Spotlight

CONFIDENT FUTURES

AI Governance and the Board:

Directors' Duties in an Era of Transformation

Gallagher

Key insights

1. Boards of directors have an essential role in driving AI adoption while at the same time facing new and emerging liabilities in this transformational era.

2. Amid calls for a "light touch" approach to AI governance to facilitate innovation, the technology presents legal, ethical and reputational concerns.

3. There is growing legal scrutiny surrounding the use of AI — including allegations of AI washing or misrepresenting AI capabilities — which presents new areas of liability for companies and their senior officers.

4. From a D&O insurance perspective, it's necessary to stress test the scope of coverage and address any gaps before they become issues related to AI risk management.

5. Keeping up with rapid onboarding and evolving regulation while maintaining open communication throughout the organisation requires a thoughtful approach.

Spotlight

Against an accelerating pace of digital adoption, boards face growing pressure to deliver complex AI transformation programs. Leadership has a key role in driving successful change as the workforce adapts, setting the right tone and expanding risk management and compliance frameworks to encompass new and emerging AI governance-related risks.

Striking the right balance between gaining efficiency and driving innovation while upholding ethical and regulatory requirements requires a strategic and thoughtful approach to governance.

While many global leaders are calling for a "light touch" approach to regulating the technology's use — to encourage rapid adoption and innovation — there are concerns linked to the quickly evolving AI phenomenon, as recent AI washing lawsuits illustrate. These issues will only become more pronounced as companies progress on their AI adoption journeys.

"We are seeing an increase in AI-related lawsuits since 2024," says Laura Parris, Executive Director of Management Liability, Gallagher. "Misrepresenting AI capabilities — AI washing — has been the biggest driver so far. But algorithmic bias and discrimination claims are growing quickly, too, as regulators focus on fairness and transparency."

Data privacy breaches related to AI are a big area of concern, especially under laws such as the General Data Protection Regulation (GDPR). Three main risks — misrepresentation, bias and privacy — are active right now and likely to grow.

Spotlight

The 2025 Gallagher "Attitudes to AI Adoption" benchmarking survey revealed a notable jump in AI being viewed as a risk by leaders worldwide, underlining the importance of effective AI risk management strategies. Business leaders say their main concerns are AI errors or "hallucinations" — where the system generates inaccurate results. Other key concerns include data protection and privacy violations (33%) and legal liabilities (31%) related to AI misuse.

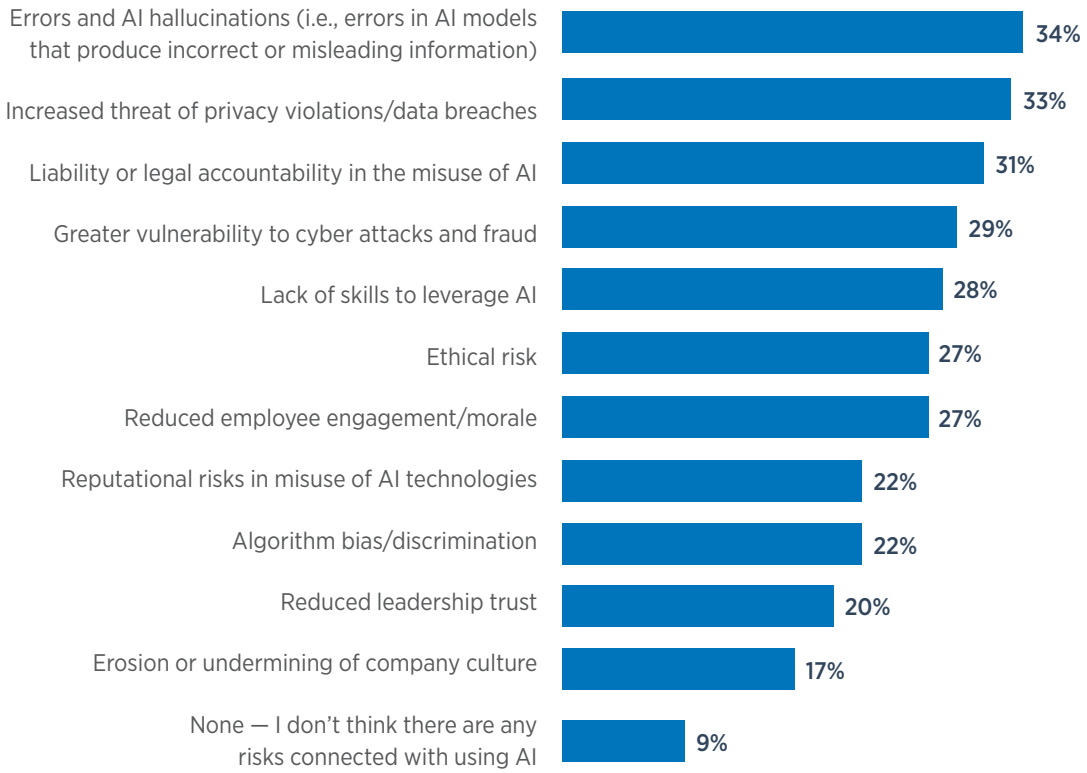
"Just because AI is a relatively new risk doesn't mean that boards are left to tackle this risk from a dead start," notes Priya Huskins, D&O expert at Woodruff Sawyer, a Gallagher company. "Consider how boards that were not necessarily tech savvy had to first learn about and then deal with cyber risk just a decade ago. Today, this exercise is still serious but also entirely commonplace."

