Computer Science and Application 计算机科学与应用, 2019, 9(8), 1473-1482
Published Online August 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.98165

Hans汉斯

Current Status and Prospects in Researches of Cyber-Insurance

Quanle Ji*, Qianwen Jiao

College of Computer Science and Technology, Silicon Lake College, Kunshan Jiangsu
Email: *1084880575@qq.com, 1987619262@qq.com

Received: Jul. 20th, 2019; accepted: Aug. 2nd, 2019; published: Aug. 9th, 2019

Abstract

With hackers, computer viruses and cyber crime seriously threatening information security, users' loss or damage caused by network security will be more probable. As an emerging risk management mode, cyber-insurance has been drawing more and more attention in both academic and industrial community and becoming an exploration of network economical time. Cyber-insurance is a kind of insurance that a policy-holder pays certain premium to insurance companies in return for compensation when network security breaks out. Because usual protection measures could never eliminate risk, cyber-insurance is an effective tool to transfer the remaining risk of information systems. This paper presents the background of cyber-insurance. The important research areas such as self-defense investment incentive, correlated risk, interdependent security, information asymmetry, as well as the cyber-insurance market are summarized. Finally, the paper discusses possible directions and challenges of cyber-insurance.

Keywords

Network Security, Security Risk, Cyber-Insurance, Information Security Investment

网络安全保险研究现状及展望

纪泉乐*，焦倩文

硅湖职业技术学院，计算机与软件学院，江苏 昆山
Email: *1084880575@qq.com, 1987619262@qq.com

收稿日期：2019年7月20日；录用日期：2019年8月2日；发布日期：2019年8月9日

摘　要

随着网络黑客、电脑病毒、计算机犯罪严重地威胁着网络信息的安全，网络信息安全问题给用户带来损

*通讯作者。

文章引用: 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): 1473-1482.
DOI: 10.12677/csa.2019.98165

失的可能性就越大。网络安全保险作为一种新的网络安全风险管理方式得到了学术界和产业界越来越多的关注，成为网络经济时代的一个新亮点。网络安全保险是指投保人因使用互联网络而遭遇网络安全问题，由此造成的损失由保险人负责赔偿的一类保险。由于通常的网络安全防护措施不能完全消除风险，因此网络安全保险是一种转移信息系统安全剩余风险的有效工具。该文对网络安全保险的产生背景进行了介绍，总结自我安全防御投资激励、安全依赖性与风险相关性、信息不对称性和网络安全保险市场重要研究内容，并最后指出网络安全保险的未来发展趋势和挑战。

关键词

网络安全，安全风险，网络安全保险，信息安全投资

1. 引言

网络安全保险(cyber-insurance)是一种新形式的网络安全风险管理方式，把网络用户的风险转移给网络安全保险公司；网络安全保险公司向购买网络安全保险的网络用户收取保险费；网络用户由于发生网络安全事件遭受的损失则由网络安全保险公司负责赔偿。

网络安全保险的研究是从 20 世纪 90 年代 Lai 等人[1]提出在分布式系统中使用数字现金进行风险分担开始。其产生原因是，长久以来，尽管学术界和产业界都研究并开发了许多先进的、用于检测各种网络攻击的网络安全工具和技术，但是实现理想的网络安全保护仍非常困难。具体表现在：1) 网络攻击类型的日益多样化导致设计出完美的网络安全解决方案较为困难。当前，随着技术的不断提高，攻击工具更加专业、易用，因此攻击类型呈现出多样化的趋势，从而导致了设计出完美的网络安全解决方案较为困难。2) 搭便车问题导致网络用户的自我安全防御投资不足。网络用户为提高自身网络安全性购买网络安全产品，在网络安全产品方面做出的投资称为自我安全防御投资。自我安全防御投资行为会产生搭便车问题，即其他用户可以不付成本而坐享他人之利，从而造成网络整体的安全防御投资不足。3) 信息不对称性导致安全防御功能多、价格高的网络安全产品逐步退出市场。在网络安全产品供应商和网络用户之间存在信息不对称性，也就是供应商对网络安全产品质量的了解比网络用户更清晰，从而导致网络用户不了解网络安全产品的真正价值、只愿意付出平均价格购买网络安全产品。进一步导致安全防御功能多、价格高的网络安全产品逐步退出市场。鉴于以上三个问题，研究人员认为由于通常的自我安全防御技术不能完全消除风险，因此网络安全保险是一种转移信息系统安全剩余风险的有效工具[2]。

