designed to help in the application of the Code to the different needs of organisations. The guidance will be updated from time to time to reflect, where appropriate, other reporting or regulatory requirements that may develop in the UK from other regulators. These will inevitably embrace AI, and voluntary codes in advance of regulation are already emerging.

AI has the potential to revolutionise cybersecurity. AI-powered solutions can enhance cyber resilience by providing advanced capabilities to detect, prevent, and mitigate cyber threats. AI has various applications in cyber resilience, ranging from real-time monitoring to anomaly detection and predictive analysis. By utilising machine learning techniques, AI can analyse vast amounts of data to identify patterns and vulnerabilities that traditional cybersecurity methods may miss. Managing risk should be based on the best available information – decisions should be informed and taken using reliable sources of data. Data should be accurate, timely, and verifiable, with quality assurance in place. However, organisations should be alert to biases which may distort information and lead to the wrong decisions being made.

A voluntary code for the use of artificial intelligence in insurance claims

The Code is a voluntary commitment to the use of AI in insurance claims, and an opportunity for the insurance industry to demonstrate it is taking a leading role in ensuring that it is connected with the potential risks and opportunities associated with AI. It covers areas including safety, security, robustness, transparency, explainability, fairness, accountability, and governance.

Further information can be found at www.aicodeofconduct.co.uk



01 Introduction

"Our lives are minefields of misinformation. It ripples through our social media feeds, our daily headlines, and the pronouncements of politicians, business leaders, and best-selling authors. Stories, statistics, and studies are everywhere, allowing people to find evidence to support whatever position they want. Many of these sources are flawed, yet by playing on our emotions and preying on our biases, they can gain widespread acceptance, warp our views, and distort our decisions."

- Alex Edmans – Professor of Finance, London Business School

May Contain Lies: How Stories And Studies Exploit Our Biases – And What We Can Do About It (Penguin, 2024).

The technology can be used with some good objectives – and misused with some bad ones. For these 'dual use' technologies, it is important that organisations and those who govern them develop an understanding of what is happening and how they want the technology to be used.

Organisations today are issuing communications and developing guidelines to keep their people informed about AI. Some even prohibit the use of certain AI tools, such as ChatGPT, until more is understood about how they work and the implications of their use. That is understandable given that there are no shortage of cases of AI being used in ill-judged ways. For example, a hiring algorithm was based on fake science when it purported to predict job candidates' suitability based on their facial expressions; banks have charged higher interest rates to borrowers living in disadvantaged areas; a system to predict when it was safe to swim in the sea was accurate less than half the time – in other words, the AI was as accurate as flipping a coin.

When things go wrong with AI, there is the potential for a range of losses, including financial and reputational as well as third-party liability. For example, if an algorithm causes financial or other loss, where does that liability fall? Where does the buck stop – would it be with the business that is using it, the AI developer or the licensor?

The lines between product and professional liability may shift in the future as regulations come online. Emerging regulations that focus on what companies and boards must and must not do could also impact on directors' and officers' liability. Regulation will play a significant role for the liability considerations of organisations – both developers and end-users – because, ultimately, it is the regulatory landscape that will inform organisations in terms of what they need to do.

"Given their non-delegable duties of oversight, the potential impact of AI on directors may appear overwhelming. We hope that by breaking the subject down to a set of topics addressed in a Q&A format, we have helped make it more manageable."

Francis Kean – Partner, Financial Lines, McGill and Partners

01 Introduction

Directors should carefully consider the risks and opportunities presented by AI, and develop a strategy that balances these factors to achieve their business objectives while minimising potential harm.

Risks:

- Bias: AI systems can perpetuate and amplify existing biases in data and decision-making processes, leading to unfair outcomes.
- Privacy: AI systems can collect and process vast amounts of personal data, raising concerns about privacy and security.
- Job displacement: AI systems can automate tasks and replace human workers, leading to job losses and economic disruption.
- Regulation: The use of AI is subject to increasing regulatory scrutiny, with potential legal and reputational risks for companies that fail to comply with relevant laws and regulations.

Opportunities:

- Efficiency: AI systems can automate routine tasks, freeing up human workers to focus on more complex and creative work.
- New products and services enabled by AI and innovation driven in industries ranging from healthcare to finance.
- Customer experience: AI systems can improve customer service and engagement, by providing personalised recommendations and support.
- Competitive advantage: Companies that successfully leverage AI can gain a competitive advantage, by improving operational efficiency, reducing costs, and delivering better products and services.

