

促进网络安全风险向资本市场转移： 巨灾债券及更多创新

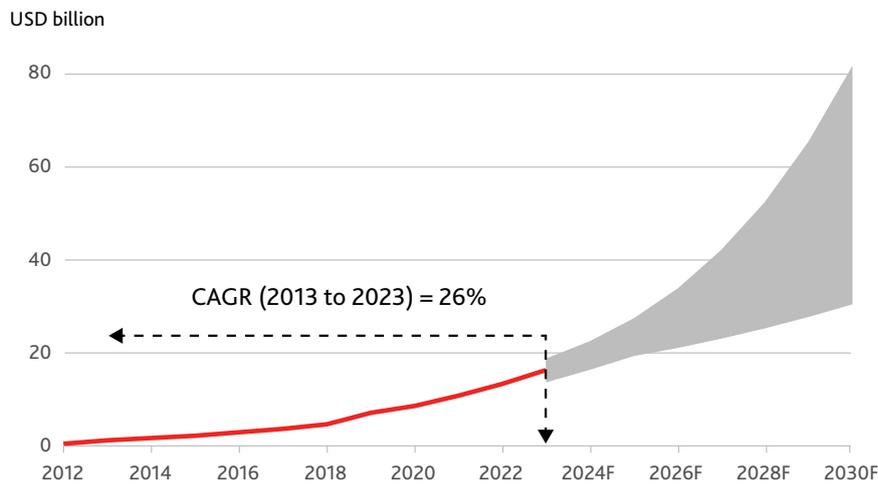
研究摘要 | 2024年12月

Darren Pain，网络安全风险与演进责任研究总监，日内瓦协会

随着网络安全风险敞口急剧上升，专门的网络安全保险迅速发展。这种保险不仅能在事故发生后提供资金来修复受影响的数据和系统，还能通过其承保过程鼓励投保人投资于最佳的网络安全实践。全球网络安全保险保费从 2013 年的不足 15 亿美元猛增至 2023 年的约 150 亿美元，但即便如此，这仍不足财产与责任保险市场总量的 1%。¹网络安全保险的覆盖范围也在扩大，涵盖了包括数据恢复、IT 取证、系统修复、

非损害性业务中断以及第三方损害责任等各种与网络安全相关的损失。随着社会持续数字化，大多数行业评论者预计网络安全保险市场将继续保持强劲增长。这反映了随着企业和个人网络安全风险意识的提升，以及对自身保险保障水平不足的认识加深，预期各个行业 and 各个国家的网络安全保险需求都会增长。通过这种方式，网络安全保险可以在缩小当前较大的保障缺口方面发挥越来越重要的作用。

图 1：网络安全保险市场展望——全球保费预测



说明：红线表示截至 2023 年的全球网络安全保险保费数据，来源为 Howden。灰色阴影区域显示了以下市场参与者和评论者的保费预测范围：Beazley, Business Research Company, Cognitive Market Research, Expert Market Research, Fortune Business Insights, Global Market Insights, Howden, Market.us, Morningstar DBRS, Munich Re, S&P, SkyQuest Technology, Spherical Insights 和 QualRisk。在预测范围不同的情况下，数据根据隐含的复合增长率进行预测。

CAGR = 年均复合增长率

来源：Howden 和日内瓦协会计算

¹ Howden 2024; Allianz 2024.

然而，要实现网络安全保险的持续快速增长，关键在于吸引足够的资本来支持相关保单。再保险对主要保险公司来说至关重要，因为它能分担极端网络安全风险，否则这些风险会给保险公司的资产负债表带来压力。尽管不同年份和国家的估算有所不同，但主要保险公司可能会将约 50% 的网络安全保险保费转移给再保险公司，这远高于其他保险种类。²

另类风险吸收资本

除了扩大传统保险/再保险公司参与承保网络安全风险外，吸引保险业外的额外风险承担资本也是必要的。极端网络损失的规模可能过大和/或不确定，保险/再保险公司难以独自承担。一项研究表明，即使根据更保守的市场预测，网络安全保险保费的增长也需要资本增加五倍。³这包括将一些网

络安全风险转移到金融市场，在那里可用于投资新兴风险（如网络安全风险）的资本池更为深厚。

网络安全保险关联证券（cyber insurance-linked securities, ILS）的前景已被讨论多年。这是一种将特定保险风险打包成独立可投资资产的金融工具。尽管自 2017 年起已有少量商业网络安全抵押再保险和侧挂车协议（Sidecar）达成，但这些交易零星，仅涉及少数特定参与者。然而，近期网络安全保险关联证券的发行加速，多笔重要交易进入市场。例如，自 2023 年初以来，至少有五家再保险/保险公司发行了网络安全保险关联证券（见表 1），其中包括首批完全证券化的网络安全巨灾债券（当重大网络安全事故的索赔金额超过预先约定的门槛时，该证券用于赔偿相关损失）。