目前，网络犯罪已令全球经济每年损失接近 4450 亿美元，网络风险已经成为企业的主要威胁之一，且势头强劲[3]。尽管网络安全保险作为一种新形式的网络安全风险管理方式有着良好的前景，但是当前的网络安全保险机构较少，而且市场竞争也不激烈。这是由于网络安全保险的发展过程中充满着许多不确定性因素，因此网络安全保险研究面临着诸多问题。企业或者个人用户在做出网络安全保险投资决策时需要进行全面而且深入的考虑。

本文主要对网络安全保险的研究现状、研究内容进行介绍分析，指出网络安全保险的未来发展趋势和挑战。首先，介绍网络安全保险的国内外研究发展现状；其次，介绍自我安全防御投资激励、安全依赖性与风险相关性、信息不对称性和网络安全保险市场重要研究内容；最后，指出网络安全保险的未来发展趋势和挑战。

2. 网络安全保险研究内容

网络安全保险就是对网络安全的不确定性进行保险。一般的商业保险并不承保网络损失，而网络安全保险则是针对网络经济的特定风险所设计的新险种[4]。用户购买网络安全保险，就等同于他与网络安全保险公司签订了保险契约。购买保险是保证用户网络寿命的最后一着，也是最关键的一步。

目前，网络安全保险研究的关键问题包括：信息不对称性、安全依赖性和风险相关性、自我安全防御投资激励以及网络安全保险市场。信息不对称性是所有保险的固有特征。安全依赖性和风险相关性是网络安全保险不同于其他类型的保险的特征。理想的网络安全保险契约保证网络安全保险公司利润、提高网络安全保险市场运行效率、进一步保证网络安全保险业务的快速增长。因此网络安全保险契约设计需要同时考虑信息非对称性、安全依赖性和风险相关性三个问题。通过网络安全保险内部化信息系统安全的负外部性，能够激励自我安全防御投资，从而改善企业和社会福利。

2.1. 自我安全防御投资激励

网络安全保险的产生最初来源于用户自我安全防御投资引起的网络外部性问题，即网络外部性导致用户自我安全防御投资较少，无法达到社会有效水平。因此，在网络外部性问题存在的情况下，如何激励用户自我安全防御投资达到社会有效水平从而提高网络整体安全性成为挑战性问题。

为了解决这一问题，Lelarge 和 Bolot [5]为用户自我安全防御投资产生的网络外部性建模，说明在自我安全防御机制水平较低的前提下，如果网络中的一部分用户做出自我安全防御投资，就会引发自我安全防御投资的级联效应，即其他用户进行自我安全防御投资，从而整体网络安全性得到提高。在 Lelarge 和 Bolot [6]的另外一项研究工作中，他们提出适用于单个实体的简单模型和适用于多个实体的一般模型，说明了经济理性的实体倾向于选择较不安全的系统的原因和网络外部性对自我安全防御投资的影响，论证了用户自我安全防御投资和网络安全保险投资在维护互联网安全性方面相互作用、相互影响，证明了网络安全保险费与自我安全防御投资数额是负相关关系以及在网络安全保险公司和网络用户之间信息对称情况下，网络安全保险能够激励网络用户自我安全防御投资，从而缓解网络外部性问题。顾等人[7]考虑通过网络安全保险内部化信息系统安全的负外部性，设计存在负外部性前提下的网络安全保险契约。他们的研究结果表明含有一定的保险免赔额的网络安全保险可以激励信息系统自我安全防御投资。

