 DOI: https://doi.org/10.12345/fm.v2i6.14507

An Indispensable Risk Management Tool in the Digital Economy Era—Network Security Insurance

Yaqi Tan

China Life Property & Casualty Insurance Company Limited, Beijing, 100033, China

Abstract

With the advent of the era of "Internet of Everything", emerging technologies such as the Internet of Things, big data, artificial intelligence, 5G communication continue to develop rapidly, and the economic development has entered the era of digital economy, the interconnected communication network not only creates convenience for people's work and life, but also provides a channel for the occurrence of network security accidents, such as network attacks, network extortion and data leakage, and the social way of production and life has changed greatly. Based on this, this paper carry out the risk research on the network security insurance in the era of digital economy.

Keywords

digital economy; risk management; network security insurance

数字经济时代不可或缺的风险管理工具——网络安全保险

谭娅琪

中国人寿财产保险股份有限公司，中国·北京 100033

摘　要

随着“万物互联”时代的到来，物联网、大数据、人工智能、5G通信等新兴技术持续快速发展，经济发展已经迈入数字经济时代。互联互通的通讯网络在为人们工作生活创造便利的同时，也为网络攻击、网络勒索、数据泄露等网络安全事故的发生提供了通道，社会生产生活方式发生巨大改变。基于此，论文研究中对数字经济时代的网络安全保险进行风险研究。

关键词

数字经济；风险管理；网络安全保险

1 引言

根据数据分析可知，现阶段的线下餐饮、交通、教育以及旅游等传统经济形式受到疫情后的冲击，线上化方式成为越来越多企业在生产经营中的选择。同时，为了应对各类突发事件，很多企业迅速启用远程工作系统，为大多数员工开通系统权限。在此背景下，对数字经济时代的网络安全保险进行风险研究势必有利于提前研判风险并加以管理。

2 现阶段数字经济风险分析

线上方式的常态化与权限控制的漏洞性无形中进一步加大了网络安全面临的新压力，全球企业面临的网络威胁日趋严重，造成的经济损失逐渐攀升。其中，表 1 为近年数字经济风险。

表 1 近年数字经济风险

时间	事件
2020 年	国际知名 GPS 设备品牌佳明（Garmin）遭到勒索软件攻击，导致在线服务受到影响，造成全球用户无法同步运动和健康数据，甚至造成飞行员无法将 Garmin 航空数据库版本下载到飞机导航系统，Garmin 公司最终向攻击者支付 1000 万美元赎金才获得解密密钥
2021 年	美国最大油气管道运营商 Colonial Pipeline 公司遭到 Darkside 勒索软件攻击。攻击者窃取了重要数据文件并劫持了其燃油管道运输管理系统，直接导致美国东部沿海各州的关键供油管道被迫关闭，给美国东海岸 17 个州造成了极大的燃油供应压力
2022 年	哥斯达黎加国家财政部 TB 数据和 800 多台服务器受到 Conti 无差别攻击影响，数字税务服务和海关控制 IT 系统瘫痪。不仅影响了政府服务，还影响了从事进出口的私营部门。清楚地展示了勒索软件攻击可能对政府组织造成的严重破坏性后果

通过表 1 总结过往事件发现，随着互联网技术的发展，网络安全面临的威胁日益严峻，主要呈现以下三个方面的特点。

【作者简介】谭娅琪（1984–），女，中国山西太原人，硕士，中级经济师，从事财产保险、产品创新研究。

2.1 网络安全事故发生频繁，类型多样

目前，企业线上化资产占比逐渐加大，遭遇网络安全事故的威胁日益加剧。据统计，数据泄露、勒索软件等是最主要、最常见的网络安全事故。数据泄露主要是指企业因遭受网络攻击造成客户信息或其他重要数据被泄露，影响范围广泛，是企业在网络安全方面的最大风险源头 [1]。勒索软件通过对受害者的数据进行加密处理，要求受害者支付赎金换取解密密钥。据统计，勒索病毒在 2022 年前十大网络威胁中位居首位，且攻击趋势及影响程度逐渐上升，预计 2023 年每 11 秒就将发生一起网络勒索事件。

