

研究摘要

企业面临的生成式人工智能风险： 保险的应对之道

贾若(Alex) Jia, 日内瓦协会数字技术研究总监、合作专家; 北京大学经济学院保险学长聘副教授
参与作者:

Martin Eling, 圣加仑大学保险经济学研究所所长、保险管理学讲席教授

王天阳, 科罗拉多州立大学金融学教授

生成式人工智能 (Generative AI, 简称 Gen AI) 指的是能够根据用户提示生成原创内容 (文本、图像、代码、音频等) 的先进人工智能系统。2022 年底以来, 以 OpenAI 的 ChatGPT 为代表的 Gen AI 工具在各行各业获得了前所未有的广泛使用。企业正在将 Gen AI 融入产品和内部流程, 以推动创新和提升效率。然而, 这些应用也带来了全新的风险, 并放大了与传统人工智能相关的既有风险。Gen AI 模型具有不可预测性——它们有时会出现“幻觉”(即自信地输出虚假或误导性信息), 或无意间复制受版权保护的内容。这类行为导致了史无前例的担忧, 同时也加剧了现有的问题, 如歧视

性偏见、错误和安全漏洞。简而言之, Gen AI 为企业带来巨大收益的同时, 也引入了全新且更广泛的风险谱系, 亟待加强风险管理。

与 Gen AI 相关的企业风险可分为七类(见表 1)。在产品层面, 使用由科技公司提供的 Gen AI 工具的企业可能因各种与 Gen AI 相关的原因遭受财务损失, 从而引发对这些工具提供方的潜在责任。在运营层面, 将 Gen AI 应用于业务决策的企业可能面临错误或有偏见的决策、运营低效以及财务损失等风险。此外, Gen AI 系统可能更容易受到网络攻击, 从而导致业务中断和财务损失, 即源自 Gen AI 系统漏洞的网络安全风险。

表 1：生成式人工智能引发的风险

	风险类别	示例
第一方运营风险	运营风险	算法错误；稳定性和可靠性问题
		黑箱问题
		恶意攻击
	网络安全与隐私	AI 驱动的网络攻击
		数据隐私泄露
第一方运营风险与第三方产品风险	声誉与市场风险	客户信任流失；品牌形象受损
	员工团队挑战	依赖性过高；竞争风险
		岗位替代
	监管与合规风险	对 AI 技能的需求
		不断变化的 AI 监管
		更严格的责任与问责
	偏见与伦理问题	歧视与偏见
	环境、社会与治理(ESG)	合乎伦理的决策
		环境与能源相关风险

来源：日内瓦协会

对生成式人工智能相关保险的需求：企业保险客户调查

为了评估企业在使用生成式人工智能(Gen AI)时的风险认知和保险需求,日内瓦协会对全球六大保险市场(德国、法国、美国、日本、英国、中国)的 600 位参与企业保险决策的人士进行了调查。结果显示,Gen AI 的使用已相当普及,但其被感知的效用因地区而异——在美国和中国最高,而在日本、法国和德国则较为保守——反映出不同国家在数字成熟度和组织文化方面的差异。

在 Gen AI 的落地过程中,主要挑战包括人才短缺、数据质量和数据整合不足,大约三分之一的企业将上述挑战视为重大障碍。在德国和法国,另一个主要障碍是对 Gen AI 的抵触情绪(员工或客户的怀疑态度)。相比之下,美国和亚洲的企业表现出更大的开放性,但难以找到足够的专家和技术人员来部署和治理 Gen AI。

许多企业已经经历过 Gen AI 带来的问题或失败,这进一步强化了它们的风险意识。例如,相当一部分受访者报告称曾遇到 Gen AI 输出不准确或误导性结果,或在将 Gen AI 融入现有 IT 系统时遭遇困难。这凸显了在将 Gen AI 引入运营时,必须对其结果进行稳健验证并做好变革管理。

在被问及与 Gen AI 相关的首要担忧时,企业最常提及的是网络安全风险。超过一半的受访者担心 Gen AI 会增加其遭受黑客攻击、数据泄露或恶意 AI 生成攻击的脆弱性。排在第二的是第三方法律责任——即 Gen AI 系统的错误可能伤害客户或合作伙伴,进而引发索赔。运营中断位列第三,反映了企业对 Gen AI 故障或错误导致业务连续性中断的担忧。声誉损害排名较低,表明目前企业更关注财务和法律等有形风险,而不是对品牌的无形冲击。