"While AI can seem exotic, good boards are well used to considering emerging threats and, where possible, turning these threats into business opportunities. The goal for a board of directors when it comes to risk oversight is less about tackling one specific risk and more about the process a board has in place to ingest new information as it becomes relevant to the business. As much as AI may have some unique elements, there is a real sense in which it is just the latest in a never-ending series of risks boards are charged with handling as fiduciaries for their shareholders."

However, Huskins notes, "This is not to say that AI will fail to have singular challenges. Consider, for example, that in addition to whatever business challenges AI may bring, AI will also make it easier than ever for dissident shareholders to analyse what boards are doing and uncover areas of strategic disagreement."

Across sectors, boards are reassessing existing governance frameworks, identifying gaps in oversight while ensuring that AI-related decisions align with their company's broader values and societal expectations.

Perceived risk with using AI in the business



Source: Gallagher

Senior leadership's role in AI governance, adoption and change management

AI is transforming the workforce by automating some roles, reshaping others and creating new opportunities. And the transformative power of AI can be a catalyst for positive change. It can enrich the workforce by shifting employees toward higher-value work in spaces such as strategy and innovation, while automation handles more routine tasks.

Forty-four percent of business leaders in the Gallagher global survey cite improved problem-solving as a top benefit, while 42% say technology is boosting employee efficiency and productivity.

"Success in digital transformation depends on instilling confidence and securing buy-in across the organisation," says Ben Warren, Managing Director and Head of Digital Transformation and AI, HR and Communications Consulting, Gallagher.

"The key to managing these fears is transparent communication. Organisations need to reassure employees that AI adoption will be a gradual process and that there will be plenty of opportunities for reskilling. It's about creating a culture where employees feel empowered to adapt," he explains.

This is where senior leadership has a clear role to play. Balancing innovation with risk awareness while creating space for experimentation helps teams navigate uncertainty and mitigate potential pitfalls. Involving staff in the process builds trust and shared ownership, which are critical for managing change and minimising resistance-related risks.

"Although AI risk is often assigned to IT or legal departments, it should be business-owned to effectively manage its interconnected nature," according to Aidan Hewitt, Client Partner — Culture Change Consulting, Gallagher. "Senior leadership is responsible for engaging cross-functional AI adoption teams and drawing on the expertise of risk owners across the organisation, including HR, legal, risk management and IT."

"Role modeling and setting out the direction of travel are critical components of AI-related change for leaders to adopt."

> There's an onus on leaders to experiment with AI to gain hands-on experience of how it works in practice and, in turn, role-model mindset and behaviors.

Successful AI adoption involves collaboration across all levels of leadership to shape a transparent and curious culture. And yet, from the perspective of statutory duties, ultimate responsibility — and liability — sits with the board.

Spotlight

Board responsibilities in AI governance and risk oversight

Investment in AI is viewed as a critical competitive lever. But while evolving use cases bring efficiency and opportunity, they also risk exposing organisations to new liability exposures. The boardroom stands at the frontline, where AI-led innovation meets legal, ethical and reputational accountability.

As with any other management, compliance, risk and disclosure topic, boards are striving to better understand how the rise of AI is impacting the company, its people and its obligations, from both a near- and longer-term perspective.

