

风险复杂性



[illegible]

高科技资产引发聚合担忧

伤亡风险地震变化

在日益复杂的背景下保障科技高管

应对不断变化的险种和保险环境

其他热门风险领域

前言

科技行业正面临日益复杂的风险格局，这要求对风险进行细致的理解和创新的管理方法。Marsh 2025年科技风险报告的主题——*风险复杂性*——反映了我们所面临当今挑战的多方面性质。在一个风险以前所未有的速度出现、交织和变得更加复杂的世界里，风险管理人员必须适应一个新的现实。

持续的全球经济波动，加上地缘政治紧张局势和供应链中断，加剧了技术行业在成本管理和战略敏捷性方面的需求。此外，人工智能（AI）和其他新兴技术的快速发展既带来了机遇也带来了脆弱性，进一步复杂化了风险格局。监管合规也变得更加错综复杂，不断变化的标准和期望要求组织比以往任何时候都要更加积极主动和适应性。

在这种情况下，有效的风险管理不仅仅是一种必要性；它是组织韧性和利益相关者信任的基石。预见、理解和缓解风险的能力对于应对当今市场的复杂性至关重要。

本报告基于客户分享的调查反馈，概述了科技行业加速面临的挑战与机遇。我们的研究发现，各相关行业正处于关键节点，积极寻求创新解决方案以应对威胁稳定与增长的多元风险。

在您探索这份年度报告的过程中，我鼓励您反思所提出的见解，并考虑如何利用这些见解来增强您的风险管理策略，并与主要利益相关者建立信任。

让我们一起将这些复杂性转化为可持续增长和面对不确定性的韧性机遇。



汤姆·奎格利
传播、媒体与科技业务领袖

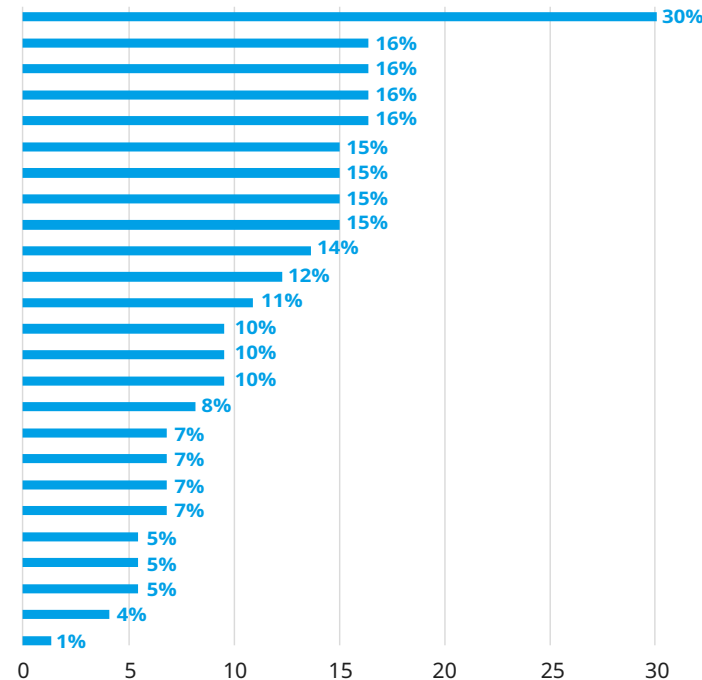
适应不断变化的风险格局

在一个由快速技术进步定义的时代，科技公司的风险格局正以前所未有的速度变化。组织必须调整其风险管理策略和保险计划，以应对来自互联系统、新兴技术和不断变化的监管环境的复杂性和不确定性。

在日益分裂的全球格局背景下，这场转型正如今年世界经济论坛所阐述的那样进行，得到了Marsh McLennan和其他合作伙伴的战略支持。不断加剧的地缘政治和地缘经济紧张局势可能会显著影响组织的决策和增长战略。科技公司也正应对相互关联的挑战，从自然灾害破坏财产和扰乱供应链，到与产品故障相关的潜在责任，再到核陪审团裁决日益普遍。此外，技术创新的速度导致了构成科技公司及其提供的产品和服务的定义的扩展（见图1）。这为

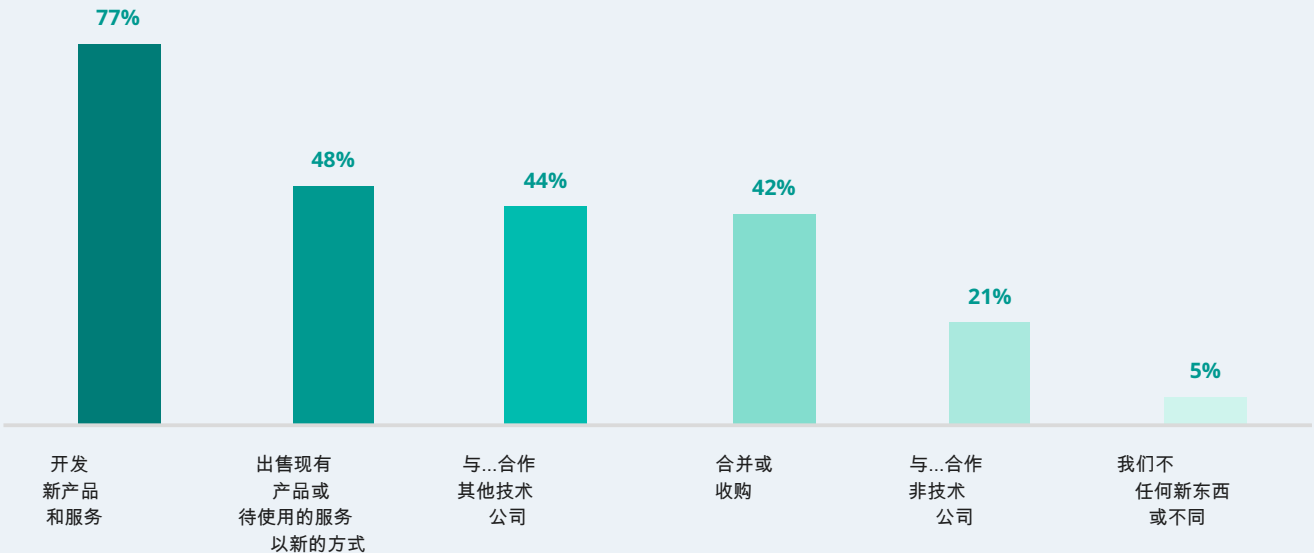
01| 科技公司提供的产品和服务

企业软件 半导体和电子元件 系统集成和定制IT开发 消费应用和软件 通信基础设施 高级汽车/自动驾驶技术 零部件和集成硬件解决方案 托管和云计算服务 通信服务（有线、无线、互联网或卫星） 业务流程外包 金融科技或金融技术 数据和事务处理 其他 数据中心和服务 媒体内容创作 个人电子产品 电子商务