Naghizadeh 等人[8]研究垄断型网络安全保险市场对网络用户自我安全防御投资的影响并分析网络安全保险市场中用户的参与自愿性，把垄断型网络安全保险公司设计成保险监管机构，提出非强制性保险方案激励自我安全防御投资达到社会最优水平。Pal 等人[9]提出非合作博弈下的用户个体最优自我安全防御投资选择与合作下的社会最优自我安全防御投资选择数学框架。他们的研究结果表明，足额保险情形下非合作用户自我安全防御投资低于合作情形下的用户自我安全防御投资水平以及部分保险比足额保险更能够有效激励非合作用户的自我安全防御投资，从而提高用户个体和社会整体福利。Hayel 等人[10]认为通过网络安全保险激励自我安全防御措施的采用能够提高网络用户安全性，从而降低网络用户被黑客成功入侵的概率，并提出包含了网络用户、黑客和网络安全保险公司之间复杂的交互关系的网络安全保险模型。

Laszka 等人[11]指出网络安全保险的特殊性在于软件一元化导致攻击者可以利用软件漏洞进行大规模破坏，从而给保险公司带来巨大负担。作者研究通过保险公司提高软件的安全性，提出适用于垄断型保险公司的供需模型和启发式投资策略。验证了安全防御投资能够降低单一风险并提高网络安全保险利润。Srinidhi 等人研究[12]企业资源有限情况下的投资分配，提出面向企业生产性资产和网络安全资产的最优投资分配模型。研究结果表明，保险能够帮助企业快速积累生产资本，并抵消管理者和投资者的利益不一致造成的负面影响；大的保险保障范围有利于小型企业加速资本积累，并促进大型企业的自我安

全防御投资。

另外，在某些情况下，网络安全保险无法促进自我安全防御投资。顾等人[7]验证了传统的网络安全保险不能促进企业信息系统自我安全防御投资，一定的保险免赔额能够激励企业投资于自我安全防御。Lelarge 等人[5]的研究结果表明道德风险阻碍自我安全防御投资，提出设计具有针对性的保险条款规避道德风险问题，比如对那些采取自我安全防御措施的被保险人进行奖励。

我们把上述研究进行了归纳总结，如表 1 所示。

Table 1. Summary of approaches with self-defense investment model
表 1. 自我安全防御投资文献总结

条件、分析方法和结论	相关文献							
	[7]	[9]	[8]	[10]	[6]	[5]	[12]	[11]
市场类型	-	竞争	垄断	-	-	竞争	垄断	-
保险公司利润	-	-	0	0	-	0	0	非零
保险类型	部分	完全 部分	部分	部分	完全	完全	完全	完全和部分
风险相关/安全依赖	√	√	-	×	√	√	√	√
信息不对称	×	-	×	道德风险	-	-	逆向选择	逆向选择
节点同质	√	√	√	√	√	√	×	√
强制性保险	×	×	×	×	√	×	√	×
数学方法	纳什均衡	纳什均衡	纳什均衡	零和博弈	纳什均衡	纳什均衡	纳什均衡	纳什均衡
激励自我防御投资	√	√ √	√	√	√	√	√	√

2.2. 安全依赖性和风险相关性

安全依赖性与风险相关性密不可分。风险相关性是指蠕虫、僵尸等具有传播特点的计算机病毒一旦感染了网络中的一台主机，就会通过各种途径传播到网络中的其他主机上，从而造成更广泛的危害。风险相关性导致安全依赖性，即网络中某台主机的安全性不仅依赖于自身的安全性水平也依赖于网络中其他主机的安全性水平，乃至网络整体安全性水平。在网络安全保险中，要首先确定用户发生网络安全事件的概率，才能确定网络安全保险费。

在安全依赖性研究方面。Srinidhi [12]指出安全依赖性导致企业信息安全管理策略也具有相互依赖性的特征，从而使得网络安全防御更复杂。作者使用经济学方法研究安全依赖性对自我安全防御投资和网络安全保险投资的影响，提出提高企业信息安全性的策略。Lelarge 等人[5]认为安全依赖性导致网络用户被黑客成功入侵的概率不仅依赖于用户自身的安全性水平还依赖于网络平均安全性水平，建立了用户被黑客成功入侵的概率模型，论证了安全依赖性导致自我安全防御投资产生用户搭便车问题，进一步导致用户个人安全性水平低于社会最优安全性水平。

