网络风险会成为下一个大空头吗?

传统的网络风险管理和承保指出保险公司和全球经济存在软肋，亟需一种新的风险管理框架来解决这些弱点。

Chris Harner, FRM
Chris Beck

在电影《大空头》（The Big Short）的一个关键场景中，当 Michael Burry 告诉投资银行家们他想购买抵押贷款债券信用违约互换（CDS）时，他们几乎忍不住笑了起来。一位投资银行家质疑这一提议，他告诉 Burry 只有在数百万美国人无法偿还抵押贷款时，CDS 才会产生赔付，而这种情况从未发生过。作为整部影片的核心场景，这一幕生动诠释了金融市场的关键参与者们如何缺乏大局观，从而最终导致了 2008 年的次贷危机和全球金融危机的爆发。“虽然这听上去很奇怪，但这是事实。”《大空头》的作者 Michael Lewis 写道，“你离市场越近，就越难以察觉它的荒唐。”从承保人、银行家、做市商到评级机构，许多市场参与者[1]对真正的风险缺乏一个足够系统性的认识。

次贷危机发展的过程与网络风险保险市场的快速增长之间存在着惊人的相似性。网络风险会把保险公司带入同样的境地吗？传统的网络风险承保和管理指证保险公司和全球经济存在软肋，亟需一种新的风险管理框架来解决这些弱点。

动荡的种子

次贷危机的核心源于人们对“没有发生过的事情就不可能发生”的信念，即房价不可能突然全面下跌。出于这种“群体思维”和“确认偏见”，市场参与者们不断放松对抵押贷款的核保标准，使得房贷沿着信贷曲线逐渐下行进入深度次贷市场。借款人和贷款人都错误地认为即使借款人陷入还款困境，贷款人也可以利用房屋进行再融资。核保人、风控经理和交易员依赖的是标准回溯模型。这些模型没有预见到低利率环境推升房价和次级贷款之间的相互关联，而这些次级贷款随后流入抵押支持债券（MBS）、担保债务凭证（CDO）和双层担保债务凭证（CDO squared），并通过 CDS 进行对冲。次贷风险的生成、累积和对冲在全球银行体系中产生了更大的交易对手风险和流动性风险、以及更高的杠杆。

市场上通用的标准风险框架无法识别导致市场出现拐点的触发因素。低利率在市场上引入了羊群效应，导致了次贷的迅速扩张。房价上涨与不断放松的核保标准和次级贷款之间的反馈循环在泡沫扩大的过程中发挥了重要作用。当利率开始上升、可变利率抵押贷款开始重置时，市场突然意识到借款人既无力支付还款也无法为自己的房屋进行再融资，购房热潮转变为突然的恐慌。

与本世纪初对抵押贷款产品的需求一样，如今能够有效转移网络风险的保险产品也需求旺盛。知名公司数据泄露事件的日益增多刺激了网络保险产品的旺盛需求、较低的赔付率、以及保险公司担心错失增长良机等等因素。这些都导致该产品保费从 2007 年的 3.5 亿美元增至 2017 年的 35 亿美元，增长了 10 倍。据摩根士丹利估计，到 2020 年全球网络风险保险市场将再增长近两倍达到 80 亿至 100 亿美元。[2]

[1] 作为一个反例，有咨询公司在次贷危机爆发之前就预见到了其中隐含的风险。参见明德 2016 年 11 月发布的文章：“What happens when credit risks come home to roost?” by Mike Schmitz and Kyle Mrotek, Retrieved on February 28, 2019, from http://www.milliman.com/insight/Articles/What-happens-when-credit-risks-come-home-to-roost/

[2] Ralph, Oliver, “Cyber attacks: The risk of pricing digital cover.” The Financial Times, March 18, 2018.