Some companies are already using AI in the boardroom, although few have gone as far as Hong Kong-based venture capital group Deep Knowledge Ventures. In 2014, it appointed an algorithm named VITAL (Validating Investment Tool for Advancing Life Sciences) to its board of directors, giving the algorithm the same right as the human directors of the corporation to vote on whether the firm should invest in a specific company or not. More commonly, 'artificial governance intelligence' is increasingly being applied in corporate decision-making processes ranging from due diligence in a mergers and acquisitions context to profiling of investors,

validating new business opportunities, and optimising procurement, sales, and marketing functions.

International organisations, governments, businesses, and scientific and legal communities are seeking to establish new regulations, laws, policies, ethical codes, and privacy requirements. It is almost impossible to keep up to date with this proliferation of published materials as to the benefits and perils associated with AI, let alone with the exponential growth in the power and applications of AI itself. So, what is the right starting point for boards?

The aim of this guide is to provide a toolkit to assist directors in understanding and keeping pace with the increasingly complex and fast-changing AI-related risks and opportunities faced by the companies they serve. It takes the form of 12 questions designed to break a diverse set of issues down into a manageable series of topics. The list is not exhaustive and the answers to each question will vary tremendously depending on the size, maturity, and nature of the company's business. Nevertheless, in response to each question, we identify a range of issues which are likely to be relevant.

1 Assuming I have no particular background or experience in computing, what level of expertise with respect to artificial intelligence will be expected of me as a member of the board?

Your legal duty to supervise your company's activities, including the development and deployment of AI, cannot be delegated. In order to discharge that duty, you will need a general understanding of the various ways in which your company uses AI and have the means to assess whether such uses are in line with the company's purpose and values, and whether they operate for the benefit of its employees, customers, and stakeholders.

Depending on your own particular expertise, you may also need a deeper understanding of this subject as it relates to any area of the company's activities for which you have specific oversight responsibilities.

Although there is scope for tremendous variation in the nature and extent of the uses to which AI may be put, one common denominator is the speed of change. Accordingly, there is a strong case for directors to keep this topic under close and regular review, both formally in board agendas and informally through briefings from experts and training.

A glossary of useful AI-related terms can be found on page 24.

2 To what extent if any does AI affect the legal duties to which I am subject (and the ways in which I discharge them) as a company director?

The legal duties to which directors are subject remain the same. However, depending on the size and nature of the business, it may be that AI can be deployed thoughtfully to assist you in the discharge of your executive and oversight functions. Some of the ways in which this might happen are summarised below:

A. Decision-making: AI technology can assist directors in making informed decisions by providing data analysis and predictive insights.

B. Risk Management: As part of your oversight function, you have a duty to identify and manage risks effectively. AI can be used to assess risks, detect patterns, and predict potential issues. Directors need to understand how AI systems operate and ensure that the risks associated with AI implementation are appropriately addressed.

C. Compliance and Ethics: Directors are ultimately responsible for ensuring that the company complies with laws and regulations. With the use of AI, compliance may require an understanding of AI algorithms, data protection laws, and ethical considerations related to AI use. Directors must oversee the ethical use of AI within the company. (See further answers to questions 1 above and 6 and 8 below.)

D. Cybersecurity: AI can be used to enhance cybersecurity measures within a company. Directors need to prioritise cybersecurity and ensure that AI systems are secure from cyber threats. You should be aware of the cybersecurity risks associated with AI technology and seek assurance that necessary precautions are being taken to protect sensitive information. (See the Airmic cybersecurity boardroom guide and question 9 below.)

E. Transparency and Accountability: Directors are accountable for the decisions made within the company. When the use of AI systems is involved in decision-making, directors must ensure transparency in how AI algorithms work and the factors influencing AI-generated outcomes. You should be able to explain and justify AI-driven decisions to stakeholders. This is increasingly crucial given the rising tide of misinformation and disinformation. (See also answer to question 4 below.) You should not be afraid to challenge the reliability and accuracy of the sources you rely on to satisfy yourself that the AI systems are used in line with the company's purpose and values.

