蚂蚁集团 ANT GROUP

CAICT 中国信通院

网络安全保险实践与效果评估研究报告

蚂蚁科技集团股份有限公司

中国信息通信研究院云计算与大数据研究所

2025年7月

版权声明

前　言

随着数字经济的蓬勃发展，网络安全风险已成为制约企业可持续发展的重要挑战，数据泄露、勒索软件攻击、APT攻击等事件频发，不仅造成直接经济损失，更可能引发业务中断、声誉损害和法律责任的连锁反应。在此背景下，网络安全保险作为融合网络安全技术与金融风险管理的创新工具，正逐步成为企业应对网络风险、保障业务连续性的关键手段。

本报告聚焦网络安全保险的实践路径与效果评估，系统梳理网络安全保险发展现状，深入分析其在风险防控、能力建设和生态协同中的价值，并结合中小企业这一核心群体的实践案例，探讨行业面临的挑战与突破方向。旨在为行业参与者提供理论支撑与实践参考，助力构建更加稳健、智能的网络安全保险生态体系，为数字经济高质量发展保驾护航。

参 编 单 位

蚂蚁科技集团股份有限公司、中国信息通信研究院云计算与大数据研究所

编 制 人 员

彭越、王虹蕊、顾为群、彭晋、白晓媛、季雨洁、王铸成、邱喆彬、郭雪、卫斌、李忠权、马铭洋

目 录

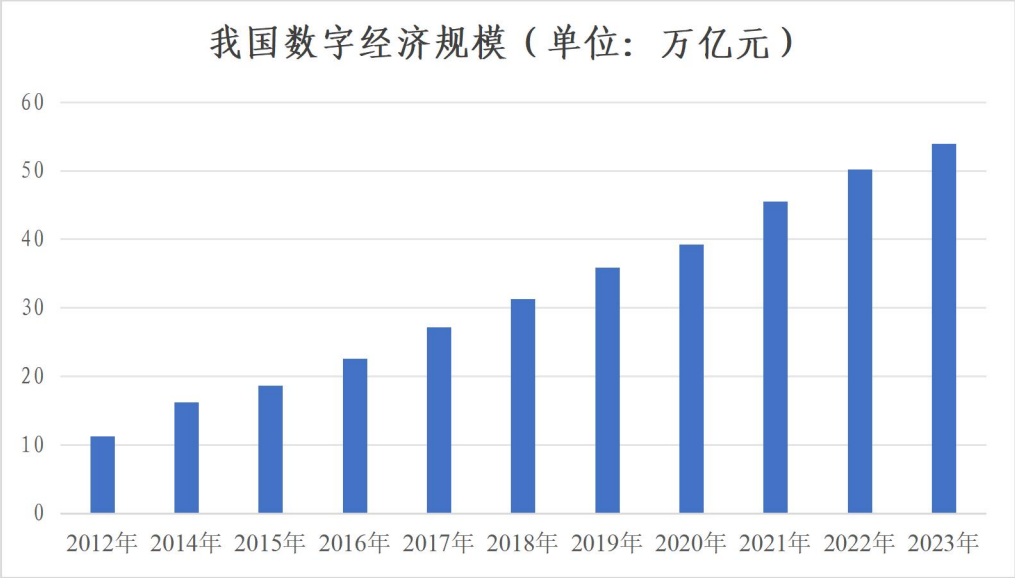
图 目 录

表 目 录

一、网络安全保险概述

（一）数字经济不断增长，网络安全风险日益凸显

数字经济已成为推动国民经济增长的关键力量。根据中国信息通信研究院《中国数字经济发展研究报告（2024 年）》，自党的十八大以来，我国数字经济进入加速发展周期，其规模从 2012 年的 11.2 万亿元迅猛增长至 2023 年的 53.9 万亿元，增长近 4 倍，数字经济正逐步成为引领经济高质量发展的重要引擎。



数据来源：中国信通院

图 1 我国数字经济规模

数字经济的高速发展与网络安全风险的共生性特征日益凸显。一方面，互联网、大数据和云计算等技术的广泛应用，使企业安全面临更加严峻的挑战。数据泄露、APT 攻击、勒索软件等新型安全事件频发，可能对企业产生财务损失、声誉损害和法律责任等一系列严重影响。**另一方面，**随着社

会数字化转型的不断深入，能源、交通、金融等关键基础设施领域已实现信息化的全域渗透，其网络攻击面持续扩大。一旦遭受网络攻击，关键基础设施的运行故障可能进一步引发网络安全事故连锁反应，造成重大的经济损失和负面的社会影响。构建更全面的网络安全防护体系，对于保障企业发展、维护社会稳定具有重要意义。

（二）数字安全已成为数字经济的关键要素，护航数字经济可持续性发展

数字安全是数字中国建设的关键防护屏障，成为推进中国式数字经济现代化的核心要素。《数字中国建设整体布局规划》中将数字安全置于核心战略地位，是保障数字中国建设全面发展的基础性支撑。面对数字化转型中数据泄露、网络攻击等风险，规划提出统筹发展与安全，既推动数据要素价值释放，又筑牢安全底线，实现数字安全与高质量发展的深度融合。

数字安全是保障数字经济可持续发展的必要条件，成为重塑战略优势的支点。在新一轮科技革命和产业变革加速迭代的背景下，数字安全已经成为争夺战略主动权、发展主动权的关键领域。随着云计算、人工智能等新兴技术的深度应用，数字安全产业范畴和影响力不断扩展，逐步成为战略布

局与现代化运营的重要支柱，对构建安全、可靠的数字生态具有重要意义。

（三）网络安全保险构建风险防控闭环，助力企业有效管理数字安全风险

面对日益复杂的网络攻击演进态势，传统网络安全体系建设存在局限性。现阶段，多数企业采用传统网络安全体系建设思路，通过部署安全防护产品、强化安全管理机制等手段，可有效降低安全事故发生的风险。但网络安全威胁的动态性本质决定了网络安全风险无法完全消除。**在技术侧，**由于网络环境和攻击手段的复杂性、多变性和超前性，使得防御体系难以实现对所有攻击的绝对阻断。**在管理侧，**人员安全意识水平不均、内部流程执行偏差及外部环境的高度不确定性，导致安全防御面临多重挑战。**在经济侧，**网络安全建设往往遵循边际效益递减规律，新增安全投入的产出效率可能显著降低。加之不同企业的风险偏好、成本承受能力存在结构性差异，难以形成普适性的投入评估框架作为行业基准。