2.2 网络安全事件影响恶劣，损失严重

企业一旦遭遇网络安全事故，不仅要承受自身的经济损失，通常还需承担对第三方造成的相关赔偿责任。营业中断损失是企业遭遇网络安全事故后所面临的最主要损失。一旦企业遭遇网络安全事故，其经营势必受到影响甚至中断 [2]。在完成网络恢复重建的期间内，企业面临的巨额营业中断损失已成为公认最严重的网络安全风险，且对各行业头部企业影响更为严重。勒索赎金及处理费用也是企业面临的一项重大损失。窃取私密数据并威胁受害者不交赎金即公开或出售数据成为勒索软件进行有效勒索的新方式，勒索的赎金金额也越来越高。除了对自身造成的经济损失外，因遭遇网络安全事故产生的对第三方的经济赔偿责任也是企业需承担的一项巨大损失。如企业因遭受网络攻击导致客户数据泄露，则需对受害客户进行补偿或承担相关赔偿责任。

2.3 网络安全风险蔓延迅速，波及广泛

共享平台为人们的生产生活带来了巨大便利，使数据得以在各方之间进行交互，在产品和服务的提供方面实现了自动化、精准化和个性化。但数字化产业链也为网络安全风险的蔓延提供了快速通道，易产生连锁反应。一旦某个环节发生网络安全风险，则可能会给所有依赖该供应链的企业造成巨大损失 [3]。例如，2020 年 2 月，作为中小企业云端商业及营销解决方案提供商的微盟公司，因其数据库遭遇人为破坏导致在线服务出现故障，宕机十天，给超过 300 万合作商家造成了巨额损失。

3 应对策略分析

在网络安全风险日益加剧以及潜在经济影响加速上升的背景下，网络安全风险管理已经刻不容缓，各国均采取了各种措施加大对网络安全风险的应对力度。

3.1 欧美应对策略

3.1.1 通过设计开发网络安全保险进行风险转移

伴随网络风险的发生与演变、攻击频率和攻击强度的不断加剧以及相关立法的不断完善，各行各业迫切需要通过保险产品进行风险转移，网络安全保险应运而生并实现快速发展。

20 世纪 90 年代，由于互联网的兴起，黑客攻击频发，美国开始出现针对网络安全风险相关的保单。1988 年，国际计算机安全协会（ICSA）推出了首款黑客保险。此后，市场上一些保险公司和 IT 公司陆续推出类似保险产品，承保范围以第一方经济损失为主。随着美国逐渐在立法中要求私营或政府组织对信息泄露承担通知义务，网络安全保险的承保责任逐渐扩展，2000 年左右开始出现包含第三方损失责任在内的网络保险保单。随后，承保范围逐渐扩展到保障企业因遭遇网络安全事故导致的营业中断损失、相关费用损失以及与之相关的第三方责任，涵盖财产险、责任险两大范畴 [4]。目前，美国有 50 多家保险（集团）公司提供独立的网络安全险保单，覆盖的网络风险包括数据泄露、病毒 / 恶意软件、拒绝服务攻击、黑客入侵等。据统计，截至 2021 年底，美国网络安全保险市场规模已达到 48 亿美元。

3.1.2 通过立法形式加强网络风险管理

2003 年，美国加州政府颁布了第一部安全漏洞的相关法令，要求企业在用户个人信息被泄露时要及时披露并通知用户。如今该类法令已遍布全美各州。2014 年，美国颁布《2014 年国家网络安全保护法》，以加强抵御网络攻击的能力。2016 年，欧洲议会投票通过《通用数据保护条例》（GDPR），旨在保护消费者的数据和隐私；2016 年欧盟立法机构通过了《网络与信息系统安全指令》，要求基础服务运营商、数字服务提供商履行网络风险管理、网络安全事故应对和通知等义务。

其他国家健全的法律体系和严格的监管要求不仅为网络安全风险的等级评估提供了标准，也有效预防了道德风险，进一步推动了网络安全保险的发展。

3.2 中国应对策略

3.2.1 中国开启通过保险产品转移风险的探索道路

随着中国信息技术产业的不断发展，企业的网络安全风险意识不断提升，对网络安全保险的需求也在增长。

2013 年，苏黎世保险在中国首次推出网络安全保险，随后在中国设有子公司或合资公司的国际保险公司，如安达保险、美亚保险等纷纷效仿。近年来，中资保险公司也在逐渐尝试开发并推广此类产品，产品内容基本与其他国家保持一致，赔偿范围涵盖第一方经济损失与第三方责任。

3.2.2 中国正逐步构建网络安全法律体系

与其他国家良好的法律环境相比，中国在网络安全方面的相关法律与配套制度尚需完善。

在网络风险持续加剧与数字经济快速发展的双重背景下，中国在 2017 年 6 月正式实施《网络安全法》，为网络安全管理奠定了法律基础，从立法角度确定了相关各方的权利和义务、网络安全等级标准等内容，并辅以相关行政法规、部门规章、国家标准、司法解释，逐渐构建起中国网络安全管理的法律体系。

