

AI liability:

The risk sitting between cyber, PI and D&O

Artificial intelligence is creating new opportunities for businesses, but it is also creating a new category of risk that doesn't sit neatly within a single insurance policy.

An AI-related incident could potentially trigger cyber, professional indemnity, privacy, regulatory or Directors' and Officers' (D&O) considerations, depending on the circumstances.

As organisations increasingly embed AI into operations, decision-making and customer interactions, understanding where accountability sits is becoming just as important as understanding the technology itself. For boards and leadership teams, the challenge is particularly significant because while AI may influence decisions, accountability for those decisions remains firmly with the organisation and its leaders.

While AI can generate recommendations, content and insights, responsibility for the outcome still rests with the organisation using it.

AI doesn't remove accountability

If an AI-generated recommendation is inaccurate, confidential information is exposed, or a customer relies on incorrect advice, accountability still sits with the organisation.

AI can generate content, provide recommendations and identify patterns, but it cannot accept responsibility for the consequences of a poor decision, governance failure or compliance breach.

- An AI-generated report contains incorrect information that influences a business decision.
- A professional relies on AI-generated advice that later proves inaccurate.
- Customer information is entered into an inappropriate AI platform.
- AI-generated content is published externally without proper review.
- Automated processes create unintended regulatory or compliance issues.

In each case, the technology may have played a role, but responsibility remains with the business.

This is why AI is increasingly becoming a governance issue rather than simply a technology issue.

A risk that crosses multiple areas

AI can create exposure across several areas simultaneously.

Professional liability

Businesses providing advice, designs, recommendations or professional services need confidence that AI-assisted outputs are accurate, appropriate and properly reviewed.

Cyber risk

Many AI tools rely on significant volumes of data. Inappropriate use, poor access controls, or the sharing of sensitive information can create cyber-related exposures.

Privacy and compliance

Businesses must carefully consider how customer, employee and confidential information is managed when using AI platforms, particularly as regulatory expectations continue to evolve.

Governance risk

Boards and leadership teams are increasingly expected to understand how AI is being used within their organisations and what controls are in place to manage associated risks.

In the same way cyber security evolved from an IT issue to a board-level issue, AI is rapidly becoming a governance issue that requires active leadership attention.

Rather than creating an entirely new category of risk, AI often amplifies existing risks and exposes gaps in governance, oversight, and decision-making.



The governance gap

Many organisations have adopted AI more quickly than they have developed the policies and frameworks required to manage it.

In some businesses, employees are already using AI tools every day with little guidance around:

- Which tools can be used
- What information can be entered
- How outputs should be reviewed
- When human oversight is required
- Who remains accountable for decisions

The organisations most likely to benefit from AI over the long term are not necessarily those with the most advanced tools. They are the organisations that establish clear expectations, responsibilities and controls around how those tools are used.

Why directors should be paying attention

AI is no longer simply a technology discussion.

For many organisations, it is becoming a strategic, governance and reputational issue.

Boards do not need to become AI experts, but they do need confidence that appropriate policies, oversight and controls exist around how AI is being used within the business.

Questions directors may wish to consider include:

- Do we understand where AI is being used across the organisation?
- Are there clear policies governing its use?
- How are AI-generated outputs being reviewed and monitored?
- Could AI-related errors, privacy breaches or poor decision-making create financial, regulatory or reputational consequences?
- Are we comfortable that governance arrangements are keeping pace with adoption?

As AI becomes more embedded within business operations, stakeholders, regulators and investors are likely to expect stronger oversight and accountability from leadership teams.

What about insurance?

As AI-related exposures continue to evolve, organisations should avoid assuming their existing insurance arrangements automatically respond to every scenario.

Depending on the circumstances, AI-related incidents could potentially involve:

- Cyber insurance
- Professional indemnity insurance
- Directors' and Officers' (D&O) insurance
- Statutory liability insurance

The response will depend on the circumstances, policy wording and nature of the loss.

This makes it important for businesses to understand how AI is being used across the organisation and whether emerging exposures have been considered as part of broader risk management and insurance discussions.

Looking ahead

For most businesses, the question is no longer whether AI will play a role in the organisation. The challenge is how to embrace the opportunities while maintaining appropriate governance, oversight and accountability.

As AI adoption accelerates, boards and leadership teams may increasingly be judged not only on how effectively they use AI, but on whether they have exercised appropriate oversight of its use.

Because while AI may help businesses make decisions faster, it does not change who is ultimately responsible for the outcome.

How Rothbury can help



AI-related risks rarely sit within a single area of responsibility. They can affect cyber security, professional liability, governance and compliance simultaneously.

Rothbury can help you understand how emerging technologies may impact your organisation's risk profile and whether your insurance programme remains aligned with the way your business operates. If your organisation is adopting AI tools or exploring new uses for AI, talk to your Rothbury broker.