在风险相关性研究方面。Naghizadeh 等人[8]指出信息安全风险相关性导致企业信息安全投资效率低下，提出使用网络安全保险促进企业信息安全投资实现最优的方法。Gu 等人[7]使用定量化模型研究风险相关性对企业信息系统安全投资的影响，证明了风险相关性较小时，企业自我安全防御投资水平随企业潜在安全损失的上升而增大，提出政府补贴企业自我安全防御投资协调企业风险管理的决策，从而改善企业安全水平并提高社会福利。

综上所述，安全依赖性和风险相关性是网络安全保险不同于其他类型的保险的特征，影响网络安全

保险费的制定。准确地评估安全依赖性和风险相关性对用户发生网络安全事件造成的影响将使得网络安全保险费制定更科学精准，有助于提高网络安全保险保障水平。

2.3. 信息不对称性

信息不对称性是保险的固有特征。发生在当事人签约之前的信息不对称导致逆向选择，发生在当事人签约之后的信息不对称导致道德风险。理想的网络安全保险契约保证网络安全保险公司利润，提高网络安全保险市场运行效率，进一步保证网络安全保险业务的快速增长。网络安全保险契约设计需要考虑信息不对称性问题。

Table 2. Summary of approaches with adverse selection model
表 2. 逆向选择文献总结

条件、分析方法和结论	相关文献				
	[13]	[9]		[14]	[15]
市场类型	竞争	垄断	竞争	竞争	竞争
保险公司利润	0	非负	0	-	非零
保险类型	-	完全	完全	部分	完全和部分
风险相关/安全依赖	√	√	√	√	√
节点同质	×	×	×	×	×
强制性保险	非强制	强制	非强制	非强制	-
数学方法	纳什均衡	纳什均衡	瓦尔拉斯均衡	纳什均衡	纳什均衡
激励自我防御投资	×	√	×	×	-

在逆向选择研究方面，Schwartz 等人[13]证明了逆向选择会降低网络安全保险市场的交易效率，并最终导致网络安全保险市场消失。为了缓解逆向选择对网络安全保险市场造成的负面影响，Hofmann [14]提出设计不同价格的网络安全保险产品的方法。也就是说，网络安全保险公司根据投保人的自我安全防御水平设计不同类型的网络安全保险产品，比如自我安全防御水平高的投保人享受保费折扣价。Pal 等人[15]提出一种基于自我安全防御投资数额和网络外部性的比例的网络安全保险契约设计方法，从而使得不同风险类型的网络用户自愿选择不同类型的网络安全保险契约；证明了纳什均衡下网络用户的自我安全防御投资与其特征向量中心度成正比，并提出了一种基于拓扑位置的网络安全保险合同设计方法。在 Pal 等人[9]的另外一项研究工作中，他们研究逆向选择对竞争型网络安全保险市场和垄断型网络安全保险市场的影响。研究结果表明，混同合同在两种类型的市场中无法激励用户自我安全防御投资，从而保险无法提高网络安全性；分离合同在垄断型保险市场中能够激励用户自我安全防御投资，从而提高网络安全性。

上述研究的归纳总结如表 2 所示。

在道德风险研究方面，Yang 和 Lui [16]论证了道德风险存在时，完全保险和部分保险都无法激励用户的自我安全防御投资。Schwartz 等人[17]针对竞争型网络安全保险市场中的道德风险进行了研究，论证了道德风险导致竞争型网络安全保险市场失灵以及不存在道德风险时，网络安全保险能够提高用户福利但无法提高用户安全性。顾等人[7]说明了免赔额条款能够规避道德风险问题，证明了企业在含有保险免赔额的情况下的自我安全防御投资额大于在保险全覆盖下的自我安全防御投资额。Hayel 等人[10]利用领导者－跟随者博弈模型处理道德风险问题。其中，投保人在签约后选择行动(如采取自我安全防御措施或者不采取自我安全防御措施)，保险人不能直接观测到投保人的行动本身但是能够间接观测到投保人的行动导致的结果。

针对道德风险导致网络安全保险市场运行效率下降问题，我们[18]对网络用户道德风险条件下的最优网络安全保险契约模型进行了研究，利用委托代理理论建立此类保险契约分析模型并对其性质进行了讨论。证明了存在道德风险时，最优网络安全保险契约要求部分保险，最优网络安全保险费小于网络安全事件造成损失的期望值。