"The board is ultimately responsible for the company's risk exposures and for managing those risk exposures," says Theresa Lewin, National Head of Professional and Financial Risks, Gallagher, Australia. "They are responsible for governance, so they need to be aware of the risk exposures of AI."

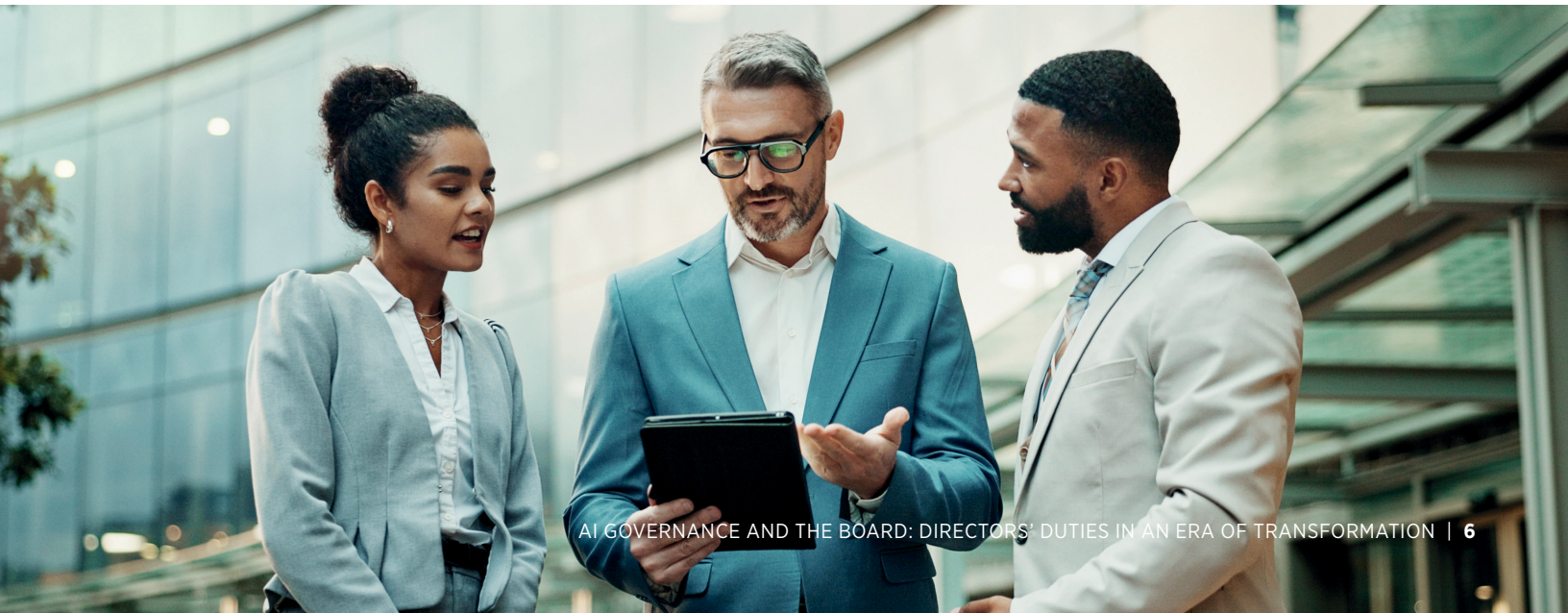
Proactively identifying, assessing and addressing the risks associated with AI adoption is not just the right thing to do; it falls squarely within the remit of directors' duties and responsibilities.

Effective AI governance is built on four essential pillars: strategic alignment, ethical oversight, risk management and operational readiness. Together, these form a governance framework that enables innovation without compromising accountability and aligns with global standards such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework, a guide to help organisations manage AI risks.

AI Governance Framework Pillars

1. **Strategic alignment**
   Ensuring AI platforms and processes are set up to support growth and scalability.
2. **Ethical oversight**
   Responsible AI implementation leverages trust and transparency as guiding principles in the operating and delivery model.
3. **AI risk management**
   Regulatory obligations, compliance and process design to mitigate risks.
4. **Operational readiness**
   Covering AI adequacy, retooling and reskilling to equip leaders for AI today and in the future.

