MARSH | Asia Pacific Risk Center

管理您的网络风险态势：从风险转移到业务持续性管理

MARSH & McLENNAN COMPANIES

作者：

Jaclyn Yeo
亚太风险中心
高级研究分析师

合作人：

Richard Green
达信亚洲常务董事
兼金融风险产品负责人

Lim Sek Seong
达信风险咨询副总裁

了解亚洲的网络保险机会

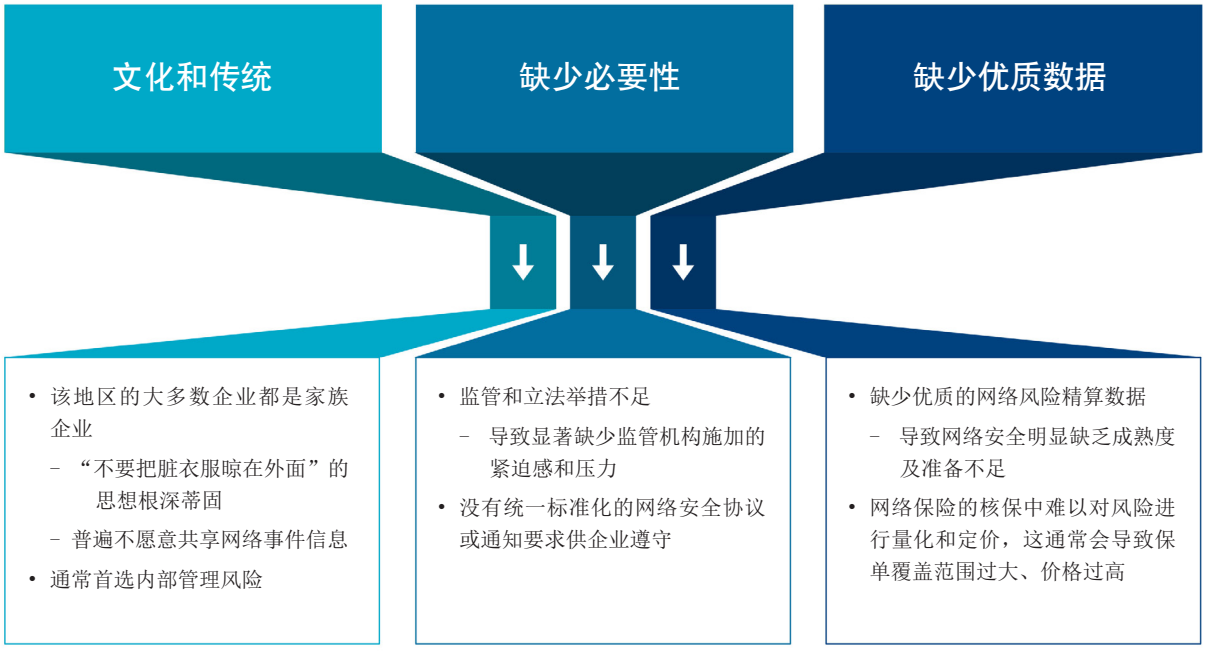
亚洲被黑客攻击的可能性比世界其他地区高80%[1]。不过，与亚太地区较高网络威胁水平不协调的是其薄弱的网络风险防范工作，例如风险意识差、网络安全投资不足、网络保险投保不足等。低网络保险投保率能够突出地反映这个问题，新加坡（<10%）和澳大利亚（14%）的投保率都显著低于欧洲（30–36%）和美国（55%）[2]。

亚洲的低网络保险投保率可归因于风险意识的普遍缺乏，而后者是由以下因素导致的，文化因素可能影响该地区的网络保险销售，当前立法格局导致的数据不足也有影响（图1）。

该地区关于网络攻击规模及频率的信息披露有限，使人们对网络安全产生错觉，而这可能会为企业带来重大经济损失。企业不应盲目自信，必须采取措施来预防和减少网络攻击，包括投入适当的资源和制定战略性应急计划来确保在发生攻击时能做出有效响应。

首先，我们重新梳理企业在网络风险保险方面的常见误解[3]，并提供关于网络风险转移的替代视角。其次，我们建议首先实施包括有效终端安全和IT基础设施在内的网络防御最佳做法，然后使用网络保险控制事件发生时的补救成本。再次，为了切实保证企业的网络弹性，强烈建议企业进一步考虑实施危机管理、业务持续性和ICT[4] (Information and Communications Technology) 灾难恢复计划。这样可以确保恢复关键业务活动，包括关键ICT应用系统和数据库。这样可以最大程度地减少运营和业务中断。

