工信安全智库
洞察系列报告

报告编号：2021-dc-23

我国网络安全保险产业发展白皮书

（2021 年）

国家工业信息安全发展研究中心

2021 年 12 月

“工信安全智库”系列报告编委会

编写组

国家工业信息安全发展研究中心

北京源堡科技有限公司

中国人民财产保险股份有限公司

中国太平洋财产保险股份有限公司

中国人寿财产保险股份有限公司

中国平安财产保险股份有限公司

国任财产保险股份有限公司

诚泰财产保险股份有限公司

中国财产再保险有限责任公司

江泰保险经纪股份有限公司

南方电网数字电网研究院有限公司

奇安信科技集团股份有限公司

绿盟科技集团股份有限公司

北京启明星辰信息安全技术有限公司

杭州安恒信息技术股份有限公司

北京亿赛通科技发展有限责任公司

上海嘉韦思信息技术有限公司

瑞士再保险股份有限公司北京分公司

诺德(中国)保险经纪有限公司

序

国家工业信息安全发展研究中心经过 60 余年的发展与积淀，在智库研究方面形成了丰硕的积累。2018 年 9 月，中心推出“工信安全智库”品牌，立足深化供给侧结构性改革和加快建设创新型国家战略需求，围绕制造强国和网络强国建设任务，聚焦网络安全、数字经济、信息技术产业、战略前沿等重点领域，开展基础性、战略性、先导性智库研究，为工业和信息化部、中央网信办、国家发展改革委等提供智力支持。

“工信安全智库”自 2019 年开始陆续推出“研判”“洞察”“瞭望”“指数”“案例”“编译”等系列研究报告，围绕党和政府决策急需的相关重大课题和关键问题，开展形势研判、专题调研、国际跟踪、景气测度、案例分析、报告翻译等方面的持续研究，为主管部门预见走势、把握机遇、应对挑战、谋划战略提供参考。

《我国网络安全保险产业发展白皮书》是在工业和信息化部网络安全管理局的指导下，由国家工业信息安全发展研究中心联合北京源堡科技有限公司等 18 家单位共同撰写。报告阐述了网络安全保险相关基本概念，梳理了国外网络安全保险的三个发展阶段，分析了当前我国网络安全保险市场发展现状及面临的问题挑战，并提出了相关对策建议。

由于成稿仓促，加之水平有限，报告中难免有疏漏和错误之处，恳请批评指正。

编写组

2021 年 12 月

摘　要

随着数字化、网络化、智能化程度不断加深，以工业互联网、车联网、能源互联网等为代表的新场景新业态不断涌现，网络空间风险格局加速演变，持续动态变化的网络风险将造成极为广泛的经济影响。据 Cybersecurity Ventures 预测，2021 年因网络犯罪造成的全球经济损失预测将达到 6 万亿美元，逼近世界经济的 10%。随着各行业企业以及国家层面对网络安全风险管理重视程度持续上升，保险作为风险转移，尤其是残余风险管理的重要手段，被越来越多企业纳入网络风险管理框架中，网络安全保险有望迎来超百亿的市场空间。

全球网络安全保险市场起源于上世纪 90 年代，伴随网络安全与数据安全相关法律法规的实施逐步发展壮大，网络安全风险管控能力持续提升，网络安全保险的保障范围不断完善、保险方案日益丰富、保费规模快速增长。广义的网络安全保险除了面向企业提供的网络安全财产险和网络安全责任险等险种外，还包含面向个人的账户安全险等个人网络安全保险，本白皮书聚焦一般意义的网络安全保险，即面向企业的商业网络安全保险。

目前，我国网络安全保险市场已迈入初步探索阶段，保费规模突破 7080 万元，最高保额超 4 亿元。保险公司在产品设计、技术服务、商业模式等方面布局加快，以网络安全公司、保险科技公司为代表的第三方风险管理技术服务机构积极发挥专业优势，向保险方与被保险方提供双向风险管理服务，深度参与网络安全保险产业生态。然而，我国企业投保需求释放不足、安全服务尚未满足保险流程需要、保险

公司风险管控能力有限等问题亟待破解。建议进一步优化产品服务供给，强化需求牵引作用，推动网络安全保险服务标准化，促进保险公司、安全服务机构、第三方风险管理技术服务机构等各类市场主体深度协同，以推动产业逐步进入快速发展阶段，打造良性的网络安全保险生态体系。

白皮书主要分为五个部分，**第一部分**针对网络安全保险定义及服务流程进行概念梳理。**第二部分**基于对国外网络安全保险市场发展阶段、主要商业模式变化趋势的分析，剖析国外市场实现快速发展的关键因素。**第三部分**明确我国网络安全保险产业已步入初步探索阶段，梳理产业发展现状，总结当前主流商业模式，并介绍分析典型的产业案例。**第四部分**分别从国内网络安全保险产业的供需两侧切入，剖析限制产业发展的主要问题。**第五部分**展望我国网络安全保险产业发展未来，并提出针对性对策建议。

目 录

以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等为重要构成的网络安全法律体系日益完善，《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）》将“探索开展网络安全保险”作为“网络安全产业资本赋能工程”的重要组成部分之一，为我国网络安全保险发展营造了良好政策环境。目前，我国网络安全保险市场正处于初步探索阶段，我国需借鉴国外经验，加速市场布局，激活市场需求，提升供给能力，强化服务保障，推动网络安全保险“本土化”发展。

一、网络安全保险概述

伴随产业数字化转型加速推进，网络安全风险日益突出，网络安全技术产品的部署应用能够很大程度上提高企业抵御网络安全风险的能力，但并不能完全消除风险。网络安全保险作为企业实现风险转移的有效手段之一，在转移残余风险、优化资源配置、保障组织财务稳定性和业务连续性等方面发挥着重要作用。

（一）网络安全保险保单形式

网络安全保险是承保与网络空间风险等相关风险为目的的保险合同[1]。具体而言，投保人根据网络安全保险单（即合同）向保险人支付保险费，当合同约定范围内的网络安全事件发生时，保险人依据合同条款就对应的财产损失和第三方责任承担赔偿保险金责任的商业保险行为。网络安全保险单应充分对应网络安全保障与风险转移需求：一是以投保人信息资产安全性（包括完整性、机密性、有效性

[1] 欧洲网络与信息安全局（ENISA）对网络安全保险的定义。

等）为保险标的；二是以网络安全事件或网络安全风险为保险事故；三是根据承保安全风险的复杂性，保险产品类型可划分为财产损失保险或责任保险。在保险实践中，网络安全保险单有**两种主要形式：一是独立保单，**即仅针对事先约定的网络安全事件、风险开展保险保障；**二是综合保险单，**在已有责任险、财产险或其他保险基础上针对网络安全风险进行扩展投保。

近年来网络与信息技术的快速发展和深度应用，使网络应用与实体设备逐渐融为一体，源自网络空间的安全风险也逐步向现实世界渗透，或将威胁人民群众的生命财产安全乃至国家安全。风险的不断演进也将持续推动网络安全保险发展更加全面的保障范围，以实现更高水平保障能力。同时，随着工业互联网、车联网、能源互联网等新兴融合技术的应用普及，网络安全风险与传统安全风险将相互交织叠加，网络安全保险预计未来可同安全生产责任险、职业责任险、车险等传统险种深度融合。

（二）网络安全保险承保范围

无论保险公司采取何种保单形式承保网络安全保险，都需要详细清晰界定网络安全保险的承保范围。保险责任需阐明“网络安全威胁（风险）可能导致何种网络安全事件，最终引发何种损失类型”，其核心为确定“可保网络安全事件”与“可保损失类型”。现阶段网络安全保险保障范围解析如表 1 所示。

