MARSH & McLENNAN COMPANIES

全球风险中心

2016年 MMC 网络手册

在数字化经济中增强网络适应力

MARSH GUY CARPENTER MERCER OLIVER WYMAN

前言

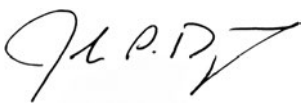
在所有领域及国家，各组织的运营中均存在网络风险。无论网络防御机制如何完善，任何公司均无法完全确保网络安全。在网络风险中，您将面临不断改变攻击战略的活跃对手。技术进步的同时，也带来新型网络风险。例如，在部署更具创新性的物联网（IoT）设备监控建筑物安全性或设备运行情况的同时，我们也将面临新的网络风险，并且需对此进行管理。技术领域的其他变化-从数据、软件迁移至云端，到人工智能在商业应用领域的应用-也在改变网络风险的性质。

有效的网络风险管理战略包括深入了解持续存在的网络威胁的范围、有效评估网络风险的潜在影响、设计网络风险预防及响应计划，以及反映所有雇员（从董事会成员到机密员工）在执行网络防御过程中的角色的管理方法。

网络是一个“风险”问题而不是“IT”问题，有效的网络管理要求广泛的跨功能部门参与。但研究表明很少有公司完成这一观念转变；更鲜有公司能做出协同一致的组织性努力，来确定可能对公司造成影响的网络风险情景，评估其供应商、客户的网络风险，并建立完善有效的网络风险预防及响应计划。

《MMC集团2016网络风险手册》包含了我司网络风险专家、与我司有合作的第三方专家的文章、报告、文章摘录及观点。这些文章涉及范围广泛的课题，包括外部环境变化、网络风险量化方法的发展及网络安全相关人力资源战略等。

我们希望本出版物能够向您提供一些新视角，帮助您加强网络风险管理方法并使您的组织在新兴的数字化环境中取得成功。



John Drzik
Marsh & McLennan Companies
达信（Marsh）公司全球风险及特险部总裁、网络风险工作组主席

目录

战略

风险

人员

战 略

不断变化的网络风险的全景展望

作者：Alex Wittenberg

六年前，Marsh & McLennan Companies和世界经济论坛共同起草的《2010年全球风险报告》发现，在当时进行的全球专家年度调查中，“大部分专家预测关键信息基础设施（CII）潜在故障和数据欺诈/损失，这两种风险的可能性及严重性相对较低。并且这两种风险还被认为是关联性最低的风险。”[1]

时光飞逝，情况随之改变

*《2016年全球风险报告》*将“日益增强的网络依赖性”视为可能导致全球风险增大的长期形式之一。网络攻击被列入全球10大风险——在未来18个月名列全球风险第7位，在未来10年名全球风险第8位（见表1）。随着公共领域及私人领域的日益数字化，网络攻击的范围、规模及影响正在迅速扩大。据预测，在2019年全球范围的数据泄露预估成本将达到2.1万亿美元，相当于2015年预估数据泄露成本的近四倍。[2] 网络攻击所带来的影响正从虚拟世界转移到现实世界。2015年，乌克兰三家配电公司遭受黑客攻击，导致80,000个能源客户受到停电。

网络风险是一直持续存在的。但是，全球各地对于网络风险的意识程度和关注度差异巨大。北美及欧洲的风险防范领导人非常关注针对网络风险及关键系统故障的应急准备工作。几个亚洲经济体（包括日本、新加坡及马来西亚）也将网络攻击认定为一项主要风险。

表1：按时间范围排列的前10大风险

	未来18个月内	未来10年内
1	非自愿移民	水资源危机
2	国家解体	气候变化应对不力
3	国家间冲突	极端气候
4	高失业率	食品危机
5	国家治理失败	社会动荡
6	财政危机	生物多样性的丧失
7	网络攻击	高失业率
8	社会动荡	网络攻击
9	极端气候	自然灾害
10	资产泡沫	国家治理失败

经济性
环保性
地缘政治性
社会性
技术性

数据来源：世界经济论坛《2016年全球风险报告》
注释：《2016年度全球风险认识调查》

不断提高的认识

对于网络风险的认知与公共或私人领域遭受的大规模攻击有关。在美国，数据泄露通告引起了公众对于网络风险的高度重视。在欧洲，《通用数据保护条例（GDPR）》将于2018年生效并要求企业报告数据泄露事故，其更关注于公共机构与企业在网络风险管理方面的合作、跨行业的数据分享、稳健的网络风险管理及响应机制。在这种不断变化的背景下，各组织必须采取稳健的网络风险管理方法，在整个企业范围内重视网络风险早期侦测、响应及恢复，以缓解并更好地管理网络风险所带来的影响，并确保业务持续性。

随着积极主动的网络风险管理策略，购买网络安全保险的企业也越来越多。网络安全保险的年保费总额已达大约20亿美元，并且预计在2025年将达到200亿美元。美国仍是最大的网络安全保险购买市场，该国近20%的企业投保了网络安全保险，并且购买网络安全保险的企业数量逐年增多，购买的保单限额也在不断提高。[3]（见表2）

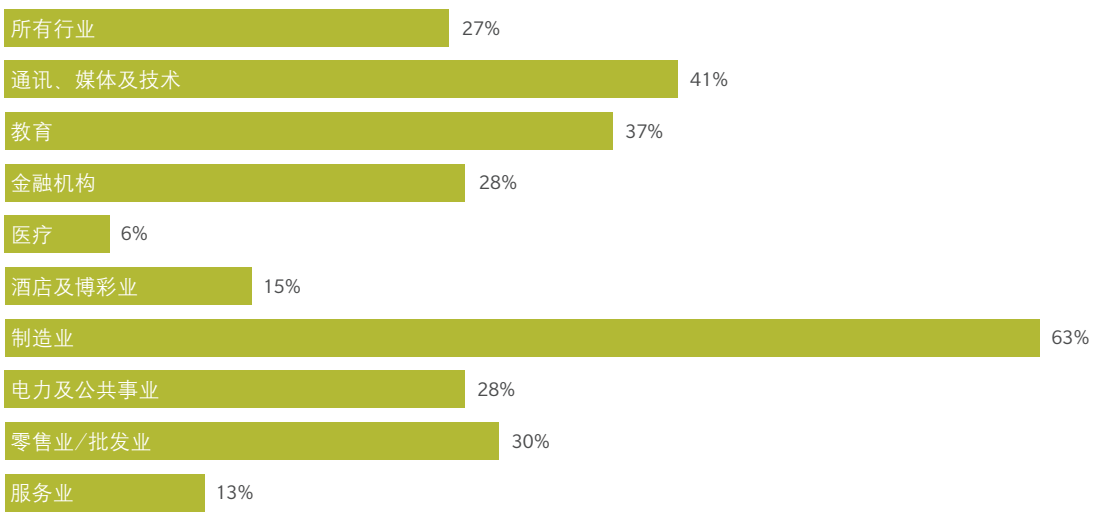
同时，其他市场对网络安全保险的兴趣也在不断提高。例如，达信公司（Marsh）的最近组织的欧洲风险经理调查发现，近25%的受访者计划在未来24个月内购买网络保险安全方案。同时，在英国组织的风险经理调查表明20.6%的企业正在购买网络安全保险。[4] 但是，英国的此项调查结果也显示，很少有企业可以量化其所面临的网络风险。缺乏对于企业自身面临的网络风险的全面了解（75%）及/或发生风险事件时潜在的财务影响及量化（64.6%），这些都导致企业在接触保险市场进行风险转移时处于不利地位。

结论

在公共机构及企业都在改组和重整为数字化组织的同时，网络风险管理必须被纳入到组织的整体战略及业务运营中。否则，企业将使自身暴露于快速变化的风险中，而无有效的管理及响应方案。♦

本文作者**Alex Wittenberg**为Marsh & McLennan Companies集团全球风险中心的常务董事，办公地点为美国旧金山。

表2：2015年各行业购买网络安全保险的增长率（达信公司客户）



信息来源：达信全球分析

1 “网络”一词在2006-2009年的年度报告中仅出现一次，但在2010年报告中被作为新出现的主要易受攻击领域。

2《网络犯罪及安全性的未来：财务及企业威胁及缓解2015-2020》Juniper调查，2015。

3 信息来源：Betterley公司报告，《网络/隐私保险市场调查》（2016）、《网络保险市场将于2020年增长三倍》（2015年9月）；达信公司（Marsh）报告《基本趋势：运营风险将驱动网络风险的购买》（2016年3月）。

4《2016年欧洲网络风险调查报告》达信公司（Marsh）。

每个人都处在危险之中

随着技术及数字化连通性的发展，即使网络安全性不断提高，但全球企业每天仍面临新的威胁。

这是一个恶性循环。
随着科技进步，我们面临的新型复杂网络攻击风险也与日俱增。

您的公司能否承受重大网络攻击并正常运营？

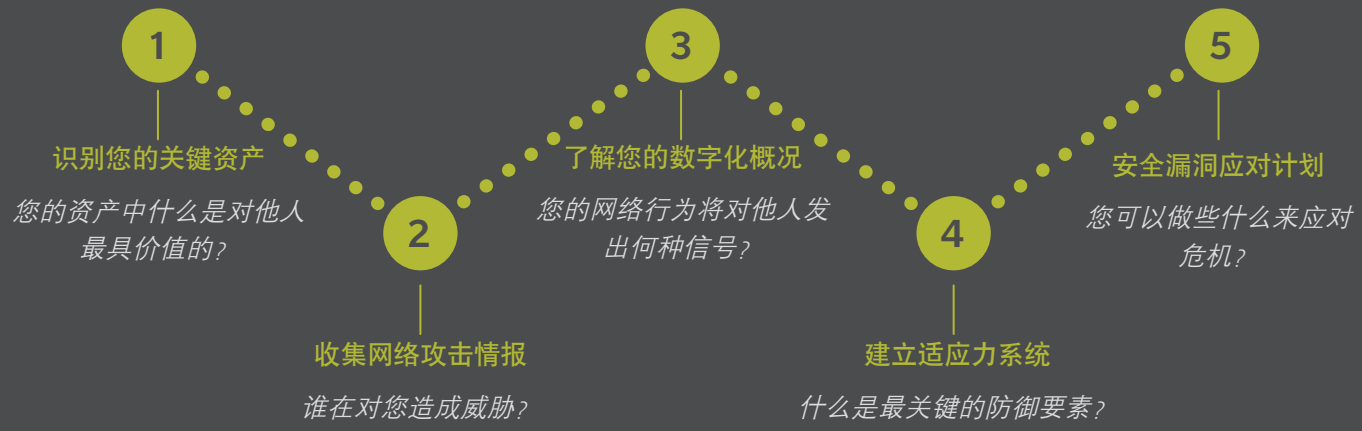
网络犯罪每年对全球经济造成的损失预估高达

4450亿美元

迎接
以网络物理系统(CPS)、物联网(IoT)及服务互联网(IOS)为基础的
第四次工业革命

网络物理系统(CPS)

实现网络适应力的路线图



数据来源：《第四次工业革命中的网络适应力》惠普、FireEye及Marsh & McLennan Companies，2016年。

网络威胁是
一个共性问题

作者： Mark Weil

网络罪犯是一群高智商、高创新性且很执着的违法人员，他们通常可以获得高额回报。网络罪犯不仅觊觎我们的个人信息，而且觊觎我们的金钱，并且会在有机可乘时偷窃我们的金钱。传统的防御方法已经不能为我们提供充分的保护。网络罪犯不仅是在伺机进入我们的系统，在许多情况下，网络罪犯已经侵入我们的系统，并且正在评估哪些数据有利可图、伺机而动。在2015年，90%的英国大型企业组织报告了网络漏洞，这说明解决网络风险的紧迫性。

不能各自为战

政府的全国性网络安全行动应得到私营企业的配合。尽管私营企业已采取一定措施确保企业安全性及从网络漏洞中恢复的能力，但还有许多工作要做。网络威胁是一个共性问题，各自为战并不是最好的选择。

例如，网络攻击及恐怖主义是两种日益增长的风险，且互相重叠交叉。关于网络安全的大量信息仍掌握在私营企业手中，而打击恐怖主义则由政府公共部门负责。显而易见，政府与私营企业必须进行更大程度的合作，以建立关键基础设施，应对这两种互相交织在一起的风险。

另外，各国目前均面临有形资产受到严重威胁的新情况，包括电网、水坝、电讯网络、交通系统及民用核设施。无处不在的互联网连接造成控制上述有形资产的行业系统的网络漏洞风险与日俱增。由于许多国家的大部分关键基础设施是由私营企业拥有并运营，政府和私营企业必须联合起来共同应对风险。

各国政府已认识到网络风险带来的经济威胁，并且正在采取一系列措施，来搭建整个经济领域的技术及人员适应力。已有30多个国家（包括德国、意大利、法国、英国、美国、日本及加拿大）公布了网络安全战略。2014年2月，中国国家主席习近平宣布成立一个新的全国性网络安全机构，以便协调安全工作。在2015年4月，新加坡设立了网络安全署，负责网络安全政策及推广宣传服务。

各国政府也通过支持网络防御的发展来促进公众的网络风险意识，包括支持相关研究创新以及培养相关知识和技能。例如，英国国家基础设施保护中心提供了良好实践做法、技术指导，并促进各领域之间的基础设施信息交流（包括能源部门及安全设备制造商）。由法国国家信息系统安全署负责协调的法国网络安全战略，同样也是基于促进公共部门与私营企业之间的合作。

各国政府都在促进公共部门与私营企业之间的信息协作分享。对于很多企业来说，要准确了解网络风险整体情况会比较困难，因此政府或行业协会向企业提供网络风险威胁及响应信息就至关重要。英国网络安全信息共享合作项目已启动，以支持英国国家网络安全战略更广泛的目标。此类共享机制使各企业能够安全地分享关于网络威胁的信息，而不会暴露本企业易受攻击的弱点、企业商业秘密、客户的个人可识别信息（PII）或使公司面临法律诉讼。该共享机制也允许同行业公司分享信息，消除对串通舞弊的担忧。

警察及执法部门在打击网络威胁方面发挥关键作用，这说明了行业及政府机构之间合作的必要性。目前，网络事件的报案数量低于实际数量；各企业必须向警察或政府部门报案并定期分享相关信息。通过与英国国家网络犯罪工作组（NCCU）等国家机关及欧盟网络及信息安全署（ENISA）等国际机构的更大程度合作，能够将更多的网络罪犯绳之以法。

目前各国均面临有形资产受到严重威胁的新情况，包括电网、水坝、电讯网络、交通系统及民用核设施。

结论

为了应对网络威胁，政府及私营企业应认识到：我们必须并肩携手，加入与共同敌人刻不容缓的战斗中。网络罪犯是看不到的敌人，潜伏在幕后、我们的组织内部及我们的设备中，伺机而动，并且难以侦测、抓捕和惩罚。在这场战斗中，失败会带来灾难性的后果，但也是可以最终避免的。只有取胜，才能保护我们的社会及我们的生活方式。♦

本文作者**Mark Weil**为达信公司（Marsh）的英国及爱尔兰地区首席执行官。

网络恐怖主义者及勒索软件

采访SHAWN HENRY

6月份，总部设于华盛顿特区的民主党全国委员会发现其整个计算机网络受到黑客攻击，民主党全国委员会邀请Shawn Henry（CrowdStrike公司总裁及前FBI网络部门负责人）核查黑客攻击造成的损害，并锁定黑客攻击者，结果黑客攻击者被认为是俄罗斯政府特工。

在“Brink”新闻网的采访中，Henry分享了他关于应对潜伏于互联网阴影中的各种敌对集团的想法。

BRINK新闻网：在您对各公司的调查中，您经常碰到的最大的网络安全错误是什么，为什么会经常发生这种错误？

Shawn Henry：各公司仍处于被动的响应状态而不是主动的前瞻状态。换句话说，各公司是在事后对网络事故被动做出响应，而非积极主动地在事前推出、部署各种技术，更好地了解网络环境并预见未来将发生的情况。在主动的前瞻式方法中，各公司能够将安全性掌控在自己手中或在网络环境中主动追踪对手，采取主动的前瞻式方法将是各企业的一个最大进步。