图1 亚太地区低网络保险投保率的关键影响因素



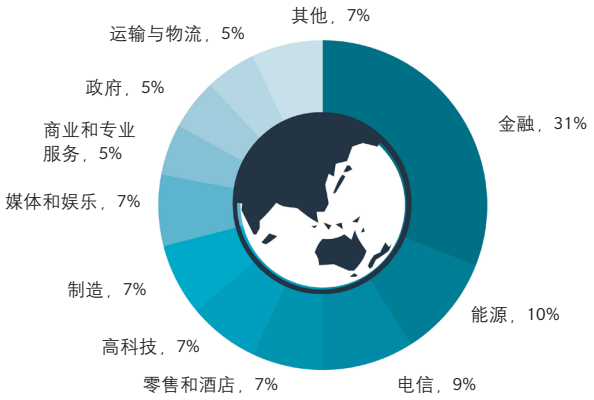
打破关于网络风险和网络保险的五个神话

“我们没有网络风险。”

很多企业认为他们能够控制他们的网络风险漏洞，因此他们不需要网络风险保险。

然而，企业应该注意的是，即使是员工也存在隐私暴露问题——员工、退休员工和员工家属的数据存储都可能受到侵害，导致隐私数据泄漏。事实上，任何使用连接到网络的电脑或移动设备的企业都存在潜在风险。即使企业可能已经外包了员工数据管理，风险和责任依然存在，因为企业有法律义务保护这些数据。

图 2 2017年亚太地区各行业成为网络犯罪目标的可能性[5]



***其他包括：**生物技术和制药、医疗卫生、建筑与工程和非营利机构*

根据FireEye iSight Intelligence[6]的最新调查，在亚太地区，金融服务业（31%）的风险最高，其他部门成为网络犯罪目标的风险基本相同（5-10%）(图2)。

例如，网络罪犯可能通过零售商销售点、保险公司计费系统、金融机构的信息处理系统或制造商的自动化流水线攻击企业的核心系统。无论在哪个部门，网络攻击都可能严重扰乱日常运作和业务流程、导致供应链和供应商通信问题以及收入和名誉损失。

在不断发展的网络风险格局中，风险已超越数据隐私扩展到网络安全系统；所以，网络安全系统和日常运营的中断都会为企业特别是其结算盈亏底线带来严重的财务影响。

“网络保险太贵了/没有预算。”

网络保险可能会很贵，但是企业管理者真正应该考虑的问题是为他们介绍的网络风险保险是否足以满足其具体需要。有时，由于缺乏优质网络风险精算数据，风险量化和定价过程可能会过于保守，导致网络风险保单范围过大和价格过高。网络保险太贵、很多企业没有预算这个问题很容易解决，只需企业聘请独立风险专家提供咨询和经纪服务来获得全面而又价格合理的网络保险。

