SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

众安科技

2022
网络安全保险科技白皮书

CYBER SECURITY INSURTECH WHITE PAPER

科技智绘网络安全保险新业态

COPYRIGHT STATEMENT

版权声明

出品方

上海赛博网络安全产业创新研究院

众安信息技术服务有限公司

编写组成员

惠志斌、秦峰、徐斌

周雪静、叶翔、张锐、余婷、金莹、郝暄霓、王文瑾、李秋娟

CONTENTS | 目录

Research Finding

概念界定

目前，业内将“网络安全保险”（Cyber Security Insurance）定义为：**保险人承保投保人因网络安全事件造成的经济损失或应承担的法律赔偿责任的保险**。然而，针对网络安全保险科技，国内外尚未形成明确的概念界定，一定程度上影响了这一产业的发展。本报告尝试首次定义“网络安全保险科技”，为网络安全保险产业的发展创新与变革奠定理论基础。

网络安全保险科技（Cybersecurity Insurance Technology；InsurTech）：**技术创新在网络安全保险产业发展及其与网络安全产业融合中的应用，将衍生新的模式、业务、流程与产品**。网络安全保险科技服务是面向投保人 / 保险公司 / 保险经纪公司，由第三方基于数据搜集、清洗整合，人工智能、云原生等技术创新应用，将保险与技术、风险工程和安全响应服务相结合，映射在投保、承保、理赔等保险环节，旨在通过科技融合保险业态与网络安全业态，以网络安全保险科技服务加强企业网络安全弹性。

网络安全保险科技模型

网络安全问题不同于传统工程问题，由于风险的变化性与规则的难以界定，网络安全领域的一大挑战在于缺少数据和模型来表述变量、制定策略。当前，围绕网络安全风险控制与管理，业界基于闭环控制、主动防御的动态安全理念，先后提出了 P2DR、P2DR2、IPDRR 等多种动态风险模型。

P2DR 模型是由美国 ISS 公司提出的动态网络安全体系的代表模型，其包括 Policy (安全策略)、Protection (防护)、Detection (检测) 和 Response (响应)。

P2DR2 模型同样以安全策略（policy）为中心，构造多层次、全方位和立体的区域网络安全环境。其包括 Policy (安全策略)、Protection（防护）、Detection（检测）、Response（响应）和 Recovery（恢复）。

IPDRR 模型 来自美国国家标准与技术研究所（National Institute of Standards and Technology；NIST）制定的 Cybersecurity Framework 的核心内容，包括 Identify（风险识别）、Protect（安全防御）、Detect（安全检测）、Respond（安全响应）和 Recover（安全恢复）。

通过对上述 3 个主要的网络安全模型的拆解，可以发现基本涵盖了安全策略、风险识别、安全防御、安全检测、安全响应及安全恢复 6 大模型因子。相关模型因子与网络安全保险相关配套服务能力进行绞合，进而可以形成一个新型的“网络安全保险科技模型”（InsurTech–PIPDR2），从而推动网络安全保险能够相对无感知地嵌入企业网络安全建设各个部分。

表 0–1 网络安全保险科技模型与网络安全模型的交叉对比

模型因子	P2DR 模型	P2DR2 模型	IPDRR 模型	网络安全保险科技模型 InsurTech-PIPDR2
安全策略 (Policy)	风险识别与评估。确定业务优先级、梳理风险、影响评估、安全资源优先级划分			制定保险风险策略
风险识别 (Identify)			风险识别与评估。确定业务优先级、梳理风险、影响评估、安全资源优先级划分	梳理企业残余安全风险
安全防御 (Protection/ Protect)	借助安全产品、技术、培训等举措预防安全事件的发生		保证业务连续性。在受到攻击时，限制其对业务产生的影响。主要为人为干预前的自动化保护措施	基于风险评估报告，制定整改建议，并针对保险风险进行承保，限制风险对业务产生的影响
安全检测 (Detection/ Detect)	检测和监控网络系统，发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能将与防护系统形成互补		在攻击产生时即时监测，同时监控业务和保护措施是否正常运行	实时监测扫描潜在风险与攻击行为
安全响应 (Response/ Respond)	紧急响应和恢复处理（系统恢复和信息恢复）	在安全策略指导下，通过动态调整访问控制系统的控制规则，发现并及时截断可疑链接、杜绝可疑后门和漏洞，启动相关报警信息	事件调查、评估损害、收集证据、报告事件和恢复系统	风险响应与处置
安全恢复 (Recover)		恢复系统、再现攻击行为	恢复系统和修复漏洞，并进行预防和修复	出险理赔

从企业网络安全建设的角度来看，网络安全保险科技模型可以与大多数企业网络安全防御体系进行有效适配，并在运营过程中实现持续改进。

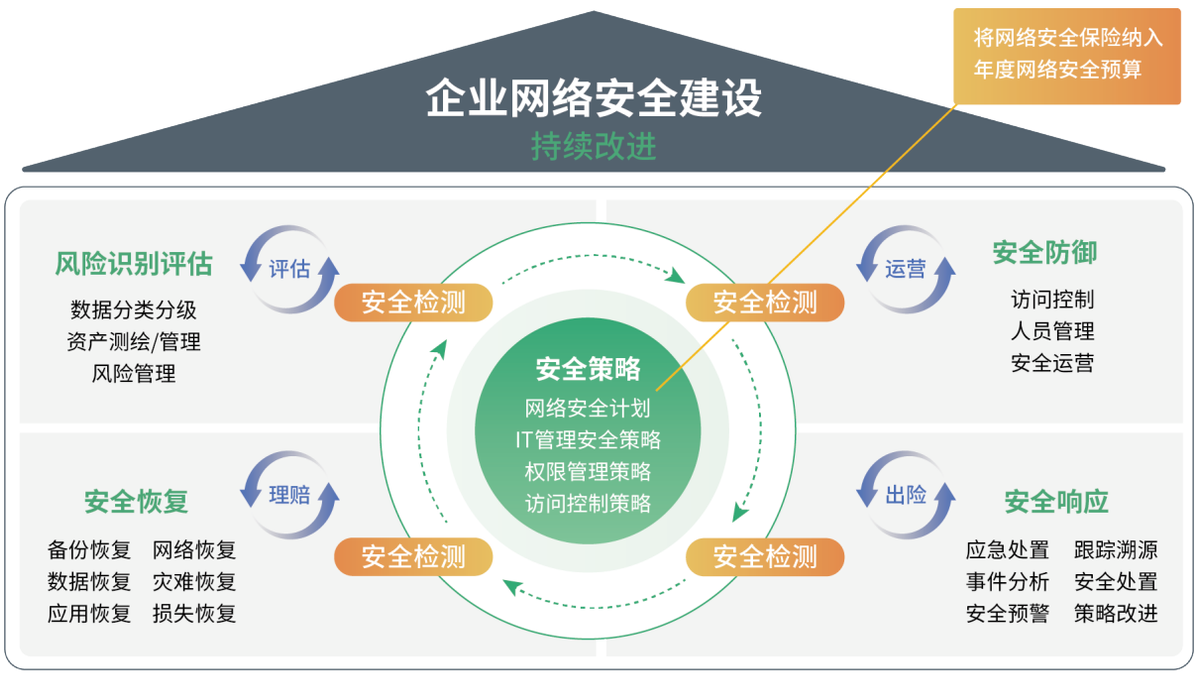


图 0–1 网络安全保险流程在企业网络安全建设体系中的呈现

在安全策略阶段，企业设计顶层网络安全策略、制定网络安全计划时，可以将网络安全保险作为风险转移的重要举措，纳入网络安全计划，并在规划年度网络安全预算时，将网络安全保险作为拟采购的安全服务考虑其中。

在风险识别阶段，基于企业已部署的漏洞扫描、资产测绘等网络安全设备 / 技术，网络安全保险科技服务提供的风险识别与评估能力将从网络安全保险的视角，对残余安全风险进行二次筛查，梳理出可保险风险（尚未发生的或使保险对象遭受损失的风险，通过企业网络安全体系建设、网络安全设备和现有的安全举措暂时无法完全覆盖或解决的风险，安全投入产出性价比低的风险，即被视为可通过保险方式转移的保险风险范畴），进而将风险评估结果通过量化、定级等方式，转化为核保依据与定价参考。

在安全防御阶段，基于风险评估结果，协助企业制定整改建议，从而对企业面临的可控风险进行事前主动干预，通过安全产品、技术、培训等举措预降低企业出险概率。

在安全检测阶段，通过实时风险监测系统重点监测承保范围内的网络安全风险，不仅可以进一步加强企业的风险发现能力，使其成为企业风险监测系统中的重要组成部分，还将为后续理赔阶段提供取证支撑。

在安全响应阶段，围绕承保风险，企业可依托于网络安全保险科技服务，借助第三方安全力量实现对安全事件的快速响应，开展事件调查、损害评估、取证报告等工作，从而为下一阶段的理赔提供参考基础。

在安全恢复阶段，企业可基于溯源调查结果，通过其原有的安全技术及能力进行系统恢复和漏洞修复，并优化安全运营。此外，依托于网络安全保险科技的配套理赔服务，保险公司能够快速完成保险义务，赔偿投保企业的直接经济损失、第三方责任赔偿及备份 / 数据恢复等所产生的费用，帮助企业在收敛风险的同时成功完成风险转移。

网络安全保险科技图谱

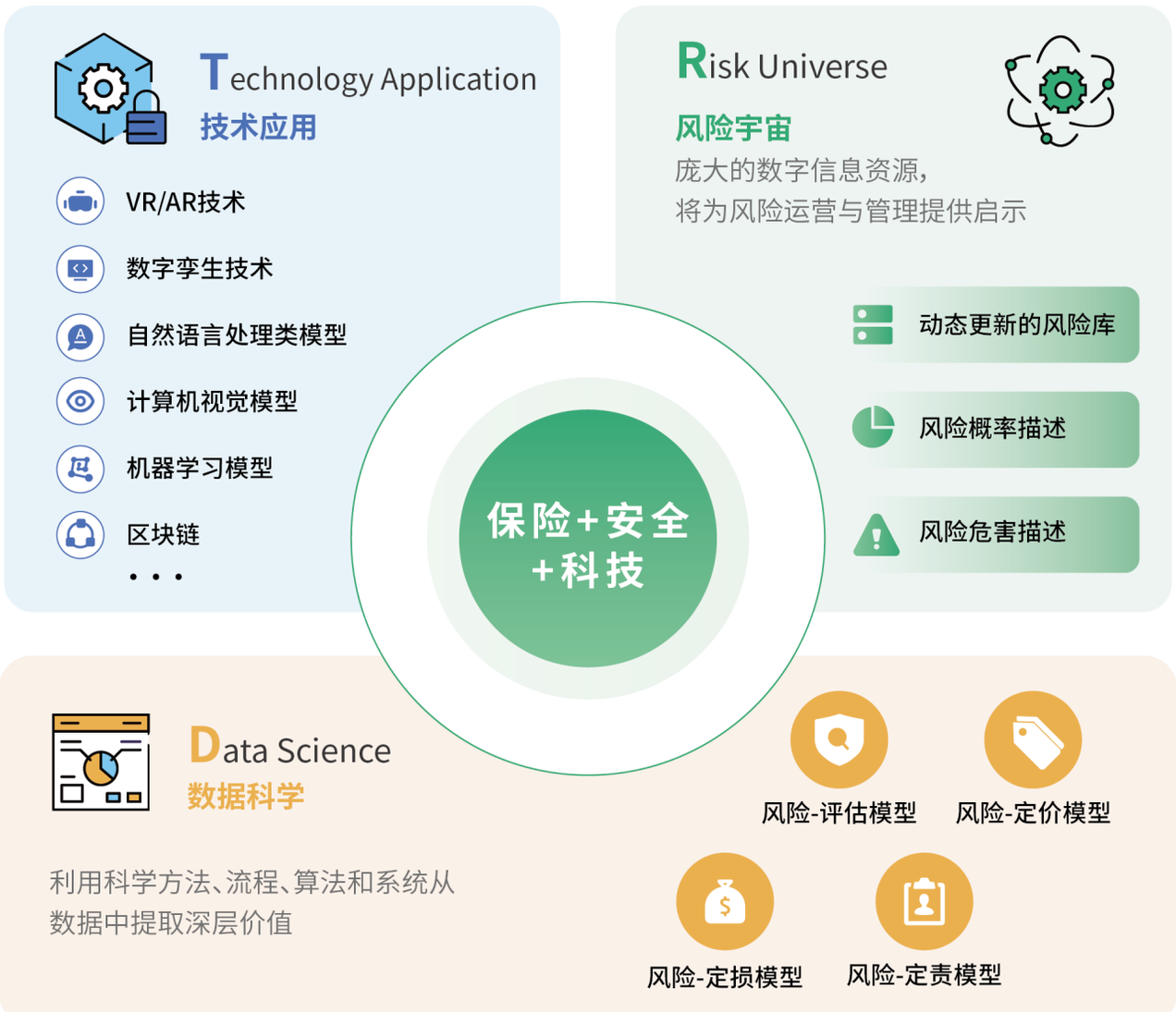


图 0–2 网络安全保险科技图谱

网络安全保险科技图谱立足于“保险 + 安全 + 科技”的新型服务模式，网络安全保险科技企业则围绕风险宇宙、数据科学及技术应用三个方向构建科技实践体系。这也是网络安全保险有别于传统财产险的主要方面。

