网络安全保险业务模型与风险管理浅析

Analysis of Network Security Insurance Business Model and Risk Management

李长连[1]，王　娜[2]，贺译册[2]，刘　果[1]，杨　飞[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Li Changlian[1], Wang Na[2], He Yice[1], Liu Guo[1], Yang Fei[1] (1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘　要：

分析了网络安全保险的定义与内涵，提出了网络安全保险产品设计需要权衡的4个要素与业务流程设计方案，并提出了一种覆盖网络安全保险业务全生命周期的风险管理方案，阐述了每个环节的关键目标、工作步骤与技术手段。

关键词：

网络安全保险；业务模型；网络安全风险管理；全生命周期

doi：10.12045/j.issn.1007-3043.2022.09.001

文章编号：1007-3043（2022）09-0001-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

It analyzes the definition and content of network security insurance, puts forward four elements and business process design schemes that need to be considered in the design of network security insurance products, and puts forward a risk management scheme covering the whole life cycle of network security insurance business, and expounds the key objectives, work steps and technical means of each link.

Keywords：

Network security insurance; Business model; Network security risk management; Full life cycle

引用格式：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（9）：1-4.

0 引言

随着信息化和网络化不断深入，网络安全的重要性日益凸显，而仅仅依靠技术手段难以完全消除网络风险。因此，保险作为风险转移的主要手段以及企业和个人进行风险管理的方式之一，理应发挥重要作用[1]。

国际上，1977年，美国AIG保险公司推出了“黑客保险”，该产品仅针对第三方责任，承保范围为美国以外地区。20世纪90年代，美国Chubb保险公司推出了第1份“网络安全保险”，2000年以后，美国市场开始发展[2]。2019年，全球网络安全保险市场达到了55.73亿美元，预计将保持10年26.3%的复合增长率，到2030年将达到706.72亿美元[3]。

在国内，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）》中在“积极创新网络安全服务模式”任务中提出“探索开展网络安全保险服务”。2020年9月，网络安全等级保护和关键信息基础设施安全保护工作宣贯会提出在网络安全领域引入保险机制，并围绕顶层设计、机制落地、服务模式探索等方面明确了重点工作。

我国网络安全保险市场目前总体规模偏低，滞后于我国数字经济的发展程度，还处于探索期。据瑞士再保估计，我国网络安全保险的总保费规模仅为约7 000万元人民币，到2025年，中国市场保费规模将增至5亿元人民币且持续维持高增长率，年均增速达

收稿日期：2022-07-04

30%以上[4]。随着我国网络安全产业的持续发展和网络安全法律法规框架的不断完善，我国网络安全保险市场具有巨大的增长空间[5]。

1 网络安全保险内涵分析

在传统的风险控制模型里，应对风险共有4种手段：消除、降低、转移和接受。保险是风险转移的基本手段，网络安全保险作为有效转移网络安全风险的工具，能够帮助企业建立全面的网络安全风险应对方案[4]。美国国土安全部将网络安全保险定义为“减轻各种网络事件造成的损失的保险”，包括数据泄露、业务中断和网络损害[6]。

相比于传统保险险种，网络安全保险更加强调服务属性，采用网络安全服务+保险机制[7]，投保人投保的时候，安全服务公司通过提供专业的安全检测评估服务，保险公司可以了解投保人信息系统的风险情况，方便保险公司进行定价和风险控制。当保单生效后，安全公司为投保人提供日常安全服务，如信息系统监测、漏洞扫描等，尽可能降低投保人出现风险的概率。如果出现了安全事件，投保人可以第一时间拨打理赔电话，会有专业的技术团队对安全问题进行定位和恢复，安全事件会给投保人造成一定的经济损失，如第一方损失和第三方索赔，安全服务公司会配合保险公司进行专业的取证、定损。

2 网络安全保险业务模型设计

2.1 产品设计

网络安全保险产品设计需要考虑以下几个因素。

a）险种分类：作为一个独立险种还是从属于其他险种。

b）保险对象：网络安全保险对象是企业客户还是个人客户。

c）承保范围与责任免除：仅承保第一方损失还是连带第三方赔偿责任，分别包括哪些费用，如何进行清晰的范围限定，哪些情况下免除保险责任。

d）投保系统特征：投保系统的网络架构（纯内网系统、互联网服务系统、混合型等）、部署类型（传统物理部署、虚拟化、容器化、云化、多分支混合部署等）、系统业务重要性（等保备案等级、是否属于关键基础设施等）。

