

关于大型企业投保网络安全保险的研究

刘汉沙

英大长安保险经纪有限公司，北京 100032

摘 要： 本文主要研究大型企业网络安全保险的投保问题。首先，提出了一个基本的风险评估框架，以分析和判断企业的数据泄露、勒索软件攻击以及网络战争等不同场景下面临的风险；其次，通过对传统商业保险的不足之处进行对比，从保险承保范围、保费与保额、免赔额和除外责任四个方面探讨了网络安全保险对企业数据安全的保障作用；最后，分析了影响企业投保网络安全保险的因素，并给出了具体的解决方案。本文的研究有助于帮助企业提高网络安全防护意识，加强信息系统的安全性，并为相关部门提供政策制定依据，同时也是一项有益于我国发展的工作。

关 键 词： 大型企业；投保网络；安全保险

Research on Network Security Insurance For Large Enterprises

Liu Hansha

Yingda Chang'an insurance brokerage Co., Ltd. Beijing 100032

Abstract： This paper mainly studies the insurance of network security insurance for large enterprises. Firstly, a basic risk assessment framework is proposed to analyze and judge the risks faced by enterprises in different scenarios, such as data leakage, extortion software attack and network war; Secondly, by comparing the deficiencies of traditional commercial insurance, this paper discusses the protection effect of network security insurance on enterprise data security from four aspects: insurance coverage, premium and insured amount, deductible and exclusion; Finally, this paper analyzes the factors that affect enterprises' network security insurance, and gives specific solutions. The research in this paper will help enterprises improve their awareness of network security protection, strengthen the security of information systems, and provide the basis for policy-making for relevant departments. At the same time, it is also a work beneficial to China's development.

Keywords： large enterprises; insurance network; safety insurance

随着互联网技术的飞速发展，企业在业务开展过程中，利用电子邮件、即时通讯软件等工具进行交流与合作，这不仅提高了工作效率，同时也给企业带来了巨大的安全风险。由于网络安全威胁的复杂性和不确定性，企业很难对其所面临的各种风险进行评估。如果不能及时发现潜在的安全隐患，则可能会造成无法挽回的损失。因此，建立一个合理的风评估框架，可以帮助企业管理者更好地识别出那些尚未被察觉的风险，并采取有效措施来降低风险的影响。本文提出的网络安全保险方案，可以帮助企业在遭受网络攻击时获得赔偿，从而减少损失。

一、网络安全保险概述

网络安全保险是一种以防范网络风险为目的的保险产品，旨在保障企业或个人在遭受恶意网络攻击后所产生的损失。它主要涵盖了以下几个方面：

（一）财产损失：当企业在使用计算机和其他电子设备时发生故障或损坏，导致企业损失的情况。例如，由于电脑病毒入侵导致系统崩溃，造成数据丢失或被篡改等^[1]。

（二）法律费用：当企业在面临诉讼或仲裁时，需要支付律师费用、调查费用等相关支出。

（三）声誉损失：当企业因遭受网络攻击而遭受重大负面影响时，可能导致客户流失或品牌形象受损。

（四）收入损失：如果企业因遭受网络攻击而无法正常工作，从而导致收入减少或中断。

由于上述风险具有较高的复杂性和不确定性，传统的商业保险并不完全适用于这些领域。因此，开发专门针对网络安全风险的保险产品成为当前市场的重要需求之一。网络安全保险的提供者通常包括保险公司、再保险公司和保险经纪机构^[2]。他们根据不同的风险类型，设计出多种不同的保险方案供客户选择。一般来说，网络安全保险方案会包括两部分：一个是基本保障方案，另一个是扩展保障方案。

基本保障方案主要针对企业最常见的安全风险，如物理破坏、网络攻击、数据泄露等。而扩展保障方案则可以覆盖更多的潜在风险，例如操作失误、管理不善、技术错误、政策变化等。

此外，许多网络安全保险方案还提供额外的附加条款，以满足客户对特定需求的需求。

总之，网络安全保险是一个复杂的金融产品，它结合了保险原理和计算机安全知识。通过购买这种保险，企业可以获得一种有效的财务保障，以便在遭受黑客攻击时能够迅速恢复生产。同时该保险也可以帮助企业管理者及时了解到自身所面临的风险程度。

二、国内大型企业面临的主要网络安全风险及保险需求分析

本文选取了国内100家大型企业作为研究对象，通过调查问卷的方式对企业员工进行访谈，收集到了企业员工关于网络安全风险方面的主要关注点和担忧。其中有59%的受访者表示他们会选择购买网络安全保险；有27%的受访者表示他们不太清楚是否需要购买网络安全保险；有5%的受访者认为他们已经购买了网络安全保险^[3]。而在这些受访者中，只有3%的受访者表示他们所在企业已经购买过网络安全保险，这表明大部分企业并没有将网络安全保险纳入自己的风险管理体系中。