PART 1
全球网络安全保险发展现状

网络安全保险作为一项投保险种，早在 20 世纪 90 年代就伴随着 IT 网络的发展及安全风险的再配置与转移而诞生。经过 20 余年全球数字化经济市场发展、网络技术更迭，网络安全保险已经成为数字市场经济条件下重要的风险管理和风险转移手段。

目前，囿于全球 IT 网络发展的起步时间不一、发展进程不对称，网络安全保险在各国各地区存在不同的市场成熟度与社会普遍接受度。其中，我国在网络安全保险行业正处于发展前期，并开始进入风口阶段。与此同时，借助科技手段，跨行业、跨领域开展网络安全保险，成为保险行业发展的又一市场增长点，有潜力挖掘一个千亿乃至万亿级的蓝海市场。

1.1 产业发展：风险与破局

风险是驱动企业投保的首要动力。企业在经营过程中，会面临内部风险和外部风险，前者包括战略风险、财务风险、运营风险、操作风险，后者包括法律合规风险、技术风险、市场风险、产业风险等。若要保证企业网络安全，就要将企业可能存在的人为、系统安全、操作风险等多重运营风险及法律合规风险降低到可控的范围之内。随着网络攻击、网络安全违规事件的频繁发生，企业为维护正常经营，除加强自身防火墙、加密与认证、网络入侵检测等安全基础设施建设之外，从成本收益优化的目的出发，也会购买网络安全保险进行增强防护。可以说，安全基础设施建设是风险缓解的主要措施，而网络安全保险是风险转移的最佳选择，两者的结合成为企业安全最高效的投资组合。

保险层面，以往其他财产保险的承保范围越来越无法全面、有针对性地保护企业免受网络风险侵害。为减少网络风险带来的巨额攻击损失和合规成本，网络安全保险应运而生。从网络安全保险推出至今，投保规模随着网络技术的飞速发展而不断增长。据 Research And Markets 发布的《2022 年全球网络安全保险市场报告》显示，2021 年网络安全保险市场规模为 92.9 亿美元，2022 年约为 119 亿美元，预计到 2027 年将达到 292 亿美元，年复合年增长率 19.47% ，体现出巨大的市场需求和发展空间。可以预见，随着万物互联、IT 劳动力短缺，全球网络安全保险市场规模将进一步爆发。

（1）网络安全保险产业发展历程

在过去 30 年时间里，全球的网络安全保险产业发展经历了起步、逐步发展和快速上升三个阶段。

20 世纪 90 年代，全球网络安全保险进入萌芽阶段，保险公司和安全企业的合作模式初步确立。在发展初期，网络安全保险的主要模式是通过保险为安全公司的服务增信，同时为用户提供涵盖保险服务的全面风险管理解决方案。**在这个时期，保险的承保范围仅涵盖对第一方损失（企业自身经营风险）的保障，主要存在投保企业获客渠道受限**，风险分散能力、量化能力薄弱，客户网络安全风险意识淡薄和法律法规缺失等问题。

21 世纪 10 年代，网络安全保险进入初步探索阶段。随着企业合规要求的提高以及企业风险意识的提升，网络安全保险产品也逐渐完善优化。一方面，合规政策推动了网络安全的发展。一系列网络安全法律法规的出台和监管政策的强化执行，使网络安全保险的投保需求得到释放。保险公司也推出综合险的产品，将第一方损失和第三方损失均纳入了承保范围。另一方面，企业的安全意识也在逐步提高。在网络安全事件频发、经济损失持续攀升的背景下，企业对网络安全风险防御的逐渐重视驱动企业进行投保。在这个阶段，行业发展更多地面向企业的风险管控需求，**将保险服务和专业技术手段结合起来**，实现对全流程风险敞口的管控。

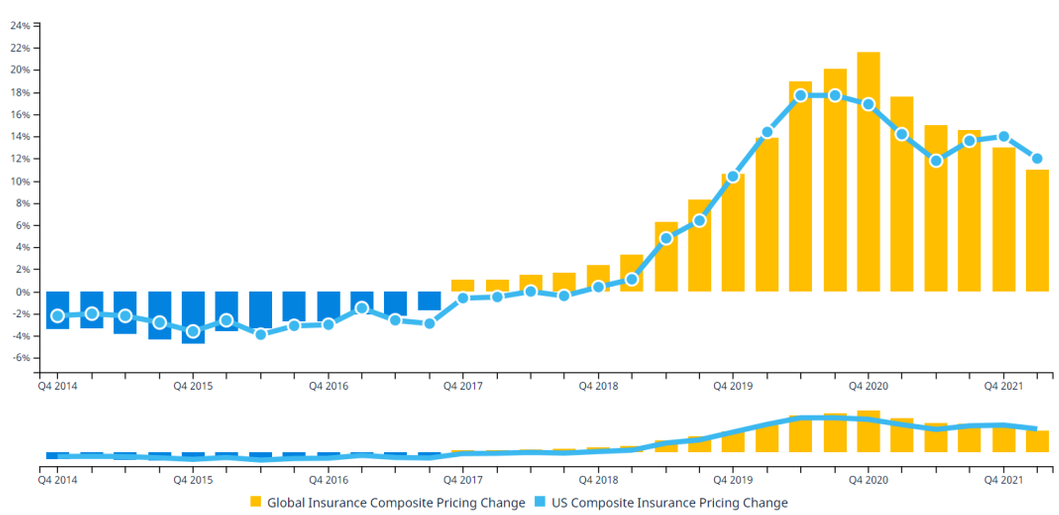
2013 年至今，全球的网络安全保险进入快速上升阶段。欧盟《通用数据保护条例》（General Data Protection Regulation，简称“GDPR”）的生效进一步强化了数据主权的保护、加大了行政处罚的力度，并且拉动了网络安全保险需求。同时，**第三方风险管理技术服务机构开始出现，保险科技公司和网络安全公司崭露头角**，围绕风险量化、保险定价、合作模式等问题进行重点发展。其中，保险科技公司负责数据收集分析、差异化保险定价、风险源头全面监控，网络安全公司负责通过漏洞扫描、威胁发现，利用专业手段协助客户方抵御安全风险。在保险服务和网络安全科技的融合助推下，网络安全保险的核保、承保可靠性提高，投保需求持续上涨，推动我国网络安全保险市场向更高水平开放、促进保险与科技双向赋能。

（2）国内外网络安全保险主要市场

欧美市场：

欧美的网络安全保险市场起步较早，目前发展较为成熟。美国是网络安全保险的最大市场，占全球份额的 90% 以上；欧洲的网络安全保险市场虽然起步比美国晚，但近几年网络安全事故的频发，也加快了欧洲网络安全保险发展与成熟的脚步。

美国方面，2021 年 5 月，美国政府问责局发布了保险经纪公司达信（Marsh）的数据，显示各行业客户购买网络保险的比例从 2016 年的 26% 上升到 2020 年的 47%。此外，2022 年第一季度，美国保险的网络定价上涨了 110% ，索赔活动的频率和严重程度的提高大大拉动了价格的上涨，超过 60% 的保险客户采取了更高的留存率来帮助抵消保费影响。网络安全保险公司也重点关注公司的风险控制环境和网络安全成熟度从而决定是否承保。欧洲方面，数据提供商 Statista 预测其网络保险市场在 2020 年至 2030 年间将呈指数级增长，在 2020 年至 2025 年间规模翻一番，年平均增长率约为 20%。



总的来说，目前欧美网络安全保险市场呈现出法律法规促进投保需求释放、专业机构指导网络安全保险规范发展、产业主体合作探索网络安全保险发展路径的特点 。

首先，立法层面的引导和监管拉动了网络安全投保需求。从发展驱动因素来看，全球已有超过 15 个国家和地区发布了超一百部的网络和数据安全相关法案，包括美国《计算机欺诈和滥用法》《消费者数据保护法》《统一个人数据保护法》、欧盟《通用数据保护条例》《网络安全法案》《数据治理法案》《数据服务法案》《数据市场法案》、德国《联邦个人信息保护法》《联邦数据保护法》《IT 安全法》、英国《国家网络安全战略 2022–2030》、法国《法国国家数字安全战略》在内的法律法规陆续出台和完善，强化了各国的行业监管。巨额罚款乃至刑事处罚的威慑撬动了企业的网络安全合规需求。以 GDPR 为例，截至目前为止罚款总额已超过 16 亿欧元，单次最大罚款达 7 亿欧元之多。因此，除加强自身网络基础设施建设外，企业也将目光投向了能够抵御法律合规风险的网络安全保险上来，激发了网络安全保险市场活力。

其次，政府部门联合行业协会等组织建立产业规范，开展网络安全保险政策研究，强化风险应对能力。例如，美国纽约州金融服务部发布《网络保险风险框架》，提出网络安全保险的七步流程，为保险公司业务的开展提供指南。欧洲保险和职业养老金管理局制定“网络承保战略”，指明网络风险监管优先事项，并鼓励优秀产业实践应用推广。德国保险协会也为中小企业制定了标准化网络安全保险保单模板，目前已被国内约 50% 的保险公司采用。

第三，产业主体合力探索，推动网络安全保险发展。一是明确承保范围、引领市场规范化发展。例如，欧洲保险公司劳合社于 2016 年发布《劳合社网络攻击风险应对战略》，要求旗下保险公司明确网络安全承保范围，促进市场规范化发展。二是促进数据共享、优化保险模型。欧洲保险和职业养老金管理局于 2021 年发布《开放式保险：访问和共享保险相关数据》一文，提倡建立“健全的开放式保险框架”、开放访问及共享保险数据，扩大网络保险保费数据获取途径。另外，伦敦大学学院教授亨利·斯科奇（Henry RK Skeoch）在 IT 安全技术领域期刊《Computers & Security》上发表文章称可以基于戈登 – 洛布（Gordon–Loeb）模型构造竞争性网络安全和投资决策的 GL–CI 保险模型，以便更科学地确定保险索赔概率。三是探索创新发展模式、发挥人工智能等技术优势。例如利用 AI 技术强化分析能力，生成实时监测图景，提高决策的速度和准确性；以及实现常规风险的选择、定价和欺诈检测自动化，从而降低赔付率与恢复费用 。

中国市场：

我国网络安全保险产业起步较晚，存在企业投保需求受众还需进一步激活、保险公司风险把控能力还需提升、网络安防技术尚待与保险评估定损流程相匹配等问题。

然而，伴随着网络安全系列法律法规的实施落地、重要行业领域网络安全顶层设计的密集出台，我国网络安全保险产业已迎来发展机遇期。根据中国工业信息安全发展研究中心基于头部财产保险公司网络安全保险保费数据以及行业集中率测算，2021 年我国网络安全险保费规模达到 7080 万元，最高保额超 4 亿元，较上一年增长 3.2 倍以上，呈现高速增长的态势。

目前我国网络安全保险市场具有发展环境持续优化、保险业与网络安全产业主体融合探索、网络安全风险投保需求逐渐上升的特点。

一是网络安全保险受到政府部门的高度关注。

国家层面，《网络安全法》《数据安全法》《个人信息保护法》陆续颁布实施，使我国网络安全法律体系框架基本搭建完成；行业主管部门层面，围绕政策制定、产品开发、服务模式创新等方面进行了积极探索与规则细化（详见“1.2 政策培育：加快试点探索”表格 1–1）。

二是保险公司开始网络安全保险“本土化”尝试，开发多种网络安全保险产品，与网络安全科技企业融合发展。例如，众安网络安全保险面向不同行业、场景的差异化网络安全风险管理需求，推出了不同层次的网络安全保险产品矩阵，服务各体量类型客户的投保需求；同时，为企业提供基于保险的主动安全合规、主动风险管理、主动安全运营的一站式服务，助力企业在数字经济时代提升数字化资产安全防护水平和风险对抗能力。