BRINK新闻网：受到政府支持的网络犯罪造成的威胁有多严重？网络威胁是否遍布所有公共及私营企业？是否超出了政府支持的网络犯罪范畴？

Henry：各种犯罪集团参与网络犯罪并且数量巨大。某些国家为了攫取知识产权、研发信息、企业战略而将目标瞄准各种组织。同时，恐怖主义集团也将目标瞄准关键基础设施。我们知道，他们正在发展其犯罪能力。有组织的犯罪集团主要以金融服务及零售业领域为目标。他们正在以其认为有投资回报价值的许多其他类型的组织为目标，并越来越多地使用勒索软件。事实也在证明他们此举获得了丰厚的回报。医疗、金融服务、制造商、政府、教育机构、能源及交通领域无一幸免于难。

BRINK新闻网：如果一位CEO说，“我们只是一家鞋厂。没什么东西值得黑客来偷”，您对此有何看法？

Henry：任何一家企业，无论他是干什么的，总会有有价值的东西。首先，每家从事经营的公司总有一些有价值的东西，否则就无法经营。他们一定会有某些商品、业务活动以及在行业内与众不同的专有信息。

其次，对手不一定只是图谋盗取数据。我们曾经遇到过一些敌对集团，他们摧毁网络的原因仅仅是他们对一家公司做生意的方式不满。这些对手将网络作为一种表达不满的方式。如果您的对手进入了您的网络，并且为了任何目的而决定施行报复、大肆破坏，那么您不仅应做好准备保护您的数据，而且应了解您所面对的重大风险。

BRINK新闻网：关于公司是否应在受到勒索软件攻击时支付赎金，您的观点是什么？

Henry：我认为公司不应支付赎金，而是将资金投入持续营业计划的开发，例如备份战略，以便能够重建网络。

BRINK新闻网：关于公司是否能进行“报复性黑客反击”最近成为热议话题。您的观点如何？

Henry：公司将其网络用于报复他人是非法的。公司不能跟踪黑客并偷回数据。公司不能向其他方发出恶意软件。由于这种情况正持续恶化，需要各公司采取某种对策，关于此课题会有更多的讨论。但目前法律的规定明确：不能进行报复性黑客反击。

BRINK新闻网：您是否支持变更法律允许公司进行报复性黑客反击？

Henry：如果这样做，您将面对公司被卷入国外争端、外国法律甚至对抗外国政府的风险。但是，在收集情报、与政府分享情报及与行业内其他公司协调以便找到攻击者方面，各公司有许多工作可以做。♦

本文中对CrowdStrike公司总裁Shawn Henry的访谈内容是2016年10月24日BRINK发表的一篇文章的摘要。Brinknews.com是Marsh & McLennan Companies的全球数字化新闻网，提供关于风险问题的观点看法。

应对网络极端情况

数字化出问题时应如何应对

作者：Claus Herbolzheimer

多年以来，占统治地位的传统观念为企业应以防止最常见网络攻击为重点而不是以可能永远不会发生的全网络灾难为重点。但在现实中，已不再可能选择这种折衷方案。全面网络危机正在变得更普遍，其中某些网络危机甚至还将威胁生命安全。日益发展的数字化及互联性使各组织更经常地暴露于复杂的网络威胁中。制定最坏情况下的应对策略已迫在眉睫。

我们必须意识这样的事实：仅去年就有5亿份个人资料被盗或丢失。勒索软件攻击增长35%，鱼叉式网络钓鱼攻击增长55%。这些攻击事件不再局限于仅针对台式计算机，他们正在开始造成关键医疗设备、应急服务及基础通信的故障。极少组织的网络防御能跟上这种趋势。我们估计仅有三分之一的公司已做好充分准备，以防止最坏情况的攻击。根据达信公司（奥纬公司的姐妹公司）的最近一次调查，四分之一的公司甚至未将网络风险作为公司的重大风险。近80%的公司没有评估其客户及供应商的网络风险。（见表1）

近**80%**的公司没有评估其客户及供应商的网络风险。

在各公司推出更多数字化创新的同时，他们也需要采纳更灵活并且更普遍的网络防御措施，以应对目前面临的更多极端威胁。如果不这样做，将会导致不可预见的成本、营业中断、名誉受损及法律后果。例如，应对与日俱增的勒索软件及鱼叉式网络钓鱼攻击，许多主要组织正在制定后备计划，以便在网络瘫痪时离线运行。某些组织甚至进一步将离线运行作为首选方式：2013年为了应对一系列黑客攻击对政府网站造成的瘫痪，新加坡切断了几乎全部政府部门计算机的互联网访问。在不要求联网的领域，美国及德国的医疗提供商及医院将对关键系统实行部分离线，并且准备在网络事件削弱数字化运行的情况下，重新拿起纸笔。

新数据战略

某些组织正在改变其使用及存储数据的方式。传统的数据形式和信息技术系统的灵活性及智能性已经难以跟上数据保护需求的快速变化。为了更快速地应对网络威胁，一些公司正在彻底简化其业务设置及技术系统。通过这种方式，各公司有效限制了黑客可能利用的潜入口及藏身之处。将数据拆分并分块存储于不同系统也有助于减少单一时点易受攻击的敏感数据数量。

其他一些公司正在备份其核心信息技术系统，以便客户在其自身系统完全崩溃的情况下，仍可以获得基本服务。例如，一些银行将其主要IT系统复制于云端，以确保其可以维持基本运营。另一些公司正在与竞争者谈判，在发生网络危机时作为竞争者的代理。这些组织知道，对其系统的攻击后果远远超出了对其自身业务造成的危害：如果数以百万计的企业及个人突然无法访问其账户，妨碍其支付工资或账单，将可能导致一次经济危机。

同时，各主要组织正在检查是否已建立起足够安全网络，以将网络攻击引起的连锁反应最小化，避免引起多个公司或多个行业的连锁破产。例如，政府资助的“网络基金”能够缓解整体网络崩溃所带来的金融冲击，类似于恐怖袭击或自然灾害之后用于救助的备用基金。

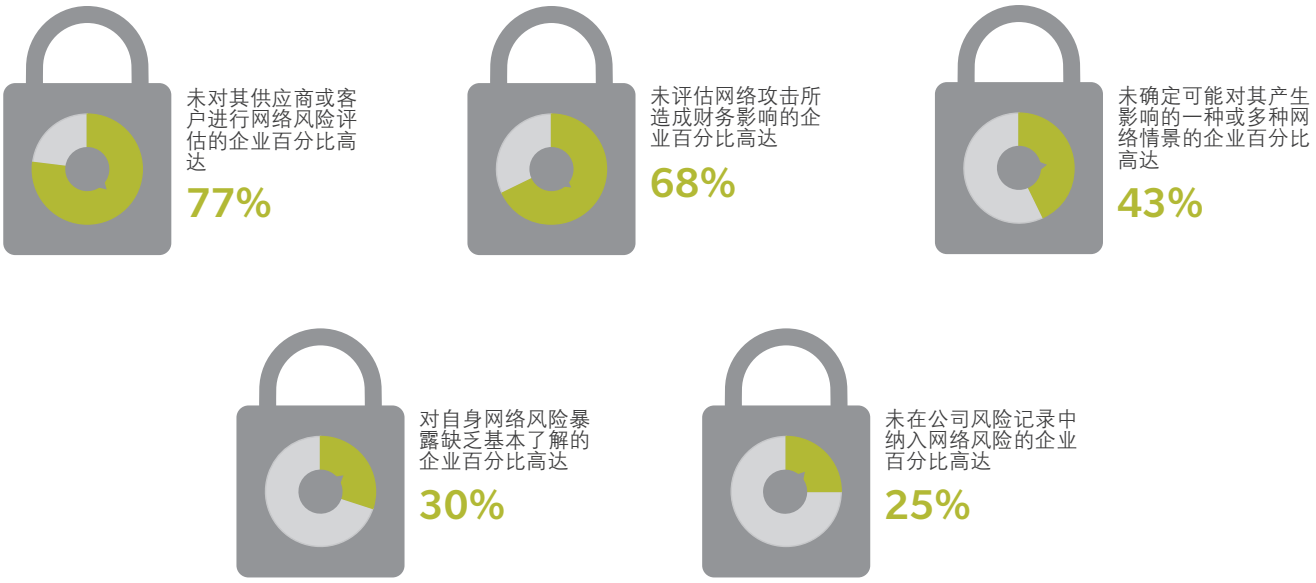
结论

从前许多公司认为不可想象的网络威胁如今已变成报纸上的每日新闻。为了避免成为头条新闻中的另一主角，各组织必须做好应对最坏情况的准备，包括不可想象的网络威胁。♦

本文作者**Claus Herbolzheimer**是奥纬（Oliver Wyman）公司数字化业务合伙人，办公地点为柏林。

表1：网络风险管理状况简述

尽管每年目标明确的网络攻击的数量在以两位数的速度增长，许多中型及大型公司仍未能在网络风险管理中投入足够资源。



信息来源：《欧洲2015网络风险调查报告》达信公司（Marsh），2015全球风险。

欧洲新数据保护法

作者： Corrado Zana

欧洲目前通过了一项新的数据保护法。从2012年1月发表该法规的第一版草案到今天最终立法，经历了四年多时间。这期间各国监管部门及其他利益相关者提出了4,000多条意见及提案，欧盟（EU）各机构经过艰苦工作，从多方面评估考虑了这些意见及提案，最终形成了今天的新数据保护法。

2016年5月4日，欧盟官方公布了通用数据保护条例（GDPR），并且该条例在公布后20日生效。但是，在欧盟各成员国必须完全执行该条例之前，还有两年的过渡期。（见表1）。该过渡期允许欧盟成员国监管部门及需执行GDPR的机构有时间做好准备，以满足GDPR所要求的业务方式变更。

对于那些未能严格遵循本法规的组织，最好能加快评估法规对其产生的业务影响并尽快完成所要求的变更。该法规将要求许多组织执行复杂的隐私管理系统，作为其信息及网络安全管理系统的有机组成部分。另外，GDPR的主要条款将影响所涉及法人实体的风险暴露情况，并且各组织应审核并更新其风险转移及风险融资战略。企业如果不合规将面临严厉处罚，因此，至关重要的是在过渡期结束前，提前论证合规性。

我们为什么需要一项新法规？

这个问题的答案显而易见：显著的技术进步，自1995年欧盟数据保护指令95/46/EC（简称指令）（英国通过1998数据保护法案执行该指令）后，技术进步已改变数据的收集及使用方法。例如，1995年是亚马逊公司成立的那一年，而此时Facebook及谷歌公司尚未成立。

GDPR承认，技术发展显著提高了数据采集和分享，这意味着公共及私营领域能够以前所未有的规模使用个人数据。欧洲委员会提出更新法规并使法规现代化的动因有两个：首先，保证欧盟基本权利宪章的第8（1）条及欧盟职能公约的第16（1）条所承认的个人数据保护权被赋予个人；其次，帮助建立网络环境中的信任，这种信任在建立统一数字化市场（DSM）中起到了核心作用。

新法规将具有更广泛的地域范围，适用于以欧盟市场为目标的非欧盟公司

该法规的适用范围？

新法规将具有更广泛的地域范围，适用于以欧盟市场为目标的非欧盟公司，无论其业务是提供货物、服务、还是与此相关的监控服务。因此，该法规不仅适用于在欧盟建立的公司及/或在欧盟内处理数据的公司，而且直接适用于“通过欧盟范围外控制方或处理方，处理欧盟范围内数据主体的个人数据，其中数据处理活动涉及：（a）向欧盟内数据主体提供货物或服务，无论是否要求数据主体付款；或（b）对发生于欧盟内的行为进行监控”。

因此，按照该法规了解您的“主体业务机构”是在哪里，就非常重要。因为这将决定，在发生投诉及任何相关执法行动时，应由哪个成员国监管部门执行主要监管职能。“主体业务机构”并不一定是公司总部，因为该法规将“主体业务机构”定义为“做出个人数据处理目的及方式决策的机构。”

由于新法规直接对数据处理方做出规定，因此对于数据处理方而言，其面临更大的改变。数据处理方的责任已经不仅局限于其与数据控制方所签的合同中的约定，GDPR同样规定了数据处理方的直接义务。因此，监管部门现在能够针对数据处理方直接强制执行该法规的条款。数据处理方的“主体业务机构”将被视为“其在欧盟的中央管理部门所在地，如果其在欧盟没有中央管理部门，则应为进行主要数据处理活动的欧盟范围内的地点。”如果其数据处理活动超出数据控制方的指示范围，那么在本法规项下将被视为联合控制方。

主要变化

罚款：最重大的变化无疑是针对违规实体或个人的罚款金额大幅增加。适用于所有欧盟成员国的

统一规则目前将罚款金额重新设定为2,000万欧元或公司全球年营业额的4%，以较高者为准（目前在英国，最高罚款金额为500,000英镑）。

对于许多组织而言，与罚款规定的最高金额相比，更令人担忧的条款修改内容是百分比数值，百分比数值基于营业额而非利润，并且百分比数值基于全球营业额而非实体在欧盟国家或发生违规所在国营业额。对于必须遵守该法规在欧盟内开展业务活动的任何全球性组织，这将引起特别关注。

地域范围：如上一段落所述，从前并不需遵守欧盟数据保护法的许多组织现在发现必须遵守该新法规。这些组织需确保关于个人数据的业务实践符合欧盟的要求以及组织一直在遵守的任何其他地区性法规。

许可：在数据处理基于许可的情况下，GDPR将针对各组织规定某些更严格的义务，导致获得许可变得更加困难。新法规要求数据控制方证明已被授予许可，并且要求有“明确确认行为”。沉默、预选框或无行为将不构成许可。另外，在数据控制方需要获得处理敏感数据的许可时，法规要求许可必须为“明示”。

用户画像：一直是数据保护实践的高度争议领域，对此，该法规将针对基于数据用户画像的精准广告营销推出新的限制。特别是，该法规禁止各组织将决策“仅仅基于自动化处理，包括用户画像，这将对[数据主体]产生法律后果或对[数据主体]产生类似地显著影响”。

隐私功能：请注意，该法规没有关于向监管部门登记数据采集及处理行动的要求或发出数据处理行动性质的声明的要求（如某些成员国监管部门的要求）。但是，该法规要求在组织内部保存（可能超出目前提交给监管部门信息的）数据采集及处理行动的详细记录。数据控制方不仅必须遵守该法律，而且必须通过执行“适当的技术及组织措施”，论证并验证合规。

数据保护官：如果公共机构进行数据处理，或“数据控制方或数据处理方的核心活动包括特征上、范围上及/或目的上的大规模定期、系统性数据主体监测的处理操作，或者数据控制方或数据处理方的核心活动包括大量特殊类别的数据”，则要求额外任命一名数据保护官，并且该法规对于谁才能担任该职位及该职位性质的某些要求做出了明确规定。

设计阶段的隐私保护：GDPR要求，对于涉及个人数据或个人数据处理技术的任何新产品或服务，必须在设计阶段就加入隐私保护考虑因素。为了确保实现这一目标，针对在相关数据处理操作“可能导致自然人权利及自由的高度风险的情况下”，明确规定了组织应该的承担数据隐私影响评估的具体要求（之前仅由某些成员国监管部门提出建议）。

数据泄露报告：法令没有关于在发生数据泄露时应通知相关监管部门或受影响数据主体的具体要

表1：GDPR执行时间表

信息来源：达信风险咨询

求，但已出现国家性法律及指导文件弥补这一空白。目前，在GDPR项下，要求所有组织“不应有延迟或在可行情况下，在获知数据泄露后不迟于72小时内”将个人数据泄露情况通知监管部门，除非数据泄露“不会导致自然人权利及自由的高度风险”。同时要求各组织在数据泄露“可能导致自然人权利及自由的高度风险”时，将个人数据泄露通知数据主体。这些严格的新报告要求使欧盟与美国更加一致，在美国，多年来数据泄露报告已成为标准规范。在数据“很难破解”（例如已加密）的情况下，可以免除通知数据主体的责任。