表 1：近期网络安全保险关联证券（ILS）交易

发行日期	发起方 (SPI)	承保限额 (百万美元)	交易类型	到期时间	触发类型 (依据)
2023年1月	Hannover Re	100	抵押再保险	未知	赔付额 (成数比例)
2023年1月-9月	Beazley (Cairney)	71.5	私人巨灾债券 (Reg4(a)(2)格式)	一年 (2024年1月到期)	赔付额 (每次事故)
2023年11月	AXIS (Long Walk Re)	75	巨灾债券 (144A格式)	两年	赔付额 (每次事故)
2023年12月	Chubb (East Lane Re VII)	150	巨灾债券 (144A格式)	两年	赔付额 (每次事故)
2023年12月	Beazley (PoleStar Re)	140	巨灾债券 (144A格式)	两年	赔付额 (每次事故)
2023年12月	Swiss Re (Matterhorn Re)	50	巨灾债券 (144A格式)	两年	PERILS行业损失 (每次事故)
2024年1月	Swiss Re	50	ILW	未知	PERILS行业损失 (每次事故)
2024年4月	HannoverRe (Cumulus Re)	13.75	私人巨灾债券 (Reg4(a)(2)格式)	一年	指数化 (美国主要云服务提供商区域的中断时长)
2024年5月	Beazley (PoleStar Re)	160	巨灾债券 (144A格式)	两年半	赔付额 (每次事故)
2024年9月	Beazley (PoleStar Re)	210	巨灾债券 (144A格式)	三年	赔付额 (每次事故)

来源：日内瓦协会，基于公开信息整理

² 引用自 [Risk & Insurance 2024](#)。尽管最新再保险续保中的网络安全风险分出率平均在 40% 左右（参见 Gallagher Re 2024），这一比例仍远高于更成熟的保险领域（如财产险和责任险）10% 至 15% 的分出率（根据 [American Academy of Actuaries 2021](#)）。

³ 具体而言，据报道，风险承保方需要 1210 亿美元的资本来应对美国网络安全保险保单中每 250 年一遇的损失，这一数额是当前估算资本基数的 5 倍增长。参见 [CyberCube 2024](#)。

尽管通过这些债券转移的网络安全风险（约 8 亿美元）在绝对值和相对于保险/再保险行业的网络安全风险敞口总额方面都较为有限，但这些交易仍标志着网络安全保险/再保险市场发展的重要里程碑。⁴一个关键问题是，市场条件是否已成熟，能够实现网络安全风险向资本市场的大规模、持续性转移，这是将网络巨灾风险分配给最有意愿和能力承担这些风险的参与者的未来关键一步。

最近网络巨灾债券的市场情报

与市场参与者的讨论强调了最近发行的网络巨灾债券在发起方与第三方投资者谈判中突出的几项设计特征。第一，交易型证券得到了青睐，尤其是 144A 规则格式的证券，这种格式简化了发行流程并拓宽了专业投资者的转售机会。第二，保险关联证券的投资者通常希望接触极端但罕见的网络安全风险，这意味着最近的大多数网络安全保险关联证券被设计为按事故发生的超额损失保险，即当单一重大网络事故的损失超过预定门槛时进行赔付。第三，初始网络安全巨灾债券的定价表明，第三方投资者承担极端网络安全风险所需的补偿比其他自然灾害风险更高，这部分与新兴且不熟悉的投资产品的高不确定性相关。

要使大型常规网络安全保险关联证券计划的风险交换条件更具可行性，降低通过保险关联证券募集资本的成本至关重要。此外，初始网络安全保险关联证券交易还揭示了一些重要的根本性挑战，最为重要的包括：

- 不同触发保险赔付事故的定义（例如包括的灾害类型、时间限制、覆盖的损失等）以及保单除外责任条款（例如战争、关键基础设施）的不同表述可能削弱合同的确定性。
- 网络安全保险的主要投资群体仍较为狭窄（尽管在扩大中），而有限的二级市场交易意味着保险关联证券作为一种资产类别仍相对缺乏流动性。

- 投资者对网络安全风险为其投资组合提供分散化收益的潜力保持谨慎态度，鉴于网络安全事故可能同时影响许多企业并广泛降低金融资产的价格。

总体而言，几乎所有受访者（包括发行方、投资者和中介）都认为网络安全保险关联证券市场仍处于开发阶段，尚未接近快速增长的起点。尽管最近的交易为未来发展奠定了重要基础，尤其是在教育投资者了解网络安全风险及其相关损失建模方面，但最可能的前景是未来发行量将保持持续、稳步增长，而非快速增长。⁵投资者群体仍然较小且是机会主义的，而当前较高的资本和交易成本可能阻碍极端网络安全风险经常性的转移至资本市场。