上述研究的归纳总结如表 3 所示。

Table 3. Summary of approaches with moral hazard model
表 3. 道德风险文献总结

条件、分析方法和结论	相关文献				
	[10]	[17]	[16]	[7]	[18]
市场类型	垄断	竞争	竞争	竞争	竞争
保险公司利润	-	0	-	-	0
保险类型	部分	部分	部分	部分	部分
风险相关/安全依赖	√	√	√	√	√
节点同质	×	√	×	×	×
强制性保险	强制	非强制	非强制	非强制	非强制
数学方法	纳什均衡	纳什均衡	贝叶斯均衡	贝叶斯网络博弈	纳什均衡
激励自我防御投资	√	×	√	√	√

2.4. 网络安全保险市场

2.4.1. 完全竞争型网络安全保险市场

在完全竞争型网络安全保险市场中，存在着大量的网络安全保险公司。每一家网络安全保险公司都能够提供同质无差异的网络安全保险商品，所有公司都是价格的接受者，而不是价格的制定者。任何一个新加入市场的保险公司都无法向投保人提供比市场中已经存在的保险商品价格更优惠的保险商品。

Table 4. Summary of approaches with perfect competitive network security insurance market model
表 4. 完全竞争型网络安全保险市场文献总结

条件、分析方法和结论	相关文献					
	[20]	[16]		[11]	[19]	[9]
保险类型	完全和部分	完全	部分	完全和部分	完全和部分	完全
风险相关/安全依赖	√	√	√	√	√	√
保险公司利润	零	零	零	零	零	零
信息不对称	×	道德风险	道德风险	道德风险	道德风险	道德风险和逆向选择
节点同质	√	√	√	×	√	×
强制性保险	×	×	×	×	×	×
数学方法	纳什均衡	纳什均衡		纳什均衡	纳什均衡	纳什均衡
市场有效	√	×	√	-	√	√
激励自我防御投资	×	×	√	×	×	×
社会最优	×	-	-	-	√	×

我们把分析完全竞争型网络安全保险市场的文献进行了归纳总结，如表 4 所示。其中，Schwartz 和 Sastry[19]的研究结果表明，投保人满足同质性条件时其个人最优安全水平能够达到社会最优安全水平；然而 Ogut 等人[20]在相同前提条件下却未得到该结论。我们认为这是两项研究中的网络规模不同导致的。另外，在完全竞争型网络安全保险市场中，投保人和网络安全保险公司之间存在信息非对称问题时，网络安全保险无法激励投保人的自我安全防御投资。因此，网络用户在参加保险条件下的自我安全防御投资水平不高于没有参加保险时的自我安全防御投资水平。而且相对于自我安全防御投资，网络用户更愿意选择网络安全保险方式。这是因为网络安全保险保证用户安全性的同时还能够减少其损失。

Yang 等人[18]和 Ogut 等人[20]研究了网络安全保险激励自我安全防御投资的前提条件，并且进行了理论证明和实验验证。其不同点在于，前者假设投保人的自我安全防御投资水平为离散型变量，并使用随机图模型为投保人的互联方式建模；后者假设投保人的自我安全防御投资水平为连续型变量，并使用完全图模型为投保人的互联方式建模。

2.4.2. 非完全竞争型网络安全保险市场

完全竞争型网络安全保险市场分析较为简单，但是现实生活中真实存在的网络安全保险市场通常是非完全竞争型的。由于网络安全保险公司需要满足被保险人的索赔要求、保证运营成本并且避免破产，因此网络安全保险公司需要赚取利润。

Shim [21] [22] [23]针对非完全竞争型网络安全保险市场中，投保人的自我安全防御投资造成的网络外部性进行了研究，并为网络外部性建模，说明了攻击类型与网络外部性之间的关系。研究结果表明，针对非目标性攻击的自我安全防御投资导致正外部性，而针对目标性攻击的自我安全防御投资导致负外部性。在这两种情况中，网络安全保险都无法激励自我安全防御投资。

