



Underinsurance: Causes and Consequences

Robust insurance cover is a key element of effective risk management. A single uninsured event can lead to severe financial disruption, halt operations and threaten long-term viability. Yet, despite these risks, underinsurance remains a frequently overlooked vulnerability. Whether due to outdated valuations or budget decisions, carrying insufficient insurance cover can leave organisations exposed. Business owners need to be aware of the causes and consequences of underinsurance and take steps to address it.

Several factors contribute to underinsurance among organisations, including the following:

- **Outdated property valuations**—Business owners may overlook the need to routinely update the value of their buildings, equipment or inventory, resulting in cover that doesn't accurately reflect current replacement costs.
- **Business growth without policy changes**—Business owners may add staff, change locations or increase assets without adjusting their insurance cover, creating new exposures and increasing the risk of uncovered losses.
- **Misunderstanding policy terms**—Business owners may misinterpret complicated insurance policy language, leading to false assumptions about what is covered, when cover applies and how indemnity limits are structured.
- **Focusing solely on premiums**—Business owners may focus on minimising insurance costs without considering the implications of reduced cover limits, broader exclusions or how higher excesses may compromise cover.
- **Neglecting emerging risks**—Business owners may fail to account for new threats such as cyber-attacks, climate-related events or supply chain disruptions that may not be covered under standard policies.

The financial and operational consequences of underinsurance can be significant and include the following:

- **Partial or denied claims**—If cover limits are too low or exclusions apply, insurance may not fully cover the cost of losses. This can leave the organisation responsible for the remaining expenses.
- **Lengthy downtime**—Without adequate cover, such as business interruption insurance, an organisation may struggle to meet ongoing expenses after a loss event, increasing the risk of prolonged closure or shutdown.
- **Regulatory and legal exposure**—Insufficient liability insurance can leave organisations vulnerable to legal claims and regulatory penalties, particularly in highly regulated industries.
- **Reputational damage**—Delays in service or failure to meet obligations due to uninsured losses can erode client trust and damage long-term relationships.

Underinsurance Prevention Strategies

To minimise underinsurance risks, business owners should regularly reassess their insurance cover, particularly after operational changes (eg expansion, new hires or equipment upgrades). Obtaining professional appraisals of property and assets is also crucial, especially during periods of inflation or supply-chain volatility.

Additionally, businesses should evaluate whether their existing policies account for emerging risks, including cyber-threats, climate-related events or evolving liability exposures. Working with a knowledgeable broker can help uncover insurance gaps and ensure cover aligns with the organisation's current operations.

Contact us today for further risk management guidance and insurance solutions.

Balancing AI Risks and Benefits

Artificial intelligence (AI) is rapidly changing how organisations function, offering powerful tools to enhance efficiency, strengthen security and improve customer engagement. To adopt AI effectively, business leaders must understand both its strategic advantages and potential pitfalls to make informed decisions that align with long-term objectives.

AI offers a range of practical applications that can help organisations operate more strategically, securely and efficiently, including:

- **Resolving problems before they happen**—AI-powered tools assist organisations with anticipating and addressing issues early. For example, route optimisation software can actively adapt delivery plans based on traffic, weather or vehicle capacity. Similarly, inventory planning tools can forecast demand to prevent shortages.
- **Automating repetitive tasks**—AI programs can streamline operations by performing repetitive tasks like generating invoices, freeing up time for high-value activities.
- **Improving security**—AI can detect cyber-threats, identify vulnerabilities and respond to suspicious activity faster than manual systems, helping organisations stop cyber-attacks before they escalate.
- **Analysing data**—AI analytic tools can efficiently examine large volumes of business data to spot trends, inefficiencies and growth opportunities, helping organisations to make informed decisions or identify new income streams.
- **Generating and managing content**—AI can create product descriptions, draft and schedule social media posts, and write responses to online reviews to support marketing and brand engagement initiatives.
- **Enhancing customer service**—AI-powered chatbots can respond to common questions, help

with orders and provide 24/7 support, improving the customer experience.

However, organisations should be aware of the following AI limitations:

- **AI depends on data that is potentially flawed or outdated.** AI systems are only as strong as the data they use. Inaccurate, biased or incomplete data can lead to incorrect decisions, poor recommendations and unreliable insights.
- **AI can weaken cyber-security.** AI integration can expand an organisation's attack surface and create new entry points for cyber-attacks. Hackers may use generative AI tools to craft phishing emails, deepfakes or automated threats, increasing the risk of breaches.
- **AI can raise ethical and privacy concerns.** Using AI to collect, store or analyse personal or sensitive data without clear consent and proper safeguards can violate privacy laws, reinforce biases and damage customer trust.
- **AI can outpace internal capabilities.** Limited in-house expertise and insufficient resources can hinder effective AI implementation and increase the risk of mismanagement. Overreliance on AI can lessen human oversight and lead to unchecked decisions, missed errors and reduced accountability in complex situations.

Using AI responsibly

Organisations can help mitigate operational, legal and reputational risks by establishing clear governance frameworks, designating AI oversight accountability and investing in staff training and education. Organisations should also review their insurance policies (eg cyber insurance, commercial crime insurance and professional liability insurance) to ensure adequate cover for AI-related exposures.

Contact us today for additional risk mitigation resources.