Source: Gallagher



AI risk governance will continue to test such frameworks, highlighted by:

- **Shifts from centralised governance** to distributed/localised risk management
- **Adaptive AI-specific processes** shaped by key stakeholders and underpinned by trust and accountability
- **Dynamic governance,** a shift from static risk registers periodically reviewed by the board and operational leaders to the use of adaptive risk management practices and controls

"To ensure effective governance, the board must have the right level of knowledge about AI," recommends Lewin. "This may involve recruiting individuals with expertise in AI or establishing the appropriate committee, such as audit and risk or risk and compliance, to advise the board to facilitate informed decision-making. The board should use AI responsibly and fully understand the risks of both using and not using AI — the responsibility to fully understand AI and its risks cannot be delegated by the board."

"Directors must also examine the legal and regulatory implications surrounding AI, which include privacy, anti-discrimination and cyber risk," she continues. "They need to stay updated on evolving regulations and should consider potential harm to organisations, such as commercial losses, reputational damage and regulatory sanctions."

"Engaging with management is essential for understanding how AI is being utilised throughout the organisation and overseeing the management and control of associated risks," adds Lewin. "Directors should also be aware of AI's impact on vulnerable and marginalised individuals and explore ways to mitigate these risks."

AI is an accelerant of existing enterprise risks; therefore, boards are expected to integrate AI considerations into their ongoing risk oversight responsibilities.

Six areas where AI may amplify or reshape traditional risk exposures

Risk 1: Intellectual property compliance

As AI systems generate and use content, the risk of infringing intellectual property (IP) rights is a growing concern, particularly in regions with strong copyright laws. Regulatory uncertainty around ownership and liability persists in evolving AI governance frameworks.

Risk 2: Cybersecurity and data breach

Many standard Directors & Officers (D&O) insurance policies exclude cyber-related claims. Issues include:

- **Inadequate cybersecurity:** Breach events caused by poor oversight may invalidate D&O coverage.
- **Liability for data breaches:** Companies can be held responsible for mishandling customer or employee data. Standard policies often exclude these claims.
- **Business losses:** While legal defense may be covered, financial losses or interruptions from cyber attacks are usually excluded.

As AI use grows, clear rules on liability, data privacy, IP and cybersecurity are essential to protect businesses and ensure accountability.

Risk 3: Supply chain and vendor risks

As companies depend more on third-party AI vendors, new supply chain risks emerge, such as bias, automation failures, data breaches and regulatory issues. These may fall outside standard D&O insurance. To avoid liability, companies' coverage needs updates to address third-party AI risks within corporate AI governance.

Spotlight

Risk 4: Employment practices liability

AI's growing use cases within HR raise major legal and ethical challenges for businesses worldwide.

- **Employee monitoring and privacy:** AI-driven surveillance tools must comply with laws such as the US Fair Credit Reporting Act (FCRA) and the EU GDPR.
- **Bias and discrimination:** AI hiring and performance tools can unintentionally reinforce bias. Companies must audit algorithms regularly and ensure training data is fair and diverse.
- **Job automation and worker rights:** AI-driven job displacement is regulated differently worldwide. The EU mandates retraining and severance, where other regions may lack protections. Employers risk legal claims if they fail to meet local labor laws or provide fair compensation.
- **Global data privacy challenges:** These also vary by region. Global companies must navigate local regulations to manage AI's impact on employment practices.

Risk 5: M&A and strategic partnerships

As companies adopt AI, they may acquire or partner with firms using their own AI technologies, presenting attached risks. Directors & Officers can face liability if AI-related issues (e.g., misrepresented capabilities or hidden risks) are not uncovered during the due diligence process.

Risk 6: Shareholder and stakeholder activism

As AI adoption increases, so does scrutiny from shareholders, employees and other stakeholders. Shareholders may challenge the ethical use or risk management of AI, particularly if they believe poor oversight has harmed the company's performance or reputation. Also, AI makes it easier for activist groups and shareholders to monitor board decisions and surface concerns.

As Huskins notes, "Boards may face increasing scrutiny because AI simply makes it easier to analyse what boards are doing and uncover areas of strategic disagreement."

AI governance and managing risk — the NIST Risk Management Framework

The National Institute of Standards and Technology (NIST) AI Risk Management Framework describes four specific functions — govern, map, measure and manage — to help organisations address AI risks.