Lelarge 等人[5]、Pal 等人[9]和 Ogut 等人[20]的研究结果表明非完全竞争型网络安全保险市场中存在信息不对称问题时，保险无法激励自我安全防御投资。从而投保人的个人最优安全水平无法达到社会最优安全水平，并且个人最优福利也无法达到社会福利最大化时的水平。针对该问题，Pal 等人[15]提出强制性网络安全保险方案，并建议政府参与网络安全保险规则的制定。我们认为在非完全竞争型网络安全保险市场中，如何使用保险激励自我安全防御投资使投保人的个人安全水平和福利达到最优水平，并且保证网络安全保险公司的利润是进一步值得深入研究的问题。

综上所述，网络安全保险市场作为网络安全保险产品交易的场所对网络安全保险业务的发展起着决定性作用。正确分析和认识网络安全保险市场状况将有助于针对保险市场的特点采取相应的网络安全保险发展策略，推动网络安全保险市场的全面健康发展。

3. 网络安全保险研究展望

目前，网络安全保险研究取得了一定的进展，作为一个热门的研究领域，未来网络安全保险研究的问题与方向，主要包括：

1) 面向动态 IT 环境的网络安全保险

某些 IT 技术(比如云计算、社交网络、移动计算、物联网等)的环境是动态的。这种动态性不仅会影响网络安全事件发生的概率而且增加了信息系统风险评估的困难性，从而使得网络安全保险变复杂。为了在这种动态 IT 环境中使用网络安全保险保障用户的网络安全，网络安全保险同样需要动态化。动态化的网络安全保险意味着网络安全风险分析和网络安全保险理赔服务流程两方面的动态化。比如，网络安全保险公司把网络安全保险设计成一种供用户购买的在线服务。如果某企业需要长期网络安全保险保障计划，那么该企业投资连续网络安全保险是最佳选择。在这种情况下，能够在线购买的网络安全保险为企业提供了便利。

2) 针对信息不对称性的解决方案

从本文第 2.3 节的分析中可以看出，信息不对称性不仅影响网络安全保险市场的交易效率而且降低网络安全性。为了缓解信息不对称性造成的负面影响，网络安全保险公司一方面可以使用数字权利管理、可信计算、访问控制和自动认证等 IT 技术提高被保险人的信息可信度，另外一方面可以与服务供应商合作，也就是前者提供保险，而后者为前者安装监控系统。

3) 基于用户安全水平的安全度量指标研究

在目前的网络安全保险研究中，计算网络安全事件发生概率的方法都是基于研究人员自定义的安全水平或者网络安全事件发生概率函数，而网络安全事件发生概率函数往往又依赖于研究人员自定义的安全水平。但是，已有文献中都没有准确说明如何计算与安全水平有关的值。比如，网络用户初始财富、遭受的经济损失、自我安全防御投资等。针对这些影响安全水平的安全度量指标还需要更深入的研究。

4) 建立统计数据的信息共享机制

使用网络安全保险提高用户安全性是一个相对新的研究领域，国外目前处于理论研究阶段，国内这方面的研究则更少。同时，由于缺乏大规模公开数据集，现有文献提出的模型和方法大都没有在数据集上得到实验验证。另外，考虑到数据隐私安全问题，企业通常不会对外公开内部数据。针对统计数据缺乏问题，需要设计激励机制促使企业对外共享内部数据，而非通过法律手段强迫企业对外进行数据共享。

5) 网络安全事件损失量化方法研究

准确量化网络用户由于发生网络安全事件而遭受的损失一直是安全风险评估中的难题。其原因一方面在于收集 IT 信息系统数据非常困难，另一方面在于具体说明网络安全事件对用户造成的影响也非常困难。因此，目前仍无损失量化的综合方法。

6) 针对安全依赖性的解决方案

2.2 节中指出，安全依赖性造成自我安全防御投资的外部性问题，从而降低网络用户自我安全防御投资的积极性。Srinidhi 等人[12]说明尽管当前网络安全保险研究面临诸多挑战性问题，但是在一定条件下，网络安全保险能够激励用户自我安全防御投资，从而提高网络整体安全性。目前，使用网络安全保险解决由于安全依赖性而导致的网络用户自我安全防御投资积极性降低问题的方法大都以网络安全保险市场信息对称为前提条件。因此，在缓解安全依赖性造成的负面影响方面，需要研究人员提出更通用的方法。