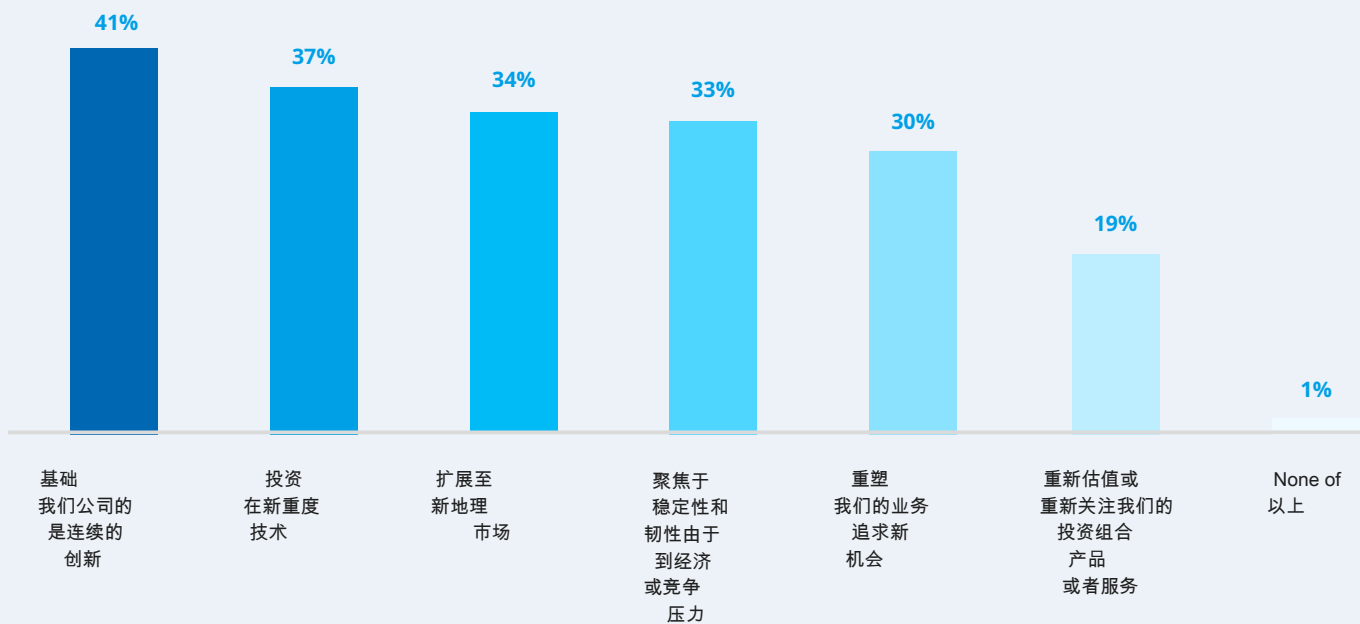
技术公司在理解和管理其非战略风险方面的作用

02| 大多数科技公司继续开发新产品和服务



然而，这一充满挑战的风险格局并未阻止科技公司开发明日之产品。事实上，今年调查的大部分受访者表示他们正在开发新产品和服务（见图2）。

03|创新是科技公司的首要任务



尽管存在潜在阻力，科技公司仍继续专注于创新（见图3）。今年调查中，有三分之一的受访者表示正在拓展新的地理市场，而另一三分之一则专注于建立稳定性和韧性，这突显了经济和竞争压力可能如何挑战该行业的增长轨迹。

随着技术渗透到日常生活中，科技公司的风险加剧并变得更加复杂。核心运营风险，如技术错误、系统故障和业务中断，仍然普遍存在，即使是导致短暂中断的轻微事件，其成本也在上升。

此外，技术的相互关联性意味着一个领域或影响一家企业的漏洞可能带来深远的影响。系统性故障的潜在可能性，加上黑天鹅事件的潜在可能性，需要强大的风险管理协议和能够应对多种复杂且广泛的挑战的保险计划。

风险管理重点正在转移，更加注重支持创新

多年来，我们与技术公司的许多谈话都集中在勤奋管理保险预算和最小化风险总成本上，但今年的调查结果表明优先事项发生了重大转变。考虑到大多数技术公司仍在开发新产品和服务，且其基础是创新，因此风险管理优先事项中，使业务和增长得以实现排在最高位（见图4）。(公式符号保持不变)

04| 你如何看待以下风险管理优先级？

	稍高优先级	非常高优先级
赋能业务和客户增长	30%	56%
应对监管要求	25%	60%
理解新兴或加速风险	27%	56%
满足合同要求	14%	64%
最小化风险总成本	32%	33%
基准测试、数据、分析以及决策支持	31%	34%
长期保险与风险管理规划	34%	24%
管理保险/部门预算	28%	29%
数字风险管理工具	29%	21%
主张倡导	28%	16%

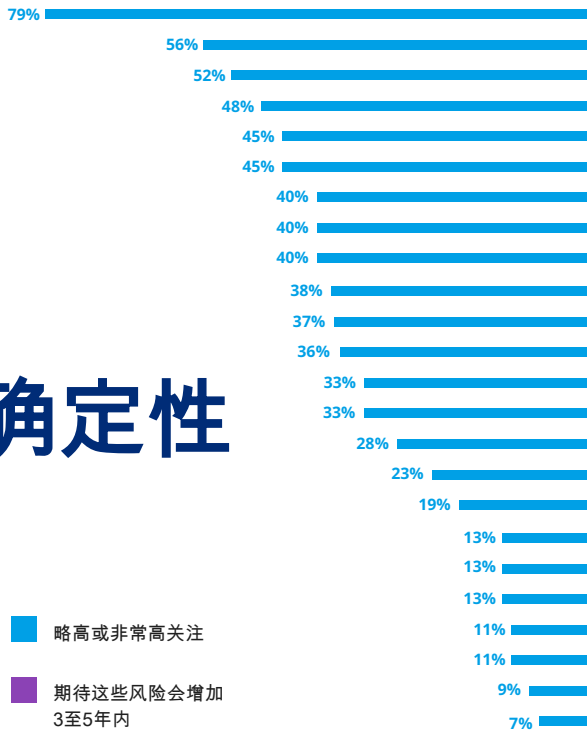
3

新技术的出现带来了众多潜在漏洞和风险，科技公司必须应对。

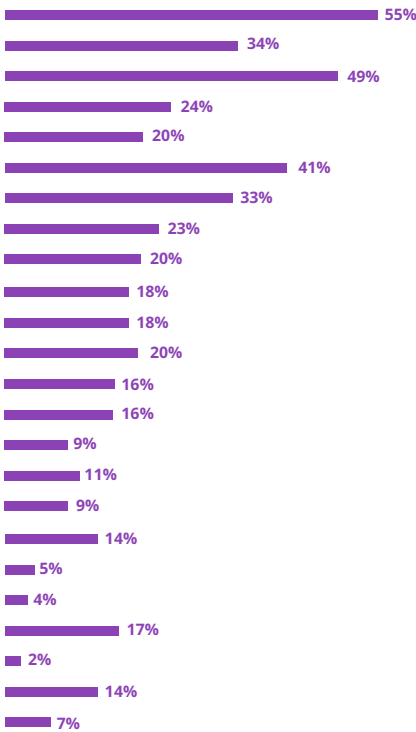
与其他年份类似，数字和技术风险仍然是我们的调查受访者最关心的问题，而监管机构的加强审查为科技公司的风险管理增加了另一层复杂性（见图5）。组织必须在全球复杂的法规迷宫中导航，这些法规可能因地区而异，包括更严格的数据保护法规要求。未能遵守这些法规可能会导致严厉的处理和声誉损害。