网络安全保险成为缓解和转移网络安全风险的有效工具。网络安全保险作为网络安全产业与金融服务业融合的一种新兴网络安全工具，将风险分散和财务保障理念嵌入企业风险管理体系，有望成为支撑数字经济发展的重要基础设施。**一方面，**通过承保低频高损型网络安全风险，覆盖事件引发的直接经济损失、业务中断引发的预期利润损失、事件处置

成本及第三方赔偿责任，构建全链条财务缓冲机制。**另一方面，**借助保险精算模型与风险评估框架，企业可系统性量化自身风险暴露水平，精准识别防护体系中的风险敞口，进而结合风险容忍度阈值，动态优化资源配置策略，实现风险成本、防护效能与业务连续性的三重均衡。

二、国内外网络安全保险发展现状

（一）供需双侧协同驱动产业深化，美国网络安全保险市场进入成熟发展期

美国网络安全保险市场已形成相对成熟的产业生态。根据 Fitch Ratings 统计数据，2023 年美国网络安全保险市场保费规模达 69 亿美元，占全球市场份额近 60%。从行业分布看，服务业与金融业因承载海量敏感数据，保费占比较高。制造业受营业中断影响，保费占比迅速提高。投保主体结构方面，中小企业占据六成以上保费，风险治理需求在大企业与中小企业间逐步呈现均衡分布的态势。

需求侧驱动机制呈现多维度特征，其核心动因可归纳为合规压力、安全效率优化、赔付价值验证及供应链风险四大维度。第一，个人信息保护立法强化风险转移刚性需求。随着全球个人信息保护法规体系的完善，企业因数据泄露需承担的民事赔偿、监管处罚及声誉损失风险显著上升。例如，美国多州立法要求企业在数据泄露事件中承担强制性信息披露责任，倒逼企业通过网络安全保险转移因个人信息泄露

引发的潜在巨额赔偿风险，推动相关保险需求快速增长。**第二，数字化韧性建设进程催生保险与安全建设的动态平衡需求。**随着企业数字化进程的不断加快，特别是在金融业、制造业等上下游协同要求高的行业，对业务连续性提出了更高要求。然而，企业无法精准预判网络攻击规模，且难以承担按最大威胁场景配置安全资源的成本，导致“安全投入不足”与“过度防御”的矛盾长期存在。网络安全保险通过营业中断险等创新产品，将业务中断损失转化为可量化的风险标的，既降低企业因攻击导致的收入损失，又避免因过度防护产生的资源浪费，成为平衡安全投入与业务韧性的有效工具。**第三，赔付案例的累积增强了网络安全保险有效性的信心。**根据惠誉评级公司（Fitch Ratings）的统计，2021 年，美国网络安全保险的赔付率达到 67%，2022 年回落至 44.6%。针对转账欺诈、勒索攻击等各类事件的赔付案例使得企业清楚认识到网络安全保险的风险缓释和财务保障作用，进一步激发了需求的增长。**第四，供应链风险管理向上下游渗透扩大市场边界。**当大型企业重视网络安全风险并加强其供应链和生态安全管理时，往往会要求与其有业务往来的中小企业也采购网络安全保险，以整体控制上下游供应链的网络安全风险。这一效应，使得中小企业也逐步成为网络安全保险市场的重要投保群体，促成市场结构从“头部集中”向“金字塔稳态”的演进。

供给侧创新动能源于技术赋能驱动的产业链协同与风险分散机制升级。第一，专业化分工与技术赋能构建全链条服务能力。美国网络安全保险市场通过精细分工和专业化技术在风险评估、保中监测、理赔定损等环节形成了标准化的支撑体系。通过网络风险建模工具融合大数据、人工智能等技术，实现了差异化的定价策略，支持保险公司风险识别与精准承保能力。通过安全风险量化、非侵入式监测、事件响应和数据取证等专业技术能力，可为网络安全保险投保、承保及理赔环节提供有力支持，促进新型保险产品的创新和行业标准的建立。**第二是再保险机制分散系统性风险，释放供给侧创新动能。**近年来，网络安全事故的巨灾属性对保险机构形成显著承保压力。例如美国 CrowdStrike 公司由于软件更新导致的网络安全事故，网络风险分析平台 CyberCube 估计，在这一事件中保险公司的损失在 4 亿至 15 亿美元之间。潜在的巨额赔偿和未知的风险概率使得保险公司陷入既要承担未知概率的巨灾风险、又需保持产品经营的持续创新的两难境地。完善的再保险机制使得保险公司可以将风险转移至再保市场，在风险敞口管理与业务拓展之间取得平衡。有效缓解保险公司对极端损失的顾虑的同时，释放保险产品创新的动能。

（二）多行业需求齐头并进，欧盟网络安全保险市场迈入规模化发展阶段

欧盟网络安全保险市场已进入规模化发展阶段，其发展特征同样体现为政策规制与产业转型的双轮驱动。一方面，个人信息保护法规的实施推动了网络安全保险需求的快速增长。GDPR 生效迅速推动了网络安全保险市场增长，带动医疗、金融、零售和互联网等多个行业的保险需求上升。另一方面，**传统制造业在智能化升级中面临业务连续性保障挑战增加。**制造业投保和理赔的案例快速增长，为网络安全保险应用积累了丰富经验。例如 2019 年欧盟某家铝制品生产商因网络攻击造成约 7000 万美元的经济损失，其中大部分损失来源为营业中断损失。

（三）生态协同加速落地推广，我国网络安全保险市场逐步完善

我国网络安全保险市场逐步完善，越来越多保险公司与安全技术企业正积极布局网络安全保险领域，目前已形成“政策驱动-生态协同-需求激活”的阶梯式发展格局。从发展阶段来看，我国网络安全保险主要经历了三个阶段:

一是萌芽起步阶段，市场认知培育期。在 21 世纪初期，我国网络安全保险开启初步探索。2013 年 11 月，苏黎世财产保险（中国）有限公司推出首款网络安全保险产品，标志着行业进入商业化试点。此阶段保险产品形态受欧美影响，受制于企业风险意识薄弱、精算数据缺失等约束，产品定价机制尚未建立，市场整体对网络安全保险的认知有一定局限