与本世纪初为弥补固定收益回报率较低而进行的“追逐收益”类似，财产险行业的疲软市场环境也凸显了网络保险的吸引力。起初对承保网络风险持谨慎态度的保险公司已越来越多地进入这个市场。在美国 2007 年仅有 18 家保险公司承保网络风险，而目前大约有 170 家，其中五家保险公司承保了大约一半的保费。

尽管这个市场竞争激烈，但网络风险与传统产品线存在本质不同。网络责任是一种全新的风险敞口，缺乏其他产品线数十年的损失经验和相关数据。没有法庭诉讼记录并且相关法律持续变化， 网络风险保单的条款隐含的责任可能并不是保险公司的设计初衷。令人尤其不安的是，在董事责任险（D&O）、错误及遗漏责任险（E&O）、营业中断险、欺诈、犯罪、财产、执业责任、航空险、海运险和其他传统业务领域，都存在非肯定性或“隐含网络风险” 。在某种程度上，网络责任的保障可以与任何产品线相关联。

目前网络风险保险的损失率在 35%左右，强烈的财务激励促使保险主体参与这个市场。但是当前的利润并不能直接反映保险公司实际承担的风险，尤其是保险公司的定价可能只是在个体损失层面，而没有考虑巨灾事件的发生。与次贷危机的反馈循环一样，对于核保人和再保险公司来说网络风险往往缺乏可视性和透明度。许多再保险公司无法通过合约看清楚底层保单，就像 CDO 和 CDO squared 的持有者无法“解读”其现金流瀑布下藏了什么样的底层抵押贷款。迄今为止似乎多数核保人都将网络责任视为风险而不是灾因。目前网络责任的大额赔款主要局限于孤立情况或个别公司，因此判断定价是否准确还为时过早。就像人们常说的那样，网络事故只是什么时候发生的问题，而不是是否会发生的问题。如果从损失分布的角度来看，那么迄今为止的赔案都还在损失曲线的“预期损失”的区间内，还没达到“预期外损失”或“尾部损失”的区间。我们的初步研究也证实大多数公司有能力应对网络事件的发生，且通常会高估最初的损失，至少目前看来是这样。当然这一切都可能会突然全部改变。

风险的关联性：为重大事件带妆彩排

2017 年 7 月初，乌克兰警方突袭了基辅当地一家家族电脑公司的办公室，该公司开发的会计软件在全国范围内被广泛使用。然而警方的行动还是为时已晚，难以弥补该公司在不知不觉中对为数众多的私人和公共机构造成的损害。

一周前，如今声名狼藉的恶意软件“NotPetya”在短短几个小时内渗透到该公司的电脑网络，并打垮了基辅的四家医院、六家电力公司、两个机场、超过 22 家银行、自动取款机、零售和运输方面的信用卡支付系统，以及乌克兰几乎所有联邦机构。据《连线》（Wired）杂志报道，一名乌克兰政府官员估计该国 10%的电脑在这次黑客攻击中受害。[3]

但损失并不仅限于乌克兰境内，世界各地大大小小的公司，包括航运巨头马士基（A.P.Moller Maersk），都成了该恶意软件的受害者。马士基的遭遇诠释了网络攻击如何对那些远在目标公司办公室之外的对象造成严重破坏—— 马士基在敖德萨办公室的一名管理员从这家乌克兰软件公司下载了该会计软件，无意中携带了俄罗斯军方黑客开发的代码，允许他们远程操控装有未打补丁的 Windows 系统的电脑。在被恶意软件感染之后，病毒快速移动，甚至能够使用来自未加补丁的电脑的密码信息来感染已经打过补丁的电脑。[4]

在计算机网络瘫痪后，马士基的港口子公司 APM Terminal 无法处理或运输集装箱，货物开始堆积。位于新泽西州伊丽莎白的港口码头平时每天处理多达 3000 辆卡车。由于卡车无法将货物运进或运出，港口管理局不得不关闭码头[5]。航运客户特别是那些分销易腐货物或即时零部件的客户，不得不高额寻找其他运输方式，新的预订单则被暂停。这就是网络攻击后数天内的情景。

[3] Greenberg, Andy. “The Untold Story of NotPetya, The Most Devastating Cyberattack in History.” Wired, August 22, 2018. p. 11.

[4] Ibid., p. 12, p. 7.

[5] Ibid., p. 12.

