Gen AI Risks for Businesses: Exploring the role for insurance

Research summary | October 2025

Ruo (Alex) Jia, Director Digital Technologies, Geneva Association
Associate Professor of Insurance, Peking University

Contributing authors:
Martin Eling, Director of the Institute of Insurance Economics and Professor of Insurance Management, University of St. Gallen
Tianyang Wang, Professor of Finance, Colorado State University

Generative AI (Gen AI) refers to advanced AI systems capable of producing original content (text, images, code, audio, etc.) in response to user prompts. Since late 2022, Gen AI adoption has surged across industries, with tools like OpenAI's ChatGPT achieving unprecedented uptake. Businesses are embedding Gen AI into products and internal processes to drive innovation and efficiency. However, these capabilities introduce novel risks and amplify existing risks associated with traditional AI. Gen AI models can be unpredictable – they sometimes 'hallucinate' (confidently output false or misleading information) or inadvertently replicate copyrighted content. Such behaviour leads to failures with few historical precedents and amplifies existing concerns like bias, errors, and security vulnerabilities. In short, Gen AI offers immense benefits but also a new spectrum of risks for businesses to manage.

Gen-AI-related business risks can be classified into seven categories (Table 1). On the product side, a business using Gen AI tools developed by tech providers may suffer financial harm, creating potential liability for the providers. On the operational side, firms that deploy Gen AI to steer their businesses face risks like incorrect/biased decision-making, operational inefficiencies, and financial losses. Additionally, Gen AI systems may be more susceptible to cyberattacks, i.e. cybersecurity risks stemming from vulnerabilities in Gen AI systems.

TABLE 1: GEN-AI-INDUCED RISKS

	Risk category	Examples
First-party operational risk	Operational	Algorithmic errors; loss of stability; unreliability
		Black-box issues Malicious attacks
	Cybersecurity & privacy	AI-driven cyberattacks; data-privacy violations
	Reputational & market	Loss of customer trust; compromised brand image
		Dependency; competitive risk
	Workforce challenges	Job displacement
		AI skill requirements
First-party operational risk & third-party product risk	Regulatory & compliance	Evolving AI regulations
		Increased accountability & liability
	Bias & ethical concerns	Discrimination & bias
		Ethical decision-making
	ESG	Environmental- & energy-related risks

Source: Geneva Association

Demand for Gen-AI-related insurance: A business customer survey

To evaluate risk awareness and insurance demand among businesses that use Gen AI, the Geneva Association conducted a survey of 600 corporate insurance decision-makers across the world's six largest insurance markets (China, France, Germany, Japan, the UK, and the US). The findings reveal widespread Gen AI adoption, though perceived usefulness varies by region – it is highest in the US and China and more restrained in Japan, France, and Germany – reflecting differences in digital maturity and organisational culture.

Key implementation challenges for Gen AI include talent shortages and poor data quality/integration, each cited as major hurdles by roughly one third of firms. In Germany and France, another top barrier is internal resistance to Gen AI (scepticism among employees or customers). Businesses in the US and Asia report greater openness but struggle to find enough qualified experts to deploy and govern Gen AI.

Many businesses have already experienced Gen AI issues or failures, reinforcing their risk awareness. For example, a significant portion of respondents report inaccurate or misleading Gen AI outputs or difficulties integrating Gen AI into existing systems. This underscores the need for robust validation of Gen AI results and careful change management when introducing Gen AI into operations.

When asked about top concerns related to Gen AI, companies most frequently cite cybersecurity risks. Over half of respondents worry about Gen AI increasing their vulnerability to hacking, data breaches, or malicious AI-generated attacks. Third-party liability – the risk that Gen AI systems' mistakes could harm customers or partners, leading to claims – ranks second. Operational disruption comes third, reflecting the fear of Gen AI outages or errors interrupting business continuity. Notably, reputational damage ranks lower, indicating that firms are currently focusing on tangible financial and legal risks over more intangible impacts to their brand.

Aligned with these concerns, there is clear market demand for related coverage. More than 90% of surveyed businesses believe they need insurance to protect against AI-related risks, and over two thirds are willing to pay at least 10% more in premiums for such coverage. Demand is strongest among medium-to-large enterprises and sectors like technology and finance. Geographically, interest mirrors adoption: respondents in the US and China (the two frontrunners in Gen AI implementation) express the greatest demand for AI risk coverage, whereas those in Japan, Germany, and France are more cautious. The UK falls somewhere in between.