e）安全风险与监测防护能力：充分考虑投保系统所面临的安全风险，包括行业历史数据与系统历史安全数据分析，对系统目前的安全攻击风险、脆弱性以及监测防护能力进行量化评估。

f）保险额度、免赔额与分项限额：需要综合考虑客户需求、承保范围、投保系统业务重要性与安全水平，结合历史数据，建立保险精算模型，确定保险额度、免赔额与分项限额。

根据以上分析，网络安全保险产品设计可以归结为4个要素的权衡（见图1）。

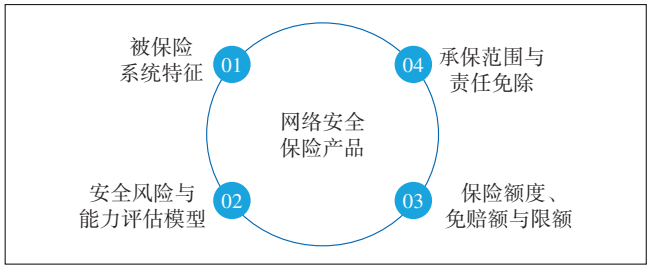

图1　网络安全保险产品设计要素示意图

进行网络安全保险产品设计，需首先梳理清楚潜在的网络安全攻击风险、损失与赔偿责任，结合投保系统的具体情况进行分类。常见的网络攻击类型包括DDoS攻击、勒索病毒、木马病毒等，由于攻击类型多样、缺乏公认的标准定义与分类、攻击手段迭代速度快等因素，网络安全保险产品承保范围不适合根据网络攻击类型确定[8]。客户遭受网络攻击后的损失类型与恢复手段比较明确，契合网络安全保险量化损失数据并予以补偿的思路，建议可考虑承保的常见赔偿责任分类如表1所示。

以上仅为常见赔偿责任举例，网络安全保险产品确定承保范围与责任时必须要充分综合考虑投保系统特征、安全服务厂商能力、保费收入等因素。

2.2 业务流程设计

2.2.1 投保与服务流程

图2所示为网络安全保险产品投保与服务流程示意。相比普通保险产品的投保流程，网络安全保险产品由于技术复杂性和缺少历史数据，需关注网络安全调研问卷的设计，全面搜集相关数据，包括系统物理环境、网络接入、系统保护等级、等保测评结果与报告、网络安全管理制度、资产管理等信息，网络安全风险、监测防护能力与历史网络安全事件是调研重点，可安排现场检查与渗透测试，以评估客户的真实安全监测与防护水平，对被保险系统的历史安全事件进行详细分析与询问，以评估客户的安全风险等级。

保险公司将所有搜集到的信息输入到自有或第

表1　网络安全保险产品建议承担范围与赔偿责任

序号	分类	承保内容	详细描述
1	直接损失	营业中断导致的利润损失	内外部网络威胁与攻击所导致的营业中断
2		数据/系统恢复费用	内外部网络威胁与攻击所引发而必须的数据/系统恢复工作
3		网络勒索费用	外部黑客组织等发起的网络勒索所引发而必须的相关费用
4		数字资产置换费用	内外部网络威胁与攻击所引发而必须的数字资产置换费用
5		漏洞修复费用	营业中断、数据/系统恢复、网络勒索、数字资产置换等责任所需的漏洞修复服务
6	间接服务	鉴定服务费用	营业中断、数据/系统恢复、网络勒索、数字资产置换等责任所需的鉴定服务
7		通报监测费用	营业中断、数据/系统恢复、网络勒索、数字资产置换等责任所需的通报监测服务
8		名誉修复费用	营业中断、数据/系统恢复、网络勒索、数字资产置换等责任所需的名誉修复服务
9		数据行政调查费用	数据行政调查服务
10		合规整改咨询服务费	合规整改咨询服务
11		网络勒索危机顾问费	网络勒索危机顾问服务