强化权利：在新法规中，数据主体的某些权利得到加强，这对各组织合规性提出了一定操作性挑战。这些权利包括强化数据主体对数据的访问权以及被更广泛讨论的数据删除权（通常称为“被遗忘权”），此类权利曾存在于关于数据删除的法律中，但已被扩展，特别是在欧洲联盟法院（CJEU）做出谷歌公司和谷歌西班牙公司须遵守西班牙资料保护局（Agencia Española de Protección de Datos）要求移除出现原告姓名之搜索结果的裁决（2014）之后。

所牵涉的保险问题：这组新数据保护义务纳入了某些附加义务、制裁及数据泄露响应要求，可能大幅度改变不合规情况下的财务影响。这些财务后果可能引起企业风险清单中数据保护项中的预估损失、潜在数据泄露风险容忍值的上调。这一调整可能引起企业重新审核自身的保险安排充分性。事实上可以预见，数据泄露的强制性通知义务将很可能引起欧盟地区的网络保险市场按照美国的模式增长，美国目前是最大的网络保险市场，市场规模超过20亿美元。

保单审核

各组织需了解其所购买保险的有效性、适用赔偿限额的充足性以及当现有保险安排不能满足要求时，增加保险保障的可行性。特别是，各组织可能需要考虑与下列内容相关的保险保障：

数据泄露统计数据

欧洲公司的数据泄露成本平均为每条泄露记录**US$146～$211**（大致为直接成本占46%，间接成本占54%）*

欧洲数据泄露的平均组织总体成本为*

$3,925,000

由于工作疏忽或IT故障造成的数据泄露百分比为*

52%

在英国，90%的大型组织及74%的小型组织报告过安全性漏洞问题**

76%

的被调查网站被发现有安全漏洞问题***

数据来源： * Ponemon研究所《2015数据泄露成本研究》；
** HM政府《2015信息安全性漏洞调查》
*** Symantec公司《互联网安全漏洞报告》2015年4月版。

表2：对GDPR的响应：高级行动计划

通用数据保护条例（GDPR）目前已生效，涉及欧盟公民个人数据处理的欧洲公司及非欧盟数据控制方及数据处理方应立即开始调整并执行隐私管理系统。

缺口评估

哪些个人数据被管理、如何及为什么管理？数据流

外部数据处理方的职能及管理情况

IT相关要点：
经过处理及存储的数字化数据、系统管理员流程、日志…

业务需求

什么是我们将继续做的？什么是我们不会再做的？什么是我们将要做的？

如何管理数据以确保符合法规？

必须执行哪些技术性解决方案及组织性解决方案？

规划

执行隐私风险管理方案，以区别于管理规划及技术规划，并对其进行整合

执行

整体隐私管理系统

技术性措施

组织性措施

第三方风险管理流程

来源：达信风险咨询

- 在GDPR项下，监管部门做出不提出起诉决定时原告寻求司法救济的能力，及/或数据主体作为团体诉讼的一部分寻求数据泄露补偿的权利。这可能导致数据主体的诉讼案例数量增加，以及监管部门执法更严格，毕竟这些监管部门不愿看到其决定受到挑战。

- 最高罚款将增大到2000万欧元或整个组织（而非违规实体）全球营业额的4%。这将极大地增加严重违规的潜在不利财务影响。各组织不仅需考虑更高水平的罚款（在欧盟各国并不总是属于完全可承保范围），而且由于所涉及金额巨大，如果组织想要挑战监管部门所做决定，可能也会面临更漫长、更昂贵的法律程序。

- 涉及大量个人数据的情况下，在数据泄露“可能对个人权利及自由造成高风险”时不应有延迟通知数据主体的新要求，将导致组织在执行并管理这一要求的实践步骤时产生极大的费用。

- 数据泄露带来的高公共关注度及新的通知责任要求、造成的相关媒体关注，将促使各组织考虑声誉及客户信任丧失所造成的任何短期业务影响。各组织也需要考虑执行任何声誉恢复战略及品牌保护所产生的附加成本，例如广告活动、雇用专业危机公关公司等。

这些变化是为了推动欧洲组织的风险暴露预测更接近美国企业，十多年来，美国企业必须承担数据泄露的通知责任并处理相关的隐私权诉讼。美国经验为未来欧盟数据泄露潜在成本（特别是风险管理响应成本）分析提供了有益基准点。对于担心现有保险安排的任何组织，其应关注下列问题：

- 保单是否能针对隐私保护法律及法规的违反提供充分的保险保障？

- 保单是否能针对按照GDPR发出数据泄露通知的成本提供充分的保险保障？

- 保单是否能针对受影响数据主体的团体诉讼提供充分的保险保障？

- 保单是否能针对与监管部门调查相关的成本提供充分的保险保障？

- 保单是否能针对数据保护监管部门合法征收的可保险罚款提供充分的保险保障？

结论

在评估现有保险安排的同时，各组织应考虑其整体风险暴露情况及完善的风险融资方案，包括下列步骤：

- 使用风险识别及相关的数据、技术风险暴露建模，建立针对组织的唯一性风险预测。
- 完成可保性评估，按照风险预测确定现有保险安排的有效性并提出关于未来保险安排的建议。
- 利用保险市场的附加功能，定义完善的保险解决方案，提供针对隐私及技术相关风险暴露的具体保险方案。♦

本文作者
Corrado Zana为达信（Marsh）欧洲大陆风险咨询的业务适应力总监，办公地点为意大利米兰。

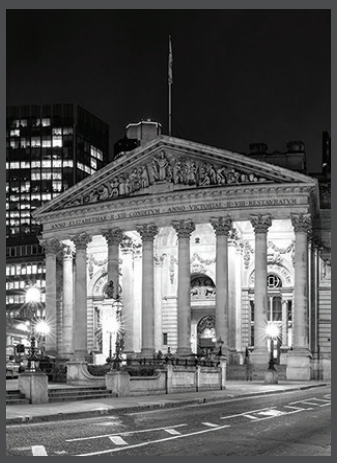
要点：

- 最严重的违规罚款提高到2000万欧元以上或企业全球年营业额的4%。
- 治外法权。
- 关于数据控制方必须证明其已获得同意的要求及关于“明确确认行为”的要求。
- 收集敏感数据的明示同意的要求。
- 数据处理方的直接责任。
- 数据主体用户画像的新限制。
- 关于组织能够论证并验证合规的要求。
- 对于“公共机构进行数据处理，或数据处理操作要求定期、系统性监测数据主体，或大规模处理大量特殊类别的数据，必须任命数据保护官”的要求。
- 对于某些新的或变更的产品及服务，要求进行数据隐私影响评估。
- 要求各组织无不应有延迟或在可行情况下在获知数据泄露后不迟于72小时内，将个人数据泄露通知监管部门，除非数据的泄露“不会导致自然人权利及自由的高度风险”。
- 要求各组织在数据泄露“可能导致自然人权利及自由的高度风险”时，将个人数据泄露“无不应有延迟地”通知数据主体。
- 数据主体的得到加强的新权利，包括删除数据权及加强的数据主体访问数据权。

各行业的网络风险

电力及公共事业

- 由于数字化及运行技术与企业IT网络及互联网的直接连接显著增大网络风险，关键电力及公共事业基础设施面临前所未有的网络风险。关键电力及公共事业基础设施所依赖的工业控制系统（ICS）、监视控制及数据采集（SCADA）系统很容易受到网络攻击。
- 风险是真实存在的。2015年12月，对三家乌克兰配电公司的黑客攻击导致80,000个电力客户停电。此次黑客攻击开始于以IT人员为目标的鱼叉式网络钓鱼攻击，然后，攻击者远程操纵了这些公用设施的SCADA系统。
- 为了减小电网中断的影响及损失，各公共事业公司持续加强网络安全措施，并合作制定跨行业的网络威胁情报方案。该行业正在加强数字技术成果转化潜力，同时继续保持电网的适应力及可靠性。



金融服务

- 针对金融服务企业的网络攻击不仅将导致财务损失，而且将增大法律诉讼风险并导致机构声誉及品牌受损，并因此有损客户信心及信任。
- 过去两年中金融机构网络犯罪损失估计近10亿美元，银行业也无法独善其身。2016年2月，对一家孟加拉银行的网络攻击通过SWIFT网络（SWIFT网络在全球范围内用于银行间交易）窃取8100万美金。孟加拉银行的攻击者至今仍逍遥法外。
- 为了管理风险，金融服务领域的各公司必须在网络安全中找到基于风险的实现网络风险防御与侦测、响应能力平衡的运营点。

医疗

- 由于医疗服务公司管理敏感、有利可图的数据，包括私人健康信息（PHI）及财务数据，医疗服务公司成为网络攻击很有吸引力的目标。
- 一项调查表明，美国88%的勒索软件攻击以医疗服务公司为目标，这导致对关键文件或系统的访问限制。
- 随着通过互联网实现的医疗设备、在线医疗端口、以客户为导向的先进应用程序及穿戴式医疗仪器的部署数量加大及电子医疗数据的使用扩大，医疗行业面临更大的挑战。

制造业

- 由于与日俱增的复杂供应链、网络控制生产线及“工业4.0”的极度互联性，制造业很容易受到网络威胁。2015年，美国制造部门是基础设施网络攻击的首要目标。
- 2014年，黑客攻击了一家德国钢厂的业务及生产网络，进入该钢厂的控制系统，并触发炼钢高炉的非计划停炉，导致设备的严重受损。
- 从供应链及贸易伙伴、服务提供商及其他关联企业等外部联系中衍生的网络风险，在制造部门中特别严重，并且必须通过完善的计划对此进行持续监控、分析及管理。

零售

- 销售终端系统（POS）一直是许多零售数据泄露的主要入口点。随着POS技术的最新进展，出现以POS系统为目标的新型恶意软件，恶意软件的目标是猎取支付卡数据并获得其他企业系统的访问权。
- 近年来，黑客们从数以百万计的零售店获取了信用卡信息，并且可以方便地在黑客暗网上通过点击电子商务功能销售信用卡信息。
- 零售商及支付系统正在作为一个整体执行的网络攻击防御技术包括端到端加密（E2EE）、标权化、符合EMV、测试系统及关于POS系统安全性的集中性工作人员培训。

教育

- 各大学及其他学习机构的开放性及信息共享文化极易受到网络风险影响。数据泄露可能变为非常现实的问题，例如身份被盗、电子跟踪、健康数据安全威胁、知识产权（第一方及第三方）被盗及其他责任。
- 在2016年年初，一家知名美国大学的财务管理软件受到攻击，导致80,000名在校及已毕业学生、雇员及供应商信息被盗。
- 各教育机构正在努力加强风险减小。例如，2015年，教育部门占网络保险投保增加额的37%。教育机构必须重点确保所有使用者的安全，包括工作人员、学术团体、学生，遵循有效的网络安全实践。

风险

网络风险的量化

有效风险管理战略的核心

作者：Arvind Parthasarathi

无论在网络安全技术上花费多少金钱，企业都无法保证不会发生网络风险。企业高管们为了实现资金投入的最优化，将钱花在最佳网络解决方案上，已将关注重点从解决这种或那种特定威胁的技术转移到了解风险并转移风险的更加可持续性解决方案。问题已从：为了保证不会发生某一种数据泄露，我需要制定何种流程并开发何种技术？转移到：我的公司遭受数据泄露的可能性有多大？以及潜在事件的严重性有多高？量化网络风险的可能性、以及潜在损失金额对于推动有意义并且有效的网络风险管理战略至关重要。

网络事件与日俱增的频率及严重性已引起主要信用评级的警惕，促使很多开始评估其受评级实体的整体网络风险，并评估网络风险对一家公司信用违约的可能性具有何种影响。另外，主要金融监管机构（例如国家保险管理部门）正在将其所管理的实体的网络风险评估纳入市场行为及资本充分性的检查。最近，纽约州提出美国首个网络安全法规，该法规要求纽约州金融服务部管理下的各机构建立并维护网络安全计划，保护消费者并确保纽约州金融服务业的及健全性。

在网络保险业方兴未艾的情况下，了解网络事件的频率及严重性对于各公司购买保险、保险经纪人排分保险以及保险公司提供承保能力并针对风险设定保险价格至关重要。在过去几十年中，网络安全技术及服务方面的支出稳步增长，2015年超过750亿美元，但在同一时期，数据泄露的频率及严重性却持续呈现指数级增长。在网络安全技术及服务方面的支出数以亿计美元的公司与在此方面支出微乎其微的公司一样遭受数据泄露损失。那么，保险公司如何区分风险并进行风险定价？

了解网络防御及网络攻击

目前，网络风险评估的重点是公司执行的网络安全技术。但尽管技术很重要，却不足以预测公司的防御网络状态；为了充分了解公司的易受攻击性，必须纳入技术背后的公司人员及流程的分析。

尽管攻击通常本质上是技术性攻击，但其关键通常在于人为因素及行为因素。例如，网络保险单承保的大部分事件与公司现有的网络安全技术无关，而是由于设备丢失或被盗及文件误发给利用合法系统访问权从事犯罪活动的恶意雇员等人为错误造成的。因此，公司网络防御状态的评估必须纳入技术背后的公司人员及流程的评估，才能准确测定公司防御网络攻击的适应力。我们必须考虑的事实是：在某些近期大规模数据泄露事件中，公司是有最新监控软件的，并且监控软件也完成了其任务并且侦测到恶意软件。但是，当技术背后的公司人员及流程未能对报警做出充分反应时，技术也无能为力。要了解某一组织的网络攻击漏洞，不能仅限于了解该组织的现有技术。

另外，主要以公司易受攻击性为重点的评估，就像在只了解一支足球队的防守能力而忽视其进攻能力就在足球比赛中下赌注一样。为了更好地了解某一公司的总体网络风险，我们必须在多因素人类行为的基础上正确建立情况模型，其中理性攻击源起方（偷窃者、间谍、蓄意破坏者、激进主义者）将优化其自身价值功能。与飓风、地震、龙卷风不同，网络攻击是故意行为，而非随机事件；在应对有动机、倾向的攻击者时，我们必须超出传统技术审核的范围，并考虑博弈理论及行为经济学的视角。漏洞（防御）及动机（攻击）提供了公司成为网络攻击潜在受害者的（导致数据泄露、营业中断及网络敲诈事件）的综合视角。

Cyence公司建立了网络风险经济建模的综合平台-包括从公司的个体风险评估到同时危害多个公司的累积事件的潜在叠加影响审查。Cyence平台通过以

技术、人员及过程为导向的视角，了解组织防御的真实情况以及犯罪分子、黑客及恶意内部人员等网络威胁源起方的真实动机。达信公司（Marsh）将Cyence公司的风险评估用于帮助其客户高效并有效地评估企业自身的风险以及供应商、业务合作伙伴或可能并购公司的风险。保险公司也利用Cyence平台做出承保及定价决策，并监控累积风险。

在对大约100万家公司的研究中，Cyence模型能够非常精确地区分高风险及低风险公司。在2015年7月到2016年7月之间，评级为最高风险公司的风险事件数量是被评级为最低风险公司的1,500倍。

对公司成为网络事件牺牲者可能性的深入了解对于评估整体网络风险并制定围绕网络风险的董事会层面的企业风险战略至关重要。各公司可以利用这一信息，讨论关于通过改进技术及流程减缓网络风险所花费资金的价值以及采用购买网络保险单等风险转移解决方案所花费资金的价值。要回答企业的问题：企业需购买多大的保险保障？或核保人的问题：保险公司应提供多大范围的保险？以及保费及自留额水平？就需要了解风险损失严重性。

网络事件潜在影响的范围广泛，包括从仅影响几个客户记录的小事件到使系统丧失功能并影响数以亿计记录并威胁公司存续的重大事件。或许公司要保护的最有价值的资产就是公司的知识产权及品牌声誉，而保险市场上缺少针对这两项内容的有意义的保险范围或承保能力，但这两项内容对公司具有巨大的财务影响。Cyence公司已建立了针对具体公司的事件严重性模型，以便于不仅量化事件发生的频率，而且量化对不同公司的损失严重性分布。

尽管围绕零售业公司及医疗公司进行了大量讨论，但现实情况是所有这些领域仍面对网络事件的风险。例如，在对一家营业额达数十亿美元的主要材料制造公司的研究中，我们从其损失分布中发现，事件的损失额从0美元到15亿美元不等。了解了这一信息，公司及董事会就可以实施数据驱动的企业风险战略，并且保险公司可以设计可持续的保险单，对潜在风险成本进行计算。