NotPetya 证明了网络风险的互联性：马士基损失高达 3 亿美元，马士基董事长在去年的达沃斯世界经济论坛上指出，恶意软件迫使该公司在 10 天内重新安装了 “一个完整的基础设施”，包括 4000 台新服务器、4.5 万台新电脑和 2500 个应用程序[8]。此外，默克损失 6.7 亿美元（包括 2017 年销售和制造亏损以及修复费用）；联邦快递的欧洲子公司 TNT 为此付出了 4 亿美元的修复和相关费用[6]。美国政府估计这次袭击的总损失在 100 亿美元左右[7]。

科技发展和全球化以仅限于想象的方式将公司和其他组织联系在一起，就像十年前网络保险首次出现时一样。事实是，物联网、人工智能和云技术等新技术如今被应用于各个领域，并指向一个日益依赖网络的世界。

近年来，企业对网络风险的管理已经从丢失笔记本电脑的风险转向了利润驱动的黑客和国家行为体，这些主体拥有足以让对手网络瘫痪的资源和技术。在全球范围内，各国政府目前正投入民用和军事资源用于增强网络进攻和防御的能力。保险公司和再保险公司竞相承保网络风险、电子设备日益网络化、国家行为体的角色以及全球化都创造了一个高度互联的网络环境，所有这些都为一场系统性事件创造了条件（图 1）。

图 1：网络风险的互联性

NotPetya 事件清楚地表明了如今公司在保持系统和安全补丁更新方面遇到了麻烦。网络安全需要企业投入巨资，但许多企业无法或不愿承担必要的资金投入，或者不清楚如何恰当地量化这种风险。即使进行了适当的投资，公司通常也难以知道它们的投入将在哪里产生最大的影响。应该将资金用于打补丁、升级加密和检测功能，还是加强监控? 面对无数的威胁场景，为了量化和合理分配资金，公司需要重新评估网络风险的演变过程。

[6] Nash, Kim S., Sara Castellanos, Adam Janofsky. “One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs.” The Wall Street Journal, June 27, 2018. Retrieved on February 28, 2019 from https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

[7] Ibid., p. 10, 11.

[8] Chirgwin, Richard. “IT ‘heroes’ saved Maersk from NotPetya with ten-day reinstallation blitz.” The Register, January 25, 2018. Retrieved on February 28, 2019 from https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