4 中国网络安全保险现状与发展建议

4.1 中国网络安全保险现状

为贯彻落实网络强国战略，切实提高企业的网络安全管理水平，截至 2022 年底，中国 30 余家财险公司通过与专业再保人、网络服务商建立合作关系等方式，探索构建“保险＋服务”全流程网络安全风险管理体系，为企业在数字时代下抵御网络风险提供了重要保障。

4.1.1 已搭建较为完善的产品体系和全面的风险保障

在面向法人客户的网络安全保险方面，中国主要财险公司相继开发了网络安全财产损失保险、网络安全责任保险及网络安全综合保险。承保范围包括第一方经济损失与第三方赔偿责任，基本涵盖常见的网络安全事件支出以及个别不可见的网络安全事件支出。其中，表 2 为各方损失对比。

表 2 各方损失对比

第一方经济损失	第三方赔偿责任
（1）网络营业中断损失 （2）网络勒索赎金或网络勒索处理费用 （3）数据修复费用 （4）咨询服务费用 （5）用于事故鉴定和影响评估的费用 （6）声誉恢复费用	（1）信息泄露责任 （2）数据安全责任 （3）媒体侵权责任 （4）为应对保险事故支出的事故响应费用

4.1.2 已与再保公司建立合作关系，具有较强的专业承保技术与风险管理手段

借鉴其他国家先进经验与成熟模式，中国财险公司与国际专业再保公司建立了合作，在产品设计、承保定价、风险管控方面借助再保公司的历史数据、定价模型和专业技术等优势，在大力拓展网络安全保险业务的同时有效控制承保风险，提升了网络安全风险管理能力并建立起可持续发展模式。

4.1.3 已开展引入专业风险管理服务商，打造全流程风险减量管理创新模式

在保险保障以外，中国主要财险公司与 360 集团、源堡科技等专业网络安全公司建立战略合作关系，为客户提供承保前 IT 资产评估、无感知测试，承保中安全检测、红蓝对抗、安全培训服务以及保险事故发生后的应急处理及事故鉴定等网络安全服务，提供事前评估、事中监测、事后补偿的全流程风险管理服务。

4.2 发展建议

2023 年 7 月，工业和信息化部、国家金融监督管理总局发布《关于促进网络安全保险规范健康发展的意见》，将有力指引网络安全保险健康有序发展 [5]。为积极开拓网络安全保险这一蓝海领域，建议中国财险公司从以下三个方面进行发展推动：

第一，加强与当地政府、公安厅（局）等部门的合作交流，因地制宜建立网络安全管理模式。通过与各地公安部门开展合作，借助网络安全周主题活动，提高网络安全保险的知悉度与认可度；主动与政府部门开展沟通交流，发挥政府引导作用，构建适合当地的业务合作模式；积极推广“保险＋服务”网络安全风险管理模式，体现行业担当，提升行业价值。

第二，加大现有资源利用率，深挖客户潜在需求。目前，中国主要财险公司与各行业头部企业均搭建有良好的保险合作关系。要深度挖掘现有客户的网络安全保险需求，主动拓展合作范围，为头部企业提供一揽子保险保障服务，同时要结合客户的网络安全实际情况安排网络安全培训、网络健康检测等网络风险防控服务，实现有形资产与无形资产的全方位风险管理，打造“企业的风险管家”品牌形象。

第三，围绕中小企业需求设计保险方案，积极拓展下沉市场。随着“互联网＋”时代以及数字化产业链的发展，任一环节发生网络安全风险都可能蔓延至其他环节。除头部企业外，中小企业所面临的网络安全风险同样不容小觑。因此，要深入一线，紧紧围绕中小企业实际的网络安全需求设计制定具有针对性的保险服务方案，抢抓先机，开拓开发中小企业网络安全保险市场。

5 结语

随着数字经济时代的发展，网络资产已成为各行各业的重要财产。在中国产业结构调整和经济转型升级的关键时期，中国财险公司应把握机会、主动出击，积极开展与各方的合作交流，抢先“牵住牛鼻子”，走好“先手棋”，占领先机，赢得优势，做大做强网络安全保险这一新兴市场。

参考文献

[1] 国家工业信息安全发展研究中心.网络安全保险发展现状研究及展望[R].2021.

[2] 安天CERT.连锁传递的威胁——从软件供应链视角看网络安全[R].2017.

[3] 21世纪经济报道.多方风险威胁数据安全 产业数字化亟待重构防护能力[N].2023.

[4] 上海保险.把控日趋复杂的互联性:网络安全风险趋势[R].2021.

[5] 中国网信.网络安全保险保障数字经济高质量发展[R].2022.