风险持续演变中应对不确定性

05| 数字和监管风险是科技公司的首要关切



- 数据安全和隐私
- 合规性
- 技术错误和遗漏
- 跨国风险敞口与合规
- 声誉风险
- 数字化/技术故障导致业务中断
- 通用软件或系统故障
- 人工智能设计缺陷
- 人工智能使用或监管错误
- 董事及高管责任
- 知识产权侵权
- 知识产权保护
- 员工保留
- 产品/平台责任或召回
- 并购风险
- 员工安全
- 因物理损坏导致的企业中断
- 媒体责任
- 雇佣实践责任
- 拥有财产的损害
- 自动或车队责任
- 员工欺诈
- 人身伤害或财产损失对他人
- 环境责任



■ 略高或非常高关注

■ 期待这些风险会增加3至5年内

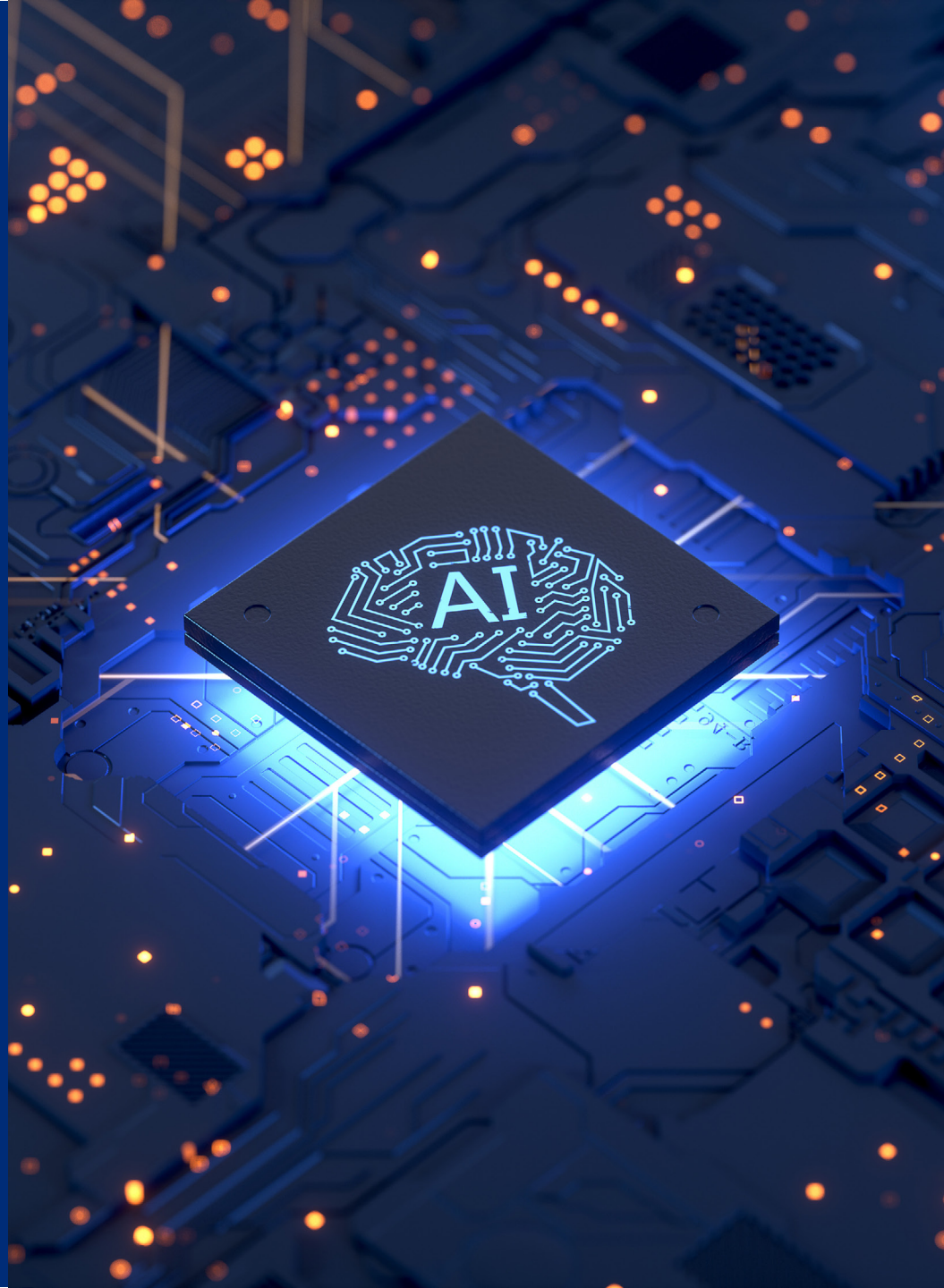
“

随着科技公司扩大其全球足迹，高级领导者必须准备好适应不断变化的地缘政治动态，这些动态可能影响从产品开发到市场战略的方方面面。这些不断变化的动态之间的相互作用创造了复杂的风险环境，要求组织采取全面的风险管理方法来应对当前和未来的不确定性。

人工智能的普及带来了机遇，加剧了风险

人工智能（AI）正在改变组织的工作方式。但许多科技公司不仅仅是AI的使用者；它们正积极开发和定制AI解决方案以提升其运营，创造出新的风险格局，其中不断演变的挑战预计将进一步放大现有漏洞。

然而，与人工智能相关的风险（如人为疏忽错误、系统设计失败等）在今年调查中被认为高度关注的技术风险中排名靠后（见图6）。同时，受访者预计与人工智能相关的风险在未来三到五年内将成为更大的关注点。这种转变表明，高级管理人员目前正专注于其他紧迫问题。此外，迄今为止尚无重大的与人工智能相关的损失，这可能造成了一种虚假的安全感，有可能导致对潜在风险的最初低估，加上对新技术风险可能出现的认识。



06|人工智能风险是当前较不紧迫的技术问题

当前	低 关注	中等 关注	高 关注
人工智能设计缺陷	37%	23%	40%
人工智能使用或 疏忽错误	35%	25%	40%
通用软件或系统故障	33%	27%	40%
数字化中断业务 技术故障	19%	36%	45%
技术错误和遗漏	23%	25%	52%
数据安全和隐私	4%	17%	79%