性，产品和服务尚不成熟，投保企业数量较少，整体市场渗透率低。

二是探索发展阶段，顶层设计构建期。《网络安全法》《数据安全法》《个人信息保护法》和《关键信息基础设施安全保护条例》等法律法规相继出台，促使企业逐步认识到网络安全的重要性。2023 年 7 月，工业和信息化部、国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》，该文件作为首份针对网络安全保险领域的政策性文件，为行业的探索发展提供了明确指导。同年 12 月，工业和信息化部发布了《关于组织开展网络安全保险服务试点工作的通知》，通过组织开展试点项目，探索适合市场的保险产品，推动行业向规范化、系统化方向发展。

三是稳步推进阶段，生态协同深化期。随着顶层设计支持力度的加强和市场需求的增加，网络安全保险发展趋势呈积极增长态势。公开数据显示，2024 年网络安全保险保费规模超过 1.5 亿，保额超 95 亿元。**在供给侧，网络安全保险产品创新与生态协同不断深化。**以蚂蚁、华为、中国移动等为代表的平台型企业致力于推动行业风险评估模型的标准化进程，利用数字化手段优化整个投保理赔流程，降低企业参与门槛与成本。以深信服、奇安信、360、绿盟、启明星辰、深信服等为代表的安全技术企业积极探索将网络安全产品及服务与保险机制融合的新模式，形成“风险预防-保险兜底”

的闭环生态。以中国信通院为代表的第三方检验检测机构深度参与风险评估、定损定责等关键环节，推动行业标准与服务规范有效落地。各类生态参与方积极参与，为行业的健康快速发展注入了强劲动力。**在需求侧，网络安全保险市场需求激活成为关键挑战。**企业对网络安全保险在风险量化、财务保障、业务连续性管理中的核心价值认知不足，导致实际支付能力未能顺利转化为投保行为。同时，网络安全风险的隐蔽性与动态性使得定价模型精度不足，部分企业因保费与保障范围的不匹配性持观望态度。网络安全保险各参与方如何有效激发市场需求，体现网络安全保险的核心价值，成为网络安全保险产业下一步发展的关键。

表 1 网络安全保险发展历程

发展阶段	政策法规/关键事件	核心挑战
萌芽起步阶段	2013 年苏黎世财产保险(中国)推出首款网络安全保险产品	产品形态受欧美影响，定价机制未建立，企业风险意识薄弱，市场渗透率低
探索发展阶段	《网络安全法》《数据安全法》等法律法规出台，《关于促进网络安全保险规范健康发展的意见》发布	政策落地与执行效率，产品标准化与适配性，试点效果评估与模式验证
稳步推进阶段	2024 年保费规模超 1.5 亿，保额超 95 亿元	企业对保险价值认知不足，风险定价模型精度不足，生态协同效率待提升

三、我国网络安全保险建设体系分析

（一）网络安全保险覆盖多种企业责任和损失类型，形成全面保障

网络安全保险根据承保责任，可分为网络安全财产类保险和网络安全责任类保险。网络安全财产类保险，主要针对网络安全事件给第一方造成的直接损失以及因此产生的额外技术服务费用等提供保障，包括直接物理损失、营业中断损失、数据资产重置费用、硬件改善成本、应急处置费用、公关费用以及法律费用等。网络安全责任类保险，主要针对网络安全事件引起的对第三方个人或机构所需要承担的赔偿责任提供保障，包括数据泄露责任、网络安全事件责任、媒体侵权责任、外包商相关责任、产品责任或技术服务职业责任等。

表 2 网络安全保险风险场景

类别	保障内容	描述
网络安全财产类保险	直接物理损失	网络安全事件直接造成的物理资产损坏或损失。
	营业中断损失	网络安全事件导致的预期利润损失及必要的费用支出。
	数据资产重置费用	数据被破坏、丢失或加密后重新创建或恢复数据时所产生的费用。
	硬件改善成本	为提升硬件安全性而进行的改进成本。
	应急处置费用	网络安全事件发生后的紧急处理工作费用。
	公关费用	危机公关活动以减轻品牌影响的费用。
	法律费用	包括因数据泄露引发的法律诉讼等费用。

网络安全责任类保险	数据泄露责任	对第三方（数据主体）赔偿责任及相关法律诉讼费用。
	网络安全事件责任	对第三方遭受的经济损失或损害承担赔偿责任及相关费用。
	媒体侵权责任	因网络空间中不当信息发布构成侵权而产生的费用。
	外包商相关责任	由外包服务提供商造成的数据泄露或网络安全事件的责任。
	产品责任	产品缺陷导致第三方损失的赔偿责任。
	技术服务职业责任	提供技术服务时失误或疏忽导致客户损失的责任。

（二）网络安全保险场景化适配风险需求，行业覆盖深度持续扩展

网络安全保险贴合实际客户风险场景，在保险产品本身设计及保险配套的网络安全服务上做出针对性保障。基于对金融、医疗、汽车等重点行业的风险特征分析，形成了针对性的风险保障和服务体系，主要体现为两大特征。一是数据安全责任的普遍性保障，以《数据安全法》《个人信息保护法》等法规要求为框架，数据泄露风险保障成为跨行业标准配置，数据泄露风险保障成为各行业普遍配置的核心保障模块，助力企业构建合规底线与基础防护能力。二是关键领域业务特性设计差异化方案，例如金融业强化支付系统中断与勒索攻击防护，医疗行业深度绑定诊疗数据恢复与合规审查，制造业重点保障工业互联网设备故障引发的生产停滞风险，

通过垂直化定制方案精准匹配高价值场景的业务连续性需求，推动风险保障从“通用型”向“场景化”升级。

数据信息泄露和营业中断是常见的两种承保场景。一方面，在数据泄漏场景中，网络安全保险通过覆盖事件通报费用、系统修复成本及数据主体赔偿金等支出费用，成为企业合规应对数据泄露风险的重要财务缓冲机制。**另一方面，**营业中断场景是企业体感最强的场景，当企业遭受网络攻击致使业务中断时，企业核心目标是尽快恢复正常运营并减少损失和负面影响。网络安全保险可以为企业提供一定的赔付保障，避免业务中断期间的利润损失，为恢复受损的 IT 系统提供费用，并支持弥补服务中断对客户体验造成的负面影响。