[1]参阅http://www.bbc.com/news/technology-37163076

[2]亚太地区的网络风险：高透明度案例，MMC亚太风险中心，2017

[3]这些是保险经纪与风险管理全球领导者达信在亚洲收集的一些常见评论和反馈意见。

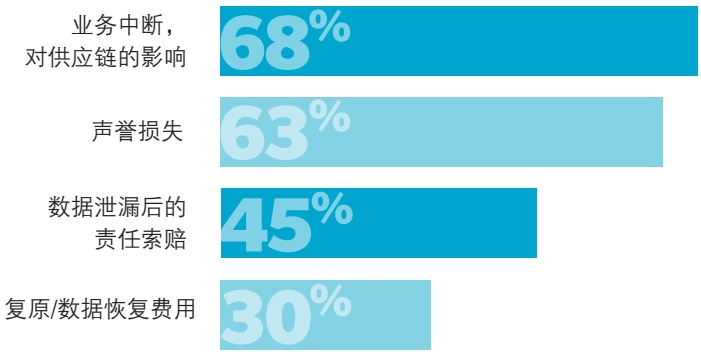
[4]ICT是信息与通信技术的缩写。

[5]调查使用情报主导的方法来衡量行业的网络威胁状况，它反映了行业成为网络犯罪目标的可能性。

[6]2017年的M趋势：一线的观点。Mandiant-FireEye，2017年3月

企业应考虑的另一个成本角度是在网络事件发生时的财务影响。根据安联《2017年度风险晴雨表》（图3），作为网络事件后导致经济损失的主要原因，业务中断（BI, Business Interruption）的影响是企业最担忧的网络问题。企业业务中断，包括关闭操作系统、重新格式化计算机和服务器，以及从备份设备恢复关键数据，造成的损失费用估计在10–40亿美元之间[7]。因此，与在发生网络事件时承担所有直接和间接费用相比，把部分风险转移给保险和资本市场可能会节约更多成本。

图 3 网络事件后导致经济损失的主要原因[8]
来源：安联《2017年度风险晴雨表》



网络业务中断量化（CBIQ, Cyber Business Interruption Quantification）是一种独特的解决方案，它帮助企业确定并根据其潜在财务影响为网络风险情景排序。它识别并评估网络风险情景和/或网络安全控制措施。该解决方案结合使用损失前业务中断分析和分析建模来为情景的影响定性和定量。这种可衡量的结果使企业能够优先考虑和分配宝贵的资金和资源，以缓解高影响力的风险情景。

资产更高效、更有效的利用解决了企业管理者的关键成本问题，与潜在攻击产生的费用相比，网络保险相对更便宜。

“我们的IT团队能够控制我们的网络风险。”

英国的大多数（56%）小型企业，仍然由IT部门承担网络风险的主要责任，在接受调查的企业中，由董事会负责网络风险的企业不到20%[9]。

IT参与是企业网络风险应对工作的重要组成部分，但在当今市场上，网络安全已经不再只是IT部门的事务。在不断变化的网络威胁环境中，网络安全是企业风险问题，必须由整个企业的利益相关者考虑和处理。

意外泄漏、雇员泄露和恶意黑客只是企业漏洞被利用的很多独特方法中的几个，所以，如果企业只侧重于直接的外部网络风险，则很可能会漏掉其风险中的很大一部分。

亚洲也正在成为诉讼日益增多的地区；企业面临着日益复杂的网络和安全问题以及诉讼和声誉损害，这些扩大了企业和董事会成员在日常运营中面临的风险范围并增加了潜在损失。

[7]参阅http://insuranceasianews.com/countries/china/wanncry-hit-asia-hard-but-wont-boost-cyber-policies/

[8]安联《2017年度风险晴雨表》主要业务风险，安联2017

[9]达信英国2015年网络风险调查报告，2015年6月

“这只是大公司的问题。”

还有一个现象是头条新闻的网络安全事件涉及的经常是大公司；然而最近的研究表明对中小型企业的水坑式攻击正变得越来越普遍。

小规模数据抓取较难检测和预防，因此被盗用的信息在黑市中似乎更有价值。而且，中小企业在网络安全基础设施上投入的资源较少，被网络罪犯视为更容易攻击的目标，并借此进入更大企业的网络。

因此，数据泄漏不仅是大企业的问题，同时也是小企业的问题。英国参与调查的中小企业中有超过一半（57%）认为内部威胁和人为操作错误（如移动设备丢失）是他们企业的最大威胁[9]，这再次表明，与大型企业一样，网络风险是中小型企业的严重问题。

无论企业的规模大小，所面临的威胁程度都是相同的，风险的防范和网络漏洞的减少更多地取决于企业本身。

“我们购买了多种保险，总有一个会涵盖这种风险的，对吗？”

不断增长和不断变化的网络风险暴露了很多传统保险的不足，这些不足导致这些保险无法快速响应网络风险。

一般责任险（GL, General Liability）、专业责任险（PI, Professional Indemnity）及其他保单可能会包含一些网络条款，但这些保单都不是针对网络攻击事件承保的。此外，这些保单通常包含特别除外条款来忽略对数据泄漏事件的承保。即使这些保单覆盖这种风险，也不会包含数据泄漏响应费用，而这种费用正是网络攻击损失的一个关键组成部分。

例如，GL保单不包含电子数据损失、被保险人或其员工的犯罪或故意行为，或者任何索赔前费用（例如通知费用、监管防范）。PI保单也常常限制对执行特定服务的疏忽提出的索赔范围，并排除被保险人或其雇员的犯罪行为以及隐私泄漏或网络攻击产生的第一方损失费用。