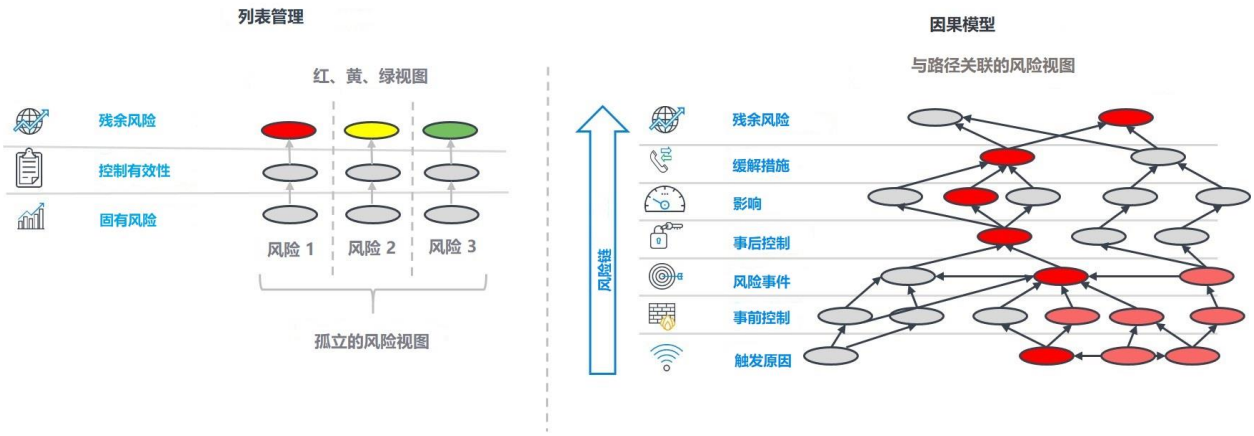
对新型风险框架的需求

随着市场的成熟，保险公司似乎仍在为如何最好地评估网络风险犯愁，尤其是隐含的网络风险。保险公司仍被困在旧的风险框架，又称“列表管理”方法中。在“列表管理”方法中，公司将风险和控制手段进行分类，通过某种方式进行评分，并估计其发生率和相应影响，最后的结果往往以热图的形式呈现，如图 2。这种评估方法遵循了其他操作风险的可预测模式，包括：1）进行定性的清单检查或公式化评估，输出红色/黄色/绿色结果（RAG）；2）运用传统情景分析；或者 3）利用经典的损失频率/案均金额法或巨灾预测模型进行一些简单的量化分析。

由于历史经验匮乏和迅速变化的威胁，这些方法并不适合量化网络风险，也不足以聚合隐含网络风险。因为它们无法认识到多重风险之间的非线性关系，而是相互关联甚至累乘的；这也忽略了一种风险可能放大另一种风险的影响，从而掩盖潜在的临界点。在“列表管理”框架中，由于每个风险都意味着增量资本需求，每次将一种风险添加到列表中，总体资本都可能进一步吃紧，这也忽略了风险可能带来的益处。许多公司在试图聚合风险、评估尾部风险以便准确地衡量资本需求的过程中都面临着这样的挑战。

由于网络风险的复杂性、新颖性、高速发展的特点，“列表管理”模型在处理网络风险时尤其困难，因此我们需要一种新的框架来量化和聚合这种风险，即因果模型方法，见图 2。首先创建一个能代表网络风险的复杂程度和互联属性的认知地图，以有效体现保险公司的风险生态系统。就像绘制出一个物种的捕食者和猎物、水和食物来源、迁移模式和其他影响因素的环境生态系统一样。这张网络认知地图可以体现不同的风险维度：利益相关者对网络风险的不同看法、有可能引发一场危机的多种相关因素、风险控制的响应程度、风险在企业中流动时带来的潜在影响等等。利用来自社会科学和复杂性科学的成熟技术，我们可以将这些信息组织成一个“最低复杂程度”系统，使其更真实、更易理解地反映保险公司所面临的风险，并能更好地帮助企业量化和证明网络风险支出的合理性。

图 2:“列表管理”模型与因果模型



这种方法让管理者远离“列表管理”的陷阱，即简单地将风险组织成为行和列的形式。采用强调因果关系的最低复杂视图，管理人员可以看到风险是如何在企业中显现和流动；可以针对一些难以量化的诱因建立模型，如投资人或被保险人对危机的反应；可以映射多个触发原因之间的关联性以显示网络风险事件如何影响保险公司，预警保险公司关注临界点等等。以 NotPetya 事件为例，因果关系模型可以帮助马士基了解哪些关键因素的组合将导致其无法在全球各地的港口装卸船只。风险管理框架将从风险监控转向事前洞察。

通过因果模型，风险管理者得以避免离散情景分析中固有的常态偏见，并对可能发生的事情做出合理而流畅的描述。他们可以避免将注意力限制在“出险频率/案均金额”方法得到的固定损失概率，而是更多去关注什么时间哪些因素以什么方式触发了风险。

在《大空头》的结尾，当 Michael Burry 对次贷市场的看法被确证之后，他认为水将是下一个陷入困境的市场。虽然水市场与住房市场有相似之处，但网络可能是更大的风险：即便是获得洁净水的渠道，也可能受到网络攻击的影响。不仅如此，金融基础设施的每一个层面、人们的沟通渠道、以及能源的获取都与网络相连，并暴露在网络风险之下。网络攻击有能力破坏我们的基础设施，因此了解和管理这种风险至关重要。通过采取一个整体性的视角，我们可能避免目前无法想象的系统性事件的发生。

作者联系方式

Chris Harner
chris.harner@milliman.com

Chris Beck
chris.beck@milliman.com

明德中国联系方式

蒋冠军，合伙人
+86 216 159 0252
guanjun.jiang@milliman.com