（三）网络安全保险体系化构建标准框架，服务流程规范不断提升

一是构建网络安全保险标准体系，针对网络安全保险规范服务进行标准化建设。深化市场对于网络安全保险概念的理解，明确其在数字化时代的重要作用，精确划分从需求分析到保单执行的各个关键业务流程，提出贯穿保险周期的流程框架与服务准则，确保网络安全保险机制的高效与合规运作。针对网络安全保险落地实施进行标准化建设，依据保险流程聚焦于三个核心环节：首先是保前的风险评估，设立统一规范的评估模型和指标体系，准确识别和量化潜在的网络风险。其次是保中的安全防护，制定安全策略和响应措施的

服务标准，增强被保险方的防御能力，在面临风险时减少网络安全事件发生的可能性，在事故发生后尽力减小其带来的负面影响。最后是保后的定损理赔，建设公正透明的损失评估与赔偿流程，保障被保险人在真实发生网络安全事故后能够迅速恢复并得到合理补偿。通过一系列标准化举措构成网络安全保险稳健发展的基石，促进整个行业的成熟与规范。

二是在实践中持续细化完善网络安全保险规范标准。中国信息通信研究院深度参与云计算保险、信息技术服务保险、网络安全保险、首版次软件保险、DDoS 保险等领域保险产品设计。同时，中国信通院作为第三方机构深度参与保险产品应用的投保及理赔的整个流程，包括事前的风险评估流程以及事后的定损定责流程。**其一，**事前对投保企业或产品进行风险评估。第一是中国信通院牵头制定的 YD/T 4568-2023《云计算风险管理框架》行业标准，于工业和信息化部公告 2023 年第 38 号文件正式发布。第二是中国信通院牵头制定的 T/IAC CCSA36-2019《云计算保险风险评估指引》于 2019 年 12 月在中国保险行业协会正式发布，标准主要针对风险量化环节进行标准化支撑。根据风险管理相关标准，形成风险的量化结果，并出具风险评估报告。第三是持续深化网络安全保险领域标准化工作，中国信通院基于已有的风险评估框架，联合多家保险公司、再保险公司、网络安全企业等多家网络安全保险相关方，研制形成具备动态评分机制的面向

通用场景的《网络安全保险风险评估规范》，为国内企业提供更为科学、准确的风险评估服务，以满足企业在信息化进程中的多样化需求，为构建客观、公正的风险评估体系奠定基础。**其二，**事后对发生的安全事件进行实地勘察，并出具定损定责报告。在发生网络安全事故后的理赔过程中，中国信通院将重点评估网络安全事件的起因以及其造成的损失是否在承保范围内，对企业业务中断损失、数据恢复成本、法律诉讼费用等进行查勘、分析、计算，形成多方认可的定损定责报告。

（四）网络安全保险配套机制驱动安全能力提升，构建风险治理闭环

网络安全保险作为网络风险治理的创新工具，正从传统风险补偿工具向主动式风险管理基础设施演进，通过“风险识别、能力提升、保险保障”的多重体系，积极引导企业加大网络安全投入，推动企业安全投入与安全防护效能的螺旋式提升。

一是建立风险评估准入机制，夯实网络安全基础能力。网络安全保险产品通常面向投保企业基本的安全能力要求，企业需通过投保前的风险评估才可进行后续的网络安全保险采购工作。例如，某平台型企业联合保险公司及第三方机构推出的网络安全保险应用场景，投保企业在投保前需进行风险评估并达成合格线，且对高危漏洞完成 100%修复，才

能符合投保条件。这种约束机制推动企业在采购网络安全保险保障的同时，需要投入一定资源进行必要的安全措施改进，如高危漏洞修复等，从而推动企业网络安全基础能力的实质性提升。

二是创新动态费率调节机制，优化网络安全投资结构。投保企业通常会设立专项网络安全预算，该预算既可用于预防性投入，如购置安全设备、购买安全服务等，也可用于风险转移，即购买保险。网络安全保险的动态费率机制通过“安全能力—保费成本”的正向关联，为网络安全管理水平较高的企业提供更优惠的保险费率或更高的保险额度。促使已投保企业调整风险管理预算在预防性措施和风险转移两者之间的分配，在预防性措施与风险转移之间寻求最优平衡点。在这一过程中，已投保的企业积极投资预防性措施，形成“投入—能力—保费”的良性循环，实现企业网络安全水平与保险保障效能的双向提升。

（五）网络安全保险亟需提升企业接受度，激发行业需求

当前网络安全保险面临的核心挑战在于如何突破企业认知与价值认同的双重瓶颈，需通过构建可验证的价值闭环与生态化风险治理机制，驱动市场需求从政策驱动向内生需求转型。

一是利用新型险种责任厘定机制推动风险案例披露。当前网络安全保险落地实践中往往缺乏典型理赔案例。一方面

是投保企业安全能力达到了一定的水位线，触发理赔事件的频率降低。另一方面企业往往由于事故曝光后导致问责、负面商誉影响等原因不愿主动发起报案理赔。当前亟需通过抗DDoS 营业中断险等新型网络安全险种的引入，厘清企业在网络安全事故中的责任，改变公开理赔案例稀缺的现状。

二是带动网络安全保险需求在供应链上下游的传导效应。随着产业数字化程度的深化，企业间数据交互与业务协同的深度增加，单点安全事件可能引发链式反应，如 A 企业营业中断可能直接导致 B 企业的供应链中断，进而无法正常生产经营，通过投保网络安全第三者责任险，当供应链某节点发生事故时，保险公司承担损失补偿责任，保护受害方企业正常运营，避免风险向供应链中心企业传导。这种风险分担机制，使网络安全保险从企业个体的防御工具升级为产业生态的治理基础设施，从而推动网络安全保险的需求爆发。

（六）网络安全保险投保场景多元化，有效应对复杂网络威胁

多元化保险策略已成为企业风险管理的核心工具，其场景化投保解决方案正推动网络安全保险向精细化、精准化方向演进。通过构建覆盖多维场景的保险生态体系，可为企业提供差异化的风险减量管理方案，显著提升其应对新型网络威胁的能力。

一是公有云基础设施投保场景。该场景聚焦数据中心与广域服务网络的安全保障，通过构建全链路保险防护体系，有效应对基础设施层的潜在安全威胁。企业可根据关键业务系统的优先级自主配置保险覆盖范围，既可防范数据泄露、服务中断等重大风险，又能将单次安全事故造成的经济损失控制在可接受范围内，实现关键信息基础设施的韧性提升。