在2015年7月到2016年7月之间，评级为最高风险的公司的风险事件数量是被评级为最低风险公司的1,500倍。

了解供应链中的叠加风险

为了对某一个体公司的风险进行评估及定价，风险事件频率及严重性是基础工作，但企业风险管理及保险业务总量管理同时要求了解实体集团中普通风险的累积。由于技术及业务选择中存在多种普通路径以及某些违法攻击源起方的无差别攻击，各公司之间存在相关联的网络安全性风险。由于各种规模风险（从普通服务提供商、普通硬件及软件技术的明显风险到更加隐秘、不明显的风险）的积累，较大个体风险的组合（或供应链）仍能造成大量风险积聚问题。风险积聚的这些路径将导致保险业务总量的梯度损失或供应链的同时营业中断。就像飓风可能对整个海岸线居民造成破坏，网络安全性风险有可能叠加单一事件或几类事件，对多方造成同步危害。

例如，许多公司在访问互联网及云计算资源时共享同一基础设施。运营这一共享基础设施的技术服务提供商的营业中断可能同时影响许多家公司。在您了解保险业务总量内的风险集聚后，至关重要的是研究灾难情景，测试从停电到ISP中断、云提供商服务中断、最常用软件零日漏洞及硬件技术及基于实时数据的许多其他技术紧急事件的潜在后果。

在亚马逊公司一个最常用数据中心的为期一周的灾害情景模拟中，我们发现，根据标准普尔100指数，一组公司的损失可能超出120亿美元。在评估其保险定价的充分性时，保险公司需要考虑这些继发的损失事件。在评估资本充分性及信用风险时，管理部门及评级机构越来越重视这些极端事件及保险公司的总计风险。

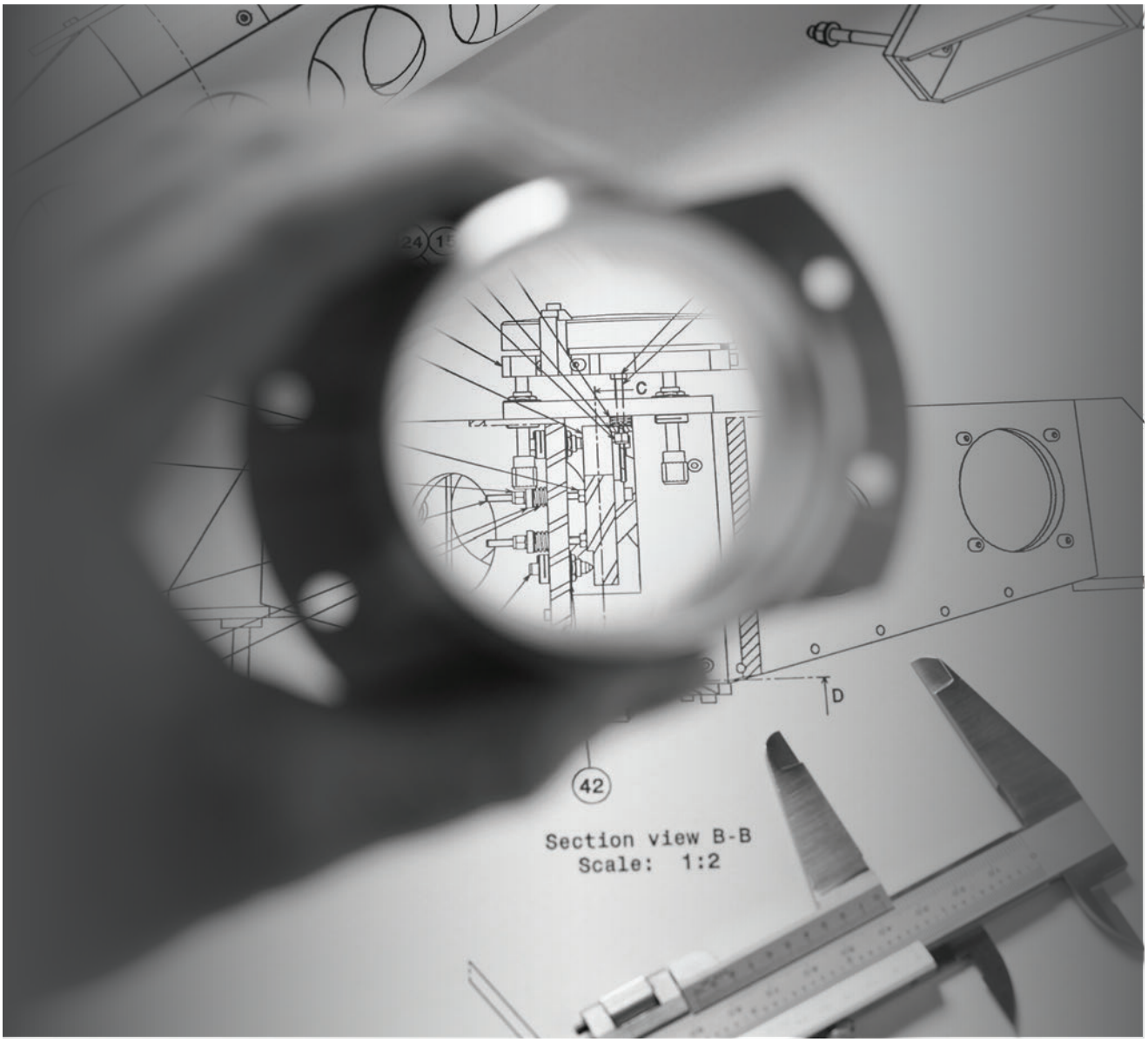
伦敦劳埃德保险公司一直坦承其了解各种网络灾难

情景总计风险的目的。但除了云服务提供商停止服务等直接网络事件之外，或许引起更大关注的是使非网络保险产品暴露于潜在网络相关损失的悄然发生的网络情景。财产等保险产品线的限额通常要比网络保险的典型最高限额高出几个数量级；另外，财产等保险产品线的保险单并未考虑网络相关风险或收取相关费用，除非另外规定网络风险责任免除，可能暴露于在网络事件及实物风险事件的交集上发生的损失。

结论

通过研究个体组织的网络风险以及具有一系列情景及后果的潜在风险积聚影响，Cyence让我们能够全面了解关于导致某一组织网络安全风险的各项因素、组织如何对标其行业竞争对手及如何管理风险。了解组织所面临的网络安全风险的主要向量有助于制定明智的企业风险管理战略，并且使保险公司及再保险公司高效、切实并且一致地评估被保险人的网络风险，并相应监视业务组合的累计风险敞口。♦

本文作者**Arvind Parthasarathi**为Cyence公司的创始人及CEO。



度量网络叠加风险

作者：Ashwin Kashyap及Julia Chu

目前，网络风险已成为全球风险全景中的一个嵌入特征，并且由于股东、客户、供应链合作伙伴及管理部门越来越关注公司如何管理网络风险，因此，预防性风险管理及事后补救措施的重要性越来越高。保险已成为帮助企业应对网络风险战略的重要一环。

对于保险公司及再保险公司，网络保险均是发展最快的业务领域之一。在保险公司开发网络风险承保的定价工具的过程中，对总计风险的关注已提高-如何了解并控制其潜在风险暴露。与按照自然地理地点监测总计风险的传统财产保险不同，网络保

险的叠加风险可能跨越超出自然地理范畴的互连系统。尽管大规模系统性风险尚不严重，但这并不意味着风险并不存在。另外，关于这种新出现的风险暴露的历史记录有限并且缺少数据，这使得保险公司难以测定网络风险并计算资本需求。换句话说：如何在不超出风险承受能力并且可实现盈利的情况下发展网络风险的保险业务总量。

几十年来，保险公司已从自然灾害角度考虑叠加风险并开发了巨灾模型。这些模型超出承保损失经验，将历史证据融合于自然灾害的专家经验，并提供对未来风险敞口的更完善理解。网络风险建模提出新的挑战，包括：

- **不断变化的危害**：网络攻击的类型以及攻击者的性质/动机不断变化。
- **延长的持续时间**：针对不同防御者的相关网络攻击可能同时发生或在几个月内重复发生。
- **损害的定义**：由于技术及业务影响之间的差异，网络损害难以量化。
- **报告滞后**：发现网络攻击可能需要几天/几年。

目前保险业及学术界的大部分网络叠加风险研究主要以确定少数潜在网络攻击情景及评估可能的影响为重点。但在谁会发起网络攻击、其主要动机是什么及未获赎金的情况下网络攻击者将如何实施攻击的理解方面存在差异。所有这些方面在这些网络攻击情景造成的风险的量化评估中均起到重要作用。

Symantec公司与佳达（Guy Carpenter）公司合作，开发了一系列框架，将这一复杂问题系统性细分为易处理的要素。这些要素中有许多无法从所承保风险或历史损失中直接观察（就像无法仅从所承保的飓风损失中推断飓风或海啸一样）。但作为一家网络安全性专业公司，Symantec公司用几十年时间跟踪新的网络威胁及攻击向量，并具备独一无二的专利遥测数据库，能够提供网络攻击每一阶段特性识别及量化的独特能力。

首先至关重要的是区分网络攻击的技术影响及业务影响。技术影响提供对攻击实施方式的了解，但难以提供对更大的业务影响的了解。为了解决这一问题，Symantec公司发明了CUBE框架，该框架能够清晰地将与企业用户相关的每一方面连接在一起。

网络保险是各保险公司及再保险公司发展最快的产品线之一。

该框架由6个互补维度组成，将网络攻击的技术复杂性细分，形成有意义、完整的叙述。这些维度包括：

- **攻击者**
- **目标**
- **目的**
- **漏洞**
- **影响**
- **后果**

我们将采用一个具体的叠加风险情景说明该框架在描述风险事件方面如何发挥有益的作用。云服务提供商服务中断的情景已被广泛用作网络保险业务总量的总计风险的一种表现形式。在以下叙述的案例中，对一家主要云平台的业务影响持续24小时，并且导致对依赖于其服务的其他企业的梯级影响。此次网络攻击是由一个由国家资助的网络威胁源起方执行的，其主要动机是向世界其他国家展示其先进的技术能力。该情景可以通过许多不同方式展示，并且我们可以用CUBE框架展示这一情景的一种实现方式。

CUBE框架提供的多维度风险视图不仅能够帮助保险公司理解某一情景的主要方面，而且能够帮助保险公司通过避免其保险业务总量高度暴露于网络攻击的“足迹”下，控制风险集聚。这种框架同时将情景描述错误的可能性最小化，并因而实现网络攻击频率及严重性的量化。实质上，CUBE框架提供了创建事件集的基础，便于业务用户在管理网络叠加风险背景下方便地理解。

在不确定性的量化成为主要目标的情况下，或许在CUBE框架之外进行考虑对于建立成熟的风险模型至关重要。因此，Symantec建议技术人员使用下

攻击者

名称： 伊朗网络部队

威胁源起方类别： 国家政府

子类别： 国家政府资助

外部攻击者/内部攻击者性质： 外部攻击者

地理位置： 伊朗

人口统计： 未知

跟踪记录： Abadil行动（2012）/ Cleaver行动（2014）

操作方法： APT

通讯渠道： 未知

目标

名称： 主要云平台提供商

垂直： 云服务

地点： 全球

主要资产： 所有类型—以政府云为重点

雇员人数： 大约15,000-20,000人

客户： 1百万（30%以上的市场份额）

纪录保持： –

年营业额： 80亿美元（2015）

网络攻击历史： 大部分为个体客户水平
同行：亚马逊网络服务、微软Azure、IBM云服务、谷歌云平台、Salesforce服务云、Rackspace云等。

目的

主要动机： 尽可能破坏目标系统的可用性

次要动机： 无

预期实现的影响： （1）造成相对较小的短期经济损失（营业中断）；（2）破坏企业及公众对云解决方案的信心；（3）显示伊朗网络部队的能力，作为近期入侵的报复（报复）

攻击升级的可能性： 较低—中等

漏洞

最可能被利用的漏洞： 人员目标（雇员人数多/用户基数非常大）、软件漏洞（红帽Linux及Xen管理程序的主机服务器使用变量）、对关键基础设施（电力、网络等）的信任

水平： 营业中断

目标的防御状态： 先进-安全的整体架构-标准DDoS攻击的模式

目标与同行相比的相对准备状态： 最高

在防御状态下成功攻击的可能性： 较低—中等

影响

损失量化设想： 从下至上的经济模型

实际经济损失： 7500万美元

实际名誉损失： 市场份额的2%-5%

损失的可保险部分： 1000万美元

攻击的持续时间及强度： 云服务无法使用时间长达24小时

所实现的影响： 对云服务行业的信心丧失导致各公司的忧虑

后果

提出保险索赔的时间： 事件发生后6个月以上

对目标产生的后果： 法务调查/向受影响客户提供的数据处理工时补偿/加强安全措施产生的附加费用

对目标的法律影响： 很可能没有

恢复时间： 完全的服务/性能恢复时间为2-3日

对第三方产生的后果： 一些公司提出网络保险营业中断索赔/某些客户对供应商提出质疑

对攻击者的法律影响： 无

信息来源：Symantec公司

表1：攻击链实例

侦察	**侦察是指**：开放源码研究及自动化网络及机器扫描 **得出的目标实体**：具有最大市场份额（31%）、巨大客户基数（1百万）但安全成熟度非常高的云服务提供商 **主要人员目标**：工作人员中的50名系统管理成员（整体15,000-20,000名工作人员中的子集）
武器制造	**所使用的武器输送物**：用于广告/横幅的JavaScript文件 **武器库**：武器输送物中恶意软件的基础8-位加密
输送	**武器输送方法**：浏览器/网络应用程序 **恶意广告采用的先进技术**：在一个知名网络博客上发表关于云服务能力的一项独特的网络安全性研究成果，一家虚假网络安全公司的广告及链接中存在恶意软件，并且网站横幅中存在同一恶意软件。
被利用对象	**所利用的漏洞**：Xen管理程序的零日漏洞（主机服务器上的虚拟机环境） **漏洞状态**：对于大多数机器未知并且适用 **易受攻击机器**：所有机器
安装	**所安装的恶意软件**：先进的远程访问特洛伊木马（RAT），并不依赖已知签名 **恶意软件行动**：（1）离开虚拟机；（2）授权升级为管理员/超级用户；（3）将恶意软件传播到其他"可使用区域"的其他机器；（4）暗中封锁其他系统管理；（5）尽可能长时间使云平台处于瘫痪状态；
命令及控制	**通讯渠道**：威胁源起方建立的命令及控制（C2）通讯渠道 **附加的恶意软件下载**：无
对目标采取的行动	**削弱系统可用性**：尽可能长时间使云平台处于瘫痪状态

信息来源：Symantec公司

述的"攻击链"方法，侦测网络攻击的不同阶段。例如，与通过网络钓鱼执行相同攻击的以财务目标为动机的威胁源起方相比，内部人员对大型数据聚集器中保密数据库的攻击具有十分不同的可能性。顺序模型可以侦测这种差异，特别是在频率量化领域。更重要的是，Symantec公司所具有的安全性遥感勘测技术可以驱动这种量化。

本文中使用攻击链说明这一概念，描述了同一情景。攻击链提供整体情景不同状态的端到端时间顺序。

攻击链趋向于更接近网络安全谱系的技术端，并且并不象CUBE框架一样具有业务友好性。但是，攻击链非常有助于理解沿攻击链向下的攻击成功概率的逐渐降低，攻击过程的每一后续步骤都对攻击者提出挑战，挑战不仅取决于攻击者的动机及能力，而且取决于目标内部的现有安全控制措施。

结论

这些框架中每一个框架的相对重要性均取决于环境背景。如果您是保险精算师或数据科学家，需要建立各种情景的发生频率及严重性模型，您将发现攻击链非常类似于您的技术工具，但如果您是保险产品组合经理或保险公司的企业利益相关者，CUBE框架能够将复杂的网络安全概念转化为简化的易于理解的内容，更好地为您服务。♦

本文作者**Ashwin Kashyap**为Symantec公司产品管理总监，办公地点为旧金山。Julia Chu为佳达（Guy Carpenter）公司的管理总监，办公地点为纽约，她的主要工作为全球战略咨询。