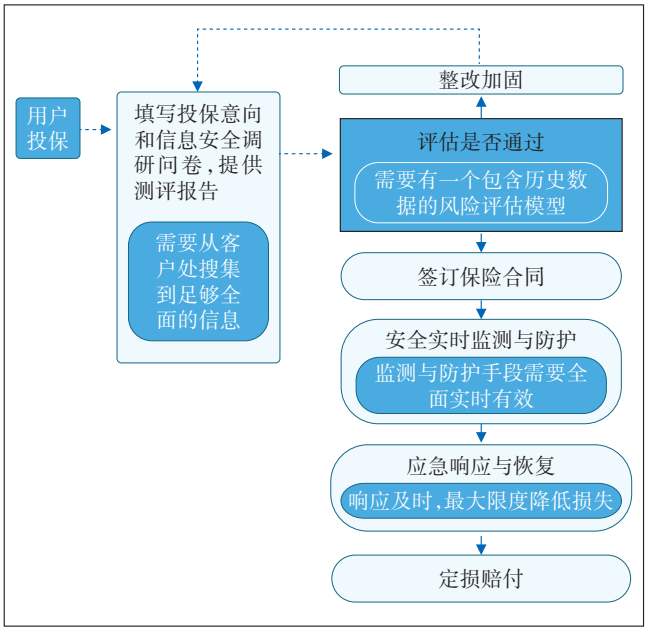

图2　网络安全保险产品投保与服务流程示意图

三方的量化风险评估模型，评估是否可以承保客户投保系统，根据评估结果确定与客户签署合同或通知整改加固后再评估。

网络安全保险一般都会强制配套提供网络安全检查、监测与防护服务，及时了解客户的安全风险，参与网络安全事件应急响应与恢复工作，以避免或降低攻击所造成的损失。

2.2.2　理赔流程

图3给出了网络安全保险产品理赔流程示意。

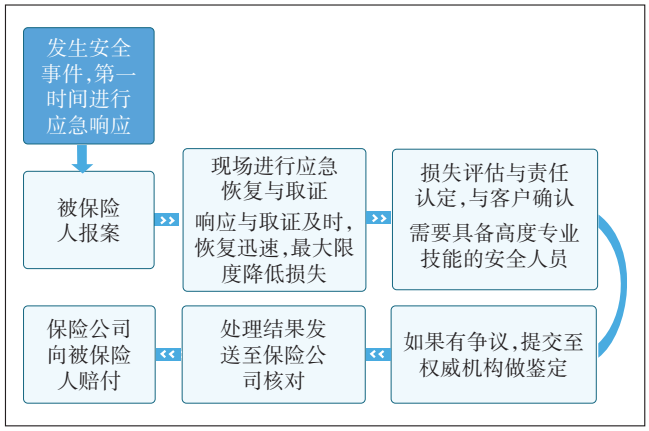

图3　网络安全保险产品理赔流程示意图

网络安全保险理赔流程遵循常规的“客户报案→现场取证→责任认定→机构鉴定→核对→赔付”流程，但现场应急恢复、攻击取证与损失评估环节需要具备高度专业技能的安全人员才可以完成，因此保险公司开展网络安全保险业务必须首先具备自有或第三方的安全服务团队，并与具备网络安全攻击事件鉴定资质的机构建立合作关系。

3　全生命周期风险管理方案

图4给出了网络安全保险全生命周期风险管理示意。保险公司开展网络安全保险业务最大的挑战是为降低网络安全攻击所造成的损失，对投保系统安全风险的识别、监测、防护和记录。

3.1　安全测评

定期对承保系统进行安全风险评估，获取并分析投保系统网络安全等级测评报告，其具有强制性、覆

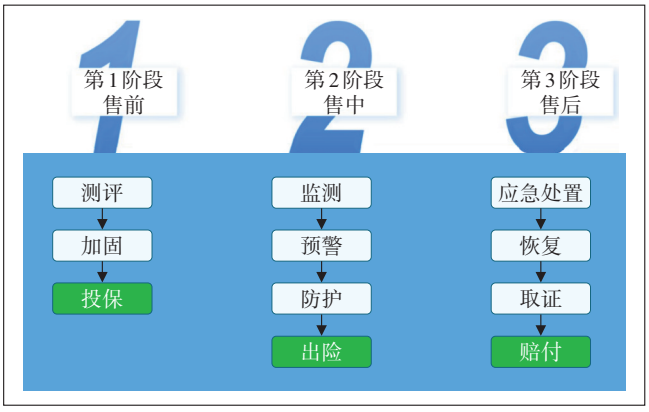

图4　网络安全保险全生命周期风险管理示意图

盖面全、权威性高的特点，可展示客户网络安全全貌。

3.2 安全加固

根据安全测评报告的结果，要求客户对系统脆弱环节进行加固，技术手段包括但不限于网络拓扑调整、新增或替换安全设备、服务器加固、网络设备加固、数据库加固、中间件加固、应用软件加固等。