二是私有化部署专属投保场景。针对企业内网资源的特殊性，设计定制化网络安全保险产品，重点防范内部人员操作失误、恶意攻击及系统漏洞等复合型风险。通过建立“风险评估-保险覆盖-应急响应”的闭环机制，不仅实现风险转移，更可推动企业完善内部安全管理制度，从而增强客户对私有化服务的信赖度。

三是产品服务全周期投保场景。面向物联网终端、智能软件等新兴技术产品，构建覆盖研发、生产、交付全生命周期的保险解决方案。通过将产品责任险、网络安全险等组合创新，既可转嫁产品故障、数据泄露等运营风险，又能为客户提供“保险+服务”的增值服务包，有效提升产品可靠性能力，打造差异化竞争优势。

四是互联网平台综合投保场景。基于云计算、信息技术应用等科技保险产品，创新开发“平台运行安全综合保险”，构建包含业务中断险、声誉损失险等在内的多维度保障体系。该场景通过建立“事前预防-事中响应-事后补偿”的全周期风

险管理模型，构建平台运行安全闭环，减轻突发事件的经济损失，推动安全管理标准化。

五是平台服务商创新投保模式。通过建立“保险+评估”的准入机制，要求平台服务商在入驻前完成网络安全能力评估及专项投保。该模式创新性地将保险工具嵌入供应链管理环节，既可提升服务商的安全合规水平，又能通过保险赔付机制分散平台整体运营风险，形成“保险赋能-风险共担-生态共赢”的良性循环。

四、面向中小企业的网络安全保险实践总结

（一）中小企业是网络安全保险发展中需重点关注的群体

一是中小企业仍面临严峻的网络安全挑战。根据《2022中小微企业数字安全报告》相关数据显示，中小企业已成为国民经济不可或缺的重要力量。贡献了我国50%以上的税收、60%以上的GDP及80%以上的城镇就业岗位。然而，中小企业面临的网络安全威胁日益凸显，85%的中小企业表示，在过去的一年内遭遇过网络安全问题，有77%的中小企业表示无法自身进行有效处置。

二是网络安全保险对中小企业的战略价值不亚于大型企业。大企业在网络安全建设中拥有更丰富的“武器库”和资源，且日常会经受严格的攻防演练。中小企业普遍缺乏针对性的防护资源，传统安全厂商的“抓大放小”策略进一步加剧

其安全能力短板，客观上造成现有的主流安全解决方案没有充分考虑中小企业需求，导致市场上缺少针对中小企业设计的安全产品或服务，使中小企业的安全能力建设捉襟见肘，其网络安全建设缺乏可参考的安全建设路径。

三是网络安全保险为中小企业提供风险导向的建设新范式。与传统以能力提升为核心的安全建设模式不同，网络安全保险构建了“风险评估—风险治理—保险兜底”的闭环机制。保险公司和技术服务商基于风险视角，动态评估中小企业的安全薄弱环节，精准识别风险敞口，针对性设计保险产品与配套安全服务。这种市场化机制倒逼保险机构开发适配中小企业特性的解决方案，既降低了安全投入门槛，又引导企业优先修复高危漏洞，以风险为导向帮助中小企业建设网络安全管理体系。

（二）中小企业网络安全保险发展仍存在诸多挑战

从供给侧来看。第一是定价机制僵化。网络安全保险由于缺乏针对中小型企业的威胁情报和攻防效果的全面数据和算法，无法依据客户面对的威胁态势和风险敞口来差异化定价，因此往往会选择偏高的定价以便避免保险产品亏损。部分保险公司倾向于采用网络安全产品/服务来稀释风险，但现有的网络安全保险解决方案，其定价多基于大型企业的“全面建设”需求设计，对中小企业而言仍显成本偏高。**第二是网络安全保险产品标准化程度低。**网络安全

领域的复杂性导致相关法规和标准体系尚不完善，增加了保险公司进行风险评估和承保的难度。缺乏统一的行业操作指引，容易造成专业术语不统一、语义界定不明确等问题。例如，不同保险公司对于营业中断损失、等待期、营业中断触发条件等定义各不相同，且保障范围也存在差异，这都增加了待投保企业理解和选择网络安全保险产品的难度。

从需求侧来看。第一是风险认知度不高。多数中小企业尚未建立网络空间责任认知框架，对潜在威胁的感知停留在"偶尔被攻击"的认知，未能意识到网络安全风险可能引发的合规处罚、商誉损失等连锁反应。导致企业将网络安全保险视为可选支出，而非必要支出，难以主动寻求网络安全保险产品。**第二是缺少对网络安全保险的价值验证。一方面是网络安全保险理赔案例缺失。**安全往往被认为是企业本身的责任。一旦出现事故，企业会尽力避免理赔，即使理赔也不希望事故被传播，导致企业自主投保的积极性受到很大限制。**另一方面是缺乏衡量证明网络安全保险有效提升投保企业网络安全水位的案例和度量衡。**在实践中，大量投保企业购买网络安全保险的动力来源，是与外部客户合作的要求或是从事某类经济活动的准入要求。也就是说，企业投保的动力来源于外部从合作伙伴或监管侧的要求，期望通过网络安全保险来有效降低投保企业的风险，提升其安全水位，而不单

纯是风险转移。网络安全保险不应仅限于风险转移，而应成为推动企业加强网络安全建设的重要工具，需要有新的案例和度量衡证明网络安全保险能有效牵引投保企业的网络安全建设。

（三）与现有产品或服务结合推动网络安全保险创新

针对中小企业共同面对的问题与挑战，目前已开展各种新型的网络安全保险实践，有望进一步推动中小企业应用网络安全保险。

一是针对供给侧网络安全保险价格偏高的问题，通过“补贴+灵活定价”的方式提供新思路。例如，宁波市推出面向中小微企业的“网络安全产品超市+网安保”组合服务模式，多家安全服务供应商提供多层次网络安全防护套餐，企业可从中自主选择，同步匹配不等的保险保障额度，并配套阶梯式保费补贴政策。创新实践通过将网安产品与网络安全保险相结合，引入网安产品降低保险赔付概率，并通过财政补贴激发企业投保积极性，为行业探索普惠型网络安全保险提供了可参考的标杆案例。

二是针对需求侧中小企业网络安全风险意识淡薄的问题，通过“业务+保险”的形式有效激发投保意愿。例如，数据类保险产品重点解决数据安全、数据产品知识产权等多项数据风险，对中小企业在数据要素流通过程中可能面临的第一方损失风险和第三方赔偿责任提供保障。该模式一方面可通