表 1 现阶段网络安全保险保障范围解析

保险产品类型	保险产品定义	可保风险事件	可保损失类型	可保损失说明
网络安全财产损失保险	主要承保第一方损失，即由于保单明确的网络安全事件直接导致的投保人（被保险人）的经济损失	营业中断事件	营业中断损失	可保威胁导致被保险人因停产、停业或经营受影响而面临的预期利润损失及必要的费用支出
		网络勒索事件	网络勒索损失	网络勒索事件导致的被保险人的勒索解密处置费用及其他必要的费用支出
		网络欺诈 社会工程学行为	资产损失	企业资金盗窃损失
		适用所有可保风险事件类型	应急响应费用	被保险人因可保风险事件发生而采取合理措施以保护自身利益进一步损失的必要合理的费用支出，如数据恢复、安全专家咨询等
网络安全责任保险	主要承保第三者责任，即由于被保险人发生网络安全事件所引起的对第三方（受影响个人或机构）依法承担的赔偿责任	数据泄露（企业或个人信息） 安全事件（数据被破坏或删除、服务中断等）	网络安全与隐私责任	被保险人对第三者（受影响个人或机构）法定赔偿责任
		外包商数据泄露 外包商安全事件	外包商责任	
		媒体侵权（知识产权被盗或丢失）	媒体侵权责任	
		适用所有可保风险事件类型	应急响应费用	被保险人因可保威胁或可保风险事件发生而采取合理措施以保护自身利益进一步损失的必要费用支出，如法律咨询、公关管理、数据恢复、安全专家咨询等

现阶段，网络安全保险可保的网络安全事件类型主要包括以下

类型：**一是**由被保险人或与被保险人订立合同的第三方看管、保管或控制的个人可识别信息遭到未经授权的获取、访问、披露、或者丢失；**二是**未经授权访问或使用被保险人的计算机系统，包括被保险人的计算机系统中的现有软件、应用程序或数据所遭受的任何丢失、更改、损毁或损坏；**三是**被保险人的计算机系统感染了恶意代码，或被保险人的计算机系统向第三方传输恶意代码；**四是**被保险人的计算机系统遭受了拒绝服务攻击；**五是**资金转移诈骗和电信诈骗；六是网络勒索威胁。近年来，随着网络风险评估等技术的不断升级，软硬件失效、人员错误疏漏等保障需求点也将纳入网络安全保险承保范围，其保障空间或将从单纯的外部攻击导致的网络安全事件上升为由人员、技术和管理[2]等疏忽过失引发的网络空间安全事件。

可保损失是网络安全事件对企业经营造成的可量化的负面影响[3]，可分为第一方损失和第三者责任。**第一方损失**主要指网络安全事件给企业自身造成的损失，包括应急响应费用、物理损失、营业中断损失、网络勒索损失等。**第三方责任**包含企业因遭受网络安全事件给第三方造成损失时应承担的责任，如数据泄露责任、网络安全事件责任、数字媒体责任等。例如互联网平台企业因遭受网络攻击导致其用户信息泄露，此时网络安全保险将承担对用户损失的赔偿。近年来，网络空间安全、计算机科学与技术等基础学科不断发展，非实物资产(intangible assets)价值持续提升，未来网络安全保险的可保损失类型

[2] 人员、技术和管理成为网络空间安全的三个关键要素，源自：网络空间安全——理解与思考,冯登国,中国科学院软件研究所，2021.

[3] 网络保险标准 ISO/IEC 27102，国际标准组织（ISO）及其信息安全技术委员会，2019.

会更加多样，例如贵州、深圳等地区的金融、交通、电信与互联网等行业主管部门陆续制定了数据安全的细化规章制度，为未来将数据资产价值等纳入网络安全保险保障范畴奠定基础。更加全面的保障范围助力企业在愈加复杂的网络环境中强化风险应对能力，同时也对保险公司提出了更高要求，需进一步加强风险定价和风险管理能力。

（三）网络安全保险服务流程

作为网络安全风险转移的重要方式，网络安全保险不仅限于为被保险企业提供经济赔偿能力，还通过全生命周期的风险管理服务进一步强化企业风险管理水平。由于网络安全保险本身的复杂性和专业性要求，以第三方风险管理技术服务机构为代表的评估方，通过其数据、技术优势连接保险方和投保方，在保险业务各流程中发挥重要作用，一方面帮助企业提高抵御网络风险的韧性及应对突发的网络安全事件的能力，另一方面帮助保险公司了解投保客户的网络风险水平并确定该客户的可保性。

整体来看，网络安全保险服务主要包括**投保前的风险评估、保单生效后的风险管控、出险后的鉴定理赔**三个阶段（如图 1 所示）。**风险评估阶段**是保险公司作出承保决策的重要支撑。在投保前，以潜在投保方配合评估方开展网络安全风险量化评估的结果作为核保的依据。这一阶段一方面要判定潜在投保方是否存在高风险、是否满足投保条件，另一方面对达到投保基线的企业开展风险量化评估，以指导核保与定价。**风险管控阶段**是网络安全保险服务流程中区别于传统

保险的重要风控手段。保单生效后，由评估方开展网络安全风险实时监测，协助保险方监控承保风险动态变化，同时为投保方提供及时的风险处置和响应，将潜在风险降到最低，最大限度缩减网络风险损失敞口。**鉴定理赔阶段**是网络安全保险充分发挥保障功能的重要支撑。在投保方完成出险报案后，评估方可为保险公司提供专业的事故调查服务，出具安全事件溯源报告。以专业网络安全事件分析、取证及溯源技术为理赔阶段的保险责任和损失确定提供数据支持。此外，网络安全保险服务还涉及主动风险减量措施，如投入配套软硬件网络安全产品、实施风险预警、组织客户开展网络安全培训等。