通过分析发现大多数企业都面临着一些主要的网络安全风险，包括：1. 网络漏洞风险：随着信息技术的不断发展，各种新型攻击手段层出不穷。企业需要不断更新系统和软件以避免被黑客利用漏洞入侵。2. 数据泄露风险：企业在日常经营活动中可能会产生大量敏感数据，如客户信息、财务报表等。一旦发生泄露事件，将给企业带来严重的经济损失。3. 勒索软件风险：近年来，勒索病毒越来越多地出现在企业和个人用户面前。一旦遭受勒索软件攻击，不仅会导致系统崩溃、文件丢失，还可能造成严重的经济损失。

三、网络安全保险基本情况介绍

网络安全保险是指将因网络攻击导致的经济损失纳入保险范围，并对这些损失进行赔偿的保险。目前国际上主要有两种网络安全保险模式：一是以美国为代表的国家主导模式；二是以英国和新加坡为代表的市场主导模式。

在美国，联邦政府与私营企业合作，共同建立了网络安全保障机制（NCCIC），该机制为企业提供了一套完善的网络安全风险管理体系。2014年5月，美国政府发布了《加强关键基础设施保护》的行政命令，要求所有关键基础设施的所有者、运营者和管理者向NCCIC购买保险，以降低发生重大网络事件的风险^[4]。英国是世界上第一个推出网络安全保险的国家，也是全球首家由政府推出网络安全保险的国家。为了解决中小企业缺乏资金支持的问题，英国政府采用PPP模式，即政府和企业合作，由政府出资设立专门的公司，然后通过招投标方式让私营企业投保。根据英国财政部官网披露的信息显示，自2016年4月起至今，共有179家企业完成投保，其中包括多家世界500强企业。新加坡在2013年开始推广网络安全保险，最初只针对政府机构，后来逐步

扩大到商业部门。这是因为新加坡认为只有这样才能更好地发挥保险的作用，既能够促进企业提升网络安全防护意识，又可以帮助政府更好地开展网络安全工作。

目前我国也在积极推进网络安全保险的发展，但由于其刚起步，所以还处于探索阶段。中国人民财产保险股份有限公司和中国太平洋财产保险股份有限公司均在2018年7月推出了国内第一款网络安全保险产品，主要承保企业或个人电脑遭受黑客入侵而造成的经济损失，如数据资料被窃取等。值得注意的是，当前我国的网络安全保险仍处于萌芽阶段，相关的法律法规还不够完善，例如缺乏明确的保险条款、费率标准、责任界定等，导致投保难度较大。而且，由于缺乏成熟的网络安全技术，大部分投保企业很难通过评估，无法获得保险保障。因此建议从以下几方面入手来推动网络安全保险的发展。

首先，需要尽快出台关于网络安全保险的法律法规，规范行业发展。具体来说，应该制定一个综合性的法律框架，规定不同类型的网络安全事故如何界定，以及相关责任方应承担的义务^[5]。其次，要加大宣传力度，提高企业的网络安全意识，引导他们认识到投保网络安全保险的重要性。最后，鼓励保险公司创新网络安全保险产品，设计出符合企业需求的保险方案。当前，随着5G、物联网等新兴技术的快速发展，网络安全问题日益突出，成为影响国家和社会稳定的重要因素。为了应对网络安全挑战，保障国家和社会稳定，我国应加快网络安全保险的发展步伐，同时加强监管和引导，使其成为维护国家和社会稳定的有力工具。

四、影响企业投保网络安全保险的因素分析及解决方案

在对网络安全保险进行详细介绍的基础上，本文进一步分析了企业投保网络安全保险的影响因素。首先，从企业层面看，信息安全意识淡薄、缺乏专业人员和相关技术支撑等原因导致企业不愿投保网络安全保险；其次，从保险公司角度看，保险条款过于复杂、价格过高、索赔流程繁琐以及缺少专业人士指导等因素都会影响企业的投保意愿；针对以上因素，本文提出了以下解决方案：

（一）完善网络安全保险发展政策

首先需要完善网络安全保险规范。建设标准体系可以引领网络安全保险市场主体，针对承保和理赔等指标出台相应的标准，规范化发展网络安全保险^[6]。其次要实现网络安全保险语言的标准化。通过遵循行业规范，统一界定有关网络安全保险的核心概念和权责归属问题。针对网络风险制定标准化的术语，同时需要出台保单语言和保单要素等方面的标准。最后完善保险公司再保险机制。为网络安全保险公司提供再保险，持续性供应网络安全保险，合理降低保险定价，有利于充分利用网络安全保险。