在未来三到五年内

	期望这不会成为大问题	无变化	期待这会成为更大的问题
通用软件或系统故障	0%	78%	20%
数字化中断业务 技术故障	7%	64%	23%
技术错误和遗漏	4%	60%	33%
数据安全和隐私	2%	50%	41%
人工智能设计缺陷	0%	49%	49%
人工智能使用或 疏忽错误	2%	39%	55%

面临独特责任风险的高科技公司

迄今为止未发生重大损失并不意味着公司可以暂时忽视风险，尤其是考虑到该领域的快速发展。从传统技术产品转向人工智能驱动解决方案带来了独特的责任风险。例如，如果一个使用人工智能的技术系统未能按预期运行，开发者可能会面临产品责任问题。

随着拟人化人工智能的兴起，这是一个日益增长的关注点，其中错误可能导致人身伤害或财产损失。例如，在仓库中运行的人形机器人出现故障，可能导致伤亡和财产索赔，并引发谁对事件负责的问题。此外，诸如欧盟的法规 [产品责任指令](#) 将软件和人工智能系统定义为“产品”，将产品责任法的适用范围扩展到这些技术。

此外，知识产权（IP）侵权的风险可能会显著升级。开发者现在可能需要对用于训练人工智能（AI）模型的数据集的策展负责。如果系统随后生成的输出与受版权保护的材料非常相似，开发者可能会面临知识产权侵权指控。科技公司必须通过审慎的许可协议来主动管理其知识产权风险。

使用人工智能辅助决策过程会带来进一步的复杂性。例如，人工智能技术可用于解释数据并为关键商业决策提供信息。人工智能错误可能导致严重后果，例如在医疗保健环境中，人工智能模型正被用于进行鉴别诊断。此类情景突显了保持适当的人类监督以降低因过度依赖人工智能生成的输出而产生的疏忽索赔风险的重要性。

人工智能的采用需要一套健全的风险缓解策略

无论在开发、部署还是使用人工智能技术时，嵌入强大的风险缓解策略都至关重要。需要跨职能领导，包括技术、业务、人力资源和法律/合规领导者。风险管理人员是此过程的核心，他们承担着评估和提供人工智能带来的多样化、企业级风险的全面视图的关键角色。

随着人工智能技术的进步，组织必须认识到它可能会放大现有风险。例如，使用生成式人工智能可能导致意外后果，例如生成误导性信息或侵犯知识产权。因此，风险管理人员必须确保其保险计划与人工智能风险的不断演变的环境相一致，包括评估与人工智能事件相关的保障范围和除外责任。代理人工智能和人形机器人的出现为组织带来了必须准备应对的多种额外挑战。一个关键的第一步是清点组织内部使用的各种人工智能类型以及它们如何在不同的业务职能中应用。

一个三叉风险策略

一个全面的AI风险框架应该涵盖三个关键风险控制，每个控制都发挥着在减轻与AI技术相关的风险方面至关重要的作用。



技术控制： 组织必须实施稳健 网络安全控制 为了保护他们的 AI 系统。这包括确保数据完整性、保护算法以及防御对抗性攻击。定期审计和更新 AI 系统对于维持安全和功能至关重要。



过程控制： 建立明确的治理结构对于监管人工智能计划至关重要。这包括董事会层面的治理以及高级管理层对生成式人工智能用例的监督，以帮助制定可接受的用法政策，开展供应商尽职调查，并确保符合监管要求。



人群控制： 组织必须培养关于人工智能使用的意识和责任感。这包括教育使用人工智能工具的员工人工智能的伦理影响、数据隐私问题以及遵守既定协议的重要性。重要的是让他们学习不要成为人工智能赋能的社会工程攻击的受害者。在某些情况下，可能有必要提供专门的再培训或技能提升。

人工智能风险管理不是一次性活动；它需要持续评估和适应，以跟上持续的技术进步。科技公司不应等待重大事件来触发其风险策略的重新评估。相反，它们应采用迭代方法，定期在全年审查和更新其风险管理框架，以考虑人工智能的新发展。



互联系统提升了网络安全风险等级

互联网络和解决方案的复杂性，加上网络攻击日益普遍和威胁行为者的日益复杂，使网络安全风险成为科技公司关注的焦点。

令人不意外的是，我们调查中近四分之五的受访者将数据安全和隐私视为当前高度重视的问题，近一半的受访者预计这些风险将在未来三到五年内增加（见图7）。

与网络威胁以及技术错误和疏忽相关的风险正变得越来越复杂。



07|技术和数字风险是高度关注的领域
您如何看待以下风险对您业务的看法？

技术或数字风险	当前				
	非常低的关注	有点低关注度	中等关注	稍高关注	高度关注
人工智能使用或疏忽错误	13%	23%	25%	29%	10%
人工智能设计缺陷	13%	25%	23%	25%	15%
通用软件或系统故障	6%	27%	27%	19%	21%
数字化中断业务 技术故障	0%	19%	36%	21%	23%
技术错误和遗漏	6%	17%	25%	21%	31%
数据安全和隐私	2%	2%	17%	19%	60%

技术或数字风险	在未来3-5年		
	期望这不会成为大问题	无变化	期待这会成为更大的问题
通用软件或系统故障	0%	78%	20%
数字化中断业务 技术故障	7%	64%	23%
技术错误和遗漏	4%	60%	33%
数据安全和隐私	2%	50%	41%
人工智能设计缺陷	0%	49%	49%
人工智能使用或 疏忽错误	2%	39%	55%

日益增长的担忧，具有多层次的复杂性

核心技术风险，例如数据泄露、勒索软件攻击和业务中断，仍然是随着威胁和漏洞在频率、复杂性和成本上的增加，科技公司关注的焦点。2024年全球平均数据泄露成本为 **488万美元** 与 2023 年相比增长了 10%，这突显了许多组织对其保护敏感数据和维护运营系统能力的担忧。

与此同时，随着人们认识到，即使拥有强大的网络安全措施和应急计划，公司也无法免受其影响，无论是直接还是通过第三方面接影响，对黑色天鹅事件的担忧在科技行业变得更加明显。这些定义上不可预测的事件可能会扰乱运营，导致重大经济损失，并进一步使风险格局复杂化。

随着组织间联系日益紧密，单点故障引发广泛中断的可能性增大，甚至可能引发系统性故障。而系统性故障又会波及企业或终端用户，提高科技公司和保险公司的风险。技术的相互关联性意味着一个领域的漏洞可能危及整个网络，这使得全面的网络风险管理变得至关重要。

隐私风险的演变，随着新法规的出现以及现有法规变得更加严格，增加了另一层的复杂性。超过一半的受访者将法规合规性描述为当前的重大关切，其中三分之一预计在接下来的三到五年内这将成为一个更大的关切（见图8）。