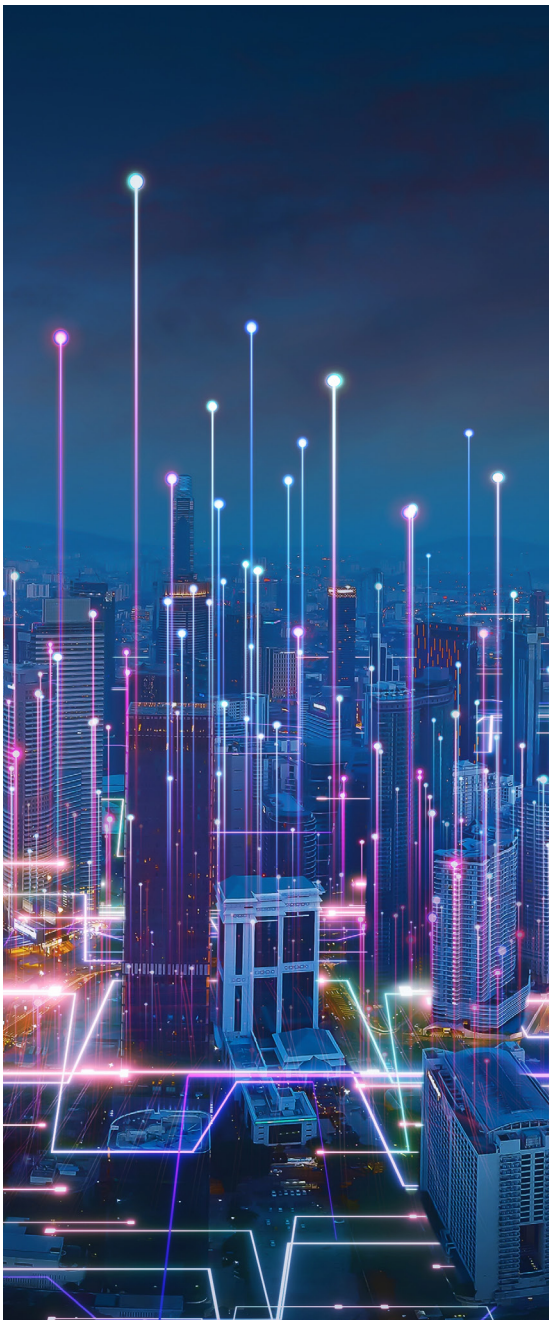
3 Is there clear and up-to-date documentation on the extent and uses to which AI is put within the company I serve?

A review is a valuable starting point for directors trying to establish the size and scope of the AI used in the company. It should entail a systematic approach to identifying, documenting, and evaluating all AI applications and initiatives across different departments and functions within the company. Relevant considerations to ensure the thoroughness of the exercise might include:

- The pre-identification of all relevant stakeholders including data scientists, IT professionals, business analysts and department heads, and others whose AI-related input, knowledge, and experience may be valuable.
- Clear definition of scope including the types of AI technologies and applications involved, such as machine learning, natural language processing, robotic process, automation, etc.
- Whether interviews and surveys with relevant teams and departments to gather information about existing AI projects tools and applications have been carried out.
- Whether all relevant documentation, reports, project proposals and contracts related to AI projects have been reviewed to identify any additional uses of AI within the organisation.
- Whether there exists a standardised inventory template or database to capture relevant information about each AI application, including its purpose, the data sources and algorithms used, the stakeholders involved, and compliance considerations.
- Whether the flow of data within each AI application is being mapped to understand sources of data, data processing activities, data storage locations, and data sharing practices.

4 Does the company have a set of written policies and guidance for the use of AI that are regularly updated and approved at board level?

As foreshadowed in the answer to question 2, the need for clear internal (and where appropriate, external) guidance and communication with respect to the company's AI policies is an important element of good governance. Published policies and guidance have their place, but you should also aim to satisfy yourself that they are observed in practice and reflect the reality on the ground. Is all AI use appropriately flagged and labelled throughout the organisation? Also, are the policies and principles which underlie them machine readable to the extent necessary to enable the company's own AI systems to apply them?



Directors should be aware of the risk that written policies and guidance with respect to AI which are merely aspirational or perhaps out of date could be used as a weapon by future disgruntled or adversely affected stakeholders to highlight a company's failings in this area. (This has already proven to be the case with other broad-ranging risk topics on which policies and guidance are typically issued, such as ESG, health and safety, and cyber risk.)

Underpinning all this is a need for the right talent with the right knowledge and skills to be deployed in the company.

5 Am I satisfied that the company's approach to AI (and its policies) is transparent, just, and responsible?

- If you have already satisfied yourself that the uses to which the company puts AI are in line with the company's purpose and values, and that they operate for the benefit of its employees, customers, and stakeholders (see answer to question 1), you will have made a good start. You will also wish to know whether the company has an appropriately skilled and empowered ethics committee, and whether it has clear terms of reference.