三是数字化转型深入推进，网络风险的防护意识不断提升。随着网络安全保险的落地案例逐渐增多，一些重点行业的投保需求逐步提高。例如易遭受网络攻击的金融、制造业企业，关键信息基础设施运营单位，外资、合资或具备海外业务的中资企业，为了规避网络攻击造成的巨大经济损失风险、寻求风险转移，都将有越来越强烈的网络安全保险购买意愿。

1.2 政策培育：加快试点探索

我国的网络安全保险产业呈现出起步晚、发展快的特点。产业的快速发展不仅源于需求侧的增长，也得益于相关政策的引导培育。“国民经济和社会发展十四五规划和 2035 年远景目标纲要”提出，要壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，催生新产业新业态新模式。2022 开年之际，我国监管部门先后发布《银行保险机构信息科技外包风险监管办法》《金融科技发展规划（2022–2025 年）》《关于银行业保险业数字化转型的指导意见》《金融标准化“十四五”发展规划》等一系列文件，明确了保险数字化转型的目标和任务，为保险创新发展提供坚实的政策基础，促进保险服务进入数字化新周期。

与此同时，聚焦试点探索起步、政府规范引导、相关标准出台、安全即服务趋势加强等发展特点，为更好地保障企业的网络安全、推进网络安全保险规范运营、夯实网络安全保险保障工作基础，各相关部门也在上述政策的指导下，接连出台了一系列关于网络安全保险的指引性文件。

表 1–1 近年来我国政府部门发布的部分网络安全保险相关政策及文件

发布时间	部 门	文 件	内 容
2022 年 7 月	中国银保监会、上海人民政府	《关于印发中国（上海）自由贸易试验区临港新片区科技保险创新引领区工作方案的通知》	鼓励保险机构加强与网络安全领域科技企业的合作，创新网络安全保险服务模式，促进网络安全产业与保险业共赢发展，为企业提供安全、可靠的网络环境。提倡发展“保障 + 风控 + 服务”三位一体的新型网络安全保险，集保险与网络安全企业合力，为企业研发综合性的保险解决方案。

表 1–1 近年来我国政府部门发布的部分网络安全保险相关政策及文件

发布时间	部 门	文 件	内 容
2022 年 6 月	公安部	《关于落实网络安全保护重点措施 深入实施网络安全等级保护制度的指导意见》	探索开展网络安全保险。研究网络安全保险相关政策和标准规范，共同培育市场，试点先行，构建“保险 + 风险管控 + 服务”模式，提升网络安全社会治理能力。
2021 年 12 月	上海市经济信息化委 市委网信办市发展改革委市科委市财政局 市通信管理局	《上海市建设网络安全产业创新高地行动计划（2021-2023 年）》	1）推进安全服务化布局，倡导“安全即服务”理念，鼓励企业设立安全运营服务中心，由提供产品向提供服务和解决方案转变。引导党政部门和重点企事业单位提升网络安全服务采购比例。 2）培育面向网络安全领域的商业保险技术、产品、管理和服务创新能力，构建覆盖多层面的保险服务机制，培育事前预防、事中防护、事后补偿的全周期网络安全保险服务保障模式。
2021 年 9 月	上海市经信委和银保监局	/	成立网络安全保险专班。
2021 年 7 月	工信部	《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》	1）应强化产融合作机制建设，探索开展网络安全保险，加快网络安全保险政策引导和标准制定，强化网络安全风险应对能力。 2）面向电信和互联网、工业互联网、车联网等领域，开展网络安全保险服务试点。
2020 年 12 月	中国银行保险监督管理委员会	《互联网保险业务监管办法》	共 5 章 83 条，包括总则、基本业务规则、特别业务规则、监督管理和附则。重点内容包括：一是厘清互联网保险业务的适用和衔接政策；二是规定互联网保险业务经营要求；三是规范互联网保险营销宣传；四是规范互联网保险售后服务；五是按经营主体分类监管，规定“特殊业务规则”；六是完善监管政策和制度措施，做好政策实施过渡安排。
2020 年 7 月	中国银保监	《推动财产保险业高质量发展三年行动方案（2020—2022 年）》	支持财产保险公司制定数字化转型战略，加大科技投入和智力支持，打造具备科技赋能优势的现代保险企业。鼓励财产保险公司利用大数据、云计算、区块链、人工智能等科技手段，对传统保险操作流程进行更新再造，提高数字化、线上化、智能化建设水平。
2019 年 9 月	工信部	《关于促进网络安全产业发展的指导意见（征求意见稿）》	探索开展网络安全保险服务。

表 1–2 近年来我国行业组织发布的网络安全保险相关团体标准一览

发布时间	部 门	文 件	内 容
2022 年 6 月	上海市信息安全行业协会	《网络安全保险服务技术要求》（征求意见稿）	技术要求共包括十章，分别为范围、规范性引用文件、术语与定义、缩略语、概述、保险服务基本规定、承保前风险评估要求、承保中风险管控要求、事件发生后应急处置服务要求、保险理赔服务要求。此外，标准中还包括附录 A，内容为保险安全服务流程。
2022 年 6 月	上海市信息安全行业协会	《网络安全保险安全服务能力评价指南》（征求意见稿）	评价指南共包括六章，分别为范围、规范性引用文件、术语与定义、网络安全保险服务特点、网络安全保险信息安全服务提供方基本要求以及评价程序。同时，标准中还包括附录 A，内容为网络安全保险安全服务评价指标。
2022 年 5 月	上海市保险同业公会	《网络安全保险服务规范》（征求意见稿）	是保险行业首个针对网络安全保险服务规范标准，规定了网络安全保险服务的服务基本条件、服务提供过程以及服务质量评价和改进，形成了网络安全保险承保、风控、理赔服务的统一标准要求。
2022 年 3 月	中国网络安全产业联盟	《面向网络安全保险的风险评估指引》	评估指引引导保险机构结合投保人网络安全保险风险评估的实际情况，对业务、资产、威胁、脆弱性分别进行计算，最终得出一个具体的风险分值，并在风险分值的基础上，再划分风险等级。风险分值与风险等级用于评判、衡量拟投保保险标的网络安全风险状况。
2021 年 11 月	中国网络安全产业联盟	《网络安全保险安全风险评估实施指南》（征求意见稿）	试图通过建立一套风险评估指标、流程、内容，规范对拟投保系统的风险评估，得出风险等级、风险分值，定量化地呈现拟投保系统网络安全风险状况，为后续开展网络安全保险业务提供参考依据。

PART 2
网络安全保险多元市场需求

需求是产业发展及创新的首要生产力，网络安全保险的发展则离不开其背后的多层次需求。聚焦成本收益、行业需求、商业场景需求等多角度，探究网络安全保险市场需求本质，以中微观视角建立风险认知，为企业是否应该选择网络安全保险、开展风险控制工作提供前置视角。

2.1 网络安全保险的需求本质

目前，在网络安全空间的威胁与防御保持持续对抗、水涨船高的状态下，企业无法通过某一个策略、产品或技术全面消除所有风险。因此，安全建设成为企业面临的一项长期性、持续性工作。当前企业的防御视角以风险管理、风险控制为主，通过调整组织架构、完善管理机制、采购或部署安全产品构建综合防御体系，最终形成涵盖扫描、检测、溯源处置的防御链条。

然而，即便企业开展大量的安全建设工作以提升网络安全成熟度，复杂且层出不穷的安全风险仍然无法穷举、无法被彻底消除。面对残余安全风险，越来越多企业将视线转向了“风险转移”——即容忍一定风险，并通过保险手段转移风险。

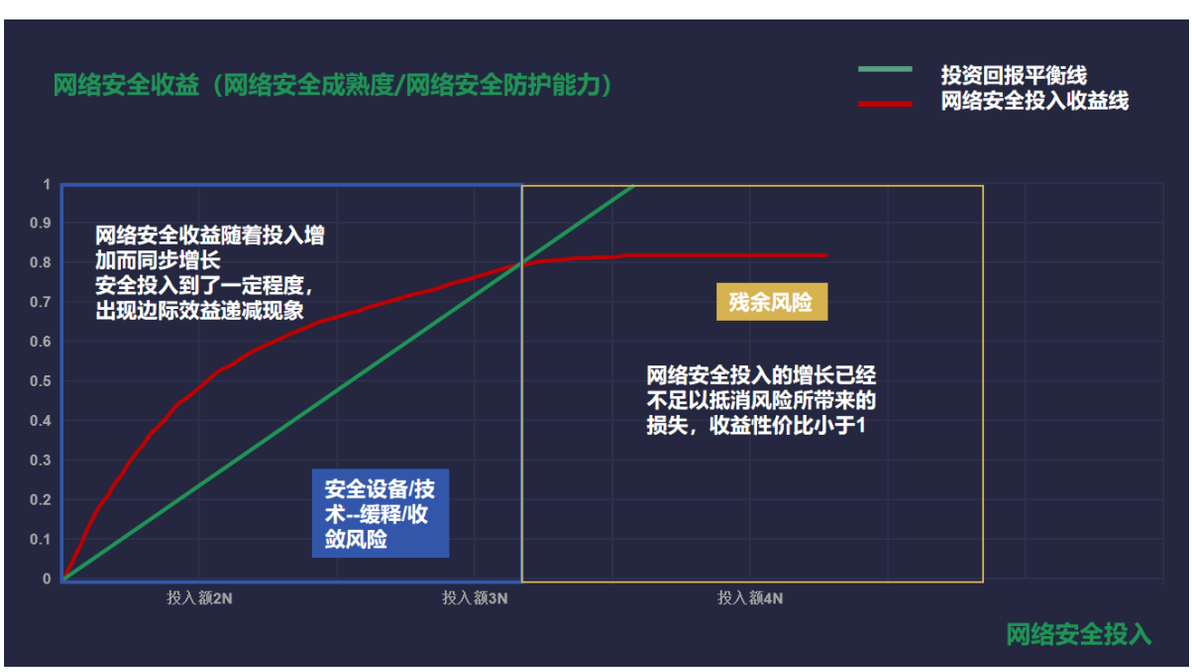


图 2–1 网络安全投入收益比

企业网络安全建设的本质不仅仅是安全问题，也是成本收益问题。而网络安全保险需求的本质也不仅仅是风险转移，还包含成本收益的衡量。风险意味着潜在损失——财产损失、名誉损失、商业价值等次级损失，而安全建设是为了以更低的成本规避风险带来的更大潜在损失。图 1 的横坐标为网络安全投入，纵坐标为网络安全收益，以投资回报平衡线为基准，企业在网络安全方面投入的增长呈现明显的边际效用递减趋势。当企业网络安全建设成熟度达到较高的水准时，企业面对残余性风险，可以选择继续加大网络安全投入。虽然仍有一定效果，但从收益性价比而言已经低于基准。这一阶段往往是企业选择网络安全保险的一个比较适当的时期，也说明当网络安全投入已经不足以抵消风险所带来的损失时，网络安全保险就成为了企业更加适宜的选择。

另外，根据敏感性分析显示，企业损失规模越大，越倾向于使用保险策略而非安全投入策略；根据收益分析显示，企业网络安全投入越大，越倾向于采购网络安全保险覆盖残余安全风险。因此，总体来看，网络安全保险作为风险转移、风险分散的重要举措，其本质上与企业原本的网络安全建设工作并不排斥，而正是企业安全建设的补充手段。

2.2 风险视角下的行业需求

随着企业数字化转型的深入，各行各业均充斥着大量已知和未知的网络安全风险。安联《2022 年风险晴雨表》指出，勒索软件攻击、数据泄露、远程办公导致的 IT 漏洞和云平台数据供应链中断是企业最为担心的 4 类网络风险 。Coalition 公司《2022 年网络安全保险索赔报告》也提出，2021 年下半年攻击者对该公司投保人提出的平均赎金要求增加了 20%，索赔率增加了 10%，小型企业受到的影响尤为严重 。

事实上，除了高频次的主要网络风险，不同行业也遭受着更具针对性的行业攻击。譬如电信互联网行业普遍面临 DDoS 攻击、网络钓鱼、网络黑灰产（撞库）等风险，工业互联网行业存在工控系统漏洞和设备后门、工业通信协议缺陷、供应链攻击等风险，车联网行业则遭受了车载信息交互系统漏洞、通信安全、配套设施（App）安全等隐患，医疗行业难免门户网站篡改风险、应用服务高危端口与安全漏洞和以勒索病毒为代表的恶意程序风险。若不加防范，上述风险还会继续导致数据被未经授权访问、泄露、丢失等次级风险，引发业务中断、成本损失。