7) 风险相关性多样化研究

目前，风险相关性方面的研究工作大都集中在网络攻击的传播性特点导致的风险相关性方面，忽略了其他原因导致的风险相关性。比如，集线器和网卡损坏产生的广播风暴同样会造成风险相关性问题。而且 Hao 等[24]的研究工作表明，只有 17%的网络攻击具有风险相关性特点。文献[13]说明了针对不同原因导致的风险相关性应采取不同的解决方法。另外，如上所述，IT 环境多样化不仅会影响网络安全保险也会造成不同类型的风险相关性，但是目前只有少数研究工作在研究风险相关性方面涉及到 IT 环境多样化问题。

8) 基于网络安全取证的网络安全保险研究

服务供应商不仅有责任控制客户上网行为而且应该承担客户恶意行为给其他人造成的损失。但是目前的网络安全保险理赔只涉及到保险人和被保险人，并未考虑到有可能实施恶意行为的被保险人的终端用户。另外，从服务供应商利益出发，服务供应商可以与执法机构合作，积极协助执法机构的网络安全取证工作。

网络安全取证是网络安全保险公司赔偿被保险人损失之前的必要工作。然而，由于个人或者普通用户占有资源有限而且发生网络安全事件后给其他人造成的影响相对较小，因此执法机构对于个人或者普通用户的网络安全取证工作通常不重视。针对这个问题，需要更加简单方便有效的处理网络安全事故和

收集事故线索的方法。

4. 结束语

即使网络用户拥有了所有的网络安全防范措施，但仍不足以保证其网络安全。网络安全保险以其承保投保人因网络的不确定风险，如黑客攻击、计算机系统遭受入侵等而造成的重要资料丢失、服务中断和营业收入损失的方式减少了用户不必要的损失，为网络安全问题提供了新的解决方案。因此，购买网络安全保险成为保证用户网络寿命的最后一步，也是最关键的一步。

本文首先对网络安全保险的国内外研究发展现状和核心概念进行了综述，然后针对现有研究成果，介绍自我安全防御投资激励、安全依赖性与风险相关性、信息不对称性和网络安全保险市场重要研究内容，最后分析网络安全保险在动态的 IT 环境、风险相关性多样化、网络安全取证等方面面临的挑战，从而提出未来的研究方向。我们相信，随着相关研究的不断深入和技术的不断成熟，网络安全保险将会得到快速发展，更好地为用户提供风险保障。

致谢

感谢杨云雪、杨琴两位老师的指导。

基金项目

本文受江苏省高等学校大学生创新创业训练计划项目(201912078003Y)资助。

参考文献

[1] Vakilinia, I. and Sengupta, S. (2019) A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, **14**, 1526-1538. https://doi.org/10.1109/TIFS.2018.2881694

[2] Kshetri, N. (2018) The Economics of Cyber-Insurance. *IT Professional*, **20**, 9-14. https://doi.org/10.1109/MITP.2018.2874210

[3] Eling, M. and Wirfs, J. (2019) What Are the Actual Costs of Cyber Risk Events? *European Journal of Operational Research*, **272**, 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021

[4] Iqbal, F., Fung, B.C.M., Debbabi, M., *et al*. (2019) Wordnet-Based Criminal Networks Mining for Cybercrime Investigation. *IEEE Access*, **7**, 22740-22755. https://doi.org/10.1109/ACCESS.2019.2891694

[5] Lelarge, M. and Bolot, J. (2008) Network Externalities and the Deployment of Security Features and Protocols in the Internet. In: *Proceedings of the* 2008 *ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, ACM, New York, 37-48. https://doi.org/10.1145/1375457.1375463

[6] Bolot, J. and Lelarge, M. (2009) Cyber Insurance as an Incentive for Internet Security. In: *Managing Information Risk and the Economics of Security*, Springer, Berlin, 269-290. https://doi.org/10.1007/978-0-387-09762-6_13

[7] 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.

[8] Naghizadeh, P. and Liu, M. (2014) Voluntary Participation in Cyber-Insurance Markets. *Proceedings of the Workshop on the Economics of Information Security*, Pennsylvania, June 2014, 1-11.