过保险为业务的安全性提供背书，既保证业务顺利开展，又可在发生意外事故时补偿其导致的损失。另一方面将网络安全风险具象化为数据流通、产品交付等具体业务场景中的风险敞口，使企业直观认识到网络威胁对其主营业务的实际影响，从而提升投保主动性。然而，在该模式当中会存在责任认定模糊的问题，例如服务提供方应将业务安全视为其责任，而非将其风险转移给保险公司，忽视其责任。当保险兜底机制削弱了服务方自身的安全投入动力，反而可能导致风险事故的高频发生,违背“业务+保险”模式提升整体安全水平的初衷。因此，可在产品设计中建立"保险责任与服务方责任"的协同机制，通过合同条款明确风险共担原则，确保该模式在推动投保需求的同时，不弱化核心服务方的网络安全主体责任。

三是通过保险推动安全能力建设路径验证网络安全保险治理价值。网络安全保险本质上属于风险缓释工具，其核心功能在于转移网络安全风险而非直接提升网络安全水平。因此该路径的验证逻辑聚焦于"保险需求传导—安全服务供给—能力提升闭环"的实现机制。例如，在“网络安全保险+托管服务”的创新模式中,其一是通过保险方案配套基础安全托管服务，涵盖保前的风险评估与修复建议、保中的常态化风险巡检、事后的应急响应处置等全流程服务内容。在此过程中，投保企业可定期接收定制化外部威胁情报分析与漏洞

扫描报告，基于动态威胁态势实现防护策略的迭代升级。其二是通过动态费率机制构建激励杠杆，以“动态费率”为代表的经济杠杆来有效撬动投保企业的网络安全建设。投保企业的网络安全水位越高，其投保费率越低的机制已在实践中落地，通过该机制可激励企业投入更多资源提升网络安全水平，达成安全能力提升与综合成本优化的双重目标。

五、网络安全保险效果评估与验证

（一）网络安全保险风险评估体系多维验证企业风险状况

建立一套行之有效的网络安全风险评估体系，证明网络安全保险可有效提升投保企业的网络安全水位，对推动企业积极应用网络安全保险，具有重要的意义。

一是网络安全保险的风险评估体系需综合考虑多项关键因素。网络安全保险通过构建多维度评估框架，系统性验证企业安全能力提升成效。该体系需覆盖企业基本信息、漏洞和风险及其历史情况、安全管理成熟度、安全能力完备性、安全运营全面性、所处行业水位等多个方面综合评估投保企业的安全能力。企业基本信息包括所属行业、组织规模、安全投入等信息。漏洞和风险及其历史情况围绕保险保障范围，对被保险人现有漏洞和风险、历史漏洞和风险、历史理赔信息等进行扫描识别和梳理。安全管理成熟度包括企业安全资质、连续性管理、数据安全管理、合作外包管理、应用安全

管理的建设和执行情况。安全能力完备性包括企业在防护能力和防护范围上的情况。安全运营包括对安全资产、网络安全、系统安全、应用安全、数据安全的具体运营情况，以及是否有威胁情报信息感知渠道等。行业水位评估包括被保险人所属行业的宏观风险状况，包括行业风险、行业要求等间接影响风险发生的可能性和损失大小。

二是网络安全风险评估体系能有效指导企业进行安全能力升级建设。其一系统梳理企业的安全投入和安全机制情况，应从 IT 系统投入、容灾及可用性管理、敏感数据管理、供应链网络安全管理及网络安全专项投入等维度，系统梳理企业信息技术基础设施规模、灾难恢复策略、数据安全措施、供应链安全机制以及资金人力投入情况，识别潜在风险敞口并构建数据基础。**其二是帮助企业识别高危漏洞并提出修复建议，**通过自动化工具与人工检测结合的方式开展漏洞扫描，重点识别注入漏洞、文件操作漏洞、信息泄露等高危漏洞并提出修复建议，同时通过安全基线测评检验企业信息系统、供应链及云环境的配置合规性，确保基础防护能力达标。**其三是帮助企业分析外部安全态势，**一方面分析外部攻击趋势、公开漏洞信息及数据泄露事件等情报，评估企业核心资产暴露风险。另一方面调研内部 WAF 覆盖率、系统漏洞数量及风险事件处置情况，综合判断企业安全防护体系与应急响应能力。通过评估体系描述的三方面内容相互印证，形成对企

业网络安全水位的全景式诊断，为保险机构量化风险敞口、制定承保策略提供科学依据。

三是网络安全保险评估体系兼容性升级。评估体系应具备动态的适应能力，考虑金融、医疗、能源等不同行业的差异化风险特征，同时兼顾中小企业与大型企业的规模差异，以及企业当前网络安全防护水平的动态演进，确保能够全面评估企业的风险水位。通过按照行业属性、企业规模和安全成熟度等要素进行参数化配置，形成具有行业特异性、规模适配性和风险针对性的定制化评估方案，切实提升网络安全保险产品的精准化服务能力和风险管控效能。

（二）网络安全保险驱动企业安全能力建设升级

通过持续优化的网络安全保险机制与安全能力建设的耦合关系，网络安全保险正从“风险转移工具”向“安全能力建设催化剂”加速转型，助力企业构建可持续的网络安全防护建设。

一是通过风险评估及技术指导推动企业完善安全防护体系建设。中国信通院“云安全及互联网平台运行安全”保险服务方案成功入选工业和信息化部《网络安全保险典型服务方案目录》。同时，中国信通院依托服务方案开展网络安全保险试点工作。其中某私有云服务商参与投保，通过提供风险评估及技术指导等全流程服务，初步验证网络安全保险在帮助企业完善安全防护体系的价值。**其一是风险评估驱动安**

全短板精准识别。在投保前，通过引入专业机构开展全维度风险评估，帮助企业厘清资产分布、威胁暴露面及管理漏洞，精准定位关键业务系统的安全薄弱环节。基于评估结果，企业实现资源优化配置，优先加固高风险区域，既提升了安全认知水平，又为后续防护策略制定提供了科学依据。**其二技术指导助力安全防护体系实现长效化运行。**在风险评估基础上，为企业定制化改进方案，建立标准化的安全运营流程，协助开展定期漏洞扫描、应急响应预案更新及合规审查机制建设。使企业将安全防护从“事件驱动”转向“能力驱动”，形成覆盖资产、人员、技术的立体化防御体系。