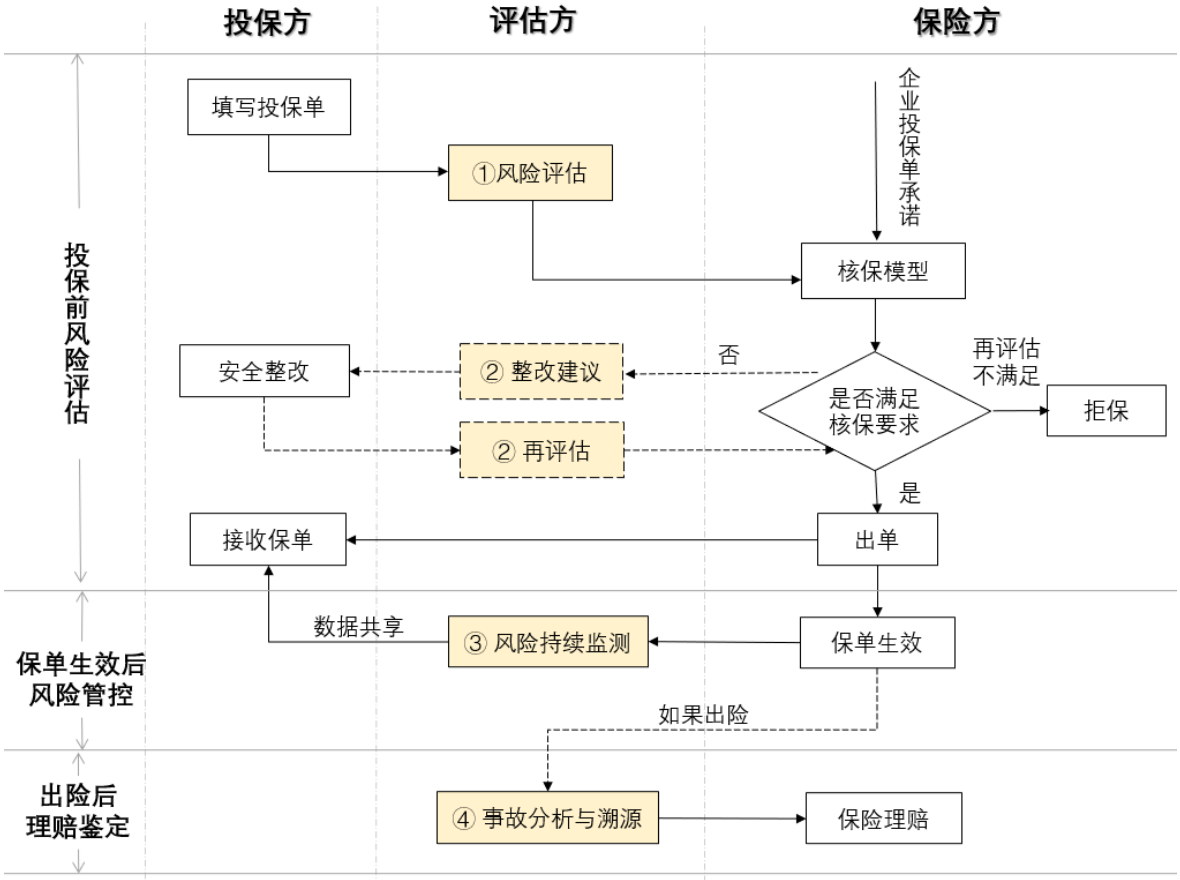

图 1 网络安全保险业务流程简图

（四）网络安全保险发展意义

传统风险越来越多地与网络安全风险交织融合，新兴风险场景为传统保险产品创新发展带来契机，比如智能网联车时代的车险、工业互联网时代的企业险等等。然而，目前市场中在售的责任险和财产险对于网络安全事件造成的非物质损失往往在承保范围中表述得模糊不清、甚至明示除外责任。随着网络安全在业务发展中的基础性、关键性作用日益凸显，网络安全保险弥补了传统保险产品在承保网络安全风险方面的缺失，为保险业发展迎来新的市场机遇。

在合规要求的驱动下，企业对网络安全建设的重视程度日益提高。然而，从企业投入—产出角度分析，当具备一定基础的网络安全能力时，网络安全软硬件投入的边际效用呈递减趋势，即通过持续增加网络安全产品部署，实现风险应对能力提升的效果会越来越小。因此，企业在网络安全能力建设的中后期，尤其是中小企业，会转向寻求“性价比”更高的网络安全服务。网络安全保险突出的服务属性可有效提升投保企业的网络安全风险应对能力和复原力。对中小微企业而言，保险服务提供的风险预警及管控能力，可以弥补自身资源和网络安全管理能力的不足。而对网络安全能力相对完善的大型企业来说，保险服务可提供有效的外部监督，帮助企业准确评估网络安全建设成效及弥补风险防护不足。此外，保险的规模化优势使得保险公司沟通联络网络安全服务的成本更低。因此，作为网络安全服务的创新模式之一，网络安全保险凭借风险转移功能、经济补偿能力以及成本优势，将为网络安全产业开拓广阔的发展空间。

二、国外网络安全保险产业发展路径

上世纪 90 年代，网络安全保险起源于海外市场，并在美国、欧洲等地区获得快速发展。其中，美国共 200 家保险公司直接开展网络安全保险业务，包括美国国际集团（AIG），丘博（CHUBB），和安达（ACE）等保险行业巨头，2020 年保费规模达 27.43 亿美元[4]。美欧等地区通过制定数据安全和网络安全相关强制性法规有效强化企业网络安全风险意识，逐步打开市场。在跨机构合作的基础上持续优化网络安全保险服务，推动网络安全保险产业走向规范和成熟，引领全球网络安全保险市场规模持续扩大。

（一）萌芽阶段：“保险公司+安全企业”模式为主，认可度与获客渠道受限

20 世纪 90 年代，全球网络安全险市场进入萌芽阶段。受到千年虫问题的警示，保险公司尝试开展网络安全保险业务。1998 年，国际计算机安全协会推出了第一款黑客保险，作为其网络安全服务的一部分。不过，由于企业因黑客攻击导致的业务影响并不显著，且尚未建立相关法律促使企业重视其网络安全合规责任，这一阶段网络安全保险的市场认可度较低，发展较为迟缓。

表 2 早期黑客产品典型市场推广模式

年度	保险公司合作机构	产品描述	保险责任说明
1998 年	国际计算机安全协会[5]	“技术服务（系统安全状况的审查以及改善建议等）+保险”	承保黑客攻击导致的第一方损失，每年限额 25 万美元（每次事故限额 2 万美元）

[4] Aon. US Cyber Market Update: 2020 US Cyber Insurance Profits and Performance, 2021.06.
[5] Poletti T. First-Ever Insurance Against Hackers, 1998.

年度	保险公司合作机构	产品描述	保险责任说明
1998 年	信诺/思科[6]	“技术服务（安全评估以及监测服务）+保险”	承保黑客攻击导致的第一方损失（包括业务中断），限额 1000 万美元
2000 年	劳合社伦敦/康特派恩[7]	为其计算机安全服务增信	承保第一方损失，保额 100 万到 1000 万美元
2001 年	美国电话电报公司/美国威达信集团公司[8]	通过美国电话电报公司互联网数据中心途径购买保险可享受折扣	承保第一方损失

依据表 2 内容，该阶段保险公司通常选择与安全服务公司合作，一方面通过保险为安全服务公司对外的技术产品或服务增信，另一方面为安全服务公司的用户企业提供涵盖保险服务的全面风险管理解决方案。但该种模式发展过程中逐渐衍生出一些突出问题：**一是投保企业较少，风险分散能力有限。**在承保需求有限的发展萌芽阶段，保险公司往往承担多个独立客户的风险，由安全服务公司推荐的高风险客户投保比例较高，保险公司往往面临极高的风险累积，且难以通过广泛承保的方式分散风险。**二是风险量化分析能力较弱，精算模型的风险定价能力不足。**传统安全服务预测能力停留在预测未来可能发生的潜在风险，缺乏针对风险发生概率、损失类型以及损失规模的预测，安全数据难以转化为适用于保险环境的数据。**三是合作模式不清晰，公允性易受质疑。**安全服务公司既作为服务提供商又作为风险评估方的模式缺乏一定公允性，保险公司难以客观地获知目标客户的可保性。

基于以上原因，保险公司在该阶段难以通过该业务获得收益，且

[6] Moukheiber, Z. Got a Hacker Policy? Forbes, 1998.
[7] Harrison A. Counterpane Offers Internet Security Insurance, Computerworld, 2000.
[8] Salkever A. E-Insurance for the Digital Age, Business Week, 2002.04.

无法准确地量化网络风险形成具有吸引力的保费，整体网络安全保险市场需要寻求新的发展突破口。

（二）初步探索阶段：合规要求与风险意识提升，产品优化升级步伐加快

21 世纪初，网络安全保险市场进入初步探索阶段。不断演变升级的网络风险和逐步严格的合规要求成为影响网络安全保险发展的主要因素，保险公司也不断优化保单定价模型，摸索并验证可行的商业发展模式。

合规要求拉动网络安全保险发展。网络安全、数据安全领域法律法规的出台不断强化行业监管，撬动企业网络安全投保需求。以美国为例，1999 年格雷姆-里奇-比利雷法案（Gramm-Leach-Bliley Act，GLB Act）[9]对金融行业个人信息处理流程进行规范，2003 年以来，美国加利福尼亚州首先率先实施《数据泄露通知法案》（又称“Senate Bill 1386”法案），随后美国各州相继颁布实施相关法案，明确故意隐瞒数据泄露属于违法行为，带动安全事件报告数量的陡增，企业的网络安全合规风险加剧（如图 2 所示）。保险公司随之采取行动开拓市场，从产品设计角度将第一方损失和第三者责任纳入保险保障范围，推出风险损失全覆盖综合险保单，为企业提供合规风险分散的有效途径。同时，为应对“沉默风险”所导致的损失，保险公司开始在其传统的财产保险和责任保险保单中将网络相关事件以及数据相关损失列入除外责任，投保企业可以通过附加险的方式扩展承保相关

[9] 该法案为美国颁布的一项联邦法律，即金融现代化法案，规定了金融机构处理个人私密信息的方式，还要求金融机构给顾客一个书面的保密协议，以说明他们的信息共享机制。