08|合规风险位居商业风险之首

商业风险	当前				
	非常低的关注	有点低关注度	中等关注	稍高关注	高度关注
合规性	8%	2%	33%	38%	19%
跨国敞口头寸 合规	13%	11%	28%	30%	17%
声誉风险	11%	11%	34%	28%	17%
知识产权保护	19%	19%	26%	19%	17%
知识产权侵权	15%	28%	20%	22%	15%
董事及高管责任	17%	25%	21%	25%	13%
产品/平台责任或召回	12%	33%	23%	21%	12%
媒体责任	29%	31%	27%	9%	4%
并购风险	23%	26%	23%	26%	2%

商业风险		在未来3-5年		
		期望这不会成为大问题	无变化	期待这会成为更大的问题
媒体责任		0%	91%	9%
知识产权侵权		0%	84%	14%
声誉风险		2%	82%	16%
并购风险		0%	80%	18%
董事及高管责任		2%	77%	18%
产品/平台责任或召回		0%	78%	20%
跨国风险敞口与合规		0%	77%	20%
知识产权保护		0%	73%	24%
合规性		0%	66%	34%

监管合规或许不足为奇，位居科技领导者关注商业问题的榜首。严格的.data保护规则，如欧盟的通用数据保护条例（GDPR）和美国各州层面的各种法规，意味着组织现在必须应对复杂的合规要求网络。不遵守相关法规可能导致严重的财务处罚和声誉损害。随着科技公司处理越来越多的敏感数据并使用各种形式的数字跟踪技术，合规压力加剧，进一步增加了其风险轮廓。



保险公司适应不断变化的网络安全风险

网络/科技E&O保险市场即使在不断变化的风险趋势下仍然保持竞争力和稳定性——尤其是对科技公司而言。尽管保险公司越来越关注系统性事件，但仍有承保能力，有新的参与者进入市场。保险公司正越来越多地探索灾害（CAT）债券作为管理系统性网络风险的一种方式，例如大规模勒索软件攻击或云服务中断。通过将风险转移至资本市场，CAT债券为保险公司提供了额外的金融保护，以帮助它们在增长的市场中维持偿付能力和承保能力。这反映了竞争激烈的市场格局，以及成熟适应不断变化的风险环境的网络保险产品。

保险公司继续关注改进网络安全卫生和控制。这意味着定期更新和培训员工网络安全最佳实践，进行漏洞评估，关注事件响应计划，并实施强大的安全措施以降低事件发生的可能性并提高整体韧性。保险公司可能会根据您现有的网络安全卫生和改进承诺提供更有利的条款和价格。

保险公司还继续要求关于公司网络安全控制和实践的详细信息。这包括关注现有控制的适当实施以及基于新兴风险的未来索赔的潜在性。对于科技公司而言，这也包括对其产品和解决方案的评估。除了价格之外，科技公司还应考虑其保险计划是否提供了足够的针对不断变化的风险的保护，是否符合其当前的风险状况。

对于组织而言，确保其保险政策能够满足其特定需求并适应风险变化至关重要，而不是依赖一刀切的解决方案。

高科技物业加剧了聚合担忧

科技公司正在扩大其物理足迹以适应不断增长的需求，导致房产和营业中断风险加剧，从而可能影响运营。

例如，一场重大灾难性事件，如地震或严重风暴，可能会损坏高科技财产，摧毁用于制造科技产品的专用设备，并扰乱供应链，导致较长时间的停机。在我们的调查受访者中，不到五分之一的人将因物理损坏导致业务中断评为高度关注（见图9）。



09|企业中断是科技公司的一个显著问题

运营风险	当前				
	非常低 关注	有点低 关注	中等 关注	有点 高度关注	非常高 关注
拥有财产的损害	23%	33%	31%	10%	2%
环境责任	40%	26%	28%	5%	2%
因物理损坏导致的企业中断	23%	31%	27%	15%	4%
人身伤害或财产损失对他人	21%	45%	26%	4%	4%
自动或车队责任	36%	27%	27%	7%	4%

运营风险		在未来3-5年		
	期望这不会成为大问题	无变化	期待这会成为更大的问题	
拥有财产的损害	4%	91%	4%	
业务中断由于 物理损伤	2%	89%	7%	
自动或车队责任	7%	84%	9%	
人身伤害或财产损失 到其他	0%	84%	14%	
环境责任	0%	83%	17%	

地理集中加剧了房产风险

由于高科技公司在地震易发地区（包括硅谷和台湾）的聚集，风险更为突出。这种地理集中是保险公司面临的潜在聚集风险，因为单一灾难性事件可能导致多个实体遭受重大损失。此外，技术供应链内部的相互依赖性，由于公司对其生产流程严重依赖其他公司，加剧了这个问题。一个设施的中断会通过网络扩散，影响众多公司和其运营，可能导致重大的或有业务中断损失。

所有这一切都发生在一个地缘政治和全球贸易紧张局势的背景下，这些紧张局势正在加剧不确定性，特别是在关键物资成本方面。许多科技公司，尤其是那些基于美国的公司，正在应对是否将关键物资本土化或等待更多确定性的决定，同时它们也面临着可能更高的成本，这些成本也需要反映在其保险估值中。

同时，具备高技能人才来维护和校准高科技设备（尤其是在经历重大中断后）的可用性，可能会延长停机时间。我们调查的受访者中有三分之一表示，员工留任是他们高度关注的议题，其中16%的人表示预计在未来三到五年内这将成为一个更大的关注点（见图10）。投资于培训和发展，包括提升技能和再培训；加强招聘策略；以及创建清晰的职业发展路径，是科技公司可以用来强化其留任策略的一些方法。

前瞻性财产保险承保商采用工程方法

保险公司了解科技公司面临广泛且不断变化的风险。高科技设施通常具有独特、高度工程化的组件，这些组件替换起来成本高昂，并且可能需要较长的采购提前期。

此外，考虑到建造制造设施的巨大成本以及损失可能带来的灾难性后果，对于保险人和被保险人来说，拥有充足的保险保障变得至关重要。

将灾难性事件不仅扰乱一家，而是多家企业的能力，促使一些保险公司采取以工程为主导的承保方式。这种方式有助于保险公司更好地评估潜在漏洞，并推荐可降低风险改进措施。许多保险公司正高度重视遵守工程建议，尤其是当他们为风险提供大容量保障时。

保险公司也正在审查意外业务中断险种的保障是否充足，并且变得更为谨慎，通常会限制承保范围或提高保费来弥补风险敞口的增加。

随着房地产市场的演变，以及科技行业继续保持快速增长势头，对高风险房产的关注度预计将加剧，这也凸显了定期审查以识别和解决漏洞的重要性。这种变化的动态也突显了高科技公司重新评估其保险覆盖范围并确保其重置价值准确的紧迫性。