（1）电信和互联网行业

DDoS 攻击：电信和互联网行业是遭受 DDoS 攻击的重灾区，目前 DDoS 攻击的类型多样，包括流量型 DDoS 攻击（如 SYNFlood、UDPFlood、ICMPFlood、ACKFlood 等）、应用层 DDoS 攻击（如 HttpGetFlood、CC 攻击等）、慢速 DDoS 攻击以及基于漏洞的 DDoS 攻击等，攻击往往出于敲诈勒索、恶意商业竞争、炫耀式攻击等原因，通过攻击穷尽目标的服务器或带宽资源，导致其服务被迫暂时中断或停止，使正常用户无法访问，进而对目标企业的经济和名誉造成损害。

伴随 DDoS 攻击的逐渐产业化与服务化，各种在线 DDoS 平台、肉鸡交易渠道层出不穷，“僵尸网络”的低价出售成为趋势，恶意个体实施 DDoS 攻击的门槛逐渐降低，为电信互联网行业带来了更大的威胁。

网络钓鱼：人往往是企业安全的薄弱点，也是

网络钓鱼攻击的锚点。Facebook 和 Google 在内的诸多互联网公司一直是网络钓鱼攻击的重点目标。从鱼叉式网络钓鱼到商业邮件欺诈，网络钓鱼的方式多样且结合时事热点，充分利用人性漏洞，引导错误操作。包括将发件人伪装成受害者信任的个体或组织，将邮件主题设置为热点事件或工资单等与受害者息息相关的内容，将邮件附件植入病毒。一场针对企业员工的网络钓鱼攻击，将引发凭证泄露、后门植入乃至系统入侵，使企业资产、内部信息暴露在攻击者的面前，最终造成企业内部数据泄露，业务中断等风险。

撞库：撞库是网络黑灰产的一种类型，也是电信企业、电商等互联网企业面临的高风险之一。攻击者通过弱密码嗅探、拖库、对高权限账号的暴力破解等方式获取数据。以拖库为例，由于大多数人倾向于在多个站点上使用相同密码，因此攻击者首先通过编写恶意程序对服务型网站发起攻击，获取大量用户信息，再基于大量的用户信息生成对应的字典表，从而对其他相关站点进行试探性登陆。一旦用户在其他站点上使用了相同密码，这也意味着撞库的成功——攻击者再次获得更多的用户信息。一旦攻击者通过撞库方式获得高价值的用户信息，其很可能将实施二次危害，譬如破解金融账户，窃取或转移受害者账户上的资金；出售用户账号、密码及其他个人信息，使用户遭受短信轰炸式营销、电信诈骗；利用用户账号推广非法业务、贩卖违法物品、承接刷量业务等活动，从而进一步延长不法获利链条，谋取更高额的非法收益。

随着黑灰产的产业链上下游分工精细、规模和技术提升，企业防御撞库的难度也在增长。被撞库的企业虽为受害者，但因其自身安全控制不到位却成为“雪球效应”中的一分子。

（2）车联网行业

车载信息交互系统漏洞：车载信息交互系统安全与车机自身的网络安全息息相关。由于部分车辆的车载网络数据加密和消息验证机制不完善，一旦攻击者发现系统漏洞、侵入车载网络设备，就会针对漏洞进行跳板式攻击、植入病毒程序，干扰车内部件功能，造成车载信息交互系统的网络瘫痪、硬件故障，并泄露车主信息和出行记录，甚至影响车辆驾驶安全。

车载信息交互系统由远程信息处理器（T–BOX）和车载信息娱乐系统（IVI）组成，主要提供对外通信、远程控制、信息采集、定位防盗以及影音娱乐等功能，是车主行车时最为常用也较容易遭遇攻击的车内配件。

通信安全风险：伴随车辆连通性的极大扩展，自动泊车、导航定位等功能已逐渐成为汽车的标配。这就为攻击者利用车辆通信系统内的身份认证或数据加密缺陷发起攻击提供了更多机会。例如，车辆通信系统一般缺乏对信息发送者身份的验证机制，难以抵御攻击者伪造身份进行的动态劫持；若信息在通信过程中加密强度不足，很可能被攻击者趁势伪造、篡改、窃取，使汽车无法识别恶意软件，从而破坏车辆通信系统，阻断车主获取正常服务的途径。

车辆的通信安全主要包括车内通信安全和车外通信安全。前者是指远程信息处理器与车内主机的双向数据传输安全，负责车辆状态信息、控制信息等的传输，通过 CAN 总线、车载以太网等技术实现车辆内部系统和设备间的通信；后者是指远程信息处理器与云平台间的双向数据传输安全，通过车载诊断接口（OBD）、无线通信技术（WiFi、蓝牙、4G/5G、C–V2X 等）与外部实体和平台进行信息交互。

配套设施（App）安全：配套设施是指车企为用户提供数字化服务、增强用户粘性而配置的 App 程序。然而，智能网联汽车端 App 普遍存在缺乏安

全保护机制的问题。大部分车辆并未对未知或来源不明的 App 进行限制，甚至还保留了浏览器的隐藏入口，部分采取软件防护机制的 App 也存在防护强度不够的问题。攻击者一旦登录 App 内部，就可以轻松获取用户的个人信息、获取到根用户权限。这就导致攻击者可以在后台下载恶意软件、破解通信协议、反编译代码、窃取用户数据，使车主失去 App 的控制权。如果配套 App 还涉及车辆控制功能，甚至可能存在车辆被远程恶意控制的风险。

（3）工控行业

工控系统漏洞和设备后门：在工业互联网中，工控系统作为关键信息基础设施的组成部分，已经成为黑客攻击的主要目标之一。传统的工控系统在设计之初通常缺乏安全考虑，因此往往存在安全配置基线未加固、大量安全漏洞与后门存在等问题。伴随工业互联网的发展，工业生产环境中的智能设备与 IT 网络、办公网络互联，原本封闭可信的工业生产环境被打破，安全风险进一步暴露。与此同时，一旦生产控制层的信息安全风险被恶意利用，攻击者极有可能以此为跳板，进行横向移动，对核心生产数据造成破坏。

工业通信协议缺陷：工业通信协议是工业互联网中通讯双方控制数据传输的协议，用于实现数字设备与网络之间的连接和信息传递，其主要有 Modbus 通信协议、RS–232 通信协议、RS–485 通信协议、HART 通信协议、MPI 通信、PROFIBUS 通信、工业以太网等众多类型。随着自动化和信息化的高度融合、物联网的发展，工业通信协议在发布后往往被工业设施重要供应商广泛应用，也常见于工业物联网，然而随之而来的是通信协议漏洞问题日益突出。

一方面，部分工业通信协议本身就缺乏相应的安全标准，安全水平不高。网络攻击者只需掌握协议构造方式，通过简单的网络接入就可以实现对目标设备的任意数据篡改。另一方面，工业通信协议存在的安全缺陷促使攻击者更为积极地挖掘协议漏洞，利用缓冲区溢出、拒绝服务等漏洞实现通信指令篡改及相应攻击。伴随工控网络与外部网络连接的进程加快，攻击者也将更容易通过网络探测、锁定和攻击目标，给工业互联网企业带来高额损失。

供应链攻击：在工业互联网发展过程中，供应链是其中不可缺少的组织形态，通过资源整合，可以有效实现产品设计、采购、生产、销售、服务等全过程的协同。与此同时，由于工业互联网供应链的全球化态势加强，工业互联网企业的核心技术产品、核心部件、敏感数据被供应链上更多的产品与服务提供商所接触，虽然通过权限设置、供应商安全审查等措施可以收敛一定风险，但供应链的全球化、精细化也使得企业的风险暴露面扩大。全球范围内工业互联网供应链安全事件频发，断供、网络攻击等威胁加剧，工业互联网企业面临着严峻的现实安全挑战。

（4）医疗行业

门户网站篡改风险：在线医疗服务的普及正在推动医疗网站成为开展公共服务、展现机构形象的重要平台载体。但由于应用组件版本较低，医疗机构网站往往存在安全等级低、安全隐患高的问题。其中，实施网站篡改、隐式植入非法信息这一攻击手法较为常见。一旦医疗机构的网页被篡改，可能被植入非正规医院的隐性广告、错误的医护信息以及色情、博彩等非法信息，不仅给机构的形象带来损害，还可能因为错误信息引导，给病患造成财产乃至健康损害。

应用服务高危端口与安全漏洞：数字化、智能化的医疗系统为数据泄露提供了可乘之机。一方面，大量健康医疗服务涉及患者姓名、手机号、身份证号、家庭住址等敏感个人信息，以及挂号记录、检查报告、缴费记录等就医诊断信息，具有高敏感性的特点。上述患者数据、诊疗数据、医保数据等被保存在医院医疗系统的数据库、打印机等应用服务当中，

并与公共互联网连通，存在高危端口和漏洞利用可能。另一方面，以手机 APP、网站、第三方医疗平台为载体的在线医疗服务不断涌现，然而受限于其安全能力，同样存在弱密码、RCE 漏洞等常见风险，可能引发批量应用服务被恶意控制、大量健康医疗数据泄露的安全事件。

以勒索病毒为代表的僵木蠕毒等恶意程序风险：在寻找到可利用端口、敏感服务或安全漏洞后，攻击者往往会尝试植入僵尸病毒、木马、蠕虫以及勒索病毒等恶意程序，实施大范围的网络欺诈、金钱勒索，甚至盗窃、贩卖医疗数据和患者个人敏感信息。在医疗系统的数据价值高、行业连续性强等背景下，医疗数据面临极大的风险。

2.3 商业视角下的场景需求

随着传统风险与网络安全风险的交织融合，新兴风险场景为网络安全保险带来突破口。聚焦商业智能网联汽车驾驶、工控生产、医疗诊断等应用场景，新一轮的保险需求正在不断涌现。

（1）场景 1：车辆自动驾驶

在智能终端的发展下，传统汽车从过去简单的出行载体演变成为一个汇聚大量数据的信息化智能终端——智能网联汽车。在智能网联汽车领域，风险场景更容易从虚拟网联空间映射到物理世界，带来更大的威胁。

在车辆远程诊断监控、自动驾驶、车路协同、智慧交通等应用场景下，为确保智能网联汽车能够适应不同路况，厂商会在车内安装大量传感器。通过这些传感器，主机厂和车联网服务平台商将采集了海量且种类众多的数据。数据显示，一辆智能网联汽车每秒产生的数据在 8G 左右，每天至少就能收集 10TB 左右的数据。以特斯拉为例，其采集的数据范围覆盖车主个人信息、车辆环境信息、车辆行驶信息、车主手机信息等约 200 多项，其中不乏敏感数据。因此，当智能网联汽车成为一个集移动、交互、智能化的信息采集终端，其所面临的风险一方面是传统的车辆风险，另一方面则是网络安全与数据安全风险。前者主要是可靠性问题，即车主经过一段时间的使用，仍可能无法在某些场景下稳定使用（比如在传统车辆风险中，往往需要考虑到累计行驶里程 / 瞬时行驶里程等因素，从而测算车辆存在的风险）；后者则依赖于车辆所配置的网络设备及系统，重点考虑易损性问题，即软硬件易受攻击，无法安全、稳定地运行。

以智能网联汽车在道路上行驶的场景为例，一旦车辆遭遇远程网络攻击，不仅直接危害智能网联汽车本身，造成车联网系统失控，引发车辆在道路上失控冲撞，从而形成多米诺骨牌，造成其他车辆混乱、城市道路拥挤、公共设施破坏，更严重者还将造成车主或其他人员伤亡。此外，汽车服务器遭受入侵、防盗系统存在漏洞等风险场景也正在现实上演。除了针对智能网联汽车，攻击还极有可能发生于整车企业、车联网信息服务提供商等相关企业和平台，一旦此类企业遭到恶意攻击与入侵，将造成“海啸级别”的重要数据泄露，对个人、企业乃至国家安全带来不可预估的损失。

全球范围内智能网联汽车的发展已势不可挡，智能网联汽车相关企业也应在研发可靠的车载芯片、建立完善的车联网通信安全体系之外，提前一步做好风险管理、控制与转移的准备。

（2）场景 2：工业安全生产

工业控制系统是支撑国民经济的重要设施，也是工业领域的神经中枢。伴随工业化和信息化融合趋势，工业安全生产场景同时面临传统的工控安全问题与工业互联网安全挑战。智能制造系统中的设