The "govern" function relates to cultivating and implementing a risk management culture and applies to all stages of an organisation's risk management. It covers:

- Policies, processes, procedures and practices related to the mapping, measuring and managing of AI risks. These must be present, transparent and implemented effectively
- Accountability structures to ensure the appropriate teams are empowered, responsible and trained to deal with the risks. Individuals must be committed to a culture that considers and communicates AI risk
- The prioritisation of workforce inclusion, diversity and accessibility processes in the mapping, measuring and managing of AI risks
- Processes for robust engagement with relevant AI actors
- Policies and procedures to address AI risks and the benefits arising from third-party software and data as well as other supply chain issues

Spotlight

Test cases point to rising scrutiny of board governance

AI-related legal cases are rapidly increasing, with class action filings in the US more than doubling from seven in 2023 to 15 in 2024. They demonstrate an increasing level of legal scrutiny surrounding the use of AI and subsequent growth in liability for organisations and their senior leaders.

Of the 15 AI-related filings in 2024, eight were in the technology sector. The communications and industrial sectors accounted for four and two filings, respectively, with one filing attributed to the consumer non-cyclical sector.[1]

As Gallagher's Lewin states, "We have seen instances of AI washing claims occurring in the US: Two asset managers have faced fines from the US Securities and Exchange Commission (SEC) for overstating or exaggerating their use of AI and its benefits for their stakeholders."

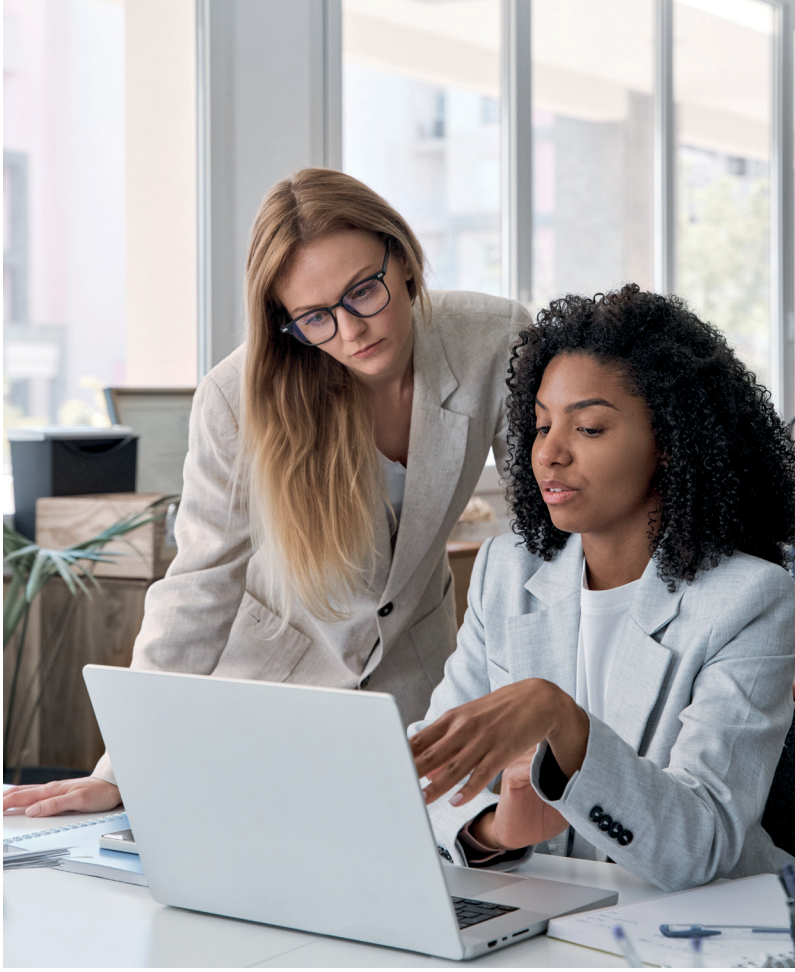
"Additionally, we're starting to see class action lawsuits emerge against companies engaging in AI washing," she continues. "The SEC has been monitoring AI closely for a significant period. Jurisdictions worldwide are being cautious about adopting overly stringent AI regulations, as they aim to avoid stifling innovation. Some regions, however, have taken a more heavy-handed approach than others."

Four litigation categories trending in 2025 include:

- AI washing claims — securities litigation
- AI-generated content — legal challenges and IP infringement
- AI hallucinations — legal sanctions
- Regulatory developments/challenges

AI washing is a relatively new and growing area of concern. While lawsuits to date haven't explicitly referred to the term, legal challenges have been raised over misleading advertising, false claims and overstated capability. This may change as legal determinations and judgments shape the basis of future legal cases and as courts set out clearer legal standards.