- The nature and degree of any further enquiries you may need to pursue will vary according to your specific sphere of expertise, and the size and nature of the company's activities. For example, does your company employ agencies whose recruitment processes are susceptible to forms of bias? To what extent is AI involved in the marketing by the company of its products or services? Does such involvement increase the risk of a lack of veracity?

6 Do I have an adequate grasp of the regulations and laws, and any emerging changes to these, that are applicable to the use of AI in the jurisdictions in which the company and its suppliers and other significant partners operate?

What is 'adequate' for this purpose will vary depending on the nature and scope of the company's operations. However, given the likely impact on all companies of law and regulation in this area, a general understanding of this topic by all directors is likely to be expected.

On 13 March 2024, the European Parliament approved the adoption of the EU Artificial Intelligence Act. Although this sweeping law will not come into force for at least two years, its scope clearly illustrates the significant impact on business that AI is expected to have. It will apply to all companies that do business in the EU, and not simply to those that are based there, and to AI products in the EU market, regardless of where they were developed. The regulation imposes requirements on companies designing and/or using AI in the European Union. It may well serve as a template for similar regulation elsewhere among developed economies, including the UK and the US.

- Among other things, the Act covers: Classification System: The AI Act introduces a classification system that assesses the level of risk posed by an AI technology to the health, safety, and fundamental rights of individuals. This system helps categorise AI systems based on their potential impact.

- Development and Use Requirements: The legislation sets out requirements for the development and deployment of AI systems, including rules related to data quality, transparency, human oversight, and accountability. The goal is to ensure that AI technologies adhere to ethical standards and respect fundamental rights. AI systems that are deemed by legislators to be high risk, such as those used for immigration or critical infrastructure, must be subject to risk assessments.

- Transparency Requirements: The legislation seeks to impose transparency around the use of AI tools. The law requires clear labelling of images, audio, or video that have been generated or manipulated by AI and that might otherwise appear to be authentic.

- Ethical Considerations: The AI Act aims to address ethical questions related to AI deployment across different sectors such as healthcare, education, finance, and energy.

- Ban on Certain Uses: The Act prohibits the use of AI technology in biometric surveillance and requires generative AI systems (such as ChatGPT) to disclose when content is AI-generated. The Act bans biometric categorisation systems based on sensitive characteristics and untargeted scraping of facial images from the Internet. It also bans emotion recognition in the workplace and schools, social scoring, and predictive policing.

With thanks to Kevin La Croix for his input in this section.

7 Does the company audit and evaluate the extent to which AI is used in its supply chain?

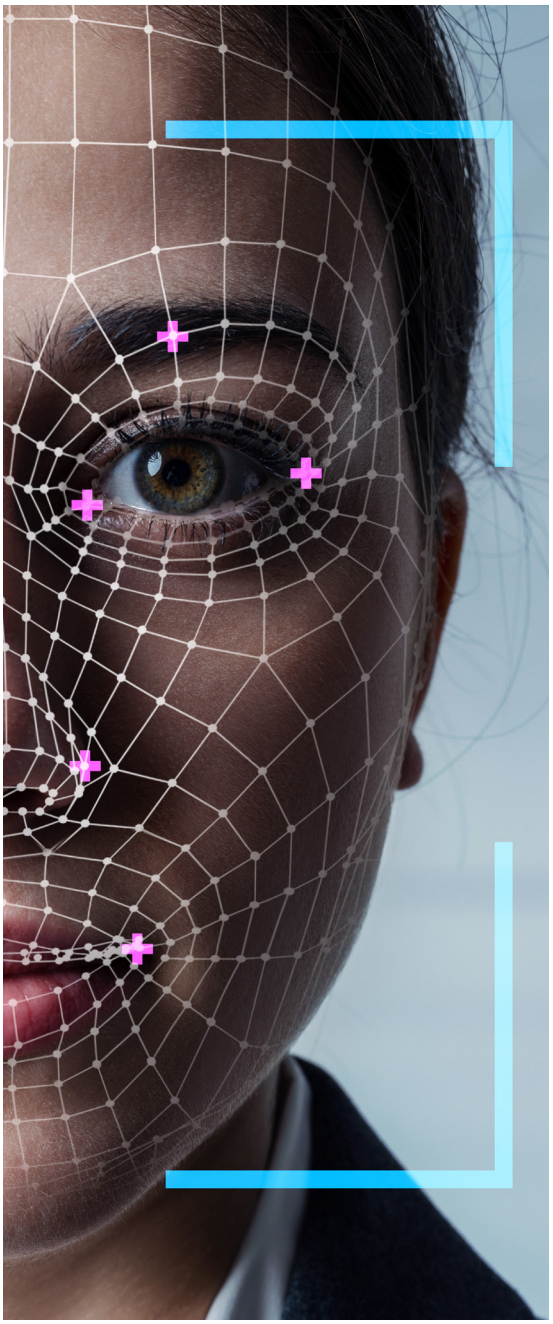
The question of supply chain management in general is addressed in a separate 2023 Airmic boardroom guide dedicated to this subject which directors should refer to. Given the increasing inter-connectedness of business and the way in which law and regulation continue to extend indirectly into the supply chains of larger companies (see for example Articles 28 and 29 of the EU General Data Protection Regulation (GDPR)), directors would be well advised to understand both how thoroughly and how frequently the company audits and evaluates the extent to which AI is used in its supply chain.

