THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

网络风险积累：
全面应对可保性挑战

研究摘要
2023年11月

Darren Pain, 网络与责任发展研究部主管，日内瓦协会

网络风险，指会破坏数据或IT服务保密性、可用性或完整性的恶意行为或意外事故，造成个人和组织的伤害，并可能在不同地域同时发生。对于那些从客户处承保网络相关风险的保险公司来说，无论是作为常规财产与责任保险的一部分，还是通过专门的网络保险进行承保，这种潜在的重大损失都是一个严重的问题。

对潜在网络损失积累的忧虑并不新鲜。然而，近年来地缘政治紧张局势加剧，网络威胁形势恶化，加剧了人们对严重网络事件的担忧。与2021年相比，2022年全球网络攻击增加了38%，其中，勒索软件攻击是一种持续的威胁。民族国家威胁行为者在网络空间变得越来越具有侵略性，其行为包括使用网络武器以达成破坏性目的，且范围不仅限于俄乌冲突。

尽管我们尚未目睹真正的灾难性网络事件，但对手们越来越多地瞄准关键基础设施和数字供应链——这些关键路径的经济损失将更为巨大。其手段包括实施大规模攻击、在广泛使用的企业软件或薄弱的遗留网络安全协议中寻找漏洞来对多个关键计算机系统和数据进行加密以及中断基于云的服务等。

网络保障缺口巨大且持续存在

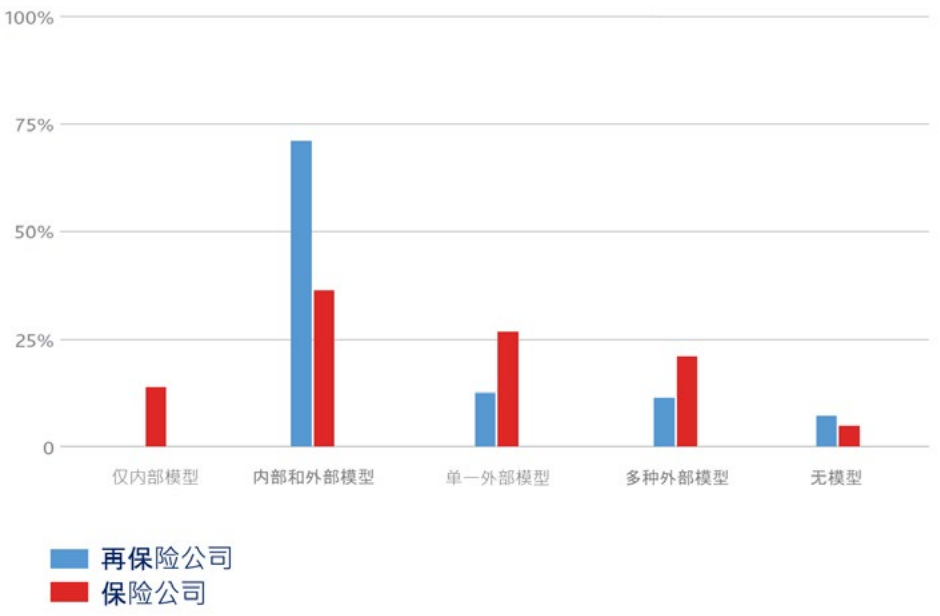
日趋恶劣的网络环境更加凸显网络风险带来的精算挑战。特别是人们对于网络损失发生频率和严重程度的驱动因素尚无深入理解，而且通常无法用常规统计方法对其建模。网络风险是一种人为风险，其损失的程度取决于受害者和攻击者双方的激励、动机和可用资源之间的相互作用，这往往涉及多个因素之间复杂的非线性关系。

在这种背景下，谨慎的保险公司以严格定义的合同措辞和有限的风险吸收能力承保网络风险，或许就不足为奇了。然而，随着企业、个人和政府越来越依赖数字技术，一次重大网络事件或攻击活动造成的总体成本持续增加。对网络犯罪每年造成的损失估计从约1万亿美元到高达8万亿美元不等，对比全球仅120亿至140亿美元的网络保费，这表明相当大一部分网络相关损失是没有保险的。