备高度互联协同，则进一步模糊了工控内网与互联网的边界，扩大了攻击面。

由于工业控制系统被广泛应用于电力、污水处理、石油和天然气、交通运输等重要领域，使其往往成为 APT 组织、恶意团队等的重点攻击目标。2018 年，Wannacry 病毒变种侵入了全球最大的代工芯片制造商“台积电”的 3 个厂区，导致其停产 3 天；2020 年，台湾石油、汽油和天然气公司 CPC 遭受攻击，引发供应链风险，使得当地加油站一度无法使用电子支付，造成一定程度上的混乱；2021 年，黑客入侵佛罗里达州奥尔德斯马市的水处理设施系统，并试图将氢氧化钠（NaOH）的浓度从百万分之 100 更改为百万分之 11100（人体若摄入高浓度氢氧化钠将对身体造成严重损害）。聚焦工业生产环境，工业控制网络与传统 IT 信息网络的不同之处在于，针对工控系统或工控网络的入侵或使攻击者直接控制到物理设备，可以直接造成生产设备、产品废弃、停工停产等严重后果。与此同时，工控安全困境还在于漏洞频出、管理体系与技术措施尚未有机结合、工控网络防护措施不够完善，使得生产、制造场景面临诸多不可控、难以预见的风险，一旦触发将导致巨大损失。综合因素下，工控企业除了采购传统的财产保险，保障资产安全，需要更密切关注因网络安全事件引发的数字资产破坏、经济损失问题。

（3）场景 3：数字医疗诊断

医疗机构的数字化转型、医疗设备的智能联网推动智慧医疗行业的发展，激发了远程会诊、三维辅助诊疗平台等新型医疗服务与模式。与此同时，网络安全风险不仅侵袭到智能医疗终端设备，同时也影响术前规划、术中导航等关键场景。

以医疗设备信息安全场景为例，医院及卫生健康机构不仅承担着健康卫生保障功能，也承载着众多医疗诊断信息和患者信息。然而，由于一些医院在建设之初没有容纳安全考量、医疗设备更新换代慢、医疗设备软件大多又具有封闭性，缺乏统一接入内网的安全管理措施，因此，相关医疗健康机构的安全防护能力薄弱，一些没有经过允许的终端可以轻松绕过而接入机构内部网络，造成数据泄露等风险。

另一方面，部分医疗健康机构加快推动“互联网 + 医疗”，陆续上线智慧医疗、惠民医疗应用服务，但其同样面临复杂的风险场景。聚焦医疗数据互联互通的场景，健康医疗机构为实现跨机构、跨地域的健康诊疗信息交互和医疗服务协同，在不同医疗机构和线上平台之间实现电子病历、检查报告等数据的信息共享。然而，相关人员对相关敏感数据进行访问浏览时，可能因为不同机构安全水平不一、人员安全意识差异，使得通过信息交互系统进行文件数据传输、存储等操作时，因操作不当而出现安全事件。以医疗勒索事故场景为例，2020 年德国一家医院的医疗系统因遭受勒索软件攻击而瘫痪，这导致一患者因未得到及时救治而不幸身亡，这也是全球首例勒索软件致死事故。整个医疗行业的网络安全形势不容乐观，且因其直接关系到病患群体，相关安全风险需引起高度重视。

2.4 | 保险视角下的产品需求

网络安全保险规模化发展面临的一个主要问题是企业在需求层面的差异化，除了上述提及的行业需求差异、场景需求差异，还存在不同类型的企业对安全的认知和具体需求存在差异的情形。因此，网络安全保险公司难以找到‘标准’的方案并投放市场。

根据《2019 年全球网络风险透视调查报告》的数据，近 50% 的企业已经购买了网络安全保险。其中，年收入超过 10 亿美元的大型公司中，有 57% 的企业选择投保，而年收入低于 1 亿美元的公司中，有 36% 的企业选择投保。不同规模的企业对于网络安全保险的需求存在差距，但差距似乎并没有预想的大。从安全需求的角度来看，**中小微企业购买网络安全保险是为了“助安全”，大型企业购买网络安全保险则是为了“保安全”**。

简而言之，大型企业对网络安全事故造成的经济损失有较高的容忍度，小额保障对其缺乏吸引力。此外，大型企业往往面临着影响范围广泛的第三方责任风险，更倾向保险公司提供额外的应急响应资源作为其既有安全能力的补充，并且覆盖责任风险。因此，大型企业对网络安全保险产品的需求主要是避网络安全黑天鹅事件带来的巨额损失，为其安全建设“锦上添花”，属于“保安全”的认知范畴。

相对而言，中小微企业在网络安全建设方面的投入有限，面对网络风险时的网络恢复弹性较弱。《中小微企业数字安全报告》的数据显示，近半数中小微企业于 2021 年遭受过网络攻击，超过九成的企业长期被黑客攻击而不能独立应对，超八成的勒索攻击针对 1000 人以下规模的中小微企业 。中小微企业由于自身体量小、资金、技术和人手有限，其安全预算难以支撑完备的安全方案落地，导致其在网络攻防对抗中处于一定弱势地位。与此同时，攻击者更“青睐于”中小企业，相比针对大型企业所需要的更复杂的攻击策略与更胶着持久的攻击链路，瞄准中小微企业的攻击门槛更低，能够逐个攻破、以量取胜，而主要攻击方式则包括恶意软件入侵、勒索攻击、系列漏洞利用和网络钓鱼。部分中小微企业在遭遇入侵攻击后并不知情，或是在长达十几天或数月后才意识到侵害。在过长的反应期中，中小微企业很可能遭遇二次、三次攻击，成为攻击者的‘战利品”之一。

因此，在生产生存威胁下，中小企业一般倾向于购买网络安全保险，使用更低的成本获得保额较低但配备了安全服务的网络安全保单，从而通过第三方的介入补充其内部的网络安全保障能力，减轻网络安全事件对企业带来的巨大冲击，属于“助安全”的认知范畴。

PART 3
科技助推多产业深度融合

风险和需求是网络安全保险产业的驱动因素，网络安全产业和网络安全保险产业的融合创新则为产品落地提供了未来方向。在产品设计、服务模式输出方面，网络安全保险的发展无法脱离网络安全服务、技术的支撑。因此，促进国内双产业的融合，将进一步丰富“网络安全即服务”的业态，同时有效推动网络安全保险产业创新，形成多产业融合、互赢的发展局面。

3.1 产业融合发展形态

在网络安全保险的完整业态中，包含网络安全企业、保险科技公司、第三方风险管理技术机构三个角色。网络安全企业采取网络安全技术与服务，协助保险公司为客户方提供全面风险管理方案；保险科技公司针对场景化网络安全风险，协助保险公司基于数据清洗整合优势，优化风险定价模型、构建全流程保险业务体系；第三方风险管理技术机构则将网络安全企业的安全技术能力与保险科技公司的科技能力进行有机的整合，逐渐成为保险生态中关键一环。

（1）解决方案：多业态融合

网络安全保险产业既脱胎于保险，又与网络安全产业息息相关。目前，两个产业的融合在网络安全保险业务模式上体现为 3 个阶段性模式：

1. 网络安全产品的附赠保单。网络安全企业销售网络安全产品后，附赠对应网络安全产品的责任保险，借助保险公司转嫁风险；

2. 网络安全服务 + 网络安全保险保单。网络安全企业提供风险评估、风险监测、应急响应等技术手段，保险公司主导保险产品开发、风险损失量化及核保定价等工作。技术与业务交融，对风险进行综合管控；

3. 网络安全技术 / 服务 + 网络安全保险科技 + 网络安全保险保单。网络安全保险科技企业与保险公司共同设计网络安全保险方案，网络安全保险科技企业将网络安全威胁库与保险定价模型、承保范围相结合，依托大数据整合、分析能力形成网络安全量化风险评估模型、自动化定价能力。同时，网络安全保险科技企业选择自研或与网络安全企业合作提供网络安全产品，为企业提供主动、动态风险防御服务。在出险、理赔阶段，则通过自动化理赔配套服务，帮助企业降低风险事件损害的同时，对于安全风险带来的经济损失通过理赔方式有效转移。

上述三个网络安全保险业务模式依次体现了网络安全产业与网络安全保险产业的融合深度，由浅入深，由产品粗放式绑定向产品服务深度交融转变。与此同时，由于网络安全保险不同于传统的物理承保的险种，其通常具有虚拟性，且不受地域限制，这也为产业融合降低了技术门槛，加速了服务耦合。

围绕多层次的市场需求，网络安全保险的产品与服务进一步细化。目前，保险公司和网络安全保险科技企业面向不同行业与场景的差异化网络安全风险管理需求，全方位开发网络安全保险产品体系，丰富网络安全保险细分险种，提供解决方案。其中，

网络安全保险服务基本涵盖网络安全风险评估、漏洞扫描服务、网络安全意识培训、渗透测试服务、网络安全加固服务、网站安全监测、网络资产测绘服务、动态防御服务、威胁情报服务、代码安全审计服务、安全众测服务、网络安全应急响应、安全事件取证服务、数据安全恢复服务。这些服务主要由网络安全公司、网络安全保险科技企业联合提供，针对性围绕保险需求进行组合，从而有效配合保险公司核保、承保、理赔。

图 3–1 众安保险 – 网络安全风险监测中心

以众安保险为例，其以“保险 + 科技 + 安全”创新模式，为企业提供基于网络安全保险的主动安全合规、主动风险管理、主动安全运营等一站式服务。服务涵盖开展网络安全核查、风险评估、风险态势监测、风险提示、责任划分、定损评估及理赔等关键环节，具有投保模块化、服务系统化、理赔快速化等特点。同时，面向企业打造了以技术服务能力为支撑的网络安全运营中心，依托安全整改建设、风险量化评估、网络安全评估、风险实时监控、应急恢复响应、公关诉讼六项技术服务模块，提供事前预防，事中监测，事发响应及事后处理的全流程定制服务。目前，聚焦企业核心需求，众安保险提供“网络安全保险（中小企业版）”、“网络安全保险（信息系统版）”、“网络安全保险（综合定制版）”等标准产品。此外，还通过“标准产品 + 定制化的解决方案”，构建多层次的网络安全保险产品矩阵。

标准保险产品		企业网络安全保险（中小企业版）	企业网络安全保险（信息系统版）	企业网络安全保险（综合定制版）（可选）
承保内容	营业中断损失	✓（可选）	✓	✓
	网络勒索			✓
	数据安全责任		✓	✓
	数据泄露责任		✓	✓
	数据修复费用	✓	✓	✓
	公关费用		✓	✓
	通知费用			✓
	防Ddos攻击费用	✓（可选）		✓
	抗辩费用		✓	✓
	通报监测费用			✓
网络安全风险预防管理服务	无感知风险评估	✓	✓	✓
	网络安全在线专家咨询服务	✓	✓	✓
	网络勒索危机顾问服务			✓
	事故溯源 & 负面影响评估服务			✓
	定期风险隐患排查			✓
	Web 网页防篡改监测	✓	✓	✓
	Web 网页木马与暗链监测	✓	✓	✓
	Web 安全测试与加固	✓	✓	✓
	渗透测试服务			✓
	网络安全人才培训			✓
	高级威胁监测			✓

图 3–2　众安保险 – 产品示例图

在网络安全保险解决方案的设计方面，保险公司一般与第三方进行合作，形成优势互补。众安保险通过与科技公司（众安科技）达成战略合作，为上述“网络安全技术 / 服务 + 网络安全保险科技 + 网络安全保险保单”阶段性模式的解决方案提供了范本。在承保范围方面，众安保险基本涵盖主流安全风险造成的财产损失与第三方责任等；在配套服务方面，众安保险与众安科技在保险的各个环节形成深度合作，由众安科技基于网络安全技术及服务能力，提供 GuardIt、LOCKet 等系列自研安全产品作为设备支撑，通过 ARMS 主动风险管理平台全流程风险管理，再辅以配套保险服务能力为网络安全保险产品提供科技支撑能力。

（2）承保范围：新边界拓展

2021 年，我国网络安全保险保费规模预计在 7080 万元左右，较 2020 年增长 3.2 倍以上。从服

务机构来看，约 20 家中资保险公司具备网络安全保险相关产品和承保能力，备案了超过 50 款网络安全保险产品。从产品类型来看，企财险接近半数，责任保险共有 10 余款，还有综合保险、应急响应专项险等其他类型险种。从服务模式来看，国内保险公司积极尝试与网络安全专业技术机构开展合作，融合保险机制与网络安全技术服务，基本形成网络安全保险产品序列。