3.3 安全监测

对客户系统进行定期/实时安全监测，全面掌握潜在的安全漏洞与攻击风险，技术手段包括但不限于漏洞扫描、全流量高级威胁分析APT、攻击入侵监测IDS、DDoS攻击监测、网站安全监测（Web扫描、挂马监测、篡改监测、敏感词监测、黑链监测等）、日志审计、蜜罐。

3.4 风险预警

接收各类安全设备、服务器设备、网络设备的监测结果，经过分析之后生成预警信息，并采取处置手段（包括但不限于自动关联防护设备进行防护），推给相应的人员进行加固，预警信息通知方式包括页面告警、邮件、短信、微信等社交软件、电话等。

3.5 安全防护

在遭受攻击后采取实时安全防护手段，包括但不限于防火墙、入侵防御IPS、DDoS防护服务或设备、高防、Web应用防火墙、上网行为管理等。

3.6 应急处置

在发生安全事件之后，应急处置一般包括：

a）保险报案：当用户投保的系统发生了安全事件后，用户在第一时间拨打保险公司客服电话；保险客服核实情况并登记，呼叫转移到安全服务公司的技术支持电话。

b）应急响应：安全服务公司技术人员和用户沟通安全事件，执行针对性安全应急预案；在规定时间内，安排安全服务团队为客户提供应急响应服务。

c）事件检测：安全服务团队在客户的配合下对出险的系统进行初步分析，确认信息安全事件的真实性，制定进一步的响应策略，并保留证据。

d）问题抑制：安全服务团队及时采取行动限制事件扩散和影响范围，避免潜在损失与破坏，同时采取封锁措施以减少对相关涉及业务的影响。

e）问题根除：安全服务团队对安全事件进行抑制后，通过对有关事件或行为的分析结果，找出事件根源，查明原因并明确相应的补救措施。

3.7 系统恢复

配合客户事先做好完善的恢复计划，在发生安全事件之后，安全服务团队需要遵照恢复计划尽快恢复安全事件所涉及到的系统，并使其还原到正常状态，恢复工作需要客户配合完成。

3.8 数字取证

在发生安全事件之后，及时进行数字取证，作为索赔与定损依据，需要第三方权威专业机构完成。

4 未来发展展望

我国网络安全保险刚刚起步，客户对于网络安全保险的接受度正在逐步增强，市场前景被广泛看好，但在产品落地和发展过程中也面临着多重的阻力和挑战，如行业缺乏统一的风险评估模型与定损模型、新网络安全攻击类型层出不穷、危害程度日趋严重、监测防护手段日新月异等[9]，这些难题都需要保险行业与网络安全行业专家联合进行研究并解决，践行网络强国战略，促进网络安全保险在中国的蓬勃发展。

参考文献：

[1] 纪泉乐，焦倩文. 网络安全保险研究现状及展望[J]. 计算机科学与应用，2019，9(8)：10.

[2] ELING M，ZHU J J. Which insurers write cyber insurance? Evidence from the U.S. property and casualty insurance industry[J]. Journal of Insurance Issues，2018，41(1)：22-56.

[3] Prescient & Strategic. Cyber insurance market research report 2030 [EB/OL]. [2022-04-25]. https://www.psmarketresearch.com/market-analysis/cyber-insurance-market，2020-06-01.

[4] 王佳欣，程然. 网络安全风险专题系列 第4辑：中国网络安全保险市场[EB/OL]. [2022-04-25]. https://mp.weixin.qq.com/s?__biz=MzA3NDQ4OTY4Ng==&mid=2651424419&idx=1&sn=ed7aa8a1565909d5383ae8ba609f872e&chksm=84822%E2%80%A6，% 202019-09-26.

[5] 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(1)：52-64.

[6] 顾建强，梅姝娥，仲伟俊. 基于网络安全保险的信息系统安全投资激励机制[J]. 系统工程理论与实践，2015，35(4)：1057-1062.

[7] 王伊琳，钱镜羽，王天硕. 后疫情时代网络安全保险的透视与思考[J]. 上海保险，2020(8)：56-60.

作者简介：

李长连，毕业于西北工业大学，高级工程师，硕士，主要从事网络安全技术研究、规划咨询、网络安全产品研发与运营工作；王娜，毕业于北京联合大学，高级工程师，硕士，主要从事网络安全运营工作；贺译册，毕业于北京交通大学，产品经理，学士，主要从事网络安全产品研究、网络安全产品规划设计工作；刘果，毕业于武汉理工大学，学士，主要从事网络安全技术研究和网络安全产品研发工作；杨飞，毕业于合肥学院，高级工程师，学士，主要从事网络安全技术的研究工作。