It is also likely that AI is used as a tool to gather and evaluate valuable data as to the location and condition of goods in the supply chain. This may be done through collaborative processes with key suppliers using and sharing output from increasingly sophisticated and automated processes under the supervision of subject matter experts. More complex supply chain vulnerabilities may create further specific AI-related challenges for the company about which directors may wish to have a general level of awareness. These include third-party components, libraries, and other shared data sources that are integral to AI systems. Cyber attackers may exploit weaknesses in the supply chain to compromise AI systems or gain unauthorised access to sensitive information. Again, it is important to work with vendors and partners to assess and mitigate supply chain risks effectively.

Another issue to explore might be the extent to which the review of the company's use of AI is within the remit of any internal audit function and, if so, whether the team has the necessary expertise to discharge that responsibility. The same may be asked of the external audit team. Allied to this is the question of the frequency with which any such reviews are carried out. Are they adequate to keep up with the pace of change in this area?

8 What are the privacy law-related implications of the uses to which the company puts AI?

Depending on the nature of the company's activities, the implications of the use of AI may be significant. Companies in the UK and beyond must already ensure compliance with the GDPR and the Data Protection Act. The EU Artificial Intelligence Act also contains privacy provisions relating for example to the restriction of biometric surveillance. If companies are transferring personal data across borders for AI processing, they will need to comply with the relevant regulations governing international data transfers.



Companies using AI also often collect and process large amounts of data including personal information. It may be necessary to revisit and update consent and user rights, such as the right to access, rectify, or delete data, since the way in which such data is processed by AI may be different from previous uses.

Also, AI's ability to process sensitive personal data makes it a prime target for privacy breaches. The potential legal impact of data theft, unauthorised access, or data poisoning attacks on individuals' rights by the company's own AI systems or those for which it may be responsible should be understood by directors at a general level.

9 What are the cyber security implications of AI?

As artificial intelligence continues to permeate various sectors, its integration raises critical cybersecurity concerns which demand the attention of board members. With the promise of enhanced efficiency and innovation, AI also brings forth a new frontier of cyber risks that must be navigated with vigilance and strategic foresight.

AI's reliance on vast amounts of data and interconnected networks expands the attack surface for cybercriminals, posing significant challenges for cybersecurity defences. Board members should recognise that AI-driven systems may be vulnerable to various threats, including adversarial attacks, algorithmic errors, and data breaches.

The integrity and reliability of AI models is also critical. Cyber attackers may attempt to corrupt AI models by poisoning training data or introducing biases, leading to erroneous predictions or decisions. This may undermine the trustworthiness of AI-driven systems and can have far-reaching implications for business operations, ranging from financial losses to reputational damage.

Directors should seek assurance that the company has a good and up-to-date grasp of these vulnerabilities. Is the company making adequate investment in AI-specific security measures to mitigate the risks posed by adversarial manipulation?

Horizon scanning to develop scenarios for analysis can help inform risk and opportunity assessment in complex environments relating to cybersecurity. Also, because of the pace of change and development in this space, it is important to assess risks and controls associated with the use of AI with sufficient regularity. Risk management must synchronise the different speeds at which the strategic (or external) risk, tactical risk, and internal (or operational) risk programmes run – to avoid the creation of time lags.

Ultimately, because of the risk complexity and the need to overlay AI across other risks – which demands collaboration across company functions – this should not be regarded purely as a technology subject.

10 What are the intellectual property implications for the company in using AI output?

Artificial intelligence has emerged as a transformative force, revolutionising industries and reshaping business landscapes. Amid the rapid advancement of AI technologies, businesses must navigate a complex web of intellectual property (IP) considerations to protect their innovations and remain competitive in the global market. Once again, directors' duties of oversight require a general level of understanding of this issue.