责任。

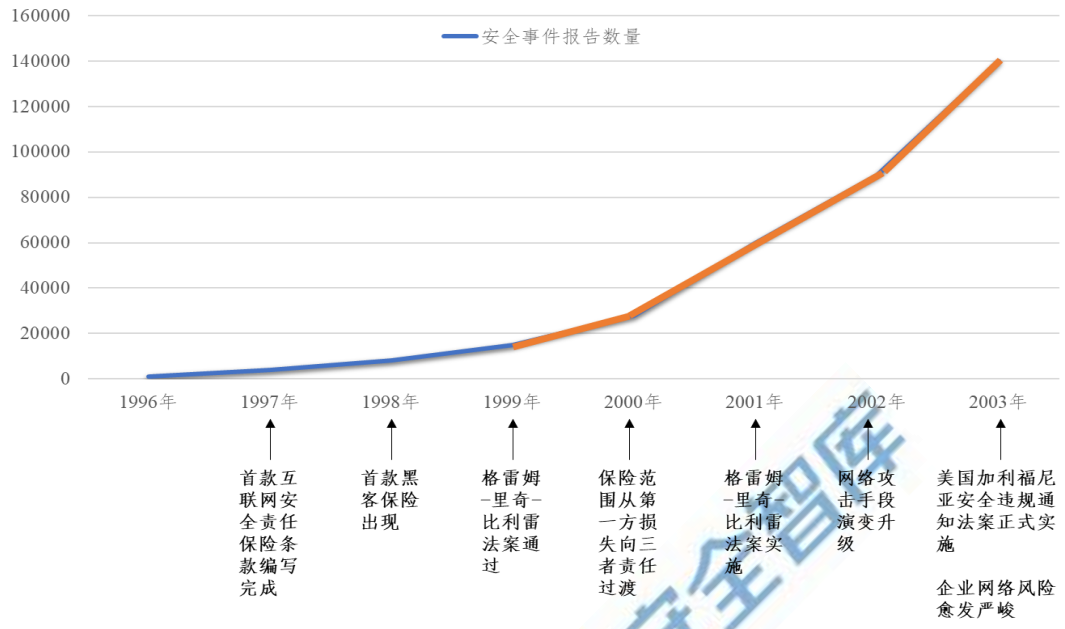

图 2 美国网络安全事件报告数量变化情况[10]

安全意识驱动企业投保网络安全险。网络安全事件频发给企业造成的经济损失持续攀升，企业开始高度重视网络安全风险防御及应对。2003 年美国行业协会保险信息研究所的数据显示，90%的企业和政府机构存在安全漏洞且 75%的企业因此遭遇攻击造成经济损失。考虑到企业风险管理的实际需求，保险公司进一步探索将保险服务与专业技术手段相结合，增强从投保、承保到理赔的保险业务全流程网络风险敞口管控能力，协助企业提高防范风险的灵活性，以及抵御风险的韧性。例如美国国际保险公司（AIG）在 2012 年到 2014 年间初步尝试组建全球网络安全团队为客户提供出险后安全服务、承保中风险管理服务，并在 2015 年开始投资网络安全服务公司以完善其

[10] 数据来源：美国计算机紧急事件响应小组协调中心（CERT/CC），2015.

向客户提供全方面的网络安全服务。

（三）快速发展阶段：流程与责任划分趋于规范，多主体参与模式逐步成熟

21 世纪 10 年代后期，全球网络安全保险市场进入快速发展阶段。2018 年 5 月，欧盟《通用数据保护条例》（GDPR）的正式生效被视为隐私和数据保护的里程碑事件，进一步强化了对数据主权的保护并加大了行政处罚力度，有力拉动了网络安全投保需求。此外，第三方风险管理技术服务机构积极参与网络安全保险市场，帮助保险公司完善核保定价能力，提供风险持续管控的手段，解决保险公司“可不可保”“如何承保”的难题。在此背景下，网络安全保险市场进一步发展，保费规模快速增长，平均年复合增长率超过 20%。

表 3 国外网络安全保险产业参与主体与技术工具[11]

对应阶段	风险管理技术服务机构类型	典型企业	技术服务工具
投保阶段-风险评估	保险科技公司	Cyence、Cybercube、Perseus、Cyquant	开发网络风险评估评级工具
			搭建网络风险量化平台
			合作开发定价模型
			开发自动化核保工具
承保阶段-风险监测	保险科技公司	Security Scorecard、Perseus	开发针对投保企业的网络安全风险监测平台
			针对投保客户外部服务商的网络安全风险监测平台
	安全服务公司	Senseono、Cyberhaven	监测敏感数据并控制访问权限，端点安全保护平台
理赔阶段-事故鉴定	保险科技公司	Soteria、Coronet	7*24 小时事件响应
			恶意软件分析
	安全服务公司	CyberCentric、Bandura	网络威胁情报平台

[11] 信息来源：北京源堡科技有限公司，2021.

根据表 3 所示，第三方风险管理技术服务机构主要分为保险科技公司和安全服务公司两类。前者具备显著的数据搜集及清洗整合等方面的优势，可基于网络安全风险基础数据实现差异化的网络安全保险定价策略，有预见性地全面监控风险敞口，缓释网络空间“黑天鹅”事件带来的累积风险。后者的核心优势在于通过资产测绘、漏洞扫描、威胁发现等专业技术能力帮助企业网络风险“减量”，配合保险公司提升其抵御风险的韧性。

实践表明，保险科技公司和网络安全服务公司发挥自身优势，积极参与网络安全保险行业价值链，在销售、核保、定价、承保及理赔等主要业务流程发挥重要作用，推动全球网络安全保险产业有序发展，促进网络安全保险保费规模持续上涨（图 3）。据市场研究公司 Research and Markets 预测[12]，到 2026 年，全球网络安全保险市场规模将达到 350.7 亿美元，平均年复合增长率达到 26.6%，展现出巨大的网络安全保险市场空间。

[12] Research and Markets, Cyber Security Insurance - Global Market Outlook, 2019.

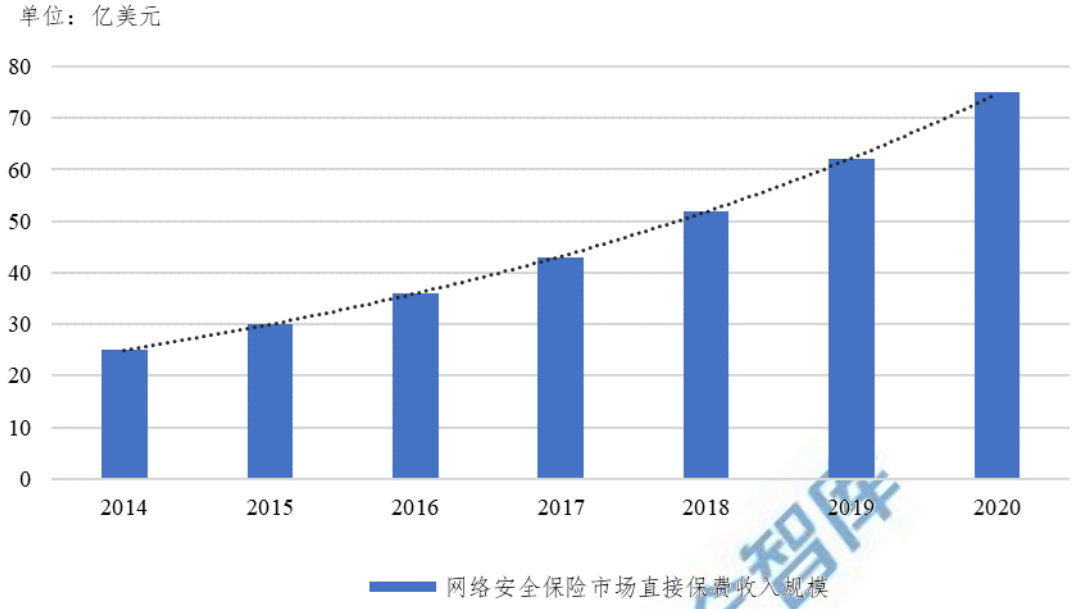

图 2 2014-2020 年全球网络安全保险市场保费收入规模[13]

三、我国网络安全保险产业发展现状

伴随着我国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，网络安全产业迎来发展机遇期。作为网络安全服务的创新模式之一，网络安全保险受到政府部门、研究机构、保险公司、网络安全企业等相关机构高度关注，各方围绕政策制定、产品开发、服务模式创新等方面展开积极探索。

（一）市场规模整体较低，保单类型数量较少

据国家工业信息安全发展研究中心测算[14]，2021 年我国网络安全保险保费规模预计 7080 万元左右，较上一年增长 3.2 倍以上，最高保额超过 4 亿元。尽管网络安全保险保费规模呈现持续高速增长态

[13] 2014-2020 年全球网络安全保险市场保费收入规模趋势图中，2020 年保费收入规模数据为预测值，源自：Marsh，Cyber Insurance in 2025，2019.07.