三管齐下的网络弹性增强方法

网络风险应被视为一种企业范围风险，而且，网络保险应辅以终端安全措施和业务持续性计划，以建立和加强企业的网络弹性。这里提供了一个较详细的行动计划来展示一种三管齐下的方法（图4），供企业在提高网络弹性时参考。

图 4 平衡用来增强网络弹性的几个关键部分

1. 有效的终端安全管理

包括威胁检测和预防在内的终端安全响应通常是网络攻击的第一道防线，而且，对于在网络事件中受到损害的企业而言，他们的第一反应（最容易和最经济的方式）是通过在终端使用并持续更新正版软件来保护自己。

终端安全遵循一定标准保护计算机网络和个人设备，这些设备通常用作企业网络的入口点。终端通常定义为最终用户设备、笔记本电脑、台式电脑以及数据中心内的服务器等硬件设备。终端安全指出了连接到企业网络的设备带来的风险。

终端安全功能通常包括IT流程和基础设施的安全基础、防病毒软件、防火墙、电子邮件加密和定期备份到与云连接的服务器上。随着网络威胁持续发展及其频率和严重程度的不断增高，传统终端安全不断升级，除了防范之外，变得更加智能[10]。

例如，多种检测和预防协议、整合工作流程以及从检测到调查的流程都在使用威胁情报进行补救和恢复。而且，随着企业的互联度和复杂度不断提高，我们正迈向数字化转型，可扩展性的主要特性是检测和防范威胁，汇聚了操作系统支持的能力。

2. 利用风险转移

保险是风险防范的重要途径之一。尽管一种保险无法完全消除风险，一张网络保单也不能为企业提供全面的网络威胁保护，但是必须知道的是，在发生重大安全事件时，它可以保持企业的财务基础稳定。

如前所述，网络保险是用来提高网络弹性的一个关键部分，它通过将一部分风险转移到保险和资本市场来抵消一部分成本。

实现这一关键部分的首要步骤是教育和培养企业，以便进行更深入、更有意义的网络讨论。企业需要真正认识到网络威胁可能带来的潜在的影响，以及合理保单提供的保障，才会把网络保险视为企业的一种必要风险管理策略。

[10]FireEye在2017年现场网络研讨会“更智能化的终端安全：如何超越预防”上讨论了下一代终端安全。

关于保险范围，当发生导致企业受到侵害或机密信息丢失的网络攻击时，网络保单提供相关费用、支出和法律费用的报销。除了第一方费用和支出（例如业务中断）以及第三方责任和辩护费用（例如诉讼、监管罚款和惩罚）外，网络保单还可以覆盖其他支出，包括取证调查、数据恢复、公共关系等。

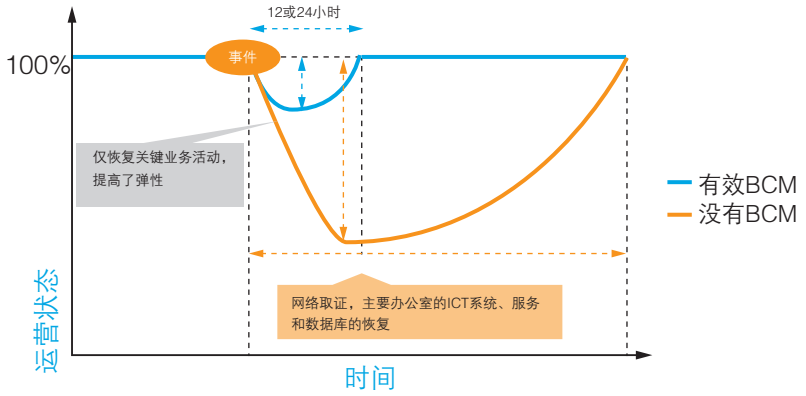
基本上，通过网络保单实现的风险转移使企业能够保护自己免受因网络事件导致的意外损失，否则这种损失会增加运营成本，破坏企业现金流的稳定性和削弱股东信心。网络保险提供了一种更有效、更高效的资产使用方法，保护企业的财务收益。