目前我国主流网络安全保险的承保范围包括网络安全财产损失、网络安全责任损失和其他损失，承保边界进一步拓展，为企业提供了更丰富、更细化的投保选择。网络安全财产损失，是指由于**投保人因网络安全事件导致的损失和费用**，包括营业中断损失、网络勒索损失、网络欺诈损失、数据修复费用、计算机修复和更换损失。网络安全责任损失，是指**投保人因网络安全事件引发的对第三方（受影响个人或机构）的法定赔偿责任所导致的损失**，包括网络安全责任、数据 / 信息泄露责任、外包商数据安全 / 信息泄露责任。其他损失，是指除网络安全财产损失、网络安全责任损失外，投保人为处理网络攻击事件所支出的其他费用，包括风险处置费用、咨询服务费用、网络安全等级评定费用、公关费用、法律费用和媒体侵权赔偿费用。

表 3–1 国内主流网络安全保险的承保范围

国内主流网络安全保险的承保范围		
网络安全财产损失（第一方损失）	网络安全责任损失（第三方损失）	其 他
营业中断损失 因网络安全事件造成的收入损失或利润损失以及增加的运营成本等，营业中断进一步的影响还包括降低运营的有效性和效率导致服务或产品的延迟交付	**网络安全责任** 投保人因网络安全事件，导致其合作伙伴或所服务的用户发生经济损失，投保人需要承担第三方经济损失的赔偿责任。如因网络安全事件使得服务客户的正常生产制造、内外部运营中断并产生收入损失，第三方合作伙伴或客户提出的经济赔偿	**风险处置费用** 投保人发生网络安全事件后，聘请服务机构针对安全事件进行应急响应所产生的处置费用
网络勒索损失 投保人因遭受网络勒索后，所产生的实际损失和相关费用，包括调查取证、数据恢复、谈判，以及所产生的其他损失等费用 注：根据中国互联网金融协会、中国银行业协会、 中国支付清算协会发布的《关于防范虚拟货币交易炒作风险的公告》，国内保险公司对网络勒索案件的损失进行承保时，不得承保与虚拟货币相关的保险业务或将虚拟货币纳入保险责任范围，不得直接或间接为客户提供其他与虚拟货币相关的服务。	**数据 / 信息泄露责任** 投保人因网络安全事件，导致其所掌握的用户数据泄露（包括个人身份信息或客户敏感信息等），而需要承担的赔偿责任、相关法律诉讼等费用	**咨询服务费用** 保险事故发生时所产生的合理必要的咨询服务费用，例如投保人与合规顾问沟通以遵守网络安全、个人信息保护等法规的咨询费用

表 3-1 国内主流网络安全保险的承保范围

国内主流网络安全保险的承保范围		
网络安全财产损失（第一方损失）	网络安全责任损失（第三方损失）	其 他
网络欺诈损失 投保人因遭遇网络钓鱼攻击或勒索病毒攻击，被要求向指定的账户转账，而产生的网络欺诈损失	**外包商数据安全/信息泄露责任** 投保人的数据托管服务商因遭遇网络攻击导致信息泄露，被泄露信息主体因此向投保人索赔，投保人可能承担的法定赔偿责任	**网络安全等级评定费用** 投保人遭遇网络安全事件后，原有的认证评级水平受到负面影响，而产生的重新评级认证的费用
数据修复费用 投保人因遭受恶意攻击，导致核心数据丢失、损毁或被篡改，由此引发的数据恢复费用		**公关费用** 投保人发生信息丢失、泄露等网络安全事件后，投保人社会声誉减损而所产生的名誉恢复费用
计算机修复、更换损失 投保人因遭遇勒索病毒攻击、供应链攻击或其他网络安全事件后影响计算机系统正常使用，企业因此可能产生的修复、更换计算机设备的费用		**法律费用** 保险人发生信息丢失、泄露事件后可能被客户索赔，而产生的聘请律师等应对诉讼的费用
		媒体侵权赔偿 投保人因其在线媒体内容（包括网站、博客和社交媒体等）不当行为，被第三方提出索赔而产生的法律费用、赔偿等损失

3.2 产业链及厂商生态现状

网络安全保险的产业链结构复杂，除了保险公司和投保企业这一供需两侧，往往还有大量不同类型的市场主体参与其中。根据产业链的结构层及不同市场主体的产业角色定位，可以将市场主体大体划分为基础设施层、解决方案层、应用层提供商。

表 3–2 网络安全保险产业链

产业链	结构层	产业角色
上游	基础设施层，提供支撑的技术服务、支撑产品及服务设计的数据源	保险数据中介、大数据 / 人工智能等技术服务提供商、网络安全厂商
中游	解决方案层，提供网络安全保险服务及解决方案	保险科技公司、网络安全厂商、其他第三方风险管理技术机构、安全事件定责定损机构
下游	应用层，提供网络安全保险保单	保险公司、保险经纪公司

由于网络安全保险所涉及的领域技术及专业性门槛高，网络安全风险复杂性明显，在网络安全产业链中，第三方风险管理技术服务机构逐渐成为整个生态中的关键角色。以网络安全厂商、保险科技公司为代表的第三方风险管理技术服务机构承担风险评估相关能力，借助其数据、技术优势链接保险供需双方，在保险流程中发挥重要作用。此外，在保险公司为投保企业提供保单之前，上游和中游的各类市场主体也将根据网络安全保险的特殊属性，不仅在风险管理方面，还在网络安全事件数据、网络安全服务及定责定损等方面提供支撑能力。

未来，仍然需要多元主体聚集，整合各方优势资源，深化跨行业合作，共同完善网络安全保险的产业发展。

3.3 产业融合发展挑战

全球网络安全保险的快速上升期在近 10 年，我国保险公司陆续开始提供网络安全保险服务则是在 2017 年前后。目前，我国网络安全保险进入快速发展阶段，正在以城市为单位发展区域试点、树立标杆场景。以上海为例，一方面保险行业发达，另一方面应用场景丰富，具备率先发展网络安全保险的基础条件。作为全球金融、经济中心，上海不仅拥有大量关键基础设施、重要信息系统和海量用户资源，而且在建设国际数据港、发展智能网联汽车产业、培育在线新经济“数商”方面重点发力，这些基础也为网络安全保险带来了更多新的应用场景。

聚焦网络安全保险市场，需求的驱动、产品的迭代、生态企业的涌现，使得这一行业亟待突破，与此同时，我国在网络安全保险产业融合发展、产品及服务的市场化探索及发展过程中，存在的相应挑战与亟待克服的难点也需要进一步引起重视。

（1）数据来源：信息披露机制不足

网络安全保险产品及服务的设计无法脱离数据源，不论是针对特定风险场景的网络安全保险还是综合类的网络安全保险，均涉及到全流程的设计——风险量化评估、定价核保、理赔定损等，这些能力的构建不仅需要技术支撑，也更需要多源数据作为

基础。当前网络安全保险行业所需求的数据包括：①保险数据，即相关行业、投保企业历史在网络安全领域的投保数据、理赔数据；②风险数据，即相关行业面临的主要网络安全风险挑战、投保企业当前切实存在的风险点、过往发生的网络安全事件信息以及风险造成的损失数据等；③公开数据，即在公开网络上可以查询和获取的事件与数据。

然而，在此背景下，网络安全保险行业却面临数据的信息披露机制不足的问题。一方面，伴随国内网络安全事件信息披露机制不足、信息不透明导致公开数据有限、风险数据不足、整体数据不完整或质量较差，使得现有数据无法侧写投保人的风险画像；另一方面，保险公司的既往保险数据与网络安全公司所掌握的风险数据存在行业壁垒，导致保险公司无法获取跨行业数据，使得数据无法有效共享和利用，继而无法发挥价值。

（2）行业标准：行业规范明显缺乏

行业标准规范体系是扩大市场规模的重要前提，《网络安全保险服务规范》等标准规范的发布意味着网络安全保险正在走向规范化。然而，网络安全保险出于所承保风险的复杂性、风险场景的多样性，在行业规范、产品标准等方面仍存在挑战，需要加快推动完善规范体系。由于风险场景、业务需求的差异化，网络安全保险难以制定通用标准类产品，市面上网络安全保险在保单术语方面大多存在差异，针对投保企业的风险量化评估、索赔依据判断也缺乏标准参考，这些问题为提升网络安全保险社会认知、优化客户服务、打造示范效应行业案例带来一定障碍。

（3）产业协同：产业链空缺亟待填补

网络安全保险的理想产业生态角色应当涵盖保险数据中介、大数据 / 人工智能等技术服务提供商、网络安全厂商；保险科技公司、第三方风险管理技术机构、安全事件定责定损机构；保险公司、保险经纪公司。目前，网络安全保险的产业链存在角色缺失、角色不明晰等现象，从而使得网络安全保险在产业化发展的过程中受到一定影响。譬如国内缺乏定责定损缺乏专门机构组织，使得网络安全事件判定模糊；缺乏数据源提供商，使得不同行业、不同领域的数据无法互通互利，为网络安全保险产品设计及产业发展造成基础设施层的阻碍，同时也一定程度上影响了网络安全产业和网络安全保险产业融合。

（4）市场态度：社会认知有待提高

从市场主体来看，部分市场主体对于发展网络安全保险已经形成一定共识。从社会层面来看，一些中小企业对于网络安全保险的认知与接受度则还有待提高。围绕网络安全保险的认知不足导致企业对于投保存在担忧，包括保险机构囿于自身业务累计，能否完全知晓并判断当前不断演变的网络安全威胁，保险机构如何根据客户不同类型安全成熟度及不同业务风险类型提供合适的产品等。造成这一问题的因素可能是网络安全保险的市场推介力度不足、网络安全保险的市场占有率不高、标杆案例缺乏等，因此导致部分企业对网络安全保险持观望态度。

PART 4
科技智绘网络安全保险新业态

在网络安全保险的新阶段探索中，无法绕开 3 个关键词：保险、安全、科技。当保险公司和网络安全企业无法通过简单的产品与服务撮合的方式，升级网络安全保险业态、解决行业发展面临的瓶颈问题，科技就在其中起到了粘合、塑造、再耦合的作用。着眼现阶段的创新，展望未来发展，科技将赋能网络安全保险，智绘全新业态。

4.1 全球范围内的创新探索

基于公开信息，本报告案头调研了国内外 8 家网络安全保险科技企业。调研对象均为成立 5 年及以上的大型网络安全保险科技企业。根据公开信息，这些网络安全保险科技企业基本具备的产品或服务能力包括：核保阶段的风险评估、保险定价、整改建议，承保阶段的风险监测，出险 / 理赔阶段的事故管理（响应 / 数据恢复 / 专家咨询）、理赔服务。

企业	企业概况		核保服务			承保服务	出险 / 理赔服务		其他	客户	
	估值	融资	风险评估	保险定价	保险定价	风险监测	事故管理（响应 / 数据恢复 / 专家咨询）	理赔服务	营销	投保企业	保险类公司
众安科技	/	/	✓	✓	✓	✓	✓	✓		✓	✓
源堡科技	/	B 轮；约 1 亿元（2021）	✓	✓	✓	✓	✓	✓	网络安全险销售工具		✓
At-Bay	13.5 亿美元（2021）	D 轮；1.85 亿美元（2021）	✓ 含报告						保险经纪人平台		✓ MGA
Bitsight	24 亿美元（2021）	E 轮；2.5 亿美元（2021）	✓ 可视化安全评级			✓ 包含供应链生态系统风险监测					✓
Coalition	35 亿美元（2021）	E 轮；2.05 亿美元	✓	✓	✓	✓	✓	✓	保险经纪人平台		✓
Cybercube	/	B 轮；3500 万美元（2019）	✓ 含报告								✓
Guidewire-Cyence	67 亿美元（2020）	被 Guidewire 收购	✓	✓	✓						✓
Resilience	/	C 轮；8000 万美元（2021）	✓		✓	✓	✓	✓	自动化分销平台		✓

图 4–1 网络安全保险科技企业服务梳理

风险评估主要依赖于公开信息、历史理赔数据、投保企业风险状况等数据源，对企业进行风险梳理与评估，一般以风险评估报告或安全评级结果为展示形态。以众安科技为例，其基于众安保险的海量理赔数据及公开情报数据形成风险数据库，并根据行业监测和风险动态对风险数据库反复更新迭代。在风险数据库的支撑下，得以构建风险评估模型，并通过资产风险核查、资产测绘、漏洞扫描、风险评估问卷等系列评估手段，对投保企业进行全面的风险摸排，进而形成风险评估结果。值得注意的是，信息安全等级保护评估结果、ISO27000 认证等也被纳为企业风险评估的参考因素。