10| 员工保留是科技公司的重大关注点

员工风险	当前				
	非常低 关注	有点低 关注	中等 关注	有点高 关注	非常高 关注
员工欺诈	30%	45%	15%	11%	0%
雇佣实践责任	24%	33%	30%	9%	4%
员工安全	14%	23%	41%	16%	7%
员工保留	7%	24%	37%	22%	11%

	期待它将是 不太成问题	无变化	期待它将是 更是一个问题
员工安全	0%	98%	2%
雇佣实践责任	0%	95%	5%
员工欺诈	0%	86%	11%
员工保留	0%	79%	16%



伤亡风险中的地震变化

一段时间里，意外险续保对科技公司来说仍是一如既往的流程，其中大部分公司能够顺利获得所需的意外险额度，且过程顺畅。但如今，科技公司面临新的现实，因为大多数保险公司——专注于提高意外险索赔成本且对科技产品的意外险风险缺乏真正理解——已大幅降低可用额度，且鲜有公司愿意将额度提高到2.5亿美元之上。

一个日益严峻的诉讼环境，加上索赔周期变长和陪审团裁决不断飙升，已经形成了一场完美风暴，正在重塑保险公司在整体上评估意外风险的方式。对于科技公司而言，随着其产品变得无处不在——从智能家居设备到可穿戴技术再到医疗设备以及汽车等等——与意外相关的议题正变得越来越突出。

并且越来越多 [社会通胀和核裁决](#)

——陪审团判赔超过1000万美元——给保险公司带来了更大的压力，促使它们更加谨慎。保险公司仔细审查可能导致人身伤害的产品，例如用于关键系统或作为车辆安全功能一部分的微型芯片，因为这些设备的故障可能导致严重的后果。如果发生故障，后果可能是灾难性的，导致严重伤害甚至死亡。并且医疗设备的软件故障可能导致危及生命的问题未被察觉。

这种高风险索赔的潜力，使保险公司对提供传统限额持谨慎态度，因为他们正努力应对这些风险带来的不确定性。

这导致科技公司在获取所需的意外责任保险限额方面面临挑战。

通过有效风险管理转移和应对挑战

这种新的风险格局要求技术领导者采取一种积极的风险管理策略，旨在减少索赔——识别潜在的问题索赔，并在其升级前及早处理。

此外，也许是时候重新思考续保策略和核保会议了，利用科技公司在网络安全和D&O保险续保方面已经使用了一段时间的做法。利用这段时间与核保人进行开放沟通，并清晰地解释你的产品，回答关于潜在相关风险的问题。这些详细见解可以帮助核保人更准确地评估风险，并有可能重新审视他们提供所需保覆盖的舒适度。

同时，展示一个稳健的风险管理体系可以给保险承保人带来信心，并使公司区别于其他公司。

随着由其他险种覆盖所形成的趋势，伤亡保险市场正在发生转变，这要求科技公司进行转型，重点是与保险公司进行开放沟通，以增加获得充足保障的机会。如果这不可行，请考虑其他替代方案，例如设立专属保险公司或其他形式的自我保险，以保护您的组织并继续专注于运营和增长。

在日益复杂的背景下保护技术高管

随着科技公司在不断变化的相互关联的风险网络中前行，为组织决策者提供充分保护变得日益重要，这使得这些公司能够吸引——并留住——最佳人才。

更是技术的快速边缘治理问题政治重要科技公司面临的危险的紧张的国际差异可能致多个司法管辖区运营的公司面临复杂的监管要求和问责责任的雷区。而且全球供应链的相互关联任意暴露于充满挑战的环境可能对其他通函保险覆盖范围远的影响管务大的紧迫的担忧是高科技人才的潜在短缺。人才短缺可能加剧运营挑战，进而导致利益相关者加强审查可能会受到董事和高级管理人员政策的重要性此外，在此类公司方面，新兴和不断变化的重大投资的环境下，做出错误的决策可能导致 随着地缘政治紧张局势加剧和法规不断发展，领域高管提供重要的保护。

理解高管风险的动态变化

董事和高管正变得越来越岌岌可危。与此同时，原告律师界不断寻找提起诉讼的机会，包括与法规变更相关的事务。新的或变更的法规可能导致合规审查，要求高管证明其监督和决策流程；若未能做到，他们可能会面临法律挑战。

重大股东或投资者风险。

而在财务及专业领域，包括D&O，均有 看到了几个季度的降息在美国，并且在2025年第二季度持平，这些是在几个季度显著增长之后出现的，这意味着基准线仍然高于2022年初。

这种现实可能导致公司主要专注于削减其D&O计划的成本。然而，在这个日益升级的风险环境中，科技公司应该强调其D&O计划为其高管提供的保护。

因此，重点应放在合同确定性上，充分理解您的保单，识别潜在的昂贵保障空白。同样重要的是与有良好索赔响应和支持记录的承运人合作。



应对不断变化的风险和保险环境

许多科技公司正在考虑替代风险转移 (ART) 解决方案。

超过四分之一的受访者表示，他们计划在未来12个月内探索整合型、结构化或替代型风险计划（见图11）。五分之一的受访者已经开始利用或探索保险 captives，另外还有17%的人预计在未来12个月内会这样做。虽然传统保险模式仍然是科技公司的支柱，但有时它们无法满足一个快速增长部门独特的需求，尤其是在保费上涨威胁到项目可负担性时。增加对ART兴趣的主要驱动因素本身是不断变化的风险格局，许多组织都在寻求更灵活和定制化的保险解决方案。

11| 探索替代风险解决方案的科技公司行动或计划

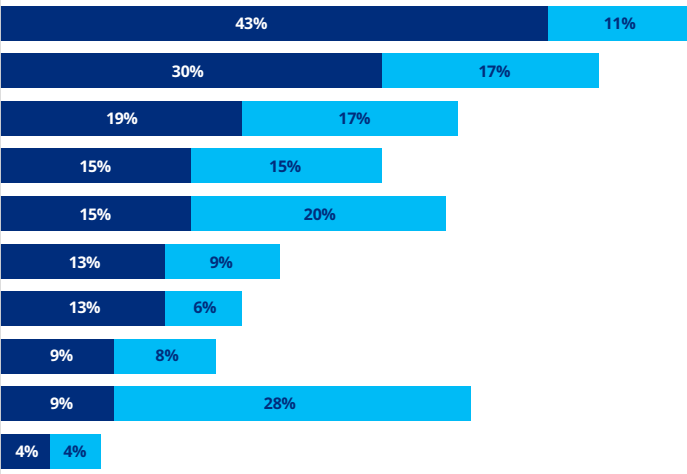
激进的项目营销 在项目层级引入新的保险人 利用或探索自保公司
更换主要保险人 提高留存 降低限额 狭窄条款、条件或服务定义
在不同保险险种之间重新分配保险预算