3. 制定业务持续性管理计划

业务持续性管理（BCM, Business Continuity Management）是一个全面的流程，它使企业能够更好地提前防备和响应可能会导致业务中断的潜在危机情形。在这里，BCM的主要目标是实施业务持续性计划（BCPs, Business Continuity Plans）来确保网络攻击情况下关键功能的持续。然后，进行消防演习，使企业熟悉所涉及的过程，以便在需要时有效执行BCP。最后，作为BCM流程的一部分，这些BCP将需要定期的压力测试和更新来不断地适应和防范不断变化的网络威胁，以提高效率和效益。

然而，企业可能担心的是，他们已经为应对网络事件规划了数据恢复和事后取证调查，因而网络BCM是既不必要也不需要的。但是，这种取证调查和事件后响应不一定能保证关键业务功能的及时恢复和持续。而且，并非所有的业务和运营功能对于一次性恢复系统同样至关重要。因此，企业必须识别其业务功能、信息与通信技术（ICT）应用程序、数据库和服务并确定其关键度，以确保有效地利用资源来迅速恢复关键功能的执行。

图 5 有效的BCM在行动中的可行途径



上面的图5说明了遇到导致业务中断的网络攻击时，实施或未实施有效BCM的企业的可操作途径（运营状态和恢复阶段）。

虽然事后网络取证调查，主要办公室的主要ICT系统、服务和数据库的恢复可能需要两周或更长时间，但企业可以启动BCP并根据业务功能的重要程度在24小时内恢复关键业务活动。另一方面，在网络攻击中，被认为非关键的功能、ICT应用系统、服务和数据库可能会暂时停止。

适当地把财力和资源集中在关键方面来实施有效的BCM，包括数据保护、损失预防备份解决方案和ICT恢复计划（DRPs, disaster recovery plans），就可以避免或者最大程度地降低在发生网络攻击时由于业务中断导致的巨大经济损失。

如果负责灾难恢复的数据库也被感染了怎么办?

有时，灾难恢复计划所需的数据库也可能被恶意软件或勒索软件感染。在这种情况下，ICT从主系统复制数据到辅助系统，使感染蔓延到关键功能，所以，备份到离线存储介质的传统策略（即终端安全性）仍然是有必要的，以确保数据备份保持完好。这样就可以恢复DRP需要的数据库而不必太担心通过网络取证恢复的数据是否可靠。

在风险和不确定性中前行

我们相信大多数企业都可以通过这种三管齐下的方法（恰当和最新的终端安全、网络保险、全面实施有效的业务持续性管理）提高网络弹性，从而大幅降低业务中断产生的费用和缩短恢复时间。

企业管理者应该专注于在终端安全管理和业务持续性计划的网络安全投资之间找到平衡，并确保获得适合自己行业和企业独特需要的网络保险。

对企业来说，不断评估和提高对网络风险态势的了解是至关重要的，以便围绕业务运营做出战略决策，提高网络弹性，并为未来日益数字化的世界中的不确定性做好准备。

关于达信

达信 (Marsh) 是全球保险经纪和风险管理领域的领先企业，通过确定、设计和提供创新的行业解决方案为客户的未来发展保驾护航。公司拥有约30000名员工，向全球130多个国家和地区的客户提供建议和服务。达信是Marsh & McLennan Companies (纽交所代码：MMC) 的全资子公司，后者旗下的国际专业服务公司为客户提供风险、战略和人力资源方面的建议和解决方案。Marsh & McLennan Companies在全球约有60000名员工，年收入达130亿美元，也是下列公司的母公司：佳达，风险和再保险经纪领域的领先企业；美世，人力资源、健康福利、退休方案以及投资咨询领域的领先企业；奥纬，管理咨询领域的领先企业。请在推特关注@MarshGlobal，并在LinkedIn、Facebook和YouTube关注达信，或者在微信公众号搜索MarshChina关注达信微信公众平台。

关于亚太风险中心

Marsh & McLennan Companies的亚太风险中心结合运用达信、美世、佳达和奥纬以及一流研究合作伙伴的专业知识，解决亚太地区各行业、政府和社会面临的主要威胁。我们指出关键风险问题，召集不同部门的领导者寻求新思路，并提供实用见解来帮助企业和政府更加高效地应对我们这个时代的挑战和机遇。BRINK Asia是聚焦该地区的数字化新闻中心，它为高管和政策领导者提供关于亚洲风险问题演变的最新见解、分析和观点。