[14] 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得出我国网络安全保险保费规模。其中，行业集中率是以近 10 年财险行业集中率平均值为基础，结合网络安全保险发展现状近似估算得出。

势，但仅占财产保险保费规模的不到万分之一，也不足网络安全产业规模的千分之一。

中国保险行业协会财产保险公司自主注册平台数据显示，目前国内市场在售网络安全保险产品超过 50 款。**从服务机构看，**除苏黎世财产保险（中国）有限公司、东京海上日动火灾保险（中国）有限公司、三井住友海上火灾保险（中国）有限公司等外资保险公司外，包括中国人民财产保险股份有限公司、中国太平洋财产保险股份有限公司、中国人寿财产保险股份有限公司、中国平安财产保险股份有限公司等在内的约 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。**从产品类型看，**企财险数量接近半数，另有责任保险 10 余款，综合保险、应急响应专项险等其他类型险种。市场上主流保险产品承保范围及承保责任如表 4 所示。

表 4 国内主流保险产品承保范围及承保责任概述

承保范围		承保比例[15]	承保责任示例
第三方责任	信息泄露责任	☆☆☆	被保险企业业务系统遭受未经授权访问，导致客户敏感信息泄露，被保险企业被客户起诉而可能产生法定赔偿责任
	网络安全责任	☆☆☆	某电商解决方案提供商由于黑客攻击导致数据库被删除，致使电商平台商户无法正常运营，被保险企业被商户起诉而可能产生法定赔偿责任
	媒体侵权责任	☆☆	被保险企业在公司网站或社交媒体上进行数字媒体活动产生侵权行为，由此可能产生法定赔偿责任
	外包商数据安全/信息泄露责	☆	被保险企业的数据托管服务商因遭遇黑客攻击信息泄露、导致被保险企业被数

[15] 北京源堡科技有限公司根据国内 21 款网络安全保险条款公开信息披露信息整理所得，承保比例列指 21 款保险产品所涉及的保险责任范围，其星标数量分别代表一半以上、30%-50%、10%-30%、少于 10%的网络安全保险公司承保该内容。

	任		据泄露信息主体索赔，被保险企业由此产生索赔损失
第一方损失	营业中断损失	☆☆☆	被保险企业因遭遇勒索病毒攻击或其他恶意攻击手段导致企业正常业务运营中断，由此产生企业净利润损失
	网络勒索损失	☆☆☆	被保险企业因遭遇勒索病毒攻击导致核心业务系统或核心数据文件加密，并被攻击者威胁交付赎金引发的费用损失[16]
	数据修复费用	☆☆☆	被保险企业因遭受恶意攻击导致核心数据丢失、损毁或被删改，由此引发的数据恢复费用
	网络欺诈损失	☆☆	被保险企业遭遇网络钓鱼攻击，被要求指定账户进行转账操作，企业有可能因此产生网络欺诈损失
	计算机修复、更换损失	☆☆	被保险企业因遭遇勒索病毒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重新更换计算机设备的费用
	公关费用	☆☆☆	被保险企业发生信息泄露等网络安全事件后，被保险企业会发生声誉风险，因此会产生名誉恢复费用
	法律费用	☆☆☆	被保险企业发生信息泄露事件后可能被受影响客户索赔，被保险人聘请律师应对诉讼而产生的一系列费用
其他	危机处理保险责任	☆☆☆	被保险企业发生网络安全事件后，需要聘请第三方服务机构针对安全事件进行应急响应，由此产生事件处置费用
	咨询服务保险责任	☆☆	保险事故引起的合理必要的咨询服务费用，例如被保险人与政府部门沟通以确定网络安全、个人信息保护等法规的适用性及遵守各个法规所需采取行动的合规顾问咨询费用等
	网络安全评级费用	☆	被保险企业遭遇网络安全事件后到导致原有的认证评级水平受到影响，因此被保险人会产生重新评级认证的费用

[16] 中国互联网金融协会、中国银行业协会、中国支付清算协会《关于防范虚拟货币交易炒作风险的公告》明确“（金融机构）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”。因此，国内保险公司对网络勒索损失的承保中并无合法途径为其提供虚拟货币相关的服务。

（二）三大模式加快探索，多方融合特征突出

早期，外资财产保险公司依托其在国外市场的先进经验以及较为成熟完整的风险管理体系开拓了中国的网络安全保险市场。近年来，在各方的共同努力下，国内网络安全保险产业发展正从萌芽阶段逐步进入到初步探索阶段。

顶层设计方面，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律的相继实施，逐步完善了我国网络安全法律体系，明确了网络安全主体责任、数据安全保护义务等，为我国网络安全保险的发展奠定了良好的法律基础。此外，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）》《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）》等政策文件中明确提出“探索开展网络安全保险服务”，产业政策利好不断释放。

产品供给方面，国内保险公司在大量借鉴国外保险公司网络安全保险条款的基础上，结合国内市场及监管要求编制保险条款，同时，积极探索标准化、易于推广的发展模式。**一方面，推动网络安全保险场景化。**发展初期，大部分网络安全保险条款设计都是在保险公司与投保企业沟通协商的基础上形成。基于前期的实践经验积累，现阶段逐渐转变为面向特定风险场景，开发标准化保险产品以匹配特定投保需求，以实现更高效的推广。**另一方面，以附加险为发展起点。**通过家财险附加险或者小额赠险的方式来销售网络安全保险，借力主流险种提升网络安全险的普及度。

融合发展方面，国内财产保险公司积极寻求与网络安全专业技术机构的合作，推动保险机制与网络安全技术措施相结合，以扩大投保企业对这一新兴险种的接受度。网络安全产业主体也逐渐意识到保险机制对于完善网络安全服务体系、形成网络风险管理闭环的重要作用，在其业务体系内增加了网络安全保险服务，进一步推动了保险产品与网络安全服务融合发展。现已发展形成了以下三种常见的合作模式：**一是“安全服务绑定保险”模式**。该模式下，网络安全企业发挥技术优势，通过风险评估、风险监测、应急响应等传统技术手段赋能保险核保、减损、理赔等主要环节。同时，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，对承保风险进行综合管控。**二是“网络安全防护产品+保险”模式。**作为上一模式的延伸，该模式以推广传统网络安全服务或安全防护产品为核心，以保险作为风险兜底手段，纳入企业风险管理体系。该模式下，销售激励以及企业风险意识水平成为推广的关键。**三是“防+保”全流程网络安全风险解决方案**。该模式下保险公司与保险科技公司共同开发网络安全保险方案，将网络安全威胁模型与保险定价模型、承保范围相结合，依托自身数据整合分析优势搭建网络安全量化风险评估模型，以提升保险公司的核保和定价能力。同时，为企业提供主动型的风险防御服务，通过定期巡检、加固、监测、预警、防护、恢复等持续周期性的网络安全服务，降低网络安全事件发生概率。

（三）风险管理深度绑定，安全服务是生态核心

“防+保”模式是以保险科技公司为代表的第三方风险管理技术

服务机构赋能传统保险业的新兴业务模式。第三方风险管理技术服务机构作为保险服务生态中的关键一环，用专业的网络安全技术能力、场景化评估分析能力和数据整合分析能力，协助保险公司和被保险企业审查风险累积水平并实施网络安全风险管控。