网络风险管理中不断变化的挑战

保护资产并优化支出

作者： Richard Smith-Bingham

尽管最近网络攻击已快速增多，各公司必须面对的现实是明年网络犯罪行为还极有可能进一步升级。网络犯罪将对准更大范围的目标，不断变化攻击向量并采取更尖端的攻击执行方式。由于技术创新及攻击者锁定、网络罪犯追踪及惩罚的困难，“攻击方”而不是“防御方”将继续处于有利地位。没有任何一家公司能够逃脱攻击者的搜索雷达，没有任何一家公司是安全的。

网络威胁前景将变得更加复杂…

由于网络攻击者为了自身或其支持者的战略及财务利益而持续重新评估回报最大、风险最低的网络攻击部署方案，网络罪犯的犯罪计划将超出简单数据盗窃的范围。安全威胁不仅将影响企业及客户的数据安全性，而且将影响产品创新、公司战略、实际执行及供应链的适应力。

上述判断基于两点显著证据。首先，由于暗网上充斥商品化的网络攻击向量及攻击武器，使善于抓住机会的犯罪分子能够渗透到防御过时技术并且攻击侦测能力较弱的公司。攻击武器库正在降低网络犯罪的门槛要求。其次，以公司具体资产为目标的高科技、多方式攻击正在变得越来越普遍，涉及多阶段行动及为了隐藏入侵及渗透而采取多层伪装的攻击数量上升。

2016年及2016年之后，大规模数据泄露及分布式拒绝服务攻击（DDoS）无疑将继续大量发生，同时，其他类型事件可能大量增多：企业敲诈黑客（威胁如果不满足某种要求，就将客户或公司数据泄露给外界）；知识产权盗窃（提供给竞争者使用）；以及数据破坏行为（操纵数字化数据削弱其完整性，因此造成高度不确定性）。

随着时间的推移，黑客们将找到更充分的动机，侵入工业控制系统并利用正在发展的物联网（IoT），因此我们可以预期将发生带来有形损失的更多网络攻击。会被这些攻击利用的漏洞已得到证明（例如乌克兰电力系统的成功侵入及针对车联网的多次黑客攻击），并且这可能标志着更多攻击即将来临。

任何单一攻击可能具有上述特征中的任何特征的组合。事实上，由于对第三方（例如供应链节点或关键基础设施）的网络攻击，不可预见营业中断的范围扩大，给各公司带来全新的风险因素。

但各公司可以逐步更清楚地了解其风险暴露情况…

良好的情景风险意识及网络风险分析对于帮助公司确定弱点、进行威胁评级、确定对策并设定情报收集的优先次序至关重要。

能够正确记录其核心信息化资产（例如数据库、知识产权或计算资源）的公司极少。没有这一信息，就难以形成取得短期、长期业务成功所需的网络内关键相关因素的充分认识。资产审查能够揭示只带来有限的附加商业价值但同时导致显著网络风险的网络组成部分。

基于这一点，对潜在对手的洞察至关重要。对手进行攻击的目的及原因是什么？对手的技术先进性如何？许多对手只是试图盗窃容易销赃的数据或盗窃资金。另外一些对手可能是为了猎取知识产权的更特殊性价值，例如保密的定价数据及创新研究或战略方向、并购目标、重要的法律争议或与关键管理部门谈判的事先情报。第三方机构可能由于与公司敌对或为了达到战略性目标（隐蔽目标），而试图破坏公司的行动。

明确公司资产及识别聪明、灵活的对手的可能企图可能，有助于重点分析企业的风险存在于哪些方面以及漏洞的潜在成本。确定对手通过防火墙

漏洞、加密失败、授权账户由公司网络设施、被盗移动设备、电子邮件、整体网络漏洞侵入公司系统的难度，就能洞察可能的破坏程度。

了解威胁的范围至关重要，但对于风险沟通、安全保护的优先级确定及资源分配而言，完善的风险量化也至关重要。对于许多公司，风险量化只是潜在损害的热图表示，并且由于热图是通过风险可能性及影响的简单预期，针对每一类事件将经常发生的较小损失及不经常发生的较大损失组合在一起，因此，热图经常带来误导。

更可靠并且更有效的方法是通过Monte Carlo模拟获得的具体公司及行业范围内的事件数据，建立分布图或风险曲线。这种方法具有一系列优点。这种方法有助于公司在概率基础上，了解每一种攻击向量的后果及相关成本的范围。跨攻击向量的应用能够实现不同成本报告的比较，并确定哪种攻击向量造成最大总体成本。通过这种方法可能发现：被最高管理层忽视的攻击向量事实上可能比那些被高度关注的攻击向量更加难以应付。另外，按照透明方式调整成本及事件假设的能力，使风险管理人有机会按照现有已知趋势进行未来功能分析。

这种建模方法不仅能够在同类比对基础上正确比较各种攻击向量，而且支持所有网络风险的叠加，以便在已确定的置信水平上量化影响。这提供了一种分析基础，用于考虑企业对网络风险程度的适应性，并讨论对风险转移及减少投资的价值。

使用同一建模方法，可以部署情景分析，调查极端事件及新出现的威胁，这方面几乎没有数据可供参考，并且要求采取“如果...怎么办”的思维模式，研究第二级及第三级后果，例如名誉影响。

实现更好地平衡安全性及商业需求的投资决策…

在高级管理层及董事会中，已出现关于更高的网络安全性预算不一定能够带来短期或长期的更高企业适应力的担忧。高级管理层更容易看到网络风险及相关支出，不会允许继续保持现状。

上述分析方法提供了一个评估不同安全保护措施价值的平台。例如，如果显而易见某一种对策将使对手无法通过网络找到感兴趣的资产，应能够将这种对策的费用与其带来的风险降低程度进行对比，然后与替代性支出方案进行对比。在进行这种分析的过程中，至关重要的是评估是否存在大量的第二级成本，例如对商业活动的限制。

同样，如果必要，各公司应将网络风险纳入新商业投资的评估，并考虑其他风险。如果考虑成本降低、保费、剩余风险，预期回报无法满足最低预期资本回收率，则没有充分理由批准投资。

事实上，由于目前网络风险是一种严重并且代价高昂的业务风险，而不仅仅是一种技术问题，所以应在风险回报基础上从战略性角度考虑安全措施。各种解决方案并不完善，资源有限，保险能力有限，并且威胁环境不断变化。因此需要将网络适应力的各种方案作为适当水平的高级管理层监管及支持的优先考虑事项。如果风险减小及风险转移机会有限或费用无法承受，那么企业不得不接受较高的网络风险。

在技术层面，各公司应首先通过制定当前最佳做法消除网络漏洞。可以通过网络的分区隔离及整个磁盘加密、将某些软件列入白名单、认真的网络监测、严格的授权、例行事件记录及定期讨论等主要安全控制措施实现这一目标。加强针对网络安全的企业风险文化也至关重要。应鼓励员工增强追责意识及责任感，通过遵守公司政策并报告可疑的网站及电子邮件，积极支持公司的工作，而不是在主动承认未能达到安全标准后受到责备。

解决方案是不完美的，资源是有限的，保险能力仍然有限，威胁环境正在改变

但就像技术屏障常常会被最顽固并具有最尖端技术的攻击者突破一样，在连续不断的欺诈面前，也难以避免人为错误。更重要的是，需要在短期需求及长期要求之间、在战术措施及战略解决方案之间找到平衡。同样，难以避免的是在安全性及业务目标之间采取折中方案，这可能也与员工对公司IT基础设施的期望值之间存在差距。其必然结果（至少在短期）是并不完善的能力、较慢的产品及服务开发及更加受限的网络访问。

有效地调整组织并满足政府关切

安全性投资的更完善事前论证可能是当务之急，但事后监测对支持未来决策的作用越来越大。管理层及董事会越来越多地要求提供关于事件及其处理结果的度量标准及数据。由于会议议程中网络问题的重要性越来越高，并且随着具有相应专业知识的董事会成员的加入，董事会越来越熟悉网络问题。IT人员不受最高管理层监管并且只需做出运营问题最低限度报告的日子一去不返。透明性及有效性是目前的头等大事。

结论

因此，上述原则要求各公司管理层关注其公司之外的情况。但具有讽刺意味的是，鉴于网络犯罪的特点，与公司领导人、其他公司、保险公司及政府部门的信息分享正在日益成为网络适应力发展需要解决的核心风险问题。但日益成熟的对话机制将在诸多方面提供帮助。通过日益成熟的对话机制，各公司可以更好地了解如何分配资源并找到风险转移的机会；保险公司可以提供更大的保险范围，并保护保险公司自己免于叠加风险；并且政府可以更有效率地确定政策及战略支持的目标。♦

本文基于Marsh & McLennan Companies全球风险中心、奥纬（Oliver Wyman）公司及国际风险治理委员会于2015年10月举办的专家讨论会。请访问www.marsh.com，获取报告全文及更详细信息。

本文作者**Richard Smith-Bingham**是Marsh & McLennan Companies全球风险中心总监，办公地点为伦敦。

充分利用现有情报

获得好的数据当然是一种挑战，但同时，与以往相比可获得的信息数量增大，需谨慎使用。安全性行业及政府的许多报告及文章均记录了攻击趋势、恶意软件的主要形式、企业的平均支出及事件成本。保险公司及保险经纪人有时也会发表基于索赔趋势的数据。网络更成熟的行业中的非正式同行工作组也会像行业-政府论坛一样，指出正在出现的非公平竞争网络威胁。基于假扮客户暗访获得的经验，独立安全专家也会提供令人震惊的秘闻。如果不滥用暗网调查，暗网调查对于了解罪犯计划及交易项目及攻击行动的价格是一种有价值的方法。

必须承认，所有这些情报均需要校核。其中某些情报被夸大、并不完整或难以获得。被广泛报道的攻击向量（例如客户数据泄露）并不一定是公司的最普遍风险或造成最大损害的风险。许多常见的攻击从未被公开报道，并且也很少能读到关于网络敲诈及关键基础设施破坏的文章，这方面信息在很大程度上被隐瞒起来。

网络最成熟的公司正在挖掘其自身数据，以便了解造成最严重风险的原因。将完善的网络事件记录链接于成本数据，这是确定攻击向量流行程度及其影响范围的基础。跟踪记录能够提供主要威胁、已知继发事件以及事件总数及成本如何随时间变化的滞后显示。尽管这种历史数据是有价值的，但在威胁不断变化的情况下，这种历史数据当然无法代表攻击类型及潜在损害的全部范围。

您能确定本企业网络风险涉及的**金额**吗?

作者：Leslie Chacko、Evan Sekeris及Claus Herbolzheimer

网络破坏是各企业面临的最常见并且代价最昂贵的威胁之一。但很少有公司能够量化其网络风险的真实程度，这将妨碍企业有效地保护自己。

大多数管理者依赖“热图”的定性指导，热图基于将经常发生的较小损失及不经常发生的较大损失组合在一起的模糊估计，将企业的易受攻击性描述为“低”或“高”。但这种方法无法帮助管理者了解企业问题涉及的金额是1千万美元还是1亿美元，也无法帮助管理者了解是应在恶意软件防御方面还是在电子邮件保护方面进行投资。因此，各公司不断做出其网络安全能力优先性的错误判断，并且所获得的网络安全性保险保障经常并不充分。

没有任何一家机构有能力完全消除网络风险。这意味着，帮助企业做出关于应减小何种威胁的正确战略选择更重要。但目前，只能根据各种漏洞成本的不完全了解

做出这些决策。各组织经常无法考虑全部潜在影响，并且对如何控制投资降低威胁概率缺乏了解。企业通常并不清楚是否已制止威胁还是仅仅减小了威胁概率，如果仅仅减小了威胁的概率，那么威胁的概率减少了多少？

至关重要的是，各公司应发展量化其网络风险的能力，以便形成减小风险的战略。问题是，是否真的能够通过难以获得并且经常难以解读的数据，将快速变化的网络风险量化为货币金额？

潜在网络破坏的真实成本估算或许永远不会成为一门精密科学。好消息是我们提高了对网络风险预测为什么总是存在不足的原因的了解。主要原因是公司按照量化其他运营风险的方式（以片面的潜在直接营业收入损失为重点）量化网络风险。但如果各公司以更广泛的网络攻击相关损失为基础评估网络风险，就能够做出更准确的预测。

在各公司从三个方面（营业收入损失及附属支出、责任损失及名誉损失）考虑风险时，就可以更贴近实际地权衡应花费多少资金减小网络风险并抑制网络犯罪。这样做的一个原因是，公司能够发现网络威胁及其业务面临的其他风险之间的一个最大区别：即使犯罪者除了获得敏感信息之外一无所得，网络攻击也将对公司造成损害。

与名誉损失相比，受到网络攻击的公司的直接营业收入损失可能微不足道，但名誉损失可能导致未来的营业收入损失。因此，对于管理者而言，在更广泛范围内量化网络风险至关重要。风险量化是可行的，并且可能为公司挽回每年数千亿美元的损失。

将网络风险量化为货币金额的第一步是确定您公司最重要的资产及最大的风险漏洞。网络风险通常分为两类：1）涉及服务中断的网络风险，以及2）造成信息损失（范围包括敏感数据、企业机密及银行账户信息）的网络风险。

但取决于企业及其客户，各种风险假定的差异巨大。例如，一家公共事业公司的最大网络风险可能是核电站停运，而医疗保险公司的最大网络风险可能是丢失医疗数据或黑客导致关键医疗设备的意外瘫痪。对于另一家企业，最大的网络风险可能是突然无法向顾客开发票，或者对于一家银行，最大的网络风险可能是突然停业，导致客户无法得到付款。

因此，我们所面临的挑战是建立智能化、设计完善的网络风险模型，网络风险模型应能够分析潜在的直接营业收入损失、责任损失及品牌损失等情景。这是因为当发生网络攻击时，公司的损失不仅限于客户停止购买产品及服务；公司将同时面临解决各种问题的相关成本，例如管理部门的罚款、法务费用及咨询费用等。

在关键数据被入侵时，同时将产生责任损失。公司可能需要向客户提供为期几年的补救措施，例如提供信用监测服务，以及解决多级法律诉讼产生的法律费用及罚款。最后，公司必须量化网络攻击损害其品牌情况下的未来营业收入损失。

为了了解风险上限及下限，公司必须收集可以按照预期情景及最坏情景建模的总体业务、运营及技术数据。使用与业务及运营的健全程度相关的内部及外部数据，管理者能够预测1-3年内预期及最高网络损失，就像能够预测未来营业收入一样。公司管理者同时能够估计，如果未来由于网络破坏导致营业中断，将有多大百分比的客户离开，或者如果网络攻击损害其声誉，将导致多大程度的股价及利润损失。各公司同时能够根据过去的事件判断哪个应用领域存在最高风险。

有了这个信息，管理者就能够更容易判断其公司是否具有适当的网络风险保护，并制定应对潜在附加支出的预算。关于公司应投入多少资金评估其供应商网络安全性状态或者根据关键数据被侵入的可能性，应投入多少资金开发鉴别软件等问题，答案将变得更加明确。

同时，管理者可以权衡是应投入资金进行更多的雇员及供应商培训，还是应投入资金建立更多的技术控制措施，以便监测潜在的数据泄露。在某些情况下，管理者甚至可以根据所涉及的网络风险，确定开发某一种新产品是否有价值。

网络风险量化具有挑战性但却是可行的，并且没有网络风险的量化，您将面临无法承受的风险。大多数企业都有相关技术知识及对所涉及风险的充分了解，帮助管理者评估减小网络风险所涉及的折中方案，并且发生差错的可能性与以前相比大大降低。目前需要的是管理者发挥领导力，将更好地了解企业需投入多少资金来控制网络风险并遏制网络犯罪作为一项首要工作。♦

2016年10月5日，本文在“哈佛商业评论”上首次发表。

本文作者**Leslie Chacko**是奥纬（Oliver Wyman）公司数字化及战略性IT业务的负责人，办公地点为旧金山；**Evan Sekeris**是奥纬（Oliver Wyman）公司财务服务业务的合伙人，办公地点为华盛顿特区；**Claus Herbolzheimer** 为奥纬（Oliver Wyman）公司数字化及战略性IT业务的合伙人，办公地点为柏林。