保险精算的进展

改进极端网络风险的量化方法，对于进一步扩大网络保险的规模和范围以及填补保障缺口至关重要。随着网络保险市场的发展和成熟，管理累积风险的承保实践也在不断发展。在对可能导致累积损失以及限制极端网络风险的因素有了普遍了解的同时，对灾难性网络风险建模和量化的新方法正在取得进展。同样，现在可以从各种来源收集到更多更高质量的数据和见解，这有助于构建网络风险全景图。这些关于不同威胁行为者以及他们的资源、动机和行为习惯的信息不仅可以揭示攻击的可能性，还有助于了解造成多个受害者的可能性和事件的严重程度。

图1: 保险/再保险公司对网络风险模型的使用(占所有公司的百分比)



基于52家拥有内部或特许外部模型的保险/再保险公司，以网络保险费加权

来源：日内瓦协会，基于*Gallagher Re*的数据

新兴的精算方法各不相同，但通常是三种主要类型的变化和组合：扩展频率-严重性模型、网络传播模型、专家主导的场景分析。许多保险/再保险公司现在使用正式的模型来支持他们对网络风险的评估，并帮助指导他们的风险管理。与拥有自己的内部模型相比，主要保险公司更倾向于依赖外部供应商（图1）。部分公司还会考虑多个外部模型，但在实践中，不同的模型设置使这一操作具有挑战性，而严格的许可安排意味着使用多个外部模型会过于昂贵。

然而，网络风险模型仍然不成熟，其结果可能是不稳定和不一致的。一些模拟分析显示，尽管这些估计对所采用的假设非常敏感，但从结果上看，一次罕见的全行业网络事件可能造成的保险损失与一些自然灾害大致相当。其他涵盖了更广义的网络相关索赔的确定性情景分析也表明，发生的灾难性损失可能是更大的。保险/再保险公司尤其警惕恶意软件攻击的巨大威胁，这种攻击会不加区别地影响许多公司或破坏关键的互联网架构（表1）。

表1: 保险/再保险公司对极端网络情景的排名

极端网络情景	平均排名
拒绝服务/中断操作	
蠕虫式恶意软件的流行	1
广泛的勒索软件攻击	2
大规模数据泄露	
关键组织/机构泄露敏感信息(PII、加密密码等)，对客户/供应商产生广泛影响	4
对关键基础设施的破坏	
对工业控制系统的监控和数据采集(SCADA)网络的勒索	4
对行业/部门关键参与者(如医院、食品制造商/分销商等)的网络攻击	5
对关键公用事业提供商(电力、水力等)的网络攻击	2
对州/市政服务的损害	5
跨部门的IT故障	2

指被调查者给出的排名得分中位数(1为排名最高的情景)。基于对日内瓦协会成员中11家网络保险/再保险公司的调查结果

来源：日内瓦协会

综合来看，这提示我们要谨慎看待任何来自一个甚至多个模型的风险指标。这也解释了为什么尽管网络积累模型被广泛用于风险评估，但迄今为止，它只被部分整合到了保险/再保险公司的承保和资本管理中。