探索综合的、结构化的或其他替代风险计划

转向纯粹的灾难性覆盖

过去12个月

在未来12个月内



科技公司如何从替代风险解决方案中受益？

随着行业的持续发展，科技公司可以利用多种替代风险解决方案来补充其传统保险计划。

1. 结构化风险（再）保险计划 允许科技公司利用其资产负债表，在多年期内承担一定量的风险，并在出现负面损失经历时提供风险转移保障。这些高度可定制的计划包括风险分担要素，并提供成本节约和稳定性的潜力，以对抗传统保险解决方案。一家科技公司可能从年度定价/覆盖范围的角度出发，将其结构化风险（再）保险计划用作其最易波动覆盖范围的替代传统保险方案。

2. 整合风险（再）保险计划 将多种类型的保障整合到单一保单或框架中，并提供与跨险种、跨多年的结构化项目相同的利益。这种方法简化了风险管理，降低了行政成本，并为组织风险状况提供了整体视角，从而允许更有效的风险缓解策略。技术客户可以将他们最具挑战性的保障领域/业务，例如网络/技术E&O、事故险和财产险，整合到单一的多年综合结构中，以稳定这些风险，并相对于保证成本保险提供潜在节约。

3. 结构前置 为组织提供一种方式，使其在保留特定险种风险的同时，持有保险单以满足合规/证据要求，并可能代表客户支付索赔，随后获得报销。如果一家科技公司需要向第三方提供保险证据，但又不想购买传统险种，那么这种解决方案是理想的选择。

4. 参数保险 根据特定事件的发生而非实际发生的损失，支付一个预定的金额。例如，一个易受命名飓风侵袭的大型数据中心可能想要定制一个基于飓风期间风速测量的触发式解决方案，以便更快地获得用于恢复的资金。

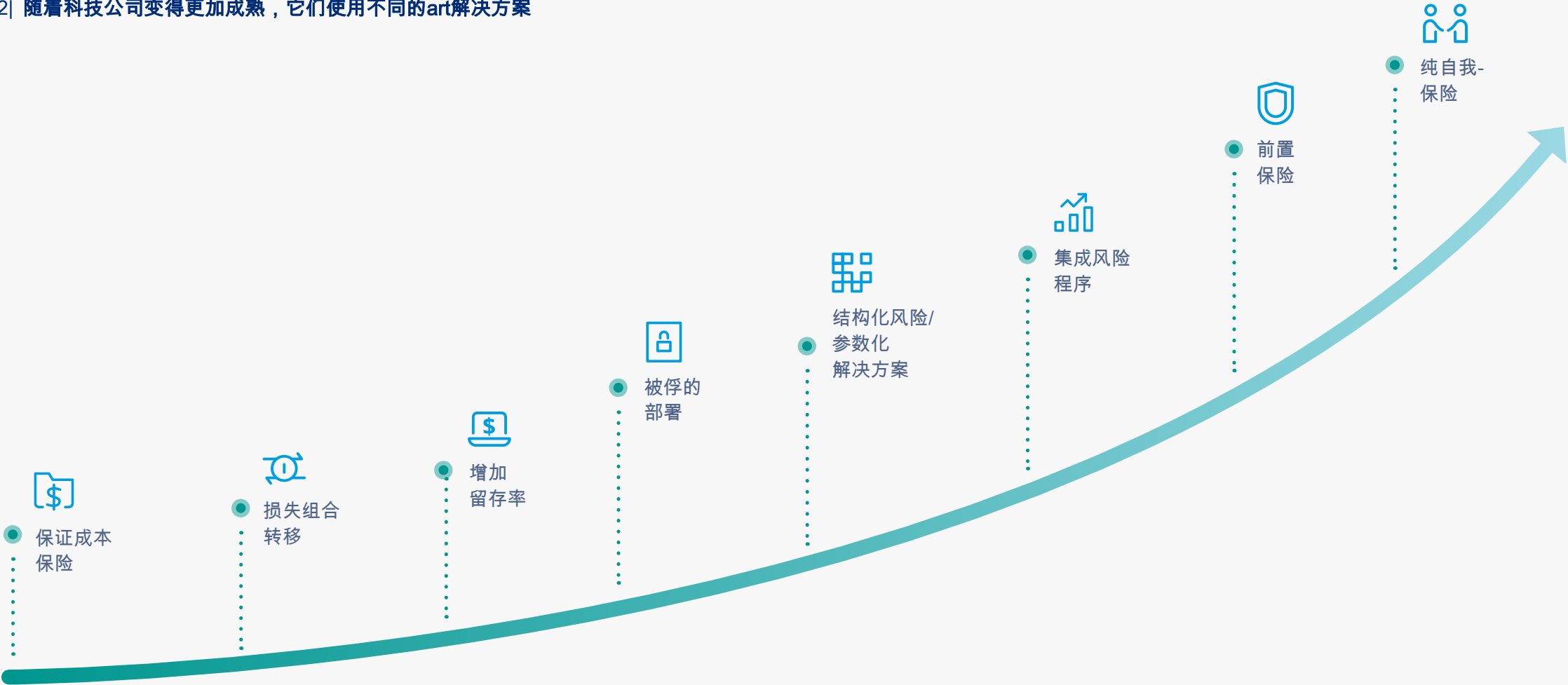
5. 专业自保险公司 是一家为母公司或公司集团提供保险覆盖的子公司。这使企业能够更好地控制其风险管理，并通过根据其特定需求定制覆盖范围来潜在地降低保险成本。科技公司可以设立一家附属公司，以帮助承保具有挑战性或目前无法承保的风险。

6. 再保险 利用结构化或集成式再保险解决方案，为保险子公司及其多年多险种的盈余提供保护。替代风险保险子公司再保险产品再保险产品在保险子公司保留一定风险金额后，提供下行风险转移保护。如果一个科技组织刚成立保险子公司，再保险产品可以协助在保险子公司初期管理其波动性。

7. 损失组合转移 涉及将特定损失组合的相关负债转移给另一家保险公司或再保险公司。它允许公司清理其资产负债表，更有效地管理其风险敞口。例如，一家科技公司在其剥离某个业务部门时，可能会使用损失组合转移，因为它不希望再承担与该剥离业务部门相关未结索赔的任何进一步责任。

ART解决方案使科技公司能够凭借其财务实力创建与其特定风险敞口相一致的定制化产品，同时在同时获得对其保险成本的更大控制权（见图12）。此外，替代风险解决方案中固有的灵活性使科技公司能够随着其运营和风险轮廓的演变而调整其保障范围。

12| 随着科技公司变得更加成熟，它们使用不同的art解决方案



其他热门风险领域

随着科技领域的不断发展，新的风险将会出现，这也突显了持续关注动态并调整风险管理及保险计划的重要性。以下是风险管理人员应密切关注的五个风险领域。

1. 资本市场波动： 资本市场持续的波动，加上利率上升，正在对公有和私营科技公司的资产负债表造成压力。这种情况影响了公司如何将风险转移、风险保留和保险作为缓解金融波动手段来应对。