为什么说建模是网络保险梦寐以求的**圣杯**

作者： Robert Parisi

您是否能够量化您的企业面临的网络风险威胁？系统性风险量化及管理的情况如何？在向一组保险公司、保险商、再保险公司、数据/分析专业人士提出上述问题时，会得到不同回答。但大家都表示赞同的一点是：我们需要更多地建模。

被保险人、保险人及保险经纪人日益重视能够确定网络损失的建模能力。

网络建模将促进理解

被保险人、保险人及保险经纪人日益重视能够确定网络损失的建模能力。网络保险市场没有其他保险产品线所具有的保险精算数据，因此我们经常处于不知如何获得相关信息的窘境。为了弥补这一空白，我们从数以千计的数据泄露事件中采集数据，建立了达信IDEAL（确定损失、评估限值的英文缩写）模型，用于网络攻击事件频率及严重性的预测。

损失预测能够使您更好地抵御网络攻击。例如，IDEAL模型使用以往攻击事件数据预估未来攻击事件的损失。一家保存有200万条支付卡记录（PCI）的公司可能面临1%的数据泄露事件风险，导致2100万美元的费用。即使您的组织的风险暴露只有一半，也会有巨大的损失。为什么说网络保险市场中建模如此重要？总的来说，建模有助于：

- 网络保险定价
- 评估索赔损失数据
- 了解网络风险
- 在面临动态网络威胁时通过预测损失使市场具有更大适应力
- 将自然灾害保险领域中先进的建模技术用于网络
- 针对可预测的情景匹配适当的网络保险范围，这有助于您确定是否能够获得网络损失的赔偿。

建模的挑战

但是，由于网络保险业中的信息估计方式不断变化，建模可能带来挑战。例如，某些模型将网络运行风险及情景的解决方案纳入考虑。对于可能遭受较大损失（例如，网站崩溃）的组织而言这是可行的。但对于不会受到此类事件影响的公司，这是否可行？

另外，建模的方式多种多样。某些威胁模型的开发基于风险价值分析或另一种方法。

另一个问题是保费编码；改进的保费编码将提高网络损失建模。目前，由于保费分配的不确定性，通常难以预测所涉及的损失。

结论

好消息是保险经纪人、保险公司及分析公司正在深入研究网络风险量化。目前，各种模型甚至可以确定一家公司及一个行业的潜在数据泄露风险，这样可以向高级管理层及董事会提供保障。

尽管行业还需更多时间来积累更多的数据，但网络分析建模的好处显而易见。♦

本文作者**Robert Parisi**为达信公司（Marsh）的执行董事及全国网络业务领导人，办公地点为纽约。

网络损失风险

承保信息的确定及改进

作者： Chris Beh

尽管网络风险仍被视为一种新出现的风险，但对网络及网络风险管理的认识正在迅速提高。由于这种认识的提高，网络风险成为管理会议及董事会谈论中的常见内容，对网络保险作为网络风险相关损失补偿途径的认识也得以提高。跨工业领域及各种公司规模的网络保险投保正在发展。美国在网络保险市场中处于领先地位，但2016年达信公司（Marsh）的一项英国网络调查表明，大约20%的被调查者已购买网络保险，另外三分之一的被调查者正在考虑购买网络保险。2016年达信公司的一项类似调查发现，被调查欧洲公司中大约25%已投保网络保险。

由于对网络保险的兴趣提高，许多公司提出很多问题。首先，保险购买人可能不了解其保险单的具体内容，在发生损失时应如何应对，保险限制及责任免除是怎样的。购买决定可能受到价格及某些形式的保险标准的影响-例如基于以往网络保险购买情况的网络保险方案的确定，以及特定类型行业、组织规模及营业额的适当限额及超赔额的确定。其次，网络保险公司及保险市场仍在发展并不断成熟。随着保险公司对网络风险了解的提高或云服务（从数据管理到软件、基础设施）、使用个人设备办公（BYOD）等技术的发展，保险公司的投保单不断变化。

网络保险的有效购买及正确的保险范围选择取决于对组织网络风险暴露情况的清晰了解。

这些投保单对于保险购买人或保险经纪人可能很复杂、难以填写，但另一方面，又可能过于简单，缺少关键的承保信息。另外，对于在多个司法管辖区内运营或拥有几个分公司的大型组织，或具有复杂报告、服务或组织架构的组织，投保单可能难以容纳需承保风险的特征及性质的正确描述；另外，投保单上所询问的问题可能无法涵盖公平评定风险性质所需的详细信息。

网络保险的有效购买及正确的保险范围选择取决于对组织网络风险暴露情况的清晰了解。评估风险暴露的结构化并且基于风险的方法，能够使组织了解

表1：评估网络风险暴露的结构化并且基于风险的方法

了解您的潜在风险领域	进行风险评估	风险转移及损失基金方案	改进承保信息
• 考虑组织的内部及外部业务环境 • 调查用于网络相关风险监测、报告及反应的现有系统、实践及控制措施 • 确定组织的网络风险消化能力 – 使用风险后果标准/影响水平	• 纳入企业内的各种人员，包括： – 关键的企业资产及关键信息系统 – 信息系统/安全、法律及风险控制人员 • 针对所考虑的每一种网络风险暴露，确定威胁源及风险因素的潜在情景 • 评估现有的管理每一种威胁源及风险因素的控制措施及实践	• 对于已确定的威胁源及风险因素，确定可用的合同性风险转移及损失融资可选方案。 • 分析第一方及第三方针对每一种风险事件/情景预期采用的保险。 • 根据需要，获取组织的保险经纪人的帮助。 • 对于未保险的关键风险事件： – 审查所导致的易受攻击性 – 制定改进系统及控制措施的战略及方案	• 向保险市场提供前期积累的信息。这将有助于： – 网络保险市场在有充分信息的基础上进行承保。 – 组织的保险经纪人通过谈判获得最佳的网络保险单保险范围、限制、定价及条款。

信息来源：达信分析

这些风险暴露可能产生的影响的潜在水平，并提供信息，帮助保险公司在充分了解情况并且具有竞争力的基础上，针对这些风险进行承保。

了解您的潜在风险领域

确定风险背景对于进行风险评估至关重要，并且包括考虑组织的内部及外部业务环境。这涉及确定您的主要业务线、组织目标及核心业务活动，并确定实现业务增长、盈利及其他战略目标所面临挑战的主要范围。除此之外，您应确定实现这些目标所依赖的主要企业资产及关键信息系统资产。

下一步是调查用于网络相关风险监测、报告及反应的现有系统、实践及控制措施，包括相关的网络及信息安全流程。通过这种调查，能够明确组织层面的主要网络风险，并且确定显著的网络损失风险。网络损失风险的实例包括：关键信息技术基础设施的故障；系统破坏；关键数据丢失；大范围的服务提供中止；云服务提供商的破坏/故障；外包服务提供商的故障。

风险背景的确定可能还包括按照风险后果标准（或影响水平）——分为“战略性紧迫风险”（有时称为巨灾、重大、严重或极高风险）及“战略性持续风险”（有时称为主要、显著或较高风险），明确说明您的组织的风险容忍能力（或风险消化能力）。可以按照影响类型考虑风险后果标准，例如财务/财政/投资（例如营业收入、EBIT、毛利润、资产价值）；声誉（媒体关注、品牌损失）；法规合规性；营业中断或服务提供；以及战略或战略性/竞争力优势。

进行风险评估

完善的风险评估程序将包括企业内的各种人员，包括：先期确定的关键企业资产及关键信息系统人员以及信息系统/安全、法律及风险控制人员。针对所考虑的每一种网络损失风险，风险评估团队将确定可能对关键企业资产及/或关键信息系统造成战略性紧迫影响或战略性持续影响的威胁源及风险因素的可能/潜在情景。

向保险市场提供经充分考虑并且完善的信息，能够使保险公司确信：潜在网络风险已得到确认、理解及管理

例如，关键信息技术基础设施故障的网络损失风险事件可能是由于老化的基础设施或温度监测/控制装置的故障；或者对于系统破坏，风险情景可能是由于通过远程连接的工作人员个人设备侵入的隐藏病毒对网络造成危害，或是由于心怀不满的雇员故意引入病毒。

然后，风险评估团队将评估用于管理每一种威胁源及风险因素的现有控制措施及实践，并量化评估控制措施的效果。这将有助于组织了解控制措施的潜在差距。同时，为了帮助确定威胁或风险事件的优先次序，建议对事件的可能性或相关性进行定性评估，并且在可能的情况下进行定量评估。

风险转移及损失融资方案

对于在风险评估过程中已确定的每一种威胁源及风险因素，组织可以确定目前可使用哪些合同性风险转移及损失融资方案，包括目前已有的保险。为了改善组织的风险管理并更好地了解损失融资方案，可以分析第一方及第三方针对每一种风险事件/情景预期采用的保险。您的保险经纪人也可以帮助您确定保险缺口，并进一步帮助您了解在发生财务损失时，按照您的特殊需要设计的网络保险将如何减小财务损失。

应注意的是，并非所有已确定的主要风险事件都是可保风险。导致供应链及服务提供中断的合同违约/问题或老化硬件故障或网络部分故障等某些风

险事件可能无法完全通过保险转移（如果还可保险的话）。在此情况下，企业可以审查由于这些事件导致的易受攻击性，并制定改进系统及控制措施的战略及方案。

改进承保信息

完成上述步骤后，组织应该已积累了丰富的已记录的信息资源。如果组织希望购买到适合其风险偏好及风险性状的网络保险，可以在进行网络保险单保险范围、限额、定价及条款的谈判时，将该行为作为提供给保险市场的一部分。

向保险市场提供经充分考虑并且完善的信息，能够使保险人核保确信：潜在网络风险已得到确认、理解及管理；并能够向保险公司提供透明并且提高的风险认知。最终，这将有助于网络保险市场在充分了解情况的基础上进行承保，并使组织的保险经纪人通过谈判获得最佳的网络保险单保险范围、限额、定价及条款。相关的承保信息包括：

- 组织的背景、组织的主要业务线、组织的目标及核心业务活动。
- 在组织内如何进行风险管理，包括管理方法、框架及风险管理的交流，特别是围绕网络及信息安全实践的培训及认识。
- 已建立的控制措施及做法，例如资产管理、业务持续性、网络及信息安全政策、程序及风险登记程序。
- 组织的主要网络资产。
- 网络及信息技术基础设施，包括任何特殊地点（风险）特性。
- 主要的继发风险。
- 风险评估结果-如上所述内容或其他网络及信息安全审查或评估

结论

通过结构化并且基于风险的方法了解组织的网络风险暴露及相关网络及信息安全及风险管理程序，就可以确定某一组织可能面临的主要潜在损失风险。某些风险因素及造成风险的偶发事件可以投保，并且可以审查针对风险因素的风险转移及损失融资方案。最后，从风险评估过程中收集的信息可用于保险市场，使保险公司在充分了解情况的基础上承保网络风险，并使保险经纪人通过谈判获得最有利的网络保障范围、限额、定价及条款。♦

本文作者**Chris Beh**为新西兰达信风险咨询公司负责人。

物联网的保险及工业4.0

矩阵视图

作者： Morley Speed

技术进步及资产积累不仅刺激了保险产品的发展；而且反过来从保险产品提供的功能中受益。

保险起源于海运业并非偶然，海运业中的船舶及贸易融资是最早期的技术及资产投资的实例。持续不断的技术进步浪潮刺激了相应保险种类（不仅是保险产品而且包括风险管理）的发展。这些新的“有价物”可能带来某些挑战，但最终保险业（再保险业）提供了“物的保险”。

当前，保险业（再保险业）面临着前所未有的巨大技术挑战。物的保险能否发展为向所谓“工业物联网”提供承保？

我们正在经历基于与互联的机器及人相结合的“物联网”的第四次工业革命。这种工业物联网也被称为“智能工厂”或简称为“工业4.0”。

根据CRO论坛：“这种新生产模式的特点是‘网络-实际生产系统’中现实世界及虚拟世界的融合。”[1]。

网络目前是一个被广泛报道的话题，并且经常在具体网络保险单中被分类为介于“必有保险”（截至目前，很大程度上涉及数据泄露）及“非明列”保险之间，“非明列”保险主要是主流P&C业务内网络危害导致的第一方损失，主要是财产损失及营业中断（BI）。

所谓的“非明列”风险为劳埃德保险公司的“停电导致营业中断”情景的标的物，其最高潜在被保险损失在214亿美元到711亿美元之间。[2]

本文研究了由于工业4.0第一方风险造成的保险范围问题。基本上，这是一个关于保险业如何处理现实世界及虚拟世界融合的问题。并不涉及第一方数据泄露问题。

广义而言，现实世界通过财产保险产品承保，虚拟世界通过网络保险产品线承保。然而，划分界限并不绝对明确，这不仅导致保险范围的某些重叠，而且更令人担忧的是，这将导致一定程度的保险缺口。

1 智能工厂-风险管理全景展望–CRO论坛，2015年11月；
2 “停电导致营业中断：美国电网网络攻击涉及的保险问题”，劳埃德保险公司的2015新风险报告。

表1：直接第一方（非违约方）保险单的保险范围

保险	标的物			
	对...造成损失		...之后的营业中断	
	A. 数据资产	B. 物质资产	C.物质损失	D. 非物质损失
网络第1层				
1. 故意行为	✓	✓	✓	✓
2. 意外行为	✓	✓	✓	✓
网络第2层（网络第1层之后）				
3. 受损硬件	✓	✓	✓	—
4. 受损软件	✓	✓	✓	✓
5.财产	✓	✓	✓	—

已保险 ✓

未保险 ✓

尽管可能存在某种保险责任或保险责任不明确

信息来源：佳达（Guy Carpenter）公司

上述矩阵（表1）显示相对于各种网络及财产险情（1-5行），直接保险单通常如何承保四种标的物（A-D列）。在财产或网络保险充分的情况下，相关图标为蓝色。在存在不明确或保险范围有限的情况下，图标为灰色。显然，这是一种示意图式的简化表示，但总体而言，在A、B及C列保险范围认定相当明确，如下所述：

A. 主要在虚拟世界并且通过网络险承保。

B. 属于财产险范畴。

C. 自然而然地遵循B，因为BI遵循B。

D. 列中概述的情况复杂，特别是关于财产。

非物质损失后的营业中断

D列概述了网络保险的预期运营领域。但是，截至目前，网络保险以数据泄露为重点，而不是以工业控制系统停运导致的BI为重点。

工业及商业领域（特别是在工业4.0背景下）对网络技术的依赖，表明这一领域是保险业（再保险业）的巨大机遇。

尽管网络保险是这种风险暴露的符合逻辑的解决方案，但存在严重的资金能力方面的实际困难。网络保险限额很少超出5亿美元，但5亿美元并非特别高的公司资产值。

因此，非物质损失BI正在寻求进入财产保单的保险范围，尽管一般存在远远低于5亿美元的二级限额。但是，即使5千万美元的二级限额，也是一个相当大的网络保险限额，并且必须要求更多的核保信息并且可能要求更高的保费。

但是，财产保险通常限定为目标明确的恶意网络攻击，而网络保险单将提供针对控制系统中断的更广泛保险范围。

主要的战略性问题是：非物质损失BI的最终界限在哪里——是在网络范围内还是财产范围内？

在很多程度上，答案将取决于再保险公司的风险偏好及控制网络风险暴露的要求，特别是叠加风险。但是，这同时要求财产保险公司必须认识到，购买BI保险的原始客户并不一定将现实世界区别于虚拟世界。

结论

为了应对这种令人激动的挑战，佳达（Guy Carpenter）公司与Symantec公司将相关、可信数据结合于传统建模方式及创新性建模方式（例如网络“攻击链”方法的应用），提出一项联合提案。

保险业（再保险业）将如何根据工业4.0调整其承保能力还有待观察，但已经显而易见的是，未来对这种承保能力的需求将不断增大并具有可持续性。♦

本文作者**Morley Speed**为佳达（Guy Carpenter）伦敦办事处的运营总监。


人
员

网络风险减缓的人员配置

业务挑战

作者： Katherine Jones博士及Karen Shellenback

随着对网络攻击损失认识的提高，各公司为了更好地应对其数据及组织所面临的与日俱增的风险，正在招募所需人才。“美世精选情报”的最新调查表明，网络风险控制职位原来主要集中于IT部门，而目前各部门的网络风险控制职位增多，以便防止并减缓风险。