保险定价是以风险量化、定级为参考基准，将风险结果转化为核保依据与定价参考，实现自动化精准定价。不过，网络安全保险的定价模型一般需要结合本国或本地区的风险数据，考虑到不同地区在法律法规、网络安全成熟度水平、监管水平上存在较大差异，网络风险所呈现的损失形态也存在区别，因此网络安全保险科技企业在设置定价模型的过程中，需要考虑到对应的风险因子。

风险监测是网络保险科技服务的一部分，其有别于企业原有的安全风险监测预警系统，更聚焦于承保风险状况，并基于保险视角对承保范风险相关的流量、日志、报警信息进行实时监测和记录。大多数风险监测服务无需额外收费，且以 SaaS 模式部署。如果企业出于管控考虑，也可以不额外部署网络安全保险科技企业提供的风险监测系统，但也可能造成最后理赔阶段，由于对承保风险的记录和分析缺失或遗落，导致理赔依据不足的可能性。

事故管理主要是应急响应工作，包含风险处置、溯源追踪、数据恢复、专家咨询等服务。目前网络安全保险科技企业更倾向于与网络安全公司合作，引入第三方安全能力，协助投保企业完成 7x24 小时应急响应。

理赔是由保险公司根据保单进行赔付，而定责定损等理赔配套服务则由网络安全保险科技企业提供。出险不一定意味着理赔，只要在确定责任、明确损失、确认相应损失属于承保范围后，才会进入理赔阶段。

除了围绕保险各个流程环节的配套服务，部分网络安全保险科技企业会提供针对保险经纪人 / 经纪商的专业分销平台。通过帮助保险公司构建网络安全保险销售工具，提高网络安全保险的销售效率。具体形式即保险科技公司基于多源数据构建自有企业风险数据库，保险经纪人可以通过工具 / 平台快速了解对应企业的风险情况，并获得针对该企业的保险方案，涵盖推荐承保范围、保险定价等信息。通过自动化的核保、即时报价和快速响应，使得保险科技公司为保险经纪商和投保人、保险公司之间构建更快捷的承保通道。

（1）案例 1：SaaS 提供商的数据泄露隐忧

SaaS 提供商的安全痛点：益于低成本和便捷部署的优势，SaaS（软件即服务）服务已成为访问重要业务应用程序的主要手段。与任何企业一样，SaaS 提供商同样会遭受恶意攻击与安全风险。不同的是，其一旦遭受攻击，往往会“殃及池鱼”，引发第三方风险、造成安全的“多米诺骨牌效应”。

案例背景：北京缔联科技有限公司作为一家典型的 SaaS 提供商，专注于企业费用管理和发票管理系统的建设，通过“费耘”进项发票管理系统、“路耘”通行费电子发票管理系统等 SaaS 产品，为不同行业企业提供专业财税服务。由于发票在企业经营过程中是保证票、库、账、款、税一致的纽带，也是唯一商事凭证，因此，缔联科技服务的大型企业十分重视发票数据存储的安全性。一旦出现网络安全事故，“费耘”系统中的数据隐私泄露安全性出现问题，很可能面临巨额赔偿等相关风险，影响品牌信誉和业务进展，后果不堪设想。

网络安全保险科技公司：众安科技

案例保单的承保范围：网络安全责任损失。由众安保险对缔联科技的数据保密责任、数据安全责任承保。不仅对于发生在保单期限内的意外事故导致的数据库泄露以及相关客户损失进行保单范围内赔偿，并且提供法律诉讼相关费用的支持。

网络安全保险及配套科技服务：由众安科技提供相应服务。承保前，基于数据科学开展数字资产风险核查、网络安全资产测绘、资产漏洞探测、数字资产健康性评估等一系列风险评估，同时定制网络安全风险评估问卷，完成缔联科技内部管理和运营安全风控的全面摸排，此外在参考等保测评结果的基础上，评估内部系统的网络安全。承保后，对承保风险进行综合管控，通过采集关键安全日志，对企业的日常运维操作合规性、网络安全健康度进行实时监测。发生安全事故时，协助缔联科技开展网络安全应急事件响应和排查，最大程度降低因网络威胁导致的损失。基于完整的解决方案链接，协助缔联科技构建事前识别与降低、事中监控与发现、事后响应与补偿的数据安全风险管理体系，形成风险闭环管理的安全运营和风险管理机制。

（2）案例 2：勒索攻击下的“安全困境”

勒索攻击引发的企业痛点：锁定或加密数据、索要高额赎金，并伴随数据泄露的风险——勒索攻击已成为困扰大多数企业的一大风险。虽然是否支付勒索赎金仍然是一个存在争议性的问题，但勒索攻击给企业带来“困境”是显而易见的，即数据损失、财产损失、信任危机。

案例背景：一家托管和 IT 服务公司的所有计算机系统和数据（包括公司客户的数据）在一场勒索软件攻击中被加密。更糟糕的是，该公司的数据备份同样未能幸免。当勒索软件攻击者索要高达 25 比特币（相当于约 20 万美元）的赎金时，该公司基本无法负担损失。然而，该公司此前通过网络安全保险科技企业、授权承保代理机构 (MGA)——Coalition 购买了网络安全保险及配套服务。

网络安全保险科技公司：Coalition

案例保单的承保范围：网络安全财产损失，涵盖业务中断损失，取证和数据恢复成本以及网络勒索本身造成的直接损失。此外，该投保公司还从 Coalition 购买了技术错误和遗漏保险，覆盖责任风险。

事件处置流程：在接到公司电话的几分钟内，Coalition 的安全事件响应团队（SIRT）与公司员工取得联系，从而诊断损坏并最大限度地减少进一步的损失。在审查了相关处置信息后，SIRT 尝试为投保公司进行数据解密。在不到 24 小时内，SIRT 与 Coalition 理赔团队合作，不仅确保投保公司免受比特币勒索威胁，还解密了公司文件。最后通过取证工作，帮助公司防范未来的攻击。从入侵到问题解决的总时间仅为 48 小时。

4.2 网络安全保险前沿科技应用

网络安全保险的未来将以“保险 + 安全 + 科技”为主流模式，其中安全侧的创新主要和网络安全新理念、前沿技术的发展息息相关，是所有网络安全从业者关注和投入的方向。网络安全保险的科技部分作为融合产业发展的重要力量，其应用与发展则是网络安全和保险行业共同关注的焦点。

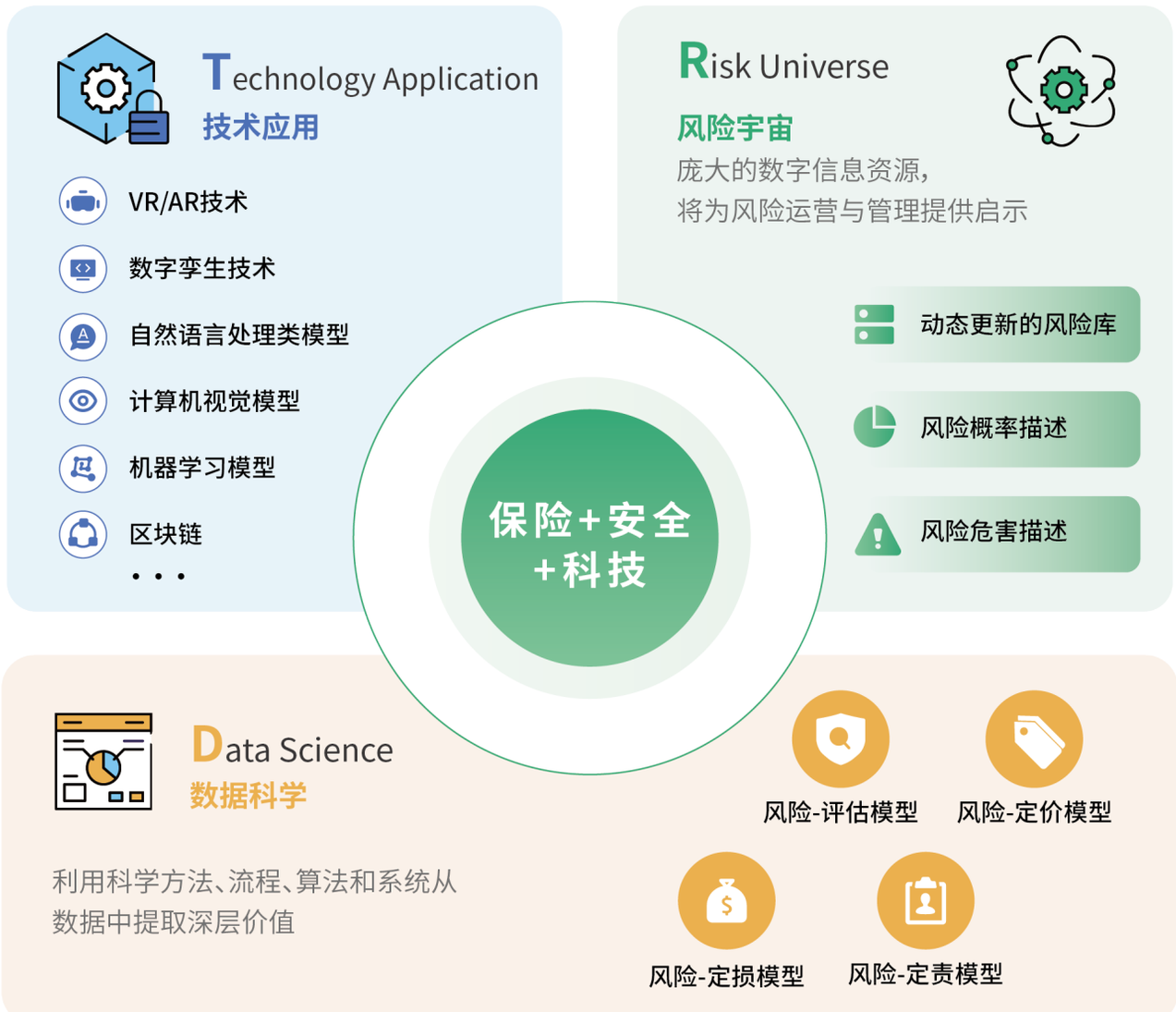


图 4–2 网络安全保险科技图谱

网络安全保险的科技创新点重点围绕**风险宇宙（The Risk Universe）**、**技术应用（Technology）**、**数据科学（Data Science）**展开。

（1）风险宇宙

风险宇宙是庞大的数字信息资源聚合，通过对风险信息的收集、汇总、分类梳理，将为整体风险运营与管理提供启示。目前网络安全保险领域的风险宇宙的落地形态最常见于风险库 / 风险列表，通过动态更新的风险库展示特定领域、特定企业的风险状态，主要包括风险频率及风险危害程度描述。

在网络安全保险的风险宇宙中，不仅涵盖攻击风险，也涵盖企业其他经营性风险，通过对风险库进行不同颗粒度的划分，形成围绕行业、企业及场景等不同维度的风险描述，较粗的层次决定了风险库可以覆盖的范围，较细的层次则决定了风险的落地性，能够支持网络安全保险在风险界定过程中有更为确切实际的解释、指导和评估。目前众安科技等国内外网络安全保险科技企业已经形成了自有风险库，预计随着行业发展，基于融合保险考量的风险库，网络安全保险科技企业将进一步形成保险行业的类“ATT&CK”的风险描述性框架。

（2）技术应用

技术应用贯穿于网络安全保险的产品设计、核保阶段、承保阶段、出险 / 理赔等各个阶段，主要

是利用人工智能、虚拟现实、智能终端等前沿技术及设备，提升保险全流程的智能化、自动化。

产品设计阶段：

通过数字孪生技术，科技公司可以为投保企业及保险公司构建实时实景的虚拟空间。根据保险公司的组织结构生成数字副本，形成“组织数字孪生”（DTO），模拟组织的内部运作与运营行为，从中发现潜在问题，改进运营流程。

核保阶段：

借助实时交互的视频 / 聊天平台改善风险评估效率，尤其适用于保险公司人力未覆盖到的偏远区域。依托VR、AR等智能终端设备，率先在传统险种（人寿保险、汽车保险、退休保险还是健康保险）成熟应用，再开展在网络安全保险中的进一步探索适用。目前国外的 Virtual i Technologies 就已经通过智能平台（VRS）虚拟风险空间，提供了一个安全的视频流通道，用于实现远程指导、取证工作。