[9] Pal, R. and Golubchik, L. (2010) Analyzing Self-Defense Investments in the Internet under Cyber-Insurance Coverage. *IEEE* 30*th International Conference on Distributed Computing Systems*, Genova, 21-25 June 2010, 339-347. https://doi.org/10.1109/ICDCS.2010.79

[10] Hayel, Y. and Zhu, Q. (2015) Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks. In: *Decision and Game Theory for Security*, Springer International Publishing, Berlin, Vol. 9406, 22-34. https://doi.org/10.1007/978-3-319-25594-1_2

[11] Laszka, A. and Grossklags, J. (2015) Should Cyber-Insurance Providers Invest in Software Security? In: *Computer Security—ESORICS* 2015, Lecture Notes in Computer Science, Springer, Cham, Vol. 9326, 483-502. https://doi.org/10.1007/978-3-319-24174-6_25

[12] Srinidhi, B., Jia, Y. and Tayi, G.K. (2015) Allocation of Resources to Cyber-Security: The Effect of Misalignment of

Interest between Managers and Investors. *Decision Support Systems*, **75**, 49-62. https://doi.org/10.1016/j.dss.2015.04.011

[13] Schwartz, G., Shetty, N. and Walrand, J. (2013) Why Cyber-Insurance Contracts Fail to Reflect Cyber-Risks. 51*st Annual Allerton Conference on Communication, Control, and Computing*, Monticello, 2-4 October 2013, 781-787. https://doi.org/10.1109/Allerton.2013.6736604

[14] Hofmann, A., Von Haefen, O. and Nell, M. (2018) Optimal Insurance Policy Indemnity Schedules with Policyholders' Limited Liability and Background Risk. Social Science Electronic Publishing, Rochester. https://doi.org/10.1111/jori.12247

[15] Pal, R. and Pan, H. (2013) On Differentiating Cyber-Insurance Contracts a Topological Perspective. *IEEE International Symposium on Integrated Network Management*, Ghent, 27-31 May 2013, 836-839.

[16] Yang, Z. and Lui, J.C.S. (2014) Security Adoption and Influence of Cyber-Insurance Markets in Heterogeneous Networks. *Performance Evaluation*, **74**, 1-17. https://doi.org/10.1016/j.peva.2013.10.003

[17] Shetty, N., Schwartz, G., Felegyhazi, M., *et al*. (2010) Competitive Cyber-Insurance and Internet Security. 8*th Workshop on the Economics of Information Security*, Cambridge, 7-8 June 2010, 229-247. https://doi.org/10.1007/978-1-4419-6967-5_12

[18] Yang, Y.X. and Wang, Y.X. (2016) The Optimal Cyber-Insurance Contracts under Moral-Hazard. *Chinese High Technology Letters*, No. 8-9, 732-738. (In Chinese)

[19] Schwartz, G.A. and Sastry, S.S. (2014) Cyber-Insurance Framework for Large Scale Interdependent Networks. *International Conference on High Confidence Networked Systems*, Berlin, 15-17 April 2014, 145-154. https://doi.org/10.1145/2566468.2566481

[20] Ogut, H., Menon, N. and Raghunathan, S. (2005) Cyber Insurance and IT Security Investment: Impact of Interdependence Risk. 4*th Workshop on the Economics of Information Security*, Cambridge, 1-3 June 2005, 1-30.

[21] Shim, W. (2012) An Analysis of Information Security Management Strategies in the Presence of Interdependent Security Risk. *Asia Pacific Journal of Information Systems*, **22**, 79-101.

[22] Qian, X., Liu, X., Pei, J., *et al*. (2017) A Game-Theoretic Analysis of Information Security Investment for Multiple Firms in a Network. *Journal of the Operational Research Society*, **68**, 1290-1305. https://doi.org/10.1057/s41274-016-0134-y

[23] Marotta, A., Martinelli, F., Nanni, S., *et al.* (2017) Cyber-Insurance Survey. *Computer Science Review*, **24**, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

[24] Hao, Y., Armbruster, D. and Hütt, M.T. (2015) Node Survival in Networks under Correlated Attacks. *PLoS ONE*, **10**, e0125467. https://doi.org/10.1371/journal.pone.0125467