中国网络安全保险的春天即将来临了吗

by Frank Wang, Gen Re, Shanghai

前言

随着网络安全法的施行及国内外一系列网络安全事件的发生，网络安全保险成为当前中国保险市场的一个非常热门的话题，一些保险人也正在开发有关的保险产品，似乎网络安全保险的春天在中国即将来临。然而，虽然其市场潜力巨大，但是网络安全保险在中国的发展还面临着很多的挑战。本文将从法律、核保、和风险管理三个角度做出初步分析，并提出几点对策供大家参考。

一、 网络安全法对保险业的影响

中国网络安全领域的基础性法律《中华人民共和国网络安全法》自2017年6月1日起施行，这部新法对我国网络安全方面存在的热点难点问题都有明确规定，内容上有六大亮点：

第一，明确了 *网络空间主权*的原则；

第二，明确了 *网络产品和服务提供者的安全义务*；

第三，明确了 *网络运营者的安全义务*；

第四，进一步完善了 *个人信息保护规则*；

第五，建立了 *关键信息基础设施安全保护制度*；

第六，确立了 *关键信息基础设施（CII）重要数据跨境传输的规则*。

其中针对个人信息泄露问题，网络安全法规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。并规定了相应法律责任。

笔者认为网络安全法第42条是与网络安全保险有关的最重要条款，其规定：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失；*在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。*这一条规定明确了网络运营者（包

提纲

关于《通用再保险中国责任险核保预警》

本预警旨在关注中国责任险市场的热点案例与新兴问题，提醒责任险核保、核赔、市场管理人士等有关方面关注与其相关的责任风险，并为我们的客户提供有一定价值的风险管理建议供参考。

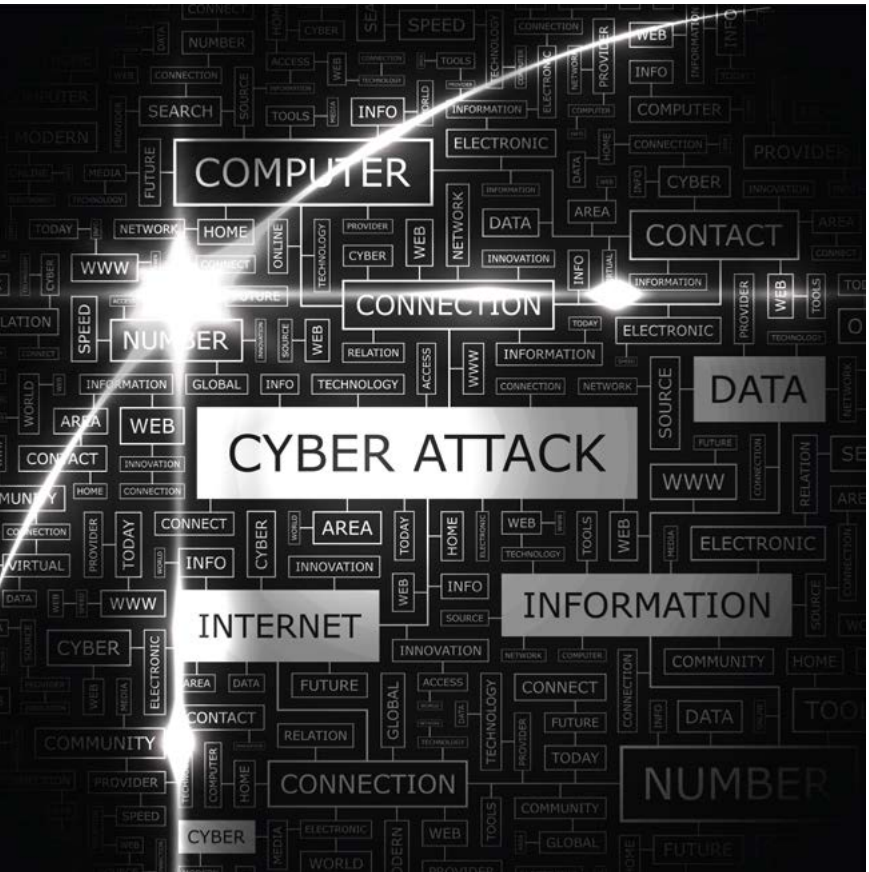
括网络的所有者、管理者和网络服务提供者）在发生个人信息泄露时的法定通知义务和补救义务，这为基于数据泄露保障的网络安全保险在中国的发展奠定了坚实的法律基础。实际上，美国的网络安全保险市场之所以能在全球独占鳌头，据达信(Marsh)保险经纪公司网络安全产品负责人Bob Parisi介绍，“最大的原因就在于过去10年《违反安全通知法案》在美国各州的推行。”

此外，网络安全法还规定：违反网络安全法的行为，直接责任人员和单位除了要承担有关的行政与刑事责任之外，还要依法承担民事责任，这也将激发网络运营者转嫁责任风险的保险需求。