各组织面临三种与网络人才相关的挑战：目前，应由谁负责减缓网络风险；为了满足这种增长的人才需求，企业应招募具有何种技能的人才；以及雇主应在目前采取何种方法留住人才。

在潜在巨大风险及其对业务机会丧失的影响的背景下（伦敦劳合社保险公司估计网络攻击造成的业务损失总计达4000亿美元[1]），但却有太多公司令人惊异的对此无动于衷。根据2016年的一项“美世精选情报”全球调查，仅有略高于一半（53%）的被调查者报告称其组织已在整个组织内强制性审查网络安全性。[2] 而同时，大部分被调查者觉得他们已被组织起来完成工作任务并应对未来挑战，并且已被召集起来建立灵活的人员团队，包括使用合适的工作员工、外部顾问及第三方外包机构，但非常少的被调查者（47%）认为已获得充分人才资源应对未来挑战。

谁应负责减小网络风险？

传统上，由IT部门负责计算机相关安全性，特别是在保持指定网络安全职能超过10年以上的公司。在许多组织中，我们已经看到网络责任转移到风险管理部门。尽管这是一种不断扩大的发展趋势，但其发展时间却不到5年（见图1）。这不外乎下面几种趋势：

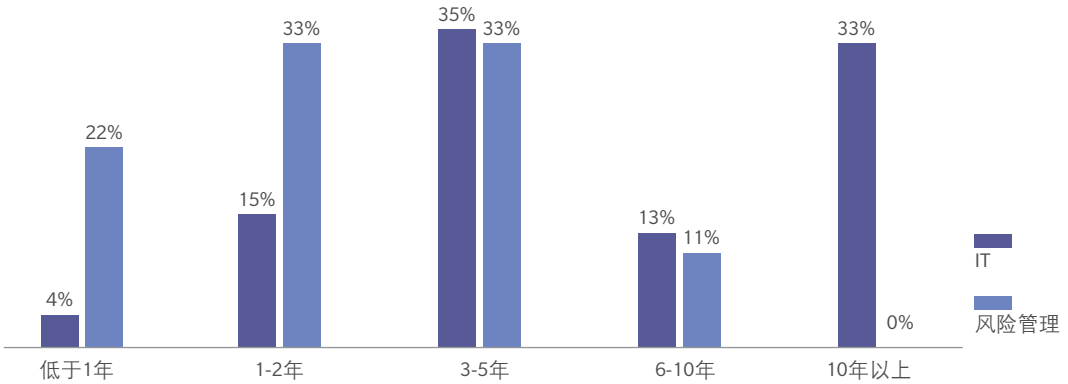
- 针对风险管理的组织职能提升
- 将网络安全性纳入整个企业的战略性风险职能而不仅是IT职能的不断扩大的趋势。
- 将网络风险管理作为最高管理层战略性风险事务的重视程度不断提高。

有趣的是，将网络安全性责任纳入IT职能的被调查组织中，有21%认为网络安全性是IT部门的首要任务，但不是企业各部门或更高管理层的首要任务。这与将网络安全性纳入风险管理部门的组织形成极大的反差，将网络安全性纳入风险管理部门的被调查组织中，没有人将网络问题视为仅限于某一部门。此项研究指出了将网络攻击应对措施作为战略性风险管理功能而不仅仅是IT部门专有职能的整体观念转变。

人才短缺情况下网络安全性方案的人员配备

大部分公司（86%）表示在未来12个月中提高网络安全性人员配备支出的意向。鉴于网络专业人员的明显短缺，对人才的争夺日趋激烈。发现人才、培训现有雇员并留住经培训的人才已成为这一重要目标的主要问题。大部分公司研究了在未来两年内扩大其网络安全性团队规模的计划，其中有25%的公司正在积极招募全职雇员，而另外25%的公司积极招募兼职、临时雇员或外部供应商提供支持。同时，一些

表1：网络安全责任及其持续时间



信息来源： “美世精选情报”项目，2016年

1 “2019年网络犯罪损失将达到2万亿美元”，作者Steve Morgan，2016年1月17日发表于Forbes杂志。
2 “美世精选情报”。2016。“前瞻性预防的第一步：正确配备网络人员”。作者Katherine Jones博士，“美世精选情报”，2016。

公司（26%）没有人员扩编意图，没有公司计划裁减人员。

雇主需要的网络安全性人员资格能力

无论是在风险管理部门还是IT部门，对网络风险减缓专业人员甚至是相关职位的新入职人员的资格要求严格，需要高水平教育、经验及资格认证。

教育：根据求职的职位，教育要求不同，大部分要求大学教育程度，高级职位要求更高学位。60-73%的被调查公司的所有职位要求具有学士学位，三分之一的公司对最高管理层（CISO、CSO、CTO、CIO）职位要求硕士学位。

经验：总体而言，即使对于初级职位，所要求的工作经验年限也相当高。例如，招募网络工程师的雇主中几乎一半要求三年以上的相关经验。具有1-2年工作经验的分析师看起来容易获得这一领域的职位，尽管有四分之一的被调查公司要求分析师职位需具有三年以上的工作经验。

安全性资格认证

由于风险管理及IT职位增多，因此各种网络安全工作岗位对经认证专业人员的需求也增大。以下表格中显示了一些更普通的网络职位以及要求特定认证的职位的百分比。

某些职位要求最好有多种认证；没有雇主不要求认证的职位。由于注册信息系统安全专家（CISSP）资质是信息安全领域为达到ISO/IEC标准17024的严格要求的第一个认证资质，因此该资质是最广泛的职位中最普遍要求的资质。

挑战：找到具有所需资格的人才

由于职位招聘要求的严格，可以想见的是，这些职位的招聘工作困难。近一半的被调查公司表示，网络安全性职位的招聘工作困难或非常困难，并且没有公司表示此项招聘工作容易。

招聘工作的困难程度取决于职位及资格要求水平：包括教育、经验及有效的认证。要求1-2年工作经验的分析师职位招聘比通常要求三年以上网络或安全工作经验的工程师招聘工作更困难。关于这种招聘工作的困难，雇主提出的原因各不相同，包括外部原因及内部原因。最重要的原因是人才市场上缺乏具有担任网络安全性职位、特别是高级职位的工作经验及教育背景的人才。但是，一半的被调查者认为公司内部未按照市场价格向此类人才提供薪酬

各职位的认证要求

	CISSP	CISA	SECURITY +	CISM	GIAC 安全性基础	CIPP	SSCP	ISO 27001 首席审计师
最高管理层或总监：CISO CSO、CIO、CTO、全球信息安全总监等	76%	34%	21%	55%	21%	17%	14%	10%
业务线官：（地区、部门或功能）信息安全官、网络安全官	83%	42%	42%	58%	13%	8%	21%	4%
首席工程师：软件安全性或安全性	73%	31%	54%	23%	35%	8%	19%	0%
经理：应用安全性	70%	35%	39%	26%	35%	4%	17%	4%
分析师：信息安全、安全操作、风险/漏洞、网络安全	68%	29%	46%	14%	39%	0%	14%	4%
分析师：威胁情报	68%	16%	36%	12%	44%	0%	8%	4%
工程师：网络安全或安全性、安全管理	74%	22%	41%	11%	37%	4%	11%	7%
安全设计师	76%	38%	41%	24%	45%	10%	17%	10%
安全审计师	52%	57%	22%	22%	9%	4%	4%	26%

信息来源：“美世精选情报”，2016年。

是无法吸引所需人才的主要原因。

招聘网络职位所需时间通常很长：23%的被调查公司表示招聘最高管理层或总监级别的职位超出120天，例如CISO CSO、CIO、CTO或全球信息安全总监等职位。五分之一（21%）的被调查公司表示在招聘这些网络安全性职位时，其薪酬目标为基本工资市场数据的第75百分位以上。16%的被调查公司表示，信息安全、安全操作、风险/漏洞或网络安全性分析师职位招聘需要61-90天时间。

略高于半数的公司在招聘时没有对安全性职位候选人提供特殊待遇，但有些公司为了吸引此类特殊人才提供了鼓励措施。灵活的上班时间、工作地点的选择、奖金及更高的基本工资是用于吸引这些职位应聘者的主要方法。

留住现有的网络人才

我们的调查中大部分公司显然建立了内部网络人才储备库；在各公司招募更多人才的同时，是否担心现有人才的保留？27%的公司表示留住现有人才是一项困难的工作；只有15%的公司认为留住现有人才相对容易。留住人才的问题主要存在于两个急缺人才的职位：信息安全、安全操作、风险/漏洞或网络安全性分析师；以及安全性审计师。23%的公司表示，最难留住这两个职位的人才。

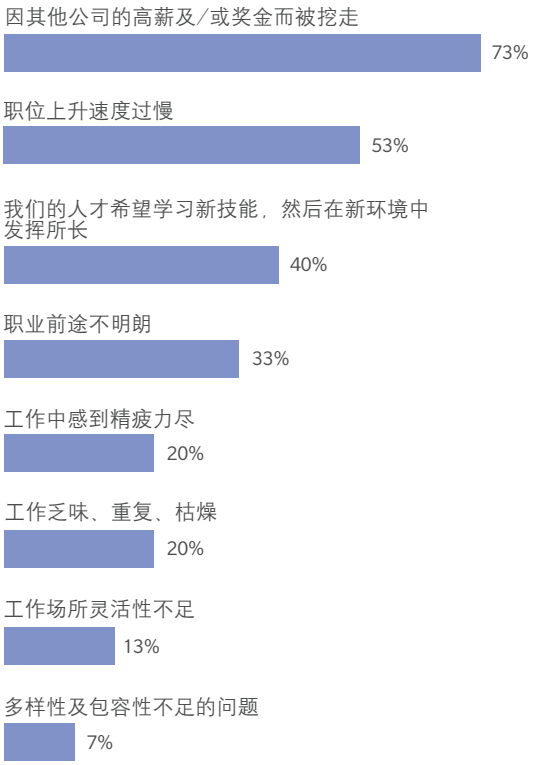
73%的被调查公司表示，网络人才流失的主要原因是其他公司的高薪吸引。对职业相关技能提高及缺乏职业发展空间的担忧是导致雇主与竞争者人才争夺战中失利的另一个原因。（见图2）

因此，大多数公司表示，希望通过培训作为留住人才的主要吸引手段。但与不采取任何措施吸引应聘者的公司相似，有许多公司未采取留住人才的手段。灵活的工作时间结合各种奖金也被用作留住人才的手段。

结论

建立良好的网络安全性组织机构开始于最高管理层，但并不局限于最高管理层。根据此项 “美世精选情报”调查，寻找、聘用、培养、留住合格人才的标准HR问题明显开始起作用。鉴于数据安全专业的具有合格资质毕业生的缺乏以及对具有相关教育背景、工作经验及认证人才的需求增大，急缺能够填补空缺职位的人才。各公司可能发现自己一方面忙于向现有员工提供教育培训，以便获得认证资格，然后又忙于向刚刚接受培训的人才提供好的薪酬，以便防止人才被竞争者的高薪酬抢走。持续减缓网络风险是一场没有终点的赛跑，网络风险是一种永不消失的威胁。♦

表2：网络安全责任及其持续时间



信息来源： “美世精选情报”，2016年。

本文作者**Katherine Jones**是美世（Mercer）公司旧金山办事处的合伙人，并且是“美世精选情报”的产品负责人。**Karen Shellenback**是美世（Mercer）公司的丹佛办事处负责人，并且是“美世精选情报”的研究负责人。

不能忽视内部人员的网络威胁

作者：Basie von Solms

公司董事会成员及CEO们因网络攻击风险及网络攻击对其公司的影响而殚精竭虑、夜不能寐。过去几年中，发生了一些令人惊心动魄的网络数据泄露事件，并且许多报道表明，网络攻击风险正在以令人震惊的速度扩大。世界经济论坛2015年全球风险报告将网络攻击风险的可能性及影响评级设定为5级（风险评级为1-7级，7级为具有巨大影响的很可能发生的风险）。

网络攻击的形式及规模各不相同，并且网络犯罪分子用于威胁公司电子资产的攻击向量范围广泛。

其中一个很容易被忽视的攻击向量是所谓的“内部人员威胁”。这是指源自于雇员的针对公司的网络攻击。

多项报告及统计数据清楚地表明，真正的内部人员网络威胁正在扩大，并且越来越成为一种严重风险。

区分外部网络攻击及内部网络攻击至关重要。外部网络攻击起源于公司外部，但可能以公司的雇员为目标。钓鱼-特别是鱼叉式网络钓鱼攻击是一种被广泛使用的攻击方法。雇员被网络攻击所击中主要是由于缺乏对此类攻击的认识及知识。这些雇员并未发起攻击，而是攻击者的目标。这些攻击经常被视为内部人员网络攻击，但事实并非如此。

内部人员攻击起源于公司内部，由被授权并且被信任可以使用公司电子资产的人执行攻击。这种雇员自己是“来自内部的威胁”。

内部人员威胁更难以应对并且仅通过技术手段难以解决。需要一种更加偏重非技术性手段并且以人为导向的防御方法。保护公司免于内部人员威胁是一项困难的工作；通常，由于各公司专注于阻止外部入侵者，甚至不考虑内部人员威胁。

多项报告及统计数据清楚地表明，真正的内部人员网络威胁正在扩大，并且越来越成为一种严重风险。

如果我们广义地将内部人员定义为获得授权使用公司信息系统的正式雇员，那么我们就低估了风险。内部人员包括可以符合逻辑地使用公司电子资产的任何人，包括第三方承包商及临时雇员。

最大的内部人员风险可能是由于任何原因心怀不满、故意盗取及破坏其公司电子资产的雇员。新技术使这种行为非常容易：一个简单的USB存储盘可以容纳大量信息，并且其体积如此之小，几乎没有办法防止雇员将其带离公司的办公场所。如果被发现时，雇员可以简单地解释说，他是为了将数据带回家加班工作。

个人云存储平台的提供使得更容易将数据及信息发送到公司之外，而不需物理性持有数据。另外，非常流行的使用个人设备办公的工作方式也是内部人员威胁的一个因素。

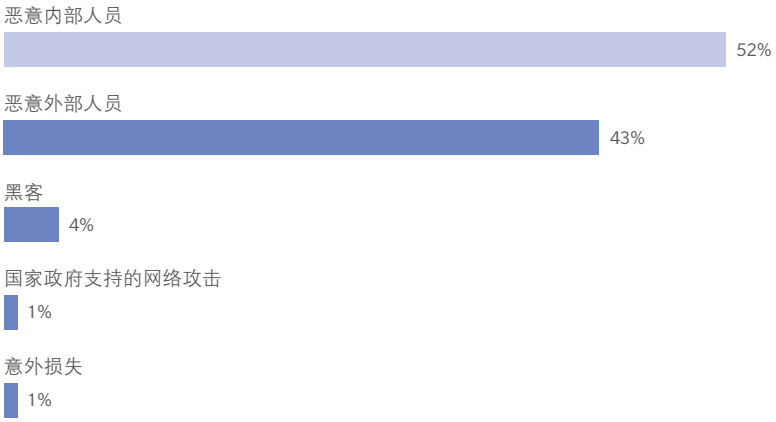
应对内部人员威胁

没有任何一种万无一失的对策能完全防止内部人员威胁。那么针对内部人员威胁应采取何种措施？公司应制定何种基本对策？

符合逻辑的是：雇员的可信程度越高，则公司对雇员“成为罪犯”并造成内部人员威胁的担心越低。一种好的做法是从一开始就尽可能管理好雇员的整个雇佣流程，从雇佣前到雇佣结束。

由国际标准化组织及国际电工委员会于2013年发布的国际标准ISO/IEC 27002专门规定了建立安全信息及网络安全环境需执行的控制条款。该标准包括14项安全性控制条款及114项安全性控制措施。