二是通过设置投保门槛与动态费率推动企业安全治理能力。在某平台型企业联合保险公司及第三方机构开展的网络安全保险试点中，设置投保门槛与动态费率机制的双重激励，初步验证网络安全保险在推动企业安全能力建设方面的治理价值。**其一是企业安全投入实现升级。**在投保前，49家中小型企业在投保初期均缺乏基础安全防护体系，其中47家企业未采购Web应用防火墙（WAF）、主机入侵检测系统（HIDS）及态势感知产品，仅2家企业部署了WAF/HIDS但未配置态势感知。在投保后，49家企业完成WAF、HIDS及态势感知产品的100%覆盖，实现从“无防护”到“全栈防护”的提升。该变化表明，保险机制有效引导企业补齐安全能力短板，构建起网络层、主机层、应用层的立体防御体系。**其**

二是漏洞风险管控取得实质性进展。在投保后，投保前存在的 11 家企业的严重/高危漏洞，试点期间完成 100%修复，有效解决初始安全隐患。在保单延续过程中，17 家投保企业经扫描发现 26 个严重和高危漏洞，其中 12 家企业的严重和高危漏洞已完成修复，剩余漏洞同步按计划整改。

三是通过保险服务赋能平台生态推动用户安全能力升级。在某 ISV 服务商的业务场景中，其平台用户涵盖大量中小型商家、第三方系统开发商及供应链合作伙伴。这些用户普遍面临网络安全投入不足、防护能力薄弱的问题，作为平台方需承担一定的连带责任风险。通过网络安全保险服务为平台用户赋能，验证了“保险+安全”模式在降低用户风险、提升平台生态安全水平方面的治理价值。**其一是动态监测构建长效防护机制**。通过平台的监控数据实时评估用户安全状态，定期生成风险报告并提出改进建议。对高风险用户（如存在未修复漏洞的商家），启动定向加固计划，通过技术升级或流程优化降低风险敞口。在此基础上，平台、用户与保险公司形成“风险共担、能力共建”的生态闭环，将事件影响控制在最小范围。**其二是平台与用户安全水平协同优化**。通过为用户投保网络安全保险，显著降低了中小商家的安全门槛，使其无需额外采购复杂工具或组建专业团队即可获得全面保障。这一模式不仅增强了平台服务的吸引力，还通过用户安全能力的集体提升，推动整个生态系统的风险防控水平。

六、发展与展望

（一）网络安全保险市场需求不断激发

标准化进程推进重塑网络安全保险市场格局。网络安全保险逐步迈入系统化、标准化发展阶段，标准化为为市场提供了统一的服务框架和操作基线。产业层面，标准化加速了“保险+安全”服务模式的深度融合,提升了保险产品的专业化与场景适配性，也倒逼网络安全服务向标准化、可量化方向演进；技术层面，为精准定价、动态风控提供了技术支撑，进一步增强了网络安全保险的可扩展性与可持续性。标准化举措通过降低交易成本、提升服务效率、扩大覆盖范围，为网络安全保险从“小范围探索”迈向“规模化应用”奠定了基础，最终推动形成技术赋能、生态协同、风险共治的新型网络安全保险发展格局。

网络安全保险产品创新成为激活市场需求的核心驱动力。网络安全保险产品根据不同行业的特点以及客户的特定需求量身定制，不再用传统“一刀切”式的保险产品满足市场需求。具体而言，针对金融、医疗保健、零售等高风险行业推出专门的保险计划，涵盖各自领域常见的安全问题如身份盗窃、支付欺诈等。允许客户根据自身实际情况自由组合保障项目，如可以选择是否包含勒索软件防护、社交媒体账户保护等内容。除了基本的经济补偿外，并提供一系列增值服务，如定期安全培训、免费漏洞扫描报告等，帮助投保单位

持续改进内部安全管理机制。这种定制化服务模式不仅提高了客户满意度，也为企业提供了更加精准的风险管理和应对策略，吸引客户从而扩展市场需求。

理赔案例的积累将成为网络安全保险价值验证与产品优化的关键路径。随着网络安全保险试点的深入应用，理赔案例的持续沉淀不仅是保险产品风险定价的基础，也是企业认知网络安全保险风险缓释价值的关键步骤。为解决理赔案例缺失的问题，网络安全保险的持续探索应尝试寻求创新理赔场景，场景需满足两项核心条件：其一，企业因网络安全事件产生可量化的直接经济损失。其二，在行业共识下，事件发生时企业作为直接受害者无需承担主要责任。这种场景设计既能通过经济补偿机制强化企业投保意愿，又能通过责任边界清晰化降低保险机构的赔付争议风险,形成“事件发生—主动理赔—风险复盘”的良性循环。**例如，基于 DDoS 攻击的营业中断险成为当前有效的理赔场景突破口。**基于 DDoS 攻击的营业中断险基本满足上述两个核心条件：一方面，企业因 DDoS 攻击导致业务中断时，每分钟的宕机时间均可转化为订单流失、客户流失等直接经济损失，损失金额具有可追溯性与可验证性。另一方面，由于 DDoS 攻击具有分布式、隐蔽性强的技术特性，企业即使部署了合规的防护体系，仍难以完全杜绝攻击发生，行业普遍认可此类事件属于不可抗力范畴。这就使得该险种可以率先积累规模化理赔案例，有

望真正让需求侧的企业认可网络安全保险的风险缓释作用。

（二）智能化与云化赋能网络安全保险创新

网络安全保险正经历从传统功能性产品向全面智能化、定制化服务的转变。随着人工智能、大数据等先进技术的不断进步，网络安全保险智能化发展贯穿于整个保险周期的各个环节，包括保前的风险评估、保中的实时监测与响应以及保后的理赔处理。在保前阶段，通过引入大数据分析和机器学习算法，准确地评估企业的网络安全状况，并据此定制个性化的保险方案。通过智能化风险评估系统自动扫描网络环境，识别潜在的安全漏洞，根据最新的威胁情报进行动态调整得到合理的保险费用。同时，动态定价机制允许保险公司根据客户实时的安全状况调整费率，激励企业持续改善其网络安全措施，形成良性循环。在保中阶段，智能化技术的应用进一步提升网络安全管理的效率与效果。通过实时监测与预警系统，可以实时监测投保企业的网络活动。当发现异常行为或潜在攻击迹象，系统将自动触发预设的应急响应程序，如隔离受感染设备、关闭可疑连接等，借助主动防御策略保护客户免受直接损害，最大限度地减少企业损失。在保后阶段，传统的理赔流程往往繁琐复杂，耗时较长，且容易出现人为错误。通过实现智能化理赔实现在线提交证明材料，快速完成审核工作，缩短理赔等待时间。同时智能化理赔可集成欺诈检测功能，通过模式识别技术和历史数据对比，有效