At the heart of the intellectual property implications for businesses using AI lies the question of ownership. Traditional principles of IP law typically attribute ownership to the human creators of a work. However, in cases where AI autonomously generates new inventions, works of art, or other creative outputs, questions arise regarding who holds the rights to the resulting IP. Determining ownership of AI-generated IP can be intricate and requires careful consideration of legal frameworks and contractual agreements.

One key area of concern is the patentability of AI-generated inventions. To qualify for patent protection, an invention must meet criteria such as novelty, non-obviousness, and industrial applicability. While AI-generated innovations may satisfy these requirements, patent offices may scrutinise the level of human involvement in the invention process. Clear documentation of human contribution and involvement in AI development is essential to strengthen patent claims and secure IP rights.

Similarly, copyright protection for AI-generated works presents unique challenges. Copyright law typically attributes authorship and ownership to the human creators of original works. However, in some jurisdictions, copyright protection may extend to AI-generated works if there is sufficient human involvement or creative input in the AI's programming or training process. Has the company established clear guidelines to determine the extent of human authorship in AI-generated works to avoid or minimise the scope for disputes, and to protect IP rights?

Moreover, businesses using AI must safeguard trade secrets and confidential information embedded within AI algorithms or datasets. Robust security measures, access controls, and contractual safeguards are essential to prevent unauthorised disclosure or misuse of proprietary AI technologies. Failure to adequately protect trade secrets can result in loss of competitive advantage and potential legal liabilities and litigation risk.

In summary, businesses should adopt a proactive approach to IP management, including clear documentation of human involvement in AI development, robust protection of trade secrets, and strategic enforcement of IP rights. A general understanding of these issues will enable directors to discharge their oversight duties with regard to the intellectual property implications of using AI.

11 With regard to the various insurances which the company buys (including cyber insurance and covers placed in a captive if a captive exists), do I understand the potential coverage implications of the extent to which the company deploys AI?

As businesses strive to fortify their digital defences against evolving threats, cyber insurance represents an important way in which companies can mitigate this risk. Directors should refer to the separate Airmic boardroom guide on cyber risk published in 2023. How, if at all, does AI have an impact on this important form of protection? Although directors may not be expected to have an in-depth understanding of so technical an issue, some general observations are relevant to the overall risk management landscape in this critical area.

- While cyber insurers are asking more AI use/exposure-related questions as part of the application process, as things stand at the date of publication of this guide, there are generally no specific AI-related exclusions or restrictions on cyber cover being imposed by insurers, but that could change quickly.

- Cybercriminals are leveraging AI to orchestrate more sophisticated and targeted attacks, presenting novel challenges for everyone including cyber insurers. From AI-driven malware that adapts to evade detection to algorithmic attacks designed to exploit vulnerabilities, companies will need to adapt their cyber policies to encompass these AI-related risks.

- No two cyber policies are the same. Insurers generally try to ensure (as they did with the advent of cloud computing) that the relevant risks are adequately and effectively transferred to the insurance market. Nevertheless, businesses seeking cyber insurance should carefully evaluate policies to ensure they adequately address the AI-driven threats most relevant to them.

- The increasing use of AI also has implications for other classes of insurance beyond cyber, including, for example, Errors & Omissions (E&O) cover. AI systems may themselves make errors or omissions in their decision-making processes, leading to financial losses or harm to third parties. Does the E&O programme (if purchased) cover claims alleging negligence, professional errors, and failure to perform, by the AI system itself as well as by its operators? If the company is the victim of an AI-generated crime, will any commercial crime policy purchased by the company respond, despite the absence of a natural person perpetrator? Finally, does the D&O policy contain any cyber/AI-related restrictions on cover?

12 What additional litigation threats both to the company and to me personally as a director does AI pose?

The nature and scope of the litigation threat posed by AI is broad and, to an extent, dependent on the nature of the company's operations. For example, the EU Artificial Intelligence Act (see answer to question 6 above) when it comes into force will allow companies with AI systems that cause harm or damage in breach of the Act to be subject to fines ranging from €15 million or 3% of annual global turnover to as high as €35 million or 7% of annual global turnover.

Then there is the reputational damage and associated potential for destructive impact on share valuations triggering shareholder litigation against companies (and their directors) implicated in the misuse or alleged misuse of AI – especially where such misuse can be tagged to a breach of existing law or regulation. This was an observable trend in US securities law following the introduction of GDPR, in which plaintiffs (albeit often with the benefit of hindsight) alleged "misrepresentations" as to the extent of the company's compliance with GDPR or SEC reporting requirements by management. Typically in these cases, board members are personally joined into the proceedings. Examples include the Alphabet Google+ data securities class action US lawsuit, in which the parties agreed to settle for $350 million.