促进网络安全风险向资本市场的转移

随着对网络安全巨灾风险的整体认识和理解不断深化，上述阻力中的一部分无疑会逐渐减弱。近期的网络安全保险关联证券交易表明资本市场投资者对网络安全风险有一定兴趣。然而，要显著提高风险吸收能力，可能需要一系列措施。与其单纯复制自然灾害保险成功的经验（例如吸引相同的投资者并采用类似的工具），我们还需要进一步创新以使网络安全风险对第三方投资者更具吸引力，这些创新包括：

- 推动保单标准化。这并不意味着必须制定统一的保单，而是采用更简单、清晰且尽量避免使用保险特有法律术语的保单措辞，从而鼓励更多资本支持分担企业和家庭难以承受的极端网络安全风险。
- 改进网络安全风险的正式建模和量化。随着对网络安全风险的理解加深，以及更多关于网络安全事故（特别是重大损失事故）实证数据的取得和分析，模型将得到改进。这将拓宽可保范围，并激发保险/再保险公司和第三方投资者对网络安全风险的兴趣。

⁴ 整个行业的网络安全保险责任限额总量难以准确评估，但根据与市场参与者的交流，一些评论者认为其可能在 400 亿至 450 亿美元之间。参见 [Johansmeyer 2023](#)。

⁵ 一位受访者认为，现有保险关联证券（ILS）基金容量的 5%至 10%原则上可以分配给网络安全风险，因为资产管理已经获得了承保网络安全风险的授权。这可能表明短期内可实现的市场规模约为 50 亿至 100 亿美元，尽管这一过程可能较为缓慢，未来三年内更可实现的发行规模可能为 20 亿至 30 亿美元。

- 更细化的保险/再保险保障项目，以更好地匹配投资者的风险偏好。保险合同可以明确设计，为常规损失和巨灾损失的网络安全相关风险提供差异化的保障。此外，针对特定巨灾网络安全情景的更有针对性的超赔再保险保障，也能够更有效地吸引传统资本和另类资本参与分担此类极端风险。

这些创新将增强对网络安全损失规模化转移的信心，并增强对其与其他金融资产回报可能相关关系的理解。同样，虽然并非网络安全风险特有，但增加保险关联证券（ILS）整体可交易性，从而提高二级市场流动性的举措（如引入新的投资工具和数字基础设施）也有助于扩大网络安全保险关联证券的投资者群体。

此外，资本市场参与承接极端网络安全风险不应仅局限于保险关联证券（ILS）的视角。许多 ILS 产品是为自然灾害风险设计的，其风险特征与网络安全风险并不相同。更广泛的风险转移解决方案也可以发挥作用，例如利用传统保险/再保险资产负债表将网络安全风险转化为可投资的产品。不同的融资工具和结构将吸引更多具有多样化风险偏好的投资者，尤其是那些更能容忍网络安全风险规模和发生概率的模糊性，以及更愿意承担系统性（即不可分散）风险的投资者。

未来网络安全巨灾损失的内在不确定性最终限制了网络安全风险的转移范围，无论是转移给保险/再保险公司还是金融市场投资者。然而，通过将极端风险分散至多个资产负债表，持续的金融创新仍能够更好地匹配资本与网络安全风险，从而推动实现更优化的风险分担。

参考资料

Allianz. 2024. *Allianz Global Insurance Report 2024: Transformative years ahead for the insurance sector.*

https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/2024_05_23-Global-Insurance-Report.html

American Academy of Actuaries. 2021. *Cyber Risk Reinsurance Issues. Cyber risk toolkit.*

<https://www.actuary.org/sites/default/files/2023-02/6Reinsurance.pdf>

CyberCube. 2024.

Projecting Cyber Insurance Growth: A 10-year US market outlook.

<https://insights.cybcube.com/projecting-cyber-insurance-growth-report>

Gallagher Re. 2024. *1st View. Balance maintained.*

<https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/news-and-insights/2024/july/gallagherre-1st-view-balance-maintained.pdf>

Howden. 2024. *Cyber Insurance: Risk, resilience and relevance.*

<https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf>

Johansmeyer, T. 2023. *How Big Is the Cyber Insurance Market? Can It Keep Growing? Lawfare.*

<https://www.lawfaremedia.org/article/how-big-is-the-cyber-insurance-market-can-it-keep-growing>

Risk & Insurance. 2024. *U.S. Cyber Insurance Market Slows, Adapts in 2023.*

<https://riskandinsurance.com/u-s-cyber-insurance-market-slows-adapts-in-2023/>