表1：按照来源分类的主要数据泄露记录



信息来源：数据泄露水平指数

关于人力资源安全性（HRS）的控制条款7专门涉及内部人员威胁。该条款规定了关于安全性控制方面的HRS，内容如下：

- **雇佣前**：在该阶段，强调了雇佣前审查，并提供了关于雇佣前阶段工作内容的整体指导。
- **雇佣过程中**：该阶段包括安全性认识、教育及培训，以及关于不遵守安全性及公司政策的纪律处分。
- **雇佣结束及雇佣变化**：在该阶段，规定了合理信息使用权的终止及相关事宜的重要内容。

已给出关于如何执行该条款中规定的建议安全性控制措施的明确指南。

各公司应详细研读该ISO标准，特别是其中第7条，并执行建议的安全性控制措施。解决内部人员威胁的工作任重道远。

结论

以下的简单三步法将有助于任何公司解决潜在的内部人员威胁：

- 应认识到内部人员网络威胁对公司而言是一种严重的网络风险，并且应严肃对待内部人员网络威胁。
- 尽管技术对策可以起到一定作用，但同时应从非技术角度应对内部人员网络威胁。
- 使用ISO/IEC 27002第7条中的控制措施作为公司应对内部人员威胁的基础。♦

本文于2015年10月21日发表于BRINK。Brinknews.com是Marsh & McLennan Companies的全球数字化新闻网，提供关于不断变化的风险问题的全景展望。

本文作者**SH （Basie） von Solms**教授是南非约翰内斯堡的约翰内斯堡大学计算机科学及软件工程学院教授及网络安全中心主任。

网络安全运营的**战略性方法**

作者：Jim Holtzclaw及Tom Fuhrman

目前，关于企业范围内网络安全性的任何讨论看来都不可避免地归结为关于技术的讨论。从安全边界保护到事件响应、漏洞管理、加密、入侵侦测、数据损失预防、记录平台、威胁情报集成及一系列其他事项，技术是保护网络、系统及数据免受网络攻击的核心。但实际上，网络安全性不仅仅要求执行技术解决方案，正如华特·迪士尼的名言，将梦想变为现实的关键因素是人。

目前，网络安全操作的最大挑战是人才方面面临的挑战-构成运营团队的IT安全性专业人才的招募、培训、职业发展、指导、管理及留住人才。问题不仅是劳动力资源中合格的网络安全人才缺乏：各公司内部网络安全操作的管理也没有得到应有的优先考虑。在许多企业中需要重视这一问题。不很好地解决这一问题将导致对安全方案效果的严重影响。

整体网络安全运营职能的复杂性及要求难以应对，没有经充分培训、高效并且完善管理的操作者，技术作用的发挥将只是一个梦想。

网络安全运营：方案的主要动力

网络安全操作包括执行、配置、调整、管理及监测安全设备的日常行动，以及对安全设备发现潜在事件时发出的警报的响应。操作人员在键盘、控制台及设备上进行实践工作，执行并直接操作、管理及监视安全设备，这不同于企业的其他网络安全职能。运营是“网络方案发挥实际作用之时”。

几个关键因素导致网络安全运营方面的人才挑战艰巨并且持久，包括：

- 网络安全运营是一个晦涩难懂并且具有内在复杂性的领域，要求具有IT及IT安全技术、网络、系统及网络漏洞的专业知识，以及对组织IT及网络安全政策的了解。网络安全运营者需要对IT漏洞如何被利用、黑客的战略、恶意攻击武器如何被输送到网络内及一系列其他技术性安全课题的专业知识。
- 网络安全运营速度及操作环境数据量很高，并且要求24x7全天候监测（例如：交通流量的监测记录、漏洞、设备状态及配置、用户资质记录、访问控制表；对于中等规模企业，安全性记录本身每天就能产生数十亿字节的工作量）。
- 富于经验的攻击方持续不断地改进其技术，这要求防御方同步改进技术。
- 劳动力资源中具有必要经验、培训及资格的人才缺乏，难以满足需求。20世纪90年代各公司的业务模型中形成对互联网的依赖，但直到后来各公司才意识到网络安全的重要性，这导致网络安全人才缺口明显。从那时起，由于企业需求超出社会通过教育及工作经验培养足够合格网络安全运营者的能力，网络安全人才缺口继续扩大。

当今网络安全操作的最重要的挑战是劳动力资源挑战

网络安全运营的劳动力资源挑战对整个网络安全性方案的效果产生直接影响。为了应对这一挑战，需要采取一种由四部分组成的战略方法。

一：建立战略性劳动力资源结构

建立战略性劳动力资源结构是指按照完善定义的需求，确定并调整特定技能。这意味着制定人员预算并规划人员的职业发展。并且这也意味着按照内部业务以及IT战略及技术、威胁的变化，从长期视角看待公司的网络安全操作需求。

定义职能：对于大多数公司而言，第一步是定义职能。最理想的是能全面、具体地定义职能。对于许多组织，第一步最好是采用白板法-从一片空白的白板开始，并以确定网络安全操作需求为重点，在很大程度上不必考虑在职员工的职责及技能。

应解决的基本问题包括：需要何种职能？执行这些职能需要何种技能？如何将这些职能及技能组合到角色及人员中？哪些职能可以外包，哪些职能应保

留在公司内部？每种职能需要多大的权力？最适合战略的专业知识水平？

这项工作应由人力资源、IT、业务线领导人及其他适当部门协同完成。由美国国家标准与技术研究院（NIST）发布的“全国网络安全劳动力资源框架”等指南可能有助于此项行动。它提供了一种描述网络安全领域所有工作及工作人员能力的通用分类法及词典。

招聘：随着200多所高等院校获得NSA的“国家信息保障教育学术专长中心”认证，劳动力市场中出现越来越多的具有网络相关学位的毕业生。大学课程、作业、研究项目、实习及其他教育经历提供了网络安全运营劳动力的非常急需的基础。

但是，没有什么可以取代工作经验，并且工作经验只能靠时间来积累。许多企业发现，他们雇佣的具有学士学位及硕士学位的大学毕业生虽然有“书本知识”，但很少有或根本没有操作经验。找到经验丰富的网络安全操作者难度极大。

招聘方法及更广泛的劳动力战略必须解决这一现实问题。一种好的方法是应认识到任何新招聘的人员，特别是网络安全操作的新招聘人员需要经过一段时间发展职业能力。在整个劳动力大军中实现这种职业能力的发展应是职业发展战略的重点。通过这样的方案，在几年内有意识地、战略性地在网络安全运营劳动力中培养所需的专业知识及经验。最好的方法是通过事先规划完成此项工作，在日常网络安全运营的动荡环境中不能仅凭运气完成此项工作。在以下段落“培训及培养工作人员”中可以找到进一步的讨论内容。

还有其他充分的理由，要求在职业发展中纳入持续教育。例如，如果能很好地重视个人职业发展，常常可以改善雇员与公司的关系并改善留住人才的工作。另外，网络安全领域的许多得到广泛承认的认证与其他领域一样，要求持续教育及培训来保持认证。将职业发展途径纳入劳动力发展战略同时能够改善人才激励并留住人才。

在大量需要合格员工的领域，薪酬是吸引并留住

表1：网络安全操作的四部分组成的行动方案

网络安全运营人员发展的战略性方法包括以下主要部分：

建立战略性人才结构

基于企业需求及现有、规划IT基础设施，确定并统筹网络安全工作人员的需求、职能、工作描述、技能及职业发展路径。

建立绩效标准

确定有意义并且可考评的网络安全业绩标准。业绩标准应反映出技术及人员的端到端业绩表现。

员工培训及培养

执行针对网络安全操作人员的培训，以便达到业绩标准、实现与技术发展、网络威胁及解决方案的同步，并按照职业发展基准模板取得进步，达到更高水平。

按照标准评估绩效

按照建立的标准进行业绩评估，确定网络安全操作功能的端到端绩效。

信息来源：达信分析

员工的主要因素。关于薪酬趋势的持续市场调查至关重要。

对于网络安全运营人员，人员的可靠性是另一个主要的考虑因素。作为企业数据及系统的监护人及管理人，网络安全运营人员实际上可以掌握最重要的企业信息---企业的“王国之钥”。关于被信任的IT内部人员泄露高度机密的政府信息的重大新闻，应引起所有企业的重视，IT人员的正直、可靠至关重要。

二：建立绩效标准

为了获得高绩效运营能力，建立“设定标准/按照标准培训/按照标准评估”的闭环结构是许多工业领域中行之有效的做法。应建立网络安全专业人员的绩效标准。绩效标准的建立应依照“全国网络安全工作人员框架”中概述的知识技术及能力，但在专业技能方面，需超出该框架的范围。

正式定义并建立标准后，应执行定期评估方案。应定期测试网络安全运营从业者的技能，以便确保其达到标准。技能测试应结合于日常工作，并且可使用多种技术工具帮助进行技能测试。

三：员工培训及培养

除了上述讨论的内容，技术的不断变化要求对有限的人才资源进行再陪训，再陪训不仅应包括技术培训，而且应包括威胁战略、攻击方法、攻击向量以及组织政策变化方面的培训。

网络安全运营人员的培训要求应包括支持目前运营工作及未来发展的其他熟练技能培训。许多组织已在内部开发的或通过网络安全培训机构提供的一种培训方法是真实网络靶场培训，网络靶场培训能在代表性网络环境中提供极好的培训机会。但是，各组织及网络安全领导人必须作为其整体战略的一部分，确定、规划这些培训方法及培训机会的成本并制定预算。最低限度应包括主要网络安全操作人员的下列培训：

- 支撑业务模型的企业IT网络及系统
- 涉及组织网络安全控制架构的特定技术
- 以企业为攻击目标的网络安全威胁技术、攻击向量及方法。

四：按照标准评估绩效

管理者应与现有员工及新员工一起，制定年度网络安全技能熟练程度记分卡或评估方法，确保对员工进行评估，并且确保员工熟练掌握与其职能相关的具体任务领域中的技能。详细的岗位描述应规定所要求的知识、技术及能力。

应通过绩效测试，评估组织的技术解决方案的端到端效果及相关人员的绩效。这种测试能够确定网络安全控制措施执行的差距或弱点，如果测试得以正确执行，就能够通过模拟不利环境的身临其境的学习，改进员工的技能掌握的熟练程度。

结论

当今，网络安全被视为企业面临的最严重潜在风险之一。网络安全运营人员是至关重要的战略性资源并将决定企业安全措施的效果。必须相应对其进行管理。♦

本文作者**Jim Holtzclaw**是达信风险咨询的高级副总裁，办公地点为华盛顿特区，**Tom Fuhrman**是达信风险咨询的常务董事，办公地点为华盛顿特区。

首席人力资源官

为什么说雇员是网络防御中的最强一环，但同时也是最弱一环

作者： Elisabeth Case

无人看管的手提电脑、丢失的手机或上下班途中员工iPad上显露的客户文件：这些问题并不以您的意志为转移，并将造成企业网络风险管理中最可怕的噩梦。由于有效的网络安全性通常开始于并结束于雇员的行为，因此首席人力资源官（CHRO）在防止网络事件中的作用至关重要。

毕竟，雇员是数据泄露或营业中断的常见原因，包括涉及信息技术（IT）的人为错误、未能严格执行的供应商登录资格要求或雇员无意中点击病毒邮件。按照IBM安全服务2014网络安全情报指标，在所调查的网络事件中，涉及人为错误的比例超出95%。

作为人力资源的领导人，首席人力资源官的工作目标是使雇员了解可能影响工作安全性或状态的事件。其中包括向员工进行网络威胁应对能力的教育。

告诫员工警惕网络风险

以下的5个预防性步骤，有助于提高涉及雇员的网络攻击防御及减小能力：

1. **监控公司的使用个人设备办公（BYOD）计划。**一个最大的挑战是如何在使用个人设备办公的过程中执行密码保护。
2. **发起网络风险认识活动。**HR及IT部门应紧密合作，将网络威胁告知雇员。
3. **制定围绕雇员从公司离职时的数据安全政策及程序。**未能及时取消离职雇员的授权的情况经常发生，这使得离职雇员仍能获取敏感数据。
4. **向雇员进行关于鱼叉式钓鱼攻击的教育。**至关重要的是与IT部门合作，进行模拟网络攻击情景的演练，确定雇员对鱼叉式钓鱼攻击的反应能力。
5. **与变化的情况保持同步。**应不断努力对雇员进行关于不断变化的网络风险的教育。

取决于网络破坏活动的动机，所有类型的雇员信息均可能陷入网络攻击，包括绩效评定、工资及其他个人信息记录。

纳入责任因素

取决于网络破坏活动的动机，所有类型的雇员信息均可能陷入网络攻击，包括绩效评定、工资及其他个人信息记录。并且数据泄露的损失可能巨大。个人数据可能在“暗网”上被出卖，例如，健康记录的出售价格通常高于信用卡信息。

数据损失有可能导致针对企业的严重雇佣责任索赔。例如，工资或管理层薪酬战略的数据泄露可能导致索赔。

结论

首席人力资源官能够促进雇员了解网络安全并帮助雇员保护自己及公司，这是一个必须珍惜的极难得的机会。首席人力资源官越积极地发挥其作用，企业及员工就越可能获得更好的保护。♦

本文作者**Elisabeth Case**是达信公司（Marsh）芝加哥办事处的全国商业E&O负责人。

其他阅读材料

未来趋势预测

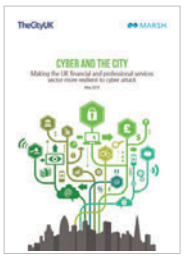
运营风险将推动网络保险的购买，2016

美国公司网络保险购买趋势的分析

欧洲大陆网络风险调查

2016年报告

关于网络风险管理方式及流程的欧洲大陆大型及中型企业风险及财务人员调查

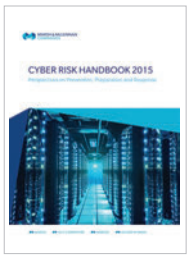


网络及城市

实现英国金融及专业服务领域的更大网络攻击适应力，

2016年5月

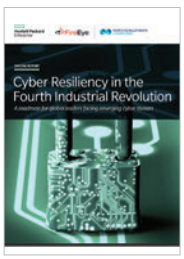
关于金融服务企业与政府部门、立法部门、监管部门、警察及情报部门合作提高网络适应力的建议



2015网络手册：

关于防御、准备及响应的远景展望

包括Marsh & McLennan Companies及外部专家的文章、报告摘要及远景展望的2015文献集。



第四次工业革命中的网络适应力，2016年

向全球领导人提供了应对物联网及服务联网的超级连接背景下新网络威胁的路线图

网络风险管理中的不断变化的挑战

保护资产及优化支出，2016

关于避免网络威胁及公司如何做好自身准备的概述

综合报告简述：风险防御人员的薪酬

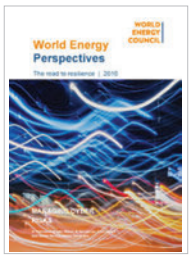
获得正确的网络工作人员

网络人才需求、雇主需要的技能及经验以及留住人才方法的概述

2016年全球风险报告

第11版全球风险报告确定了未来10年的主要风险及风险的交互作用，包括网络威胁。

PETER BESHAR在美国国家安全促进委员会上的证词



实现适应力之路

网络风险管理，2016年

关于日益数字化及互联化能源基础设施的网络风险管理的改进建议

2016年十种数字化思路

研究金融服务、制造、运输、医疗、零售、能源及储运业领导人如何进行数字化创新投资的文集。

英国2016年网络风险调查报告

在英国大型及中型企业风险及财务人员中进行的网络风险管理程序调查。

简介

Marsh & McLennan Companies全球风险中心吸收达信（Marsh）、美世（Mercer）、佳达（Guy Carpenter）和奥纬（Oliver Wyman）公司及全世界范围内顶级研究合作伙伴的专业知识，用于解决各行业、政府及社会面临的主要威胁。我们重点研究了严重风险问题，并将不同行业的领导人召集在一起，鼓励其提出新思维及可付诸实施的想法，帮助企业及政府更迅捷地对我们的时代所带来的各种挑战及机遇做出响应。我们的全球数字化新闻网BRINK提供关于不断发展的风险问题的最新洞察及基于充分信息的远景展望；我们的亚太风险中心及BRINK亚洲新闻网专注于亚洲市场的相关风险问题。

Marsh & McLennan Companies（纽交所代码