Staying with the potential for your personal liability as a director, it is possible that companies may seek to recoup losses (including fines and penalties) suffered as a result of misuse of AI by alleging inadequate supervision of the relevant operational risks. (See answer to question 1.) Such claims could either be brought directly by the company or through a 'derivative' claim, a statutory remedy under the Companies Act in which a shareholder seeks permission of the court to bring the claim against the board, on behalf of the company.

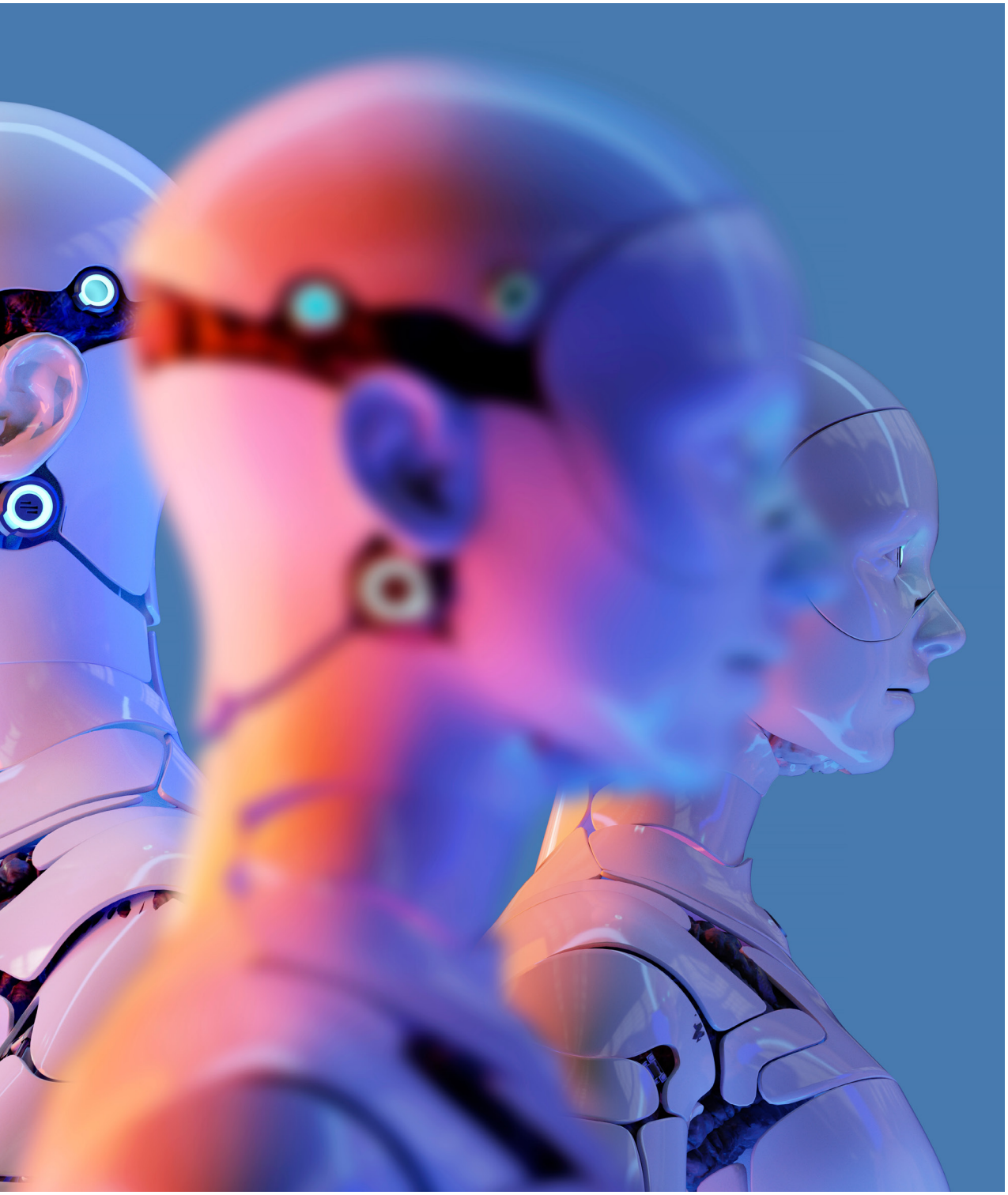
Finally, there are a whole range of potential civil causes of action, ranging from intellectual property violations to defamation, to which a company may be susceptible as a result of deliberate or unwitting use or misuse of AI.