一方面，提升被保险企业网络安全能力。第三方风险管理技术服务机构立足于投保企业的网络安全风险管理需求，协助保险公司为企业提供一揽子、全周期管理方案，包括承保后的风险管理服务，险情出现后的应急响应服务，以及日常网络安全维护，如网络漏洞扫描、网站安全认证等。网络安全保险服务可以有预见的全面监控风险敞口，加强对网络攻击的反应能力和恢复能力，帮助被保险企业建立全面的网络安全防御体系，进而帮助保险公司控制承保风险敞口。

另一方面，赋能保险公司产品定制化开发。第三方风险管理技术服务机构可针对不同场景下的网络安全风险，协助保险公司开展产品定制，充分发挥技术服务优势，协助构建并优化承保、风控、理赔等全流程业务体系。第一，基于承保前的安全评估，保险公司可了解客户企业的网络安全投入及安全管控的持续性和有效性，以有效预测企业网络安全风险潜在发生的可能性及损失影响，厘定合理的费率。第二，通过定期巡检、加固、监测、预警、防护、恢复等持续周期性的网络安全服务，可一定程度降低网络安全风险发生的概率，有效控制损失，降低保险赔付率，达到风险减量管理的目的。第三，依托第三方风险管理技术服务机构数据搜集及清洗整合等方面的显著优势，保险公司可建立网络风险数据库，持续性收集、筛选、丰富网

络安全风险池的基础数据，持续优化保险公司定价模型，进而实现差异化的网络安全保险定价策略。

（四）落地案例逐步增多，关键行业需求萌发

现阶段，网络安全管理的深层次发展不仅将网络风险看作技术问题，还将其纳入了企业全面风险管理框架之中，表现为认识到网络风险无法完全消除、制定风险管理流程、通过既定方案保护企业资产并优化资源配置等。此外，《个人信息保护法》对企业应承担的部分第三方责任加以明确，规定了个人信息处理者对于信息泄露的法定补救与通知义务，并且确立了个人信息侵权的“过错推定”归责原则以及有关公益诉讼制度。在此背景下，网络安全保险日益成为企业风险管理的手段之一。

目前，以制造、金融、医疗、信息技术等重点行业企业正在积极进行网络安全保险询价，希望通过保险的方式转移企业网络安全风险。部分网络安全保险市场承保情况如表 5 所示。这些企业往往具备以下特征之一：一是属于网络攻击吸引度较高的行业，例如金融、制造等行业；二是属于关键信息基础设施运营单位，其业务的正常运营直接关乎国民的根本利益，因此需要建立全面的风险管理体系；三是外资企业、合资企业或具备海外业务的中资企业，海外业务部门已投保或计划投保网络安全保险，同时带动国内业务部门主动或应合规要求寻求网络安全保险进行风险转移。

表 5 不同行业企业网络安全保险投保情况简述

行业企业类别	承保前风险评估初判	企业投保原因	投保险种类型	保险附加服务项目
某大型能源电力企业	企业安全能力顶尖，风险管理体系较为完善	转移剩余的财务风险，完善风险管理体系	网络安全保险，保障网络勒索、营业中断、应急响应费用等第一方损失	风险持续监测服务，如出现高级威胁及时通告报警
某上市电子商务企业	线上业务比例极高，尽管该企业自身网络安全防护体系较为完善，但该企业的业务属性决定其遭受网络攻击概率较大，其信息泄露责任、网络安全责任等三者连带责任较高	风险管理驱动	网络安全综合险（保障第三者责任和第一方损失）	通过专业的安全整改建议提升企业整体安全建设水平
某医疗机构	风险中等偏上，需继续完善其安全防护能力	事件驱动	勒索软件防护保险	防勒索软件防护服务
某自动驾驶企业	新场景需求客户，对于系统失效需求较高	政策要求	网络安全保险以及算法失效保险（保障自动驾驶车辆的软硬件系统失效、算法失效等网络安全事件导致的第一方损失）	-
某大型合资汽车制造企业	自身网络安全意识较高，安全管理能力较强	集团合规和风险管理要求	网络安全保险	-
某中大型金融机构	网络安全建设能力较强	风险管理驱动	网络安全保险（保障第一方损失和第三者责任）	风险监测、人员安全意识培训等技术服务

行业企业类别	承保前风险评估初判	企业投保原因	投保险种类型	保险附加服务项目
某专业技术服务业企业	网络安全整体水平较高	风险管理驱动	勒索软件防护保险	勒索攻击应急响应服务
某中型贸易公司	业务线上依赖度较高，整体网络安全风险中等	风险管理驱动	网络安全保险（保障第一方损失和第三者责任）	风险持续监测服务，如出现高级威胁及时通告报警
某银行	整体网络安全风险可控	完善企业自身风险管理机制	网络安全保险（保障第一方损失和第三者责任）	准入风险评估、无感知风险评估、网络安全差距分析服务、定期风险隐患排查、渗透测试、网络安全培训等

四、我国网络安全保险产业现阶段发展问题分析

现阶段，我国的网络安全保险业务尚不成熟，险种类型较为单一、参保率相对较低。网络安全企业与保险公司专业能力不匹配的问题依旧突出，风险评估、风险监测、溯源取证等技术服务与保险业务需求仍有一定差距。此外，风险理赔数据收集、保险服务规范化等系统性的策略难题和理论空缺也制约着网络安全保险产业的发展。

（一）需求侧网络安全保险投保动力不足

作为需求方，企业对网络安全保险的了解较少、对通过保险渠道转移网络安全风险的接受程度仍处于较低水平。**一是对网络安全风险管理的重视不够。**由于网络攻击短期内可能不会造成明显损失或损失并不直观，现阶段企业“重发展、轻安全”的现象依旧普遍，网络安全建设规划时往往以“合规”底线作为标准，更加注重网络安全设备的部署，而很少从降低风险的视角出发实施风险监测、处置及管

理措施。因此，网络安全保险作为典型的风险转移策略还未得到企业的关注。**二是对信息泄露的维权意识不高。**我国并未建立网络安全事件通知披露机制，企业无需对外公开网络安全事件造成的损失及对第三方合作伙伴、关联机构和用户的影响，且鲜有因信息泄露而引发的民事索赔，致使企业忽视对第三方主体的网络安全责任，也较少关注网络安全保险对于赔偿第三方损失的转移作用。**三是对网络安全保险的认识不足。**目前对网络安全保险宣传推广的有效途径较少，多数企业对投保网络安全险的认识仅仅停留在传统意义上“在出险后获得赔偿”的层面，也有部分企业片面地了解到其对降低合规风险或是实现增信的作用，然而对其同步提供风险管理服务的内涵知之甚少。**四是网络安全保险投保意愿不强。**不同行业、不同规模企业所处网络安全风险环境的差异性，以及业务场景对风险应对能力要求的不同，使企业网络安全投保需求日趋多样化。然而，目前市场中的网络安全保险种类单一，且缺乏应对个性化需求的灵活性，致使企业购买驱动力不足。

（二）供给侧安全服务尚未契合保险流程

网络安全服务贯穿于保险业务的全流程，但现有服务模式无法直接与保险业务形成衔接，难以有效支撑保险公司核保、承保、理赔等业务环节。**一是风险评估结果难以直接服务于核保分析等流程。**由于目前网络安全风险评估服务多用于辅助网络安全能力建设决策或判断企业是否达到合规等监管要求（如网络安全等级保护要求等），风险评估方法往往停留在定性分析层面，缺乏对网络安全投入收益