二、 网络安全保险的市场现状与前景

安联保险最近发布的一项网络安全研究报告[1]显示，每年中国因网络攻击损失为600亿美元，损失额位列亚洲第一、全球第二，仅次于美国。

今年5月12日以来，一种名为“想哭(WannaCry)”的勒索病毒在全球大范围入侵人们的电脑，恶意加密电脑信息并勒索解密赎金。据报道，全球有150多个国家沦陷：英国的几十家医院被迫暂停急救等服务，俄罗斯内政部千台电脑遭攻击，德国铁路系统、美国联邦快递公司等纷纷“中毒”，中国也有近3万家机构的计算机遭受影响。据报道，“想哭”勒索病毒在全球范围内已造成近80亿美元的直接经济损失，然而受到影响的很多公司并未购买网络安全保险，需要自担高昂的经济损失。



近年来国内外发生了多起数据和安全事故案件，人们对网络风险的担忧日益增加。同时，是否有网络安全保险来转嫁此类风险、降低损失，日益成为企业和个人关心的问题。从上世纪90年代诞生相关概念开始，网络安全保险至今也已经过了二十余年的发展。2016年第三季度，普华永道发布了一份题为《保险2020与超越：从网络弹性中获取红利》的报告，其预测到2018年，全球网络安全保险市场将增至50亿美元，到2020年将增至75亿美元。

从全球网络安全保险市场分布来看，北美，特别是美国，是网络保险的最大市场，占到全球网络安全保险市场的90%。欧洲的网络安全保险市场可以说正处于快速发展前的酝酿阶段，虽然落后于美国数年，但随着近几年网络安全事故频现以及强制要求公司发布违反安全通知的《一般数据保护条例(GDPR)》的颁布，促进欧洲网络安全保险快速发展的因素逐渐成熟。亚洲方面，和其他很多经济领域一样，网络安全保险市场的起点是最低的，但是需求日益增大，类似保险产品正在从欧美市场逐渐扩散到以中国为代表的新兴市场。在中国，随着今年6月1日《网络安全法》的实施以及一系列网络安全事件的发生，众多中国企业对于网络安全风险及保险的认识也正在逐渐增强，网络安全保险的市场潜力巨大。

目前，在中国提供全面的网络安全保险的机构主要是一些外资保险公司，其主要保障范围分成三块：

- 第一块保障主要集中于减少企业因黑客攻击导致正常营业中断而产生的经济损失，可以赔偿企业在系统安全失效期间，扣除正常营运开支而损失的部分经济损失。
- 第二块保障则是在鉴定服务以及数据恢复上。可以承保那些因聘请鉴定服务顾问证实是否已发生数据安全事故并判断原因，提供避免或降低数据安全事故的建议所产生的费用。
- 第三块保障则主要是帮助企业承担法律成本，承保依法向资料所有人披露个人信息泄密或数据安全事故所产生的费用及支出。同时还包括修复企业受损名誉，承保向独立的专业公关顾问寻求建议以减轻其名誉受损所发生的费用。

从上述网络安全保险的主要保障范围可以看出，其既保障第一方经济损失又保障对第三方的法律赔偿责任，因此笔者认为*网络安全保险不属于传统的财产保险或责任保险，而是在互联网+和保险科技时代涌现出的一种独立的新型险种*，需要我们用全新的互联网思维去研究和推广它。

三、 发展网络安全保险的挑战与对策

美国保险代理和经纪理事会(CIAB)2017年4月数据显示，在网络安全保险市场相对成熟的美国，大约有32%的商业机构投保了网络安全保险，平均购买的保额大约600万美元，这一数字在2016年10月还仅为300万美元，极少数客户现在购买的网络安全保险总保额甚至已达6亿美元。虽然网络安全保险在欧美等国家已被广泛应用并具有巨大增长空间，但在国内目前尚处于早期市场开拓与培育阶段。

从保险公司的角度看，在中国发展网络安全保险主要有三大挑战：一是缺乏完善的法律法规配套制度；二是缺乏有效历史损失数据，产品定价和核保困难；三是缺乏网络安全风险管理技术与资源。具体问题与对策如下：

首先，虽然中国网络安全的基础性法律《网络安全法》自6月1日起已经施行，个人信息保护基本规则已经建立，但相关的配套实施细则和相关法规还需要完善。针对我国个人信息被滥用的严重事实，在个人信息的法律保护方面，我国保护个人信息的法律条款数量较为有限、适用范围相对狭窄，没有专门 的针对所有信息控制人均适用的统一的个人信息保护法；同时，就个人信息的法律保护手段而言，重“刑事处罚”和“行政管理”，轻“民事确权”与“民事归责”，导致个人信息遭受侵害后，即使侵权行为人最终遭致刑事处罚或行政处罚，但信息主体的财产及非财产损失却得不到任何实质性的民事赔偿。针对这些问题，国家正在推动《个人信息保护法》的立法过程。同时，国家网信办自2016年就陆续发布一系列与网络安全法相关的实施细则，包括《关键信息基础实施确定指南（试行）》、《个人信息安全规范（征求意见稿）》、《个人信息和重要数据出境安全评估办法（征求意见稿）》、《国家网络安全事件应急预案》、《关键信息基础设施安全保护条例（征求意见稿）》等。从网络安全保险发展的法律基础角度出发，未来的相关法律法规要提高司法层面上的可操作性，不仅要规定对个人信息的保密义务，更要明确违背该义务的法律后果，特别是民事损害赔偿的标准。