"The rapid proliferation of AI brings with it a potentially massive shift in how society interacts with the digital world. New opportunities and challenges are emerging in unprecedented fashion and speed. AI however, comes with its own risks, including the potential for bias and discrimination, reputational harm, and the potential for widescale redundancy of millions of jobs. Many prominent technologists have voiced their concern at the existential risks to humanity that AI pose. So how do we ensure that AI remains our servant and not our master?

"We need to identify and address these key risks looking at current approaches to regulation and governance of AI internationally in both the public and private sector, how we meet and mitigate these challenges, avoid inadequate or ill-considered regulatory approaches, and protect ourselves from the unforeseen consequences that could flow from unregulated AI development and adoption."

Lord Tim Clement-Jones

Living with the Algorithm: Servant or Master? AI Governance and Policy for the Future (Unicorn Publishing Group, 2024).



03 Glossary

Artificial Intelligence (AI): AI represents computer systems designed to mimic human intelligence, facilitating tasks such as problem-solving, learning, and natural language understanding. AI lacks independent thought and reasoning, relying instead on data input and predefined algorithms created by humans to govern its behaviour.

Other forms of AI include:

Machine Learning (ML): ML is a subset of AI that focuses on developing algorithms capable of learning from data without explicit programming. ML algorithms improve their performance over time as they are exposed to more data, making them valuable for tasks such as predictive analytics, pattern recognition, and recommendation systems.

Deep Learning: Deep learning is a type of ML that utilises artificial neural networks with multiple layers to extract high-level features from raw data. Deep learning algorithms excel in tasks such as image and speech recognition, natural language processing, and autonomous driving.

Reinforcement Learning: Reinforcement learning is an AI technique where an agent learns to make decisions by interacting with an environment and receiving feedback in the form of rewards or penalties. This approach is commonly used in applications such as robotics, gaming, and autonomous systems.

Expert Systems: Expert systems are AI programmes designed to mimic the decision-making process of human experts in a specific domain. These systems use a knowledge base, inference engine, and rule-based reasoning to provide recommendations or solutions to complex problems in fields such as medicine, finance, and engineering.

Natural Language Processing (NLP): NLP is a branch of AI focused on enabling computers to understand, interpret, and generate human language. NLP algorithms are used for tasks such as sentiment analysis, language translation, text summarisation, and chatbots.

Computer Vision: Computer vision involves the development of algorithms and techniques to enable computers to interpret and analyse visual information from images or videos. Applications of computer vision include object detection, facial recognition, autonomous vehicles, and medical image analysis.

Robotics: Robotics combines AI with mechanical engineering to create autonomous or semi-autonomous machines capable of performing tasks in real-world environments. Robotic systems range from industrial robots used in manufacturing to service robots for healthcare, agriculture, and household assistance.

Autonomous Systems: Autonomous systems integrate AI technologies to enable machines or devices to operate independently without human intervention. Examples include autonomous vehicles, drones, smart home systems, and industrial automation systems.

AI Bias often stems from biased training data used to teach AI systems. To uphold accuracy and impartiality, regular reviews of both the training data and AI outputs are essential to identify and address any bias present.

Generative Artificial Intelligence (GenAI): GenAI is a notable subset of AI capable of generating diverse data types, including images, videos, audio, text, and 3D models. By analysing patterns in existing data, GenAI produces novel and distinctive results.

Hallucinations, in the context of AI, refers to instances where the system generates inaccurate results, such as content, resources, or references. This may occur due to incomplete or biased data, reliance on repeated inaccurate information, overly complex task requests, or a failure to generalise properly, posing potential risks for insurers relying on AI-generated outputs.

Large Language Models (LLMs): LLMs are AI variants trained on extensive datasets, primarily utilised for generating human-like text and excelling in tasks such as language translation. In the insurance sector, LLMs can streamline communication processes, improve customer service, and enhance underwriting and claims processing efficiency.

Prompting is a crucial aspect of AI utilisation, involving the input of specific text to guide subsequent outputs. Effective prompting requires expertise to ensure optimal results, enabling insurers to harness the full potential of AI technology for data analysis, decision-making, and customer interaction.

Marlow House
1a Lloyd's Avenue
London
EC3N 3AA
+44 207 680 3088
enquiries@airmic.com
www.airmic.com