（二）建立金融业网络事件数据共享库

建立网络事件共享库，有利于保险公司建立网络风险精算模型，可以对保险费率进行控制，提高网络安全保险的吸引力，吸

引更多的金融机构，提高网络安全保险的应用率。通过完善网络安全事件信息共享机制，可以发挥出预警作用，提醒金融机构及时对网络安全漏洞进行修复，避免不断地扩散网络安全风险事件。首先需要完善金融网络安全事件的报告机制，合理分类金融网络安全事件，确定事件报告过程中需要利用的各种要素。其次需要构建金融网络安全提示的感知平台，可以进一步优化监管工作，避免瞒报和漏报金融网络安全事件。最后需要完善数据共享激励机制，引导相关参与方积极共享相关数据。

（三）提高金融机构构面网络安全保险的意识

首先需要积极宣传网络安全险种，引导更多的金融机构了解网络安全保险的重要性，提高金融机构构面网络安全保险。完善交流平台，引导金融机构和保险机构以及安全服务商等积极合作，进一步完善保险+安全服务的模式，使网络安全保障水平得以提升^[7]。其次需要建立机构试点。针对再保险过程中的风险，进一步完善分散和补贴机制，在银行机构开展试点工作，对金融网络安全保险的发展总结经验，建立科学的发展对策，充分发挥出示范的作用。最后落实细分领域试点。针对金融数据安全和个人金融信息保护等需求，对网络安全保险的细分领域开展试点工作，通过试点运行可以推动市场发展，完善金融数据安全共享机制，保护金融消费者的权益。

（四）加强金融网络安全保险业的合作

首先需要加强国际合作。因为发达国家建设网络安全保险机制的时间比较早，因此逐步建立了完善的网络事件共享机制和监管机制，有利于更好地普及网络安全保险，通过构建合作机制，可以积极借鉴学习相应的管理经验^[8]。其次需要完善网络安全保险产业生态。一系诶保险公司逐渐完善网络安全风险业务，并且积

累了丰富的工作经验。各保险公司可以建立合作关系，保证精算定价的合理性，推动产品研发，合理分担再保险的风险，为被保险人提供针对性的保险保障，获取优质的安全服务，对其承担的网络安全风险进行控制。

（五）提高保险科技应用能力

大型保险企业不断发展保险科技，可以使网络安全保险的风险识别水平不断提升。针对当前存在的问题，保险企业需要加大力度利用各种保险科技，有效控制风险点。例如当前在实际工作中数据存储存在一定的风险，可以利用区块链技术加密处理保户数据，在不泄露隐私数据的同时安全地共享和利用数据^[9]。针对保险科技应用场景，企业需要充分利用人才优势，在网络安全保险的价值链中利用保险科技。

（六）加快数据化转型

利用数据化技术优势，可以进一步完善生产价值链，增强技术渗透效果，合理控制企业运营成本，推动企业实现数字化转型，高效地经营网络安全保险^[10]。以网络安全保险业务需求为基础，企业可以合理改造当前业务模块和系统功能模块，充分发挥出信息技术的作用，使生产价值链得以进一步强化。

五、结束语

本文针对网络安全保险市场发展过程中存在的问题，提出针对性的发展对策，通过加大力度宣传大型企业投保网络安全保险的重要性，吸引更多的企业投保，同时需要积极利用先进的技术，解决当前网络安全保险发展过程中遇到的技术难点，提高整体服务水平，充分拓展网络安全保险市场。

参考文献

- [1] 何启豪. 应对网络安全风险的保险保障机制论要[J]. 比较法研究, 2024,(03):125-138.
- [2] 周瑞珏. 面向网络安全风险的保险合同义务理论创新[J]. 学术交流, 2024,(05):73-87.
- [3] 周瑞珏. 数据泄露风险治理中网络安全保险的介入路径[J]. 北方法学, 2024,18(02):76-90.
- [4] 李晓翾, 雷牧晨. 相对指数型网络安全保险产品的量化分析研究[J]. 保险职业学院学报, 2023,37(06):16-20.
- [5] 唐金成, 刘榕. 数字经济时代我国网络安全保险承保范围优化研究[J]. 保险职业学院学报, 2023,37(03):5-13.
- [6] 赵亚宁. 数字经济时代保险参与网络安全治理的制度困境与纾解之道[J]. 保险研究, 2023,(05):37-50.
- [7] 刘秒. 我国网络安全保险投保率提升路径探析[J]. 上海保险, 2022,(11):52-54.
- [8] 李长连, 王娜, 贺译册, 等. 网络安全保险业务模型与风险管理浅析[J]. 邮电设计技术, 2022,(09):1-5.
- [9] 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[J]. 工业信息安全, 2022,(03):6-12.
- [10] 唐金成, 莫赐聪. 数字经济时代网络安全保险创新发展研究[J]. 西南金融, 2022,(01):52-64.