[1] "Securities Class Action Filings Increase for Second Consecutive Year in 2024," *Cornerstone Research,* 29 Jan 2025.



Companies and directors also may be exposed to litigation through biased algorithms — such as for screening recruitment candidates — even where these have been accessed via a third party.

"Increased use of AI may expose companies to employment practices liability claims, depending on how hiring algorithms are designed and used," notes Cassandra Shivers, Claims Advocacy Leader, Executive Risk and Cyber, Gallagher.

"There is also potential D&O liability if public claims about AI quality or controls prove inaccurate, possibly leading to fiduciary breaches."

"There are examples in legal contexts where a lawyer or law firm has used AI to generate briefs and insights about case law that simply do not exist," says Shivers. "This can lead to serious consequences, including sanctions against lawyers or firms involved. Therefore, it's crucial to evaluate the information generated by AI to ensure that it is both valid and effective."

Recently, a wave of litigation has emerged around artificial intelligence: companies overstating capabilities, misleading marketing, hallucinated outputs and regulatory challenges. These cases offer a view into how the adoption of AI is colliding with legal action.

Spotlight

Stress testing can help identify gaps in cover

With all the promises and opportunities AI presents, there are also new exposures for both companies and individual Directors & Officers (D&O). These need to be considered as senior officers carry out their duties and responsibilities in relation to AI adoption.

Partnering with your broker

From a D&O insurance perspective, it's important for senior leaders to explore various scenarios — with the support of their broker — to determine how coverage might respond and where there may be gaps in risk management or cover.

As AI evolves, legal challenges will continue to increase, setting precedents and revealing how D&O policy wording responds when tested. For the insurance industry, this also will test underwriting appetite and determine whether "silent AI" is an issue that needs to be tackled in a similar way to "silent cyber." Claims disputes could drive a more pronounced shift with the market explicitly excluding AI-related claims or offering affirmative cover.

As Kevin LaCroix anticipates, "We are likely to see increasing amounts of corporate and securities litigation having to do with AI-related risks — and not just the failure to disclose AI-related risks but also allegations relating to AI misuse or the faulty deployment of AI tools, or the failure to adapt to or address the competitive urgency of AI development."

"Litigants will also seek to hold corporate managers and their employers accountable for the failure to avoid, in the deployment of AI tools, discrimination, privacy and IP violations, or consumer fraud," he notes.

Indeed, the scope of D&O liability insurance has already begun to evolve, with insurers starting to offer more specialised coverage that reflects:

- Risks tied to misleading AI claims and the legal liabilities that can arise from AI washing
- Coverage for data breaches, cyber attacks and privacy violations resulting from AI-driven systems
- Protection for risks tied to AI ethics, including algorithmic bias and unethical practices
- Adaptation to evolving regulations on AI; environmental, social and governance (ESG) concerns; and the responsibility of Directors & Officers in overseeing AI systems

Preparing for an evolving landscape

In the meantime, companies should continue to test how their current D&O policy wordings would respond to AI-related liabilities while keeping abreast of legal and regulatory developments. Partnering with underwriters and brokers can help stress test the scope of coverage and address any gaps before they become a problem.

"With no clear rules or safe harbors for AI development, boards remain ultimately accountable," says Steve Bear, Executive Director of Professional and Financial Risks, Gallagher. "Given the breadth of AI application within a business, involving D&O specialists can help boards better understand the full spectrum of risks across all stakeholders."

"While D&O insurance offers some protection, many AI-related risks fall outside the scope of today's standard policy wording and must be addressed through strong governance frameworks. This will continue to be an evolving risk management landscape."

Spotlight

Five critical considerations for senior leadership

1. Conduct regular risk assessments to identify bias, privacy breaches and system failures. High-risk AI needs ongoing audits for fairness and accuracy, with quick responses to issues.
2. Data security must focus on encryption, access control and vendor oversight. Companies should track AI performance and risks in real time using strong metrics and reporting.
3. Promote ethical AI through training and collaboration, clear accountability and transparency.
4. Document AI systems, applying human oversight to sensitise decisions, using independent audits to stress test governance frameworks.
5. Engage stakeholders, build trust and help navigate complex and evolving regulations. Central oversight combined with decentralised flexibility facilitates responsive and effective compliance and risk management.

AJG.com/au **The Gallagher Way.** Since 1927.