识别出虚假索赔请求，保护保险公司免遭经济损失。在服务交付上，随着 SaaS（软件即服务）、PaaS（平台即服务）等云技术的发展，越来越多的网络安全保险服务开始采用线上交付模式，降低运营成本的同时，也为企业提供了更加灵活的选择。从最初的现场风险评估到全链条数字化管理，智能化转型标志着网络安全保险行业向着更加高效、透明的方向迈进。通过线上平台，企业可以轻松获取各种增值服务，如定期的安全培训、免费的漏洞扫描报告等，进一步提升自身的网络安全防护能力。

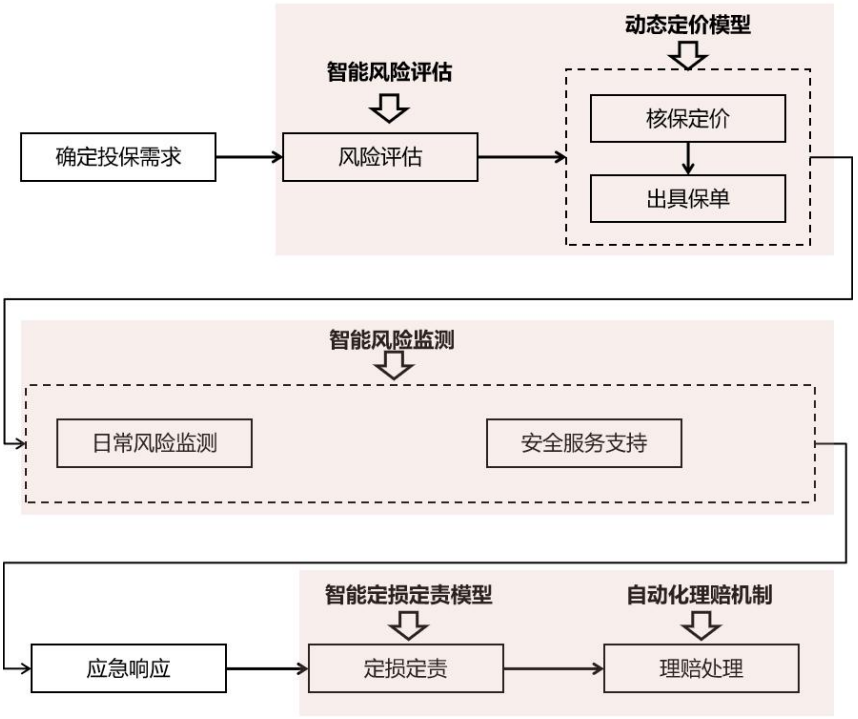


图 2 网络安全保险智能化流程

（三）跨职能合作构建网络安全保险生态系统

网络安全保险由不同职能参与方形成行业生态合作系统。包括保险公司、再保险公司、中介机构以及网络安全企

业和第三方检验检测机构，产业各方依托自身优势发挥不同作用，共同构成了一个完整的网络安全保险生态系统。

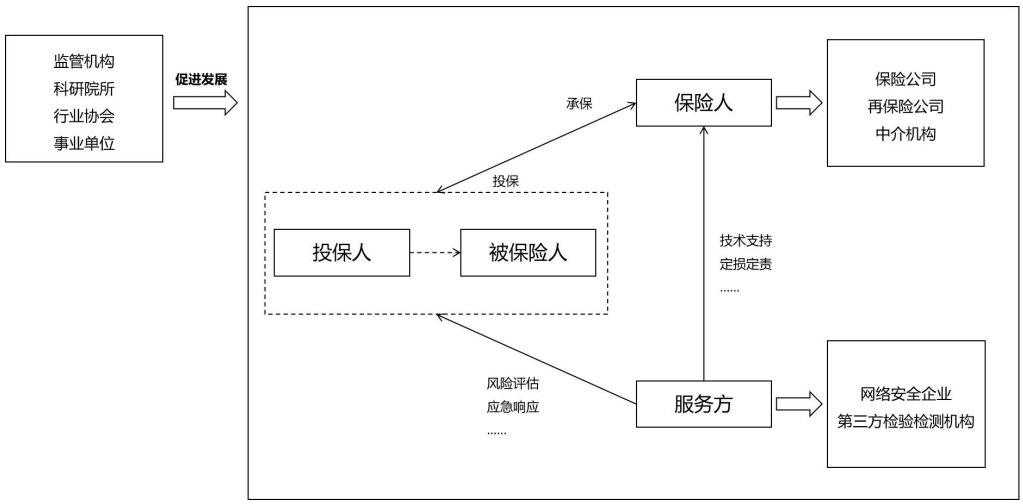


图 3 网络安全保险生态系统体系图

跨职能的生态系统成为网络安全保险领域的重要趋势。网络安全保险不仅是保险公司和被保企业之间的双边关系，也将吸引网络安全公司、第三方检验检测机构、法律服务提供商和技术服务商等多方力量共同参与。提供从风险评估、安全培训、技术支持到应急响应等一系列服务，构建形成全方位的安全保障链条。**首先，**面对不断变化的安全环境，网络安全保险产品和服务也将趋向多样化发展，涵盖前沿技术与经济赔偿机制的一站式解决方案，并配套定期风险评估、员工安全意识提升、持续性安全监控及快速响应支持等增值服务，满足不同行业和规模企业的特定需求。**其次，**面对日益增多的新型风险场景，保险公司将与更多网络安全保险需求方形成紧密合作关系，如与工业互联网企业进行协作，深

入贴近实际需求，不局限于传统IT设备保障场景，充分考虑到工业互联网环境下OT设备的特殊需求及其与IT设备之间的相互作用，更准确地识别和评估工业互联网环境中的独特风险，推出贴合场景需求的网络安全保险产品。

若您对本报告有任何建议，请联系:

welcome@caict.ac.cn