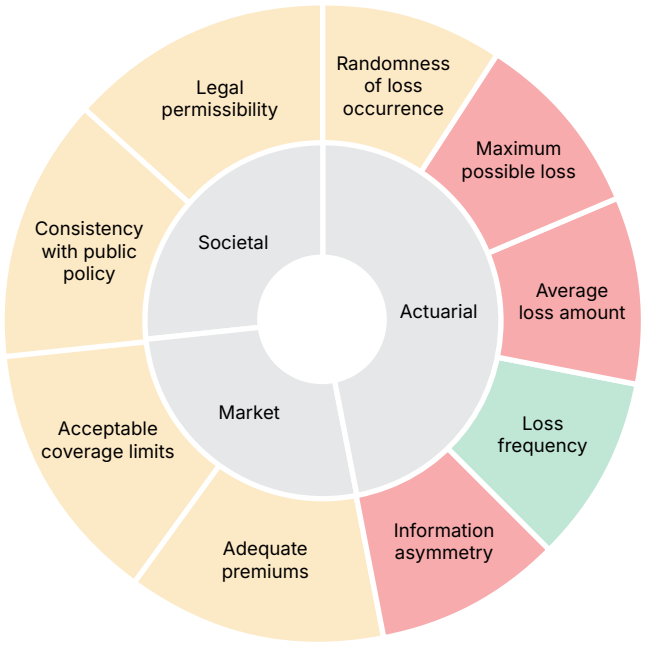
The survey also hints at adverse selection dynamics. Firms that use Gen AI extensively, or those that have already encountered serious AI-related incidents tend to report higher interest in insurance than others.

Insurability challenges and market responses

Gen AI challenges Berliner's classical insurability criteria in several ways, but excessive maximum possible losses, large average loss amounts, and information asymmetries stand out (Figure 1).[1]

1 Berliner 1982.

FIGURE 1: INSURABILITY OF GEN-AI-RELATED RISKS



● Minimal challenges to insurability ● Some challenges to insurability ● Violation of insurability under traditional insurance models

Source: Geneva Association

Despite these headwinds, insurers are starting to respond to and innovate in covering Gen AI risks. Early market responses include:

- **Extending existing policies.** Many insurers are augmenting traditional cover, like cyber insurance and professional liability (E&O), to explicitly include Gen-AI-related perils. For instance, cyber policies may now encompass AI-driven cyberattacks or data leaks, and E&O policies might cover errors from AI-generated content. These extensions are often provided via endorsements and typically come with sublimits or conditions to control exposure.
- **Underwriting adjustments.** Insurers are experimenting with new underwriting strategies. Some are using parametric triggers (paying a preset amount when a specific AI failure event occurs) to simplify claims in an uncertain environment. Others are tightening underwriting standards by scrutinising insureds' AI systems and governance practices (akin to a technical audit) before granting coverage. This helps mitigate information asymmetry.
- **Standalone AI insurance products.** A few carriers have piloted dedicated AI insurance policies that bundle multiple AI risk coverages. For example, an insurer might offer a policy to cover an AI developer's liability for algorithmic errors and IP infringement by AI outputs in one package. These products are still nascent and many insurers are proceeding cautiously, but they indicate movement toward bespoke AI coverage solutions. It remains to be seen whether such standalone policies will gain traction or if Gen AI risks will be mostly handled through modifications of existing insurance lines.

Insurers are extending coverage where they can, but often with careful limitations, higher premiums, and a focus on data-gathering. This mirrors the progression of other emerging risks (like cyber a couple of decades ago).

Conclusion and recommendations

To effectively address Gen AI risks, insurers should consider the following:

- **Act proactively and learn by doing.** Insurers need to define Gen AI risk boundaries and start piloting coverage now, rather than waiting for perfect data. This means introducing controlled policy extensions or trial products for AI risks and using these to gather experience. By starting small (as with cyber insurance) and iterating, underwriters can learn about loss patterns and client needs in real time. Early engagement will allow insurers to scale up coverage intelligently as the Gen AI risk landscape matures.

- **Collaborate on risk assessment and governance.** Insurers cannot address Gen AI risks alone. They should work with AI developers, clients, and regulators to establish governance standards covering bias testing, output validation, data safeguards, and accountability. Shared standards and industry-wide incident data will reduce uncertainty, clarify liability, and improve insurability.

- **Promote risk mitigation and preparedness.** Insurance must be paired with strong AI risk management. Insurers should require safeguards such as human oversight, bias checks, cybersecurity controls, and contingency plans. They can also provide value-added services like AI risk audits. Combining prevention with tailored coverage will help build resilience, ensuring firms benefit from Gen AI while controlling their exposures.

Insurance for Gen AI risks will evolve in the coming years. Insurers that step up now – carefully but decisively – will not only tap into growing demand but also shape how society manages the risks of this transformative technology. By staying adaptable, investing in knowledge, and working collaboratively, the insurance industry can help ensure that Gen AI's benefits are realised safely, with robust risk-transfer mechanisms to support its development.

References

Berliner, B. 1992. *Limits of Insurability of Risks*. Prentice Hall.