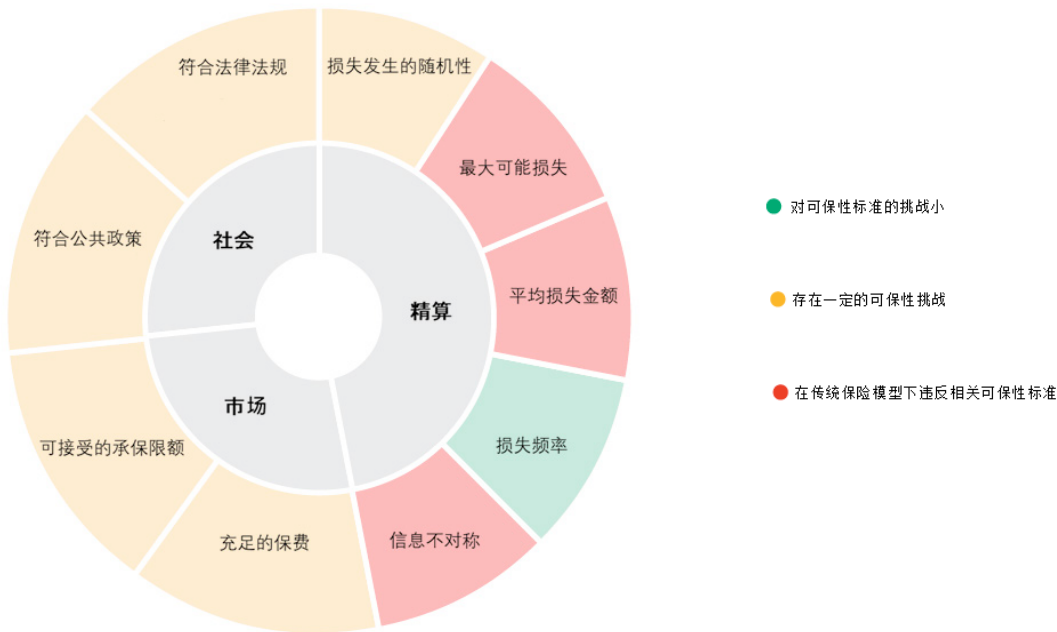
与这些担忧相一致,市场上对相关保险的需求十分明确。超过 90%的受访企业认为有必要通过保险来管理 AI 相关风险,其中超过三分之二愿意为此支付至少 10% 的额外保费。保险需求在中大型企业以及科技、金融等行业最为强烈。从地区分布看,保险需求与 Gen AI 应用程度相关: 美国和中国(Gen AI 应用最领先的两个市场)的受访者表达了最强烈的保险需求,而日本、德国和法国的企业则相对谨慎,英国居于中间水平。

调查还暗示出逆向选择的倾向。那些对 Gen AI 使用程度极高,或已经遭遇过严重 AI 损失事件的企业,比其他企业表现出更高的保险需求。

可保性挑战与市场回应

Gen AI 在多个方面对 Berliner 的经典可保性标准提出挑战,其中最突出的问题包括: 潜在最大损失过大、平均损失金额较高以及信息不对称(见图 1)。¹

图 1：生成式人工智能相关风险的可保性



来源：日内瓦协会

尽管面临这些阻力,保险公司已经开始针对 Gen AI 风险进行响应和创新。早期的市场反应包括:

- **扩展现有保单。**许多保险公司正在扩展传统保障范围,如网络保险和职业责任险(E&O),明确纳入与 Gen AI 相关的风险。例如,网络保险现在可能涵盖 AI 驱动的网络攻击或数据泄露,而 E&O 保单可能涵盖 AI 生成内容带来的错误。这类扩展通常通过附加条款提供,并常常附带子限额或更严格条件以控制风险敞口。

- **承保策略调整。**保险公司正在尝试新的承保策略。一些公司使用参数触发机制(即在特定的 AI 故障事件发生时支付预设金额),以在不确定的环境中简化管理。另一些公司则通过在承保前审查被保险企业的 AI 系统和管理实践(类似技术审计)来收紧承保标准,从而缓解信息不对称问题。

¹ Berliner 1982.

- **独立的 AI 保险产品。**少数保险公司已经试点推出专门的 AI 保险保单,将多种 AI 风险保障打包在一起。例如,某些保单可能涵盖 AI 开发商因算法错误和 AI 输出的知识产权侵权所承担的责任。这些产品仍处于初期阶段,许多保险公司态度谨慎,但它们显示了向定制化 AI 保障解决方案发展的趋势。

目前尚难以确定 Gen AI 风险将主要通过独立保单还是完善现有保单来承保。

保险公司正在尽可能扩展 Gen AI 风险保障,但通常附带严格限制、更高保费,并注重数据收集。这与其他新兴风险的保险(如过去十几年的网络安全保险)的演进路径类似。

结论与建议

为了有效应对 Gen AI 风险,保险公司应考虑以下几点:

- **积极行动,以实践积累经验。**保险公司需要界定 Gen AI 风险边界,并立即开始提供试点保障,而不是等待完美的数据。这意味着推出受控的保单扩展或试点性 AI 保险产品,并通过这些产品积累经验。通过小规模起步(如当年的网络安全保险)并不断迭代,承保人可以实时了解损失模式和客户需求。早期介入将使保险公司能够在 Gen AI 风险格局逐步成熟的过程中实现有序增长。
- **在风险评估与治理方面加强跨行业合作。**保险公司无法单独应对 Gen AI 风险。他们应与 AI 开发商、客户和监管机构合作,建立涵盖偏误测试、结果验证、数据保护和问责机制的治理标准。共享标准和全行业事故数据将有助于降低不确定性、明确责任并提升可保性。

- **推动防灾减损。**保险必须与完善的 AI 风险管理相结合。保险公司应要求企业采取保障措施,如人工监督、偏误检测、网络安全控制和应急预案。同时,保险人也可以提供增值服务,例如 AI 风险审计。通过将防灾减损与定制化保障结合起来,可以增强企业的韧性,确保企业在受益于 Gen AI 的同时控制风险敞口。

未来几年,Gen AI 保险将不断发展。那些现在便谨慎而果断行动的保险公司,不仅能满足日益增长的市场需求,还将塑造社会应对这一变革性技术风险的方式。通过保持灵活、加大风险技术投资并加强合作,保险业可以帮助确保 Gen AI 的优势得以安全释放,并提供稳健的风险转移机制来支持其发展。

参考资料

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