的量化计算，评估结果难以满足保险公司核保、承保以及再保过程中对数据的需求。**二是风险监测手段指标需高度关联保障范围内的网络安全风险。**传统网络安全风险监测目的和范围并不完全适用于保险承保过程中的风险持续监测环节。保险风险监测对象应为网络安全保险保单中列明的保险责任，监测的内容宜偏重于活跃组织内部或外部的威胁、新增的脆弱性等。如何定义保险服务中的风险持续监测数据指标，如何通过对监测数据的分析实现风险的预先处置以及对保险定价模型的优化，是值得持续加强研究的方向。**三是溯源取证服务与保险理赔目标不一致。**传统溯源取证服务的目标在于追溯事件源头，确定网络安全事件责任方，形成法律证据作为报案依据。而对于保险理赔环节而言，溯源取证更加关注如何控制或减少进一步的损失、以及网络安全事件的定责和定损，即网络安全事件造成的损失或应承担的赔偿责任类型[17]是否满足理赔的条款和范围，同时注重第一方财产损失、信息泄露责任、媒体侵权责任等各类损失的量化。此外，定责定损过程中涉及的第三方机构多为利益相关的网络安全企业，客观性、公正性、准确性恐难以得到业界的一致认可。

（三）多主体协同风险管控能力相对有限

我国网络安全保险起步较晚，实践经验和基础数据不足，尚难以通过精准测算实现对风险敞口量化和有效管控。**一是历史数据缺失制约了对风险的预判能力。**保险精算模型一般基于长时间、连续稳定的同类型风险的事故概率、损失规模等的历史数据，实现未来风险发

[17] 网络安全事件造成的损失可能包括物理损失、营业中断损失、网络勒索损失等；应承担的赔偿责任类型可能包括数据泄露责任、经济损失赔偿责任、数字媒体责任、法律费用等。

生的概率及损失的预测。然而，国内尚无网络安全保险出险案例，缺乏历史理赔数据。网络安全风险数据仍停留在少数企业间的一对一共享模式，依靠有限的网络安全风险基础数据的保险精算模型无法科学合理地为网络安全风险实现定价。**二是传统精算模式难以有效反映和量化未知风险。**由于网络安全威胁的快速演变，新的漏洞和攻击层出不穷，仅通过历史数据开展分析预测的有效性大大降低。此外，随着云计算和物联网等前沿技术的快速发展，网络风险的复杂度和关联性不断上升，网络风险引发的级联效应[18]可能超出传统精算模式的测算范围。**三是部分高风险因素未被纳入承保范围。**由于保险公司对风险敞口的把控能力有限，目前针对软硬件系统失效、内部人员错误疏漏等强需求点持谨慎承保态度，因此国内主流的网络安全保险产品可能因未涵盖上述保险责任而抑制了企业的投保意愿，造成网络安全保险参保率总体处于较低水平。

五、对策建议

随着各行业各领域数字化转型的深入推进，网络信息安全防护理念逐渐从“被动安全”步入“主动安全”时代，网络安全需求持续增加，网络安全保险有望加速发展。可在借鉴国外网络安全保险产业演进模式的基础上，进一步推动适应企业保障需求的产品服务创新发展，强化法规政策对需求的牵引作用，加快推进技术服务标准规范制定，促进市场主体实现跨行业深入合作，开启网络安全保险产业健康有序发展的新时期。

[18] 级联效应是由一个动作影响系统而导致一系列意外事件发生的效应。在网络中，一个或少数几个节点或连线的失效会通过节点之间的耦合关系引发其他节点也发生失效，最终导致大量节点故障甚至整体系统失效。

（一）加强产品服务创新

面向信息化水平较高的重点行业领域，深入调研网络安全保险投保需求，引导市场主体创新突破，丰富产品种类，优化服务内容，提升供给能力水平。

一是全方位开发网络安全保险产品体系。面向不同行业场景的差异化网络安全风险管理需求，开发网络安全保险细分险种。同时，从扩大业务场景风险保障范围的角度出发，有针对性地结合传统险种提供一揽子的保险风险保障，例如财产损失保险类的企业财产保险、运输保险、利润损失保险；责任保险类的产品责任保险、职业责任保险、公众责任保险和雇主责任保险；信用保证保险类的产品保证保险、雇员忠诚保险等，以匹配多元化风险管理需求。此外，面向不同规模投保企业，设定多档的保费配套不同层级的风险管理服务能力：面向中小微企业，为其相对有限的风险管理投入提供可灵活搭配的“保障+风控+服务”一体化保险服务方案；面向大型企业集团，为其较高的保费匹配全方位、全流程、全覆盖的网络安全风险管理服务体系和更高数额的经济补偿能力。

二是创新网络安全保险服务模式。鼓励保险服务机构提升专业服务能力，以“服务优先、保险兜底”为原则，形成覆盖主动防御、保前诊断、保前加固、保中监控、保险补偿、出险救援的全流程保险解决方案，实现网络安全风险管理的闭环。搭建网络安全保险一站式服务平台，集合保险公司、网络安全服务商、评估服务商、应急服务商等各类服务商，以及会计师事务所、律师事务所、公关公司等相关

专业机构，提供全流程网络安全风险管理、保险保障服务以及出险后的损失审计、法律支持、公关咨询等服务支持。

三是开展新兴风险场景研究。围绕工业互联网、车联网、物联网等新兴技术风险，及其相关新业态、新模式的业务风险，开展安全风险场景研究，支撑保险产品设计与风险管理服务优化，使网络安全保险保障能力加速融入新技术、新业态、新模式的发展进程。

（二）强化需求牵引作用

探索构建“强制、鼓励、补贴”三位一体的政策引导体系，指导企业通过网络安全保险服务监控风险敞口，构建并完善自身网络安全风险管理体系。

一是鼓励关键信息基础设施运营者将网络安全保险纳入企业网络安全建设体系。公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域关乎国计民生，其重要网络设施、信息系统等的稳定运行需要全面的风险管理机制保驾护航。网络安全保险可有效减缓风险，强化关键信息基础设施运营者网络安全主体责任，提升网络安全保障能力水平。未来，针对此类群众关切、风险高发的行业领域，可考虑适时通过立法形式将网络安全保险上升为强制保险。

二是开展网络安全保险试点。2021 年 7 月，《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）》公开征求意见，其中“产融合作深化行动”中提出“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”工作。在各级主

管部门的引导和支持下，充分发挥保险公司、网络安全企业、保险科技公司等各类市场主体作用，形成一批符合行业特征的网络安全保险服务方案。面向数字化水平较高、网络安全需求迫切的重点行业、重点企业，开展网络安全保险试点工作，协助企业完善安全风险体系建设、提升网络安全治理水平，并在实践过程中探索、提炼示范性网络安全保险解决方案。

三是充分发挥财税支持政策导向带动作用。主管部门及地方政府可充分发挥财政资金导向作用，商请财税行业主管部门联合推出配套优惠措施，制定网络安全保险等相关优惠政策，例如为中小型企业提供保险购置减税政策[19]、保险购买补贴政策等，以鼓励中小型企业主动投保网络安全保险，扩大客户数量，拉动整体市场需求。

（三）推动行业标准规范建设

针对目前网络安全技术服务对网络安全保险业务支撑能力不足的问题，鼓励产学研协同合作开展网络安全保险服务标准化研究，推动形成网络安全保险条款、技术标准和服务要求体系框架，引导网络安全保险产业健康有序发展。

一是加强术语标准化。明确网络安全保险相关专业概念的含义，减少或尽可能消除一义多词或一词多义、含义不清等问题，使专业术语尽可能的规范统一。例如，对网络保险、网络安全保险等相似概念进行明晰和统一，结合网络安全风险对具体承保责任相关概念和含义进一步明确等。在术语标准化基础上，探索实现网络安全保险产品

[19] 2018 年，国家税务总局颁发了《关于责任保险费企业所得税税前扣除有关问题的公告》，明确提出“企业参加雇主责任险、公众责任险等责任保险，按照规定缴纳的保险费，准予在企业所得税税前扣除。”

框架标准化。

二是统一技术服务标准要求。在现有国家标准的基础上，形成适用于网络安全保险的风险评估标准，开发全行业横向及行业内纵向网络安全风险分级标准，明确风险持续监测和事件应急处置及溯源取证的技术要求，形成系列标准规范。