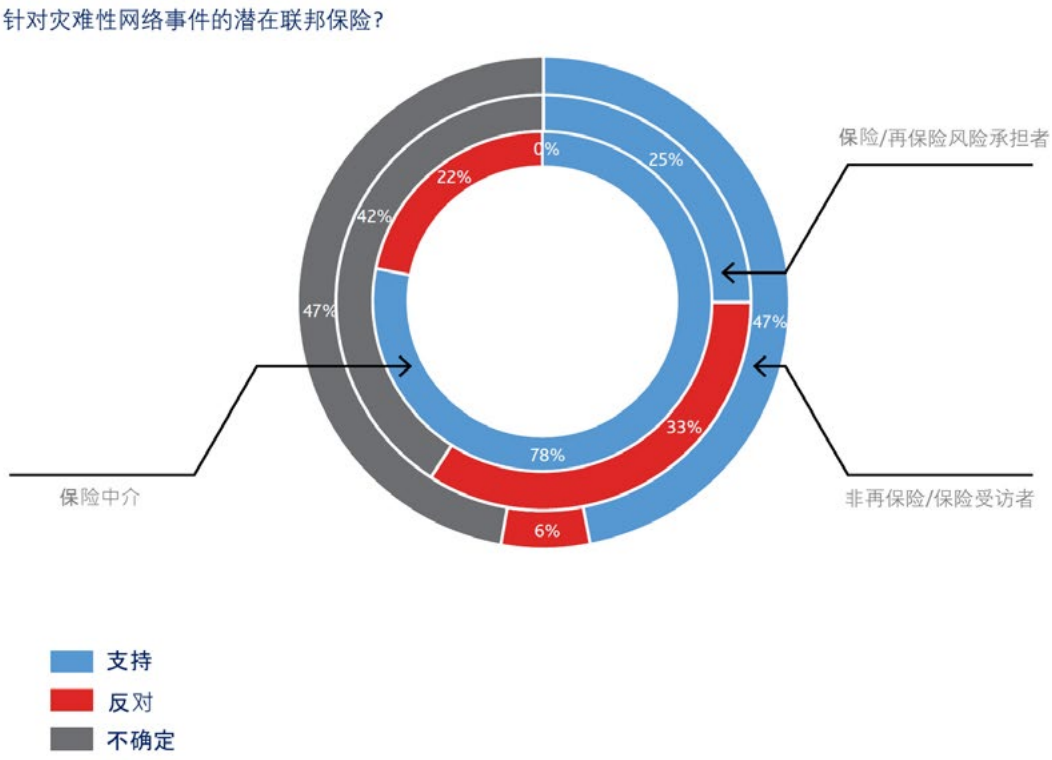
超越更好的模型

更好的风险建模虽然是必要的，但可能还不足以吸引大量额外的资本用于风险吸收。剩余的网络不确定性仍然存在，限制了可知的和能够可靠建模的内容，这降低了保险/再保险公司承保更大网络风险的意愿。因此，可能需要其他制度创新来建设一个更大的、可持续的网络保险/再保险市场，以满足投保人未来的保障需求。这些措施包括：

- 获取标准化索赔数据，协调有关网络风险和风险暴露的信息共享和知识交流。这可能涉及加强与关键利益相关者的合作，如政府安全机构和主要技术公司，他们可能对不断变化的网络威胁和漏洞有独特的见解。最近云服务提供商和保险/再保险公司之间的多个合作关系说明了这种合作的潜在好处。
- 建立机制，在网络风险承担者之间建立风险池，并通过创新工具将网络风险转移到资本市场，以更好地满足投资者的需求，并允许更大程度地转移网络风险峰值。最近的发展表明，网络保险相关证券(ILS)市场虽然很小，但正在趋于成熟，投资者的兴趣也在增长。
- 建立强化的法律责任制度，以激励IT公司开发更能抵御网络攻击的安全软硬件。这种方法是美国国家网络安全战略的核心支柱，旨在降低网络风险，并将网络安全不良的后果从最脆弱的人群身上转移。

最终，为了解决巨大的网络保障缺口，可能还需要政府融资来支持极端的保险/再保险损失。这可能会鼓励和支持保险/再保险行业承担更多的网络风险敞口，因为他们知道自己的下行损失是有限的。近期美国财政部一项公众咨询活动的回应表明，一些回应表示支持针对灾难性网络事件的联邦保险计划，或至少是在保险/再保险行业内和行业外进一步探索相关可能性。与此同时，相当大比例的回应者，包括保险公司，仍然表示无法确信针对网络的公私合作的保险安排在目前是一个合适的选择（图2）。

图2：对美国联邦网络风险保险机构的行业看法



基于55个不同的回复。代表不同组织提交的联合答复被分别计算。风险承担者中还包括代表保险/再保险公司的行业机构的回应，而中介机构指的是经纪人、评级机构和模型供应商的回应

来源：日内瓦协会对已公布的美国财政部咨询活动的回应的分析

质疑方（以及一些表示观点不确定的回应者）的一个共同想法是担心任何政府支持都可能产生意想不到的后果。这些担心包括政府支持可能会鼓励投保人在网络安全方面松懈，并削弱保险公司促进良好网络卫生和开发创新保险解决方案的动力。一些市场参与者还担心，政府提供支持会强制要求保险公司为所有网络风险提供保护，甚至是那些目前不可保的风险。

然而，由于纳税人最终可能会被要求承担网络灾难造成的巨额未投保损失的很大一部分，似乎唯一明智的做法是采取措施促进保险/再保险市场的运作，而不是在重大事件发生时应对其后果。如果设计、校准和实施得当，包括支付政府担保费用的保费，以及在重大网络事件发生后收回纳税人资助损失的程序，可以确保政府只对超过某个商定阈值的极端损失承担责任，同时还可以调整激励措施，促进网络保险的持续发展和普及，以增强社会复原力。