2. 合同风险： 政府部门和大型企业之间存在一个显著的趋势，即在合同中要求更广泛的赔偿条款和显著更高的责任限额，有些人甚至寻求无限责任。

3. 相互关联的生态系统： 科技企业越来越依赖复杂且相互关联的供应商生态系统。运营停机、供应商故障或外部事件带来的中断可能产生连锁反应，影响业务连续性、声誉和法律风险。此外，对共享基础设施的依赖增加了级联故障的风险，而威胁行为者可能会利用供应链中的漏洞造成更广泛的影响。

4. 供应链和基础设施压力： 生产实体产品和服务的科技组织由于全球供应链压力而面临更高的风险。关税、地缘政治不确定性以及竞争动态等因素影响着对关键组件的获取，同时计算能力的需求超过了现有基础设施，给数据中心容量和电网带来了巨大压力。为了跟上创新步伐，技术和基础设施生态系统必须快速扩展。对第三方供应商和云服务提供商的依赖增加也提高了遭受网络攻击和运营中断的风险。

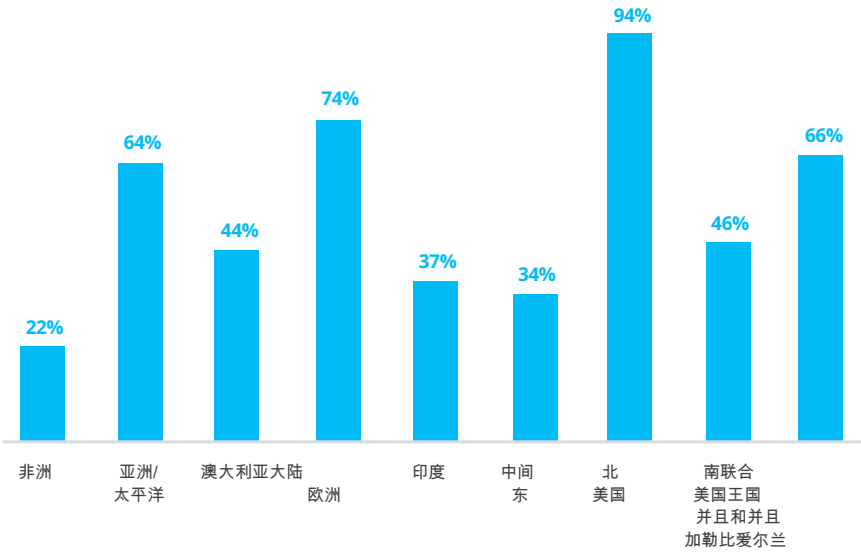
5. 合成媒体责任： 视频、音频、图像或通过人工智能创建或修改的文本，包括深度伪造、人工智能生成的图像、合成语音和大型语言模型生成的文本，会引发各种风险，包括知识产权和诽谤问题，以及与人工智能生成内容相关的潜在诉讼和监管处罚。使用未披露或恶意的合成媒体可能会损害品牌声誉，而在受版权保护的内容上训练人工智能模型则引发了关于合理使用和所有权的法律问题。公司面临着这些风险带来的重大声誉和财务损害。

调查人口统计

本报告基于我们73位技术客户的直接调查反馈，以及我们在2025年马什硅谷科技风险论坛上的对话和见解。

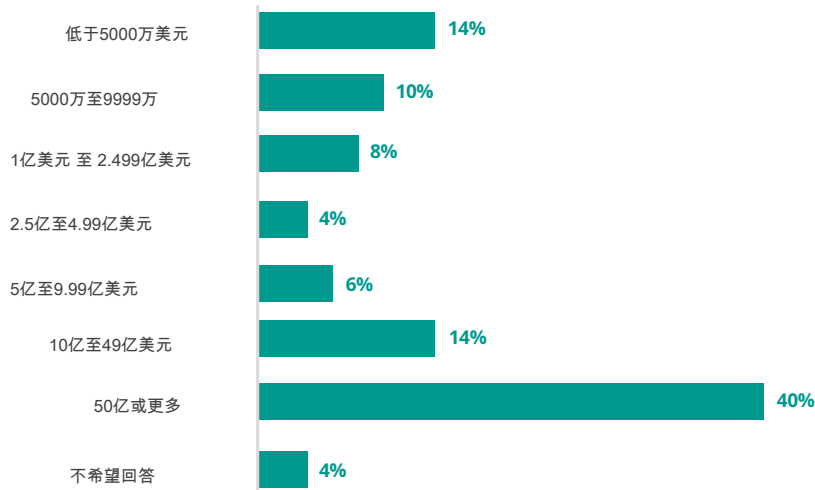
今年调查样本的人口统计和公司统计分布详情在以下图表和图形中详细说明。

13| 贵组织在哪些地区设有办事处或开展业务？



14| 您组织的年营业额是多少美元？

年营业收入(美元)





关于Marsh

Marsh公司是Marsh McLennan (纽约证券交易所：MMC) 的企业，是世界顶级保险经纪和风险管理顾问。Marsh McLennan是风险、战略和人才领域的全球领导者，通过Marsh、Guy Carpenter、Mercer和Oliver Wyman四大业务，为130个国家的客户提供咨询服务。Marsh McLennan年营收达230亿美元，拥有超过85,000名同事，通过提供独特的视角帮助客户建立成功所需的信心。欲了解更多信息，请访问marsh.com，或在领英和推特上关注我们。

马什是马什·麦克伦南公司的一家业务。

本文件以及Marsh提供的任何建议、分析或意见（统称为“Marsh分析”）均不旨在被视为针对任何具体情况的建议，也不应被视为此类建议而依赖。本文件包含的信息基于我们认为是可靠的来源，但我们对其准确性不作任何陈述或保证。Marsh没有义务更新Marsh分析，且对于因本文件发布或其中包含的任何事项而产生的对你或任何其他方的责任概不承担。任何关于精算、税务、会计或法律问题的陈述均仅基于我们作为保险经纪人和风险顾问的经验，不应被视为精算、税务、会计或法律建议，对此你应该咨询你自己的专业顾问。任何建模、分析或预测均存在固有不确定性，如果任何基础假设、条件、信息或因素不准确、不完整或应发生变化，Marsh分析可能受到实质性影响。Marsh对保单措辞的应用、保险公司或再保险公司的财务状况或偿付能力不作任何陈述或保证。Marsh对保险保障的可用性、成本或条件不作任何保证。尽管Marsh可能提供建议和推荐，但关于保障金额、类型或条件的所有决定最终由保险购买者负责，其必须决定对其具体情况和财务状况适当的特定保障。

1166美洲大道，纽约10036

版权所有 © 2025, Marsh LLC。保留所有权利。25-641100-US