三是推动业务流程规范化。结合我国网络安全保险实践，以降低风险管控技术侵入性、部署成本为目标，由保险公司联合安全服务机构、高校与研究机构对网络安全保险的风险评估流程、风险监测范围、风险处置及应急响应服务、定责定损标准、出险理赔程序等开展研究，明确基本原则、主要业务、配套服务等，为网络安全保险业务流程设计提供总体框架和通用要求。

四是开展信息资源标准化建设。在目前已形成的系列《保险业务要素数据规范》基础上，结合网络安全领域《信息安全技术网络安全威胁信息格式规范》等信息共享标准，对应核保、承保、保障、理赔等业务活动及业务面向的对象，探索标准化数据描述方式，进而形成适用于网络安全保险的数据收集标准、格式规范与传输共享模式，为网络安全风险数据共享奠定基础。

（四）促进各类主体深度协同

充分发挥政府的引导作用，紧密联系企业、科研机构以及高校等行业机构，深入推进跨行业研究合作，推动网络安全保险产业持续稳健发展。

一是建立协同联动工作机制。在工信部和银保监会的指导下，汇

集保险公司、再保险公司、保险经纪公司、网络安全企业、风险评估服务机构、科研机构、高校等多方力量，成立网络安全保险工作组，聚焦优化供给、扩大需求、建立标准体系、加强示范推广等方面，深化跨行业合作，凝聚发展共识，合力推进网络安全保险本土化发展。

二是推动数据资源共享流动。2021 年 7 月 12 日，《网络产品安全漏洞管理规定》由工业和信息化部、国家互联网信息办公室、公安部三部门联合印发，其中第三条指出“有关主管部门加强跨部门协同配合，实现网络产品安全漏洞信息实时共享”，意味着我国主要网络安全漏洞平台之间的共享机制即将建立。在此基础上，主管部门还应进一步探索网络安全风险数据资源共享机制与实施模式，逐步推动政府、企业、科研机构以及高校等相关机构之间网络安全威胁情报、安全事件分析、历史损失数据等资源流动共享，助力风险感知与管控能力提升。此外，探索构建网络安全保险数据共享机制，统筹保险公司、再保险公司或网络安全企业等相关方共享有关承保情况、出险情况、赔付金额等保险数据，为网络安全保险定价提供指导。

三是建立风险分散机制。探索政府补贴支持、共同保险、保险公司风险分出、自留网络风险专项基金、巨灾风险债券等金融衍生工具等在内的多层次风险分散方式，以政府注资带动社会资本，共同组成多层级风险分散体系。联合再保险公司开展网络安全领域潜在大型风险的分析、研判和管理，充分发挥再保险公司在风险分散和转移方面的优势和能力，强化对直保公司的支持与服务，助力网络安全保险市场的平稳运行。

四是形成多层次推广渠道。行业主管部门及地方政府可结合工业互联网企业网络安全分类分级管理试点工作、企业上云工作等相关工作的开展，同步向需求突出的企业推介网络安全保险服务。鼓励第三方专业机构、产业联盟和行业协会在解决方案遴选、示范案例展示、产融合作比赛、论坛峰会等活动中加入网络安全保险这一重点方向，扩大对网络安全保险服务的宣传推广力度。此外，借助论文期刊、学术会议等平台媒介，深入研究或交流研讨承保范围、除外责任、道德风险等网络安全保险相关问题，推动跨学科知识交叉融合、跨学科研究创新发展。

参考文献

[1]冯登国. 网络空间安全——理解与思考. 中国科学院软件研究所. 2021 年.

[2]网络保险标准 ISO/IEC 27102. 国际标准组织（ISO）及其信息安全技术委员会. 2019 年.

[3] Aon. US Cyber Market Update: 2020 US Cyber Insurance Profits and Performance. 2021 年

[4]Poletti T. First-Ever Insurance Against Hackers. 1998 年.

[5] Moukheiber Z. Got a Hacker Policy? Forbes. 1998 年.

[6] Harrison A. Counterpane Offers Internet Security Insurance. Computerworld. 2000 年.

[7] Salkever A. E-Insurance for the Digital Age. Business Week. 2002 年.

[8] Marsh. Cyber Insurance in 2025. 2019 年.

[9]Research and Markets. Cyber Security Insurance - Global Market Outlook（2017-2026 年）. 2019 年.

2021 年“工信安全智库”系列研究报告

报告编号	报告名称	发布时间
2021-yp-01	2020-2021 年度工业信息安全形势分析	2021 年 1 月
2021-yp-02	2020-2021 年数字经济形势分析	2021 年 1 月
2021-yp-03	2020-2021 年度信息技术产业形势分析	2021 年 1 月
2021-yp-04	2020-2021 年度全球网络空间形势分析	2021 年 1 月
2021-dc-01	2020-2021 年我国工业互联网产融合作发展报告	2021 年 2 月
2021-dc-02	2020 年我国网络安全产业产融合作发展报告	2021 年 2 月
2021-lw-01	拜登政府网络安全政策走向及影响研判	2021 年 2 月
2021-lw-02	数字税的概念详解、全球进展和有关影响	2021 年 3 月
2021-dc-03	网络安全保险发展现状研究及展望	2021 年 3 月
2021-dc-04	数字中国建设扎实推进——解读《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 远景目标纲要》第五篇“加快数字化发展 建设数字中国”	2021 年 3 月
2021-dc-05	全球跨境数据流动相关问题研究	2021 年 4 月
2021-lw-03	欧盟《数字市场法案》《数字服务法案》的影响、趋势和建议	2021 年 4 月
2021-lw-04	2020 年东盟数字经济发展情况报告	2021 年 5 月
2021-lw-05	“小院高墙”下美国产业政策走向及我国应对措施	2021 年 5 月
2021-by-01	全球趋势 2040 一个竞争更加激烈的世界	2021 年 5 月
2021-dc-06	国内外个人信息保护政策和立法探究	2021 年 5 月
2021-yp-05	2021 年工业信息安全半年形势分析	2021 年 6 月
2021-yp-06	2021 年数字经济半年形势分析	2021 年 6 月
2021-yp-07	2021 年信息技术产业半年形势分析	2021 年 6 月

报告编号	报告名称	发布时间
2021-dc-07	2021 年上半年我国工业互联网产融合作发展报告	2021 年 7 月
2021-dc-08	2021 年我国网络安全产业产融合作半年形势分析	2021 年 7 月
2021-dc-09	智能网联汽车数据安全研究	2021 年 7 月
2021-dc-10	我国智慧农业发展情况及对策建议	2021 年 8 月
2021-dc-11	中国—东盟数字经济合作白皮书	2021 年 8 月
2021-dc-12	2020 年我国企业数字化转型进程报告	2021 年 8 月
2021-lw-06	主要工业国家和地区推动制造业数字化转型的做法和启示	2021 年 8 月
2021-dc-13	我国网络安全产业调研报告	2021 年 9 月
2021-dc-14	我国《数据安全法》构建的数据安全治理框架及政策趋势研究	2021 年 9 月
2021-dc-15	新一代人工智能算力基础设施发展研究	2021 年 9 月
2021-dc-16	面向数字基建的网络安全监管体系构建研究	2021 年 9 月
2021-dc-17	人工智能安全风险及治理研究	2021 年 9 月
2021-dc-18	我国数据开放共享报告 2021	2021 年 9 月
2021-dc-19	美国加大科技遏制对我国工业和信息化重点领域的影响	2021 年 10 月
2021-zs-01	2021 长三角数字经济发展报告	2021 年 10 月
2021-dc-20	共同富裕：企业社会责任助力工业和信息化大中小企业融通发展	2021 年 10 月
2021-dc-21	算力：数字经济发展的基石	2021 年 11 月
2021-dc-22	新形势下我国工业互联网+智能制造产业发展研究	2021 年 11 月
2021-lw-07	国外数据信托制度研究	2021 年 11 月

联系人：赵铭晨　　19800323351