其次，在发展网络安全保险的过程中有一个世界性难题，即如何核保与定价，因为独立的网络安全保险是一个全新的险种，其发展历史很短，没有什么完善的市场经验可以借鉴，而且网络安全风险日新月异，这些都对保险人的承保工作提出了很高的挑战。网络安全保险在中国的发展历史更短，不过几年时间，甚至没有什么可参考的保险损失经验，而且保险人获取有效定价基础信息的渠道非常有限，因为中国网络安全事件被公开报道的比实际发生的要少很多，可利用的公开历史损失数据可能难以代表中国实际的网络安全风险水平。对此，笔者认为保险人需要采取“摸着石头过河”的谨慎承保策略，一边开展业务，一边积累经验教训，及时做出调整与修正，因为任何新保险产品的开发与发展都需要经历这一过程，网络安全保险在发展最快的美国市场也是经历了这一过程。在开展网络安全保险业务过程中，笔者认为保险人应首先选取一两个目标行业，从调研客户的风险管理需求出发设计产品，先行试点，同时保障范围不宜大而全，而应该从解决目标行业网络安全风险的痛点出发，开发出有针对性的保险产品。同时，保险人应注意控制风险累计，保单赔偿限额应从小到大，随着承保经验的积累逐步提高。

最后，网络安全风险管理是一个非常复杂的技术问题，需要有专业的网络安全专家全程参与，这一点对于保险人尤其重要，因为发展网络安全保险所需要的承保前风险评估、承保后风险控制以及损失发生后的定责与损失理算都需要与网络安全专家合作。在美国，每一家开展网络安全保险业务的保险公司和经纪人都有至少一家网络安全顾问公司作为其合作伙伴，近年来也因为网络安全保险在美国的迅速发展而产生了一批为保险人服务的网络安全科技初创公司，最典型一个例子的就是赛恩斯(Cyence)公司。这家公司由两位技术专家于2014年联合创立，是一家致力于量化网络风险的创业公司，他们为保险公司打造了一款数据分析平台，帮助保险公司对网络风险这一新兴险种进行建模和定价。其分析平台和解决方案可以让保险公司更高效地选择、勘测和管理网络风险，并且引入动态风险定价，帮助保险公司能够灵活应对快速变化的网络风险。赛恩斯公司在2016年9月获得了4000万美元的A轮投资。[2]虽然中国目前已有不少从事互联网安全相关工作的公司，但是还缺少像赛恩斯这样能够为保险人提供建模和定价支持的公司。据了解，随着中国网络安全保险需求的逐步提升，有些原来从事与保险业务无关的网络安全公司也正在思考和推动如何与保险公司合作，共同开发包括风险评估、监测预警、应急处理以及保险补偿在内的网络安全风险全方位解决方案，希望在不远的未来中国也能涌现出更多的像凯恩斯这样的专业服务提供商，与保险人一起共同推动网络安全保险在中国的健康发展。

尾注

1 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/

2 张翀，《量化网络风险，Cyence能带领保险公司击败黑客吗?》，“互联网保观”微信公众号，2017-8-23。

作者介绍

王民 **(Frank Wang)** 先生是一名律师，目前为通用再保险上海分公司资深合约承保人，主要负责亚太区责任险及意外险合约的承保、管理、市场开发以及责任险相关问题的咨询研究工作。他曾供职于多家国际保险集团，具有十多年责任险承保、理赔及业务管理经验。

王民拥有中国法律职业资格、北美特许财产责任险核保师(CPCU)、北美注册职业责任险核保师(RPLU)、美国保险学院再保险管理师 (ARe) 及澳大利亚新西兰保险金融学会会员(ANZIIF)等国内外专业资格。他同时为CPCU协会的国际大使和认证讲师。

王民作为演讲嘉宾经常出席国内外保险业和相关行业的研讨和培训会议。

他的联系方式如下：

电话：+86 21 6100 6318
邮件：frank.wang@genre.com

关注更多《通用再保险中国责任险核保预警》文章，请点击：
genre.com/casualtymatterschina

或者直接扫描下面的二维码：

Read our Casualty articles and blogs in English at
genre.com/casualty

通用再保险公司上海分公司
中国上海浦东陆家嘴东路161号
招商局大厦1803室
Tel. +86 21 6100 6300
Fax +86 21 6100 6388

Photos: © Thinkstock: istock, Kirill_Savenko, zjzpp163, StudioM1

The difference is...the quality of the promise®

genre.com | genre.com/perspective | LinkedIn: linkedin.com/company/gen-re