承保阶段：

借助数字孪生技术，通过模拟数据流预测并评估投保企业存在的可能性风险情境，预测未来安全风险，同时为网络安全保险服务的整体方案提供洞察和优化支持。

出险 / 理赔阶段：

索赔处理直接影响到网络安全保险的运营效率与客户满意度，借助数字孪生、人工智能、区块链等技术加快理赔流程将是科技赋能保险的重要方向。通过聊天机器人引导投保企业自主拍摄、上传有关出险的视频和照片，借助光学字符识别（OCR）设备识别纸张文档中的数据，基于自然语言处理（NLP）类模型，将视频和照片即时转换为损坏描述；通过机器学习（ML）模型，对投保企业相关网络行为进行分析，判断是否存在欺诈行为；基于区块链技术创建智能合约，将小额保险政策嵌入到利用区块链技术进行保护和记录的数字交易中（例如 CloudCover 的 CC/B1 CyberSafety 平台已支撑实时区块链承保流程），通过算法来分析网络流量，进行风险评分并构建精算模型，从而实现实时设置、重置保费的“动态数据”的增量保险，并且在满足理赔的情况下自动进入索赔。

（3）数据科学

数据科学及相应模型是保险公司及保险科技公司共同认定的网络安全保险最重要的底层科技支撑。利用科学方法、流程、算法和系统从数据中提取深层价值，映射在网络安全保险领域则体现为风险 – 评估模型、风险 – 定价模型、风险 – 定损模型、风险 – 定责模型。在风险模型中，确保其与传统财产险的区别、对模型的科学性进行保障，这些是网络安全保险科技发展的核心问题。

简而言之，数据科学是将数据转化为决策和行动（tradecraft）的艺术，是人和计算机一起工作将数据转化为知识发现的工具、技术和流程的整合。数据学科通过收集数据、描述数据、发现知识，进而进行合理的有针对性的预测和建议。

在网络安全保险领域，数据科学的具体应用包括：

1. 保险欺诈的相关检测

据估计，保险欺诈为保险公司带来的损失高达 340 亿美元。在网络安全空间，检测保险欺诈的难度很大，厘清事件具体情况可能非常耗时，也无法得出明确的结果。但现在，随着技术的不断发展，保险公司基于防欺诈性索赔的工具，将网络安全风险数据与数据科学相结合，通过算法，找到欺诈索赔和潜在欺诈索赔之间的相似性，从而及时发现潜在的欺诈行为，以便开展进一步调查。

2. 风险管理的预测分析

过去，保险公司往往依靠大量网络安全风险数据进行风险评估。现在，使用数据科学技术，通过对外部网络安全威胁数据及内部风险数据进行分析、从而评估企业遭受网络安全威胁的可能性，能够实现风险提前发现、率先规避。

PART 5
网络安全保险科技发展建议

着眼网络安全产业发展，相关市场“产品”的形态已经有了明显的转变趋势。首先是从软硬件产品转向安全服务的趋势愈发明显。此外，产品从功能性转变为智能化，即相关的安全产品或服务不再是提供特定的某项或数项功能，而是具备了智能化、定制化的自动化调整策略，从而更贴合企业应用场景。产品运营模式也出现几个变化，包括①产品或服务提供者逐渐从独立运营转变为协同合作；②现场部署或驻场等线下的服务逐渐转战线上，通过 SaaS、PaaS 部署等模式快速、低成本完成服务交付。最后，网络安全防护模式从被动防御转向主动防御策略，对企业在网络安全建设方面提出了更高的要求和更全面的需求。

随着网络安全市场的趋势变化，基于科技创新的网络安全保险新型服务及解决方案正在成为企业网络安全建设的重要组成部分。未来，随着网络安全保险的覆盖范围、场景的丰富，多产业协同创新将进一步激发网络安全保险产业新的爆发点。

围绕网络安全保险产业发展进程中存在的挑战，本报告提出四点建议：

5.1 加强宣传推介力度

针对网络安全保险的社会认知不足问题，在发展初期，由保险公司、网络安全保险科技企业联合其他安全产品及服务提供商，通过网络安全保险搭载产品的模式，快速提升网络安全保险这一险种的国内市场占有率，率先打开市场。

建议关键信息基础设施运营者、网络数据处理者和部分公共部门率先将网络安全保险纳入企业网络安全建设体系。进一步发挥产学研深度融合，保险公司与网络安全保险科技企业协同企事业单位、协会组织及高校及研究机构，发布网络安全保险行业指引，提升企业及机构对于网络安全风险的认知以及网络安全保险的基础认知。充分利用网络安全保险科技企业的科技优势，加快推动创新技术在网络安全保险科技领域的落地和实践，开展最佳实践的业内共享。

5.2 推动数据要素流动

网络安全保险的数据源方面，目前国内外网络安全保险科技企业主要依赖于历史理赔数据、投保企业内部数据、公开信息形成自有数据库，部分国外网络安全保险公司还会引入一部分暗网数据（例如美国发布的《从非法来源收集网络威胁情报和购买数据时的法律参考指南》（Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources1）为此提供了法律依据）。不同来源不同类型的数据通过汇整、分析、机器学习和训练，将演变为网络安全保险产品的费率标准、网络攻击损失概率预测模型、定价模型等。

因此，当数据源作为网络安全保险发展的基础之一，为促进其多样化、流通性、开发利用效应，建议：①加强政策、标准引导和规范，明确网络安全事件

披露机制，包括信息系统功能性风险和信息安全内容风险的披露范围和披露内容；②倡议相关政府机构推动形成全面集中的网络攻击信息库，建设各行业网络安全威胁和漏洞信息共享平台，有限或有偿地授权保险公司、网络安全保险科技企业等市场主体访问使用；③鼓励市场主体对于风险数据进行二次开发利用，推动国内网络安全险的产品多样化及定价灵活，实现对风险数据类别、特征的精准判断，为定价和核保提供相应的精算量化数据依据；④支持保险科技公司联合保险公司、安全厂商及各行业企业逐步建立跨行业数据共享分析机制。

5.3 落实行业标准规范

既要加强市场监管，也要开放市场，依托行业规范促进行业健康快速发展。

监管层面，6 月 20 日，由上海市信息安全行业协会归口的《网络安全保险服务技术要求》《网络安全保险安全服务能力评价指南》两项团体标准已形成标准征求意见稿。下一步建议相关立法机构继续推动完善、细化网络安全保险相关法律法规。

市场层面，保险公司和网络安全保险科技企业应重点培育面向网络安全领域的商业保险的技术、产品、管理和服务创新能力，推动形成行业认可的网络安全保险实践，联合联盟、公会、协会等组织，加快细化网络安全保险服务、技术等相关行业标准规范。

5.4 提升产业链路能力

产业持续发展需要科技创新，以创新链引领网络安全保险产业链。政府方面，建议加强市场牵引，鼓励网络安全保险科技领域建立一批试点企业，发展成为产业链上下游具有话语权的“链主”企业，形成示范带动效应。企业方面，建议加快产业创新融合，聚焦关键前沿技术攻关、技术创新融合应用。

此外，为加快培育产业链上下游企业共生发展生态，建议在《国家网络安全检查操作指南》《国家网络安全事件应急预案》等基础上形成“网络安全事件判定及公布指南”，并依法依规设立网络安全保险定责定损中立第三方机构，为定责定损提供参考标准。与此同时，随着国内外数据交易所、数据中介等模式的快速发展，网络安全保险产业生态可以引入网络安全保险数据中介机构，为产业发展提供基础数据支撑。在产业链路的完整、完善、深度融合之下，网络安全保险产业将进一步补足市场参与角色缺口，激发产业发展活力。

附录
网络安全保险科技企业生态 —— 以众安科技为例

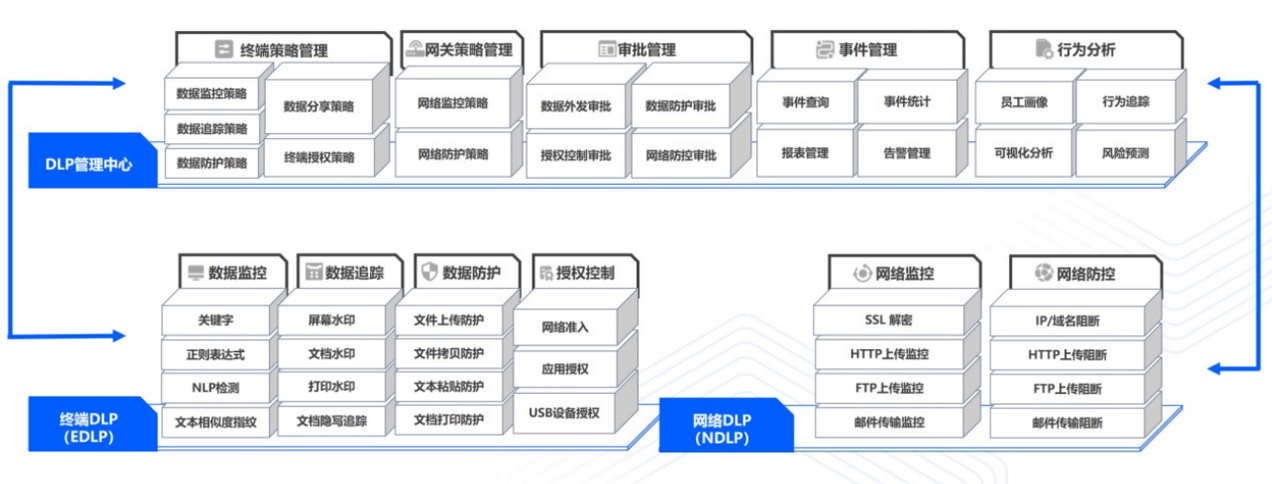
网络安全保险科技企业生态包含内部生态圈和外部生态池，前者依赖于企业生态系统本身具有的整体结构和整体性，后者则基于内部生态系统与外部的有机联动，进而激发新的生态价值。

以众安科技为例，众安科技基于区块链、人工智能、大数据、云计算等前沿技术探索，以科技构建生态新基建。在内部，联动安全公司保险公司（众安保险），形成整体资源优势。在外部，联动更多的安全厂商、研究机构、律所等生态合作伙伴，拓展资源边界。

目前，基于整体生态体系支撑，众安科技围绕三大核心产品系列——业务增长系列、业务生产系列、业务基建系列，覆盖保险经营中的产品设计、精准营销、核保核赔、服务与运营管理等关键环节，打造高效、安全、可靠的技术产品与解决方案。例如：

LOCKet DLP 办公环境数据安全解决方案：基于用户行为分析的数据防泄漏解决方案，利用大数据技术，通过分析企业员工终端行为及网络行为，准确识别数据泄漏风险并进行阻断。

LOCKet DLP 产品逻辑架构



生产环境数据安全解决方案：面向切面的架构设计，实现低耦合，高可重用的数据安全能力建设，既可满足快速的业务迭代的需求，又可实现统一严格的数据安全管控。

从企业生态到安全服务（产品）生态为例，众安科技的生态体系已具有一定前瞻性和网络安全保险科技发展代表性。

REFERENCES
参考文献

[1] Nist，“Cybersecurity Framework”，https://www.nist.gov/cyberframework.

[2] Research and Markets，“Cybersecurity Insurance Market”，https://reurl.cc/qNZnVR.

[3] Marsh，“US Pricing Q1 2022”，https://www.marsh.com/us/services/international-placement-services/insights/us-gimi-q1-2022.html.

[4] Allianz，“Allianz Risk Barometer”，https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

[5] Coalition，“2022 Cyber Claims Report”，https://info.coalitioninc.com/download-2022-cyber-claims-report.html.

[6] 360 天枢智库、中国中小微企业协会：《中小微企业数字安全报告》，https://mp.weixin.qq.com/s/7IYDrraJ4qvJfHsfymAh8Q.

[7] 参见蒋艳、陈羽凡：《从全球发展历程看我国网络安全保险发展机遇》，《工业信息安全》2022 年第 3 期。

[8] 德勤：《2022 年保险行业展望》，https://www2.deloitte.com/cn/zh/pages/financial-services/articles/financial-services-industry-outlooks-2022/pr-insurance-industry-outlook.html.

SICSI
CYBER RESEARCH INSTITUTE
赛 博 研 究 院

众安科技

出品方

上海赛博网络安全产业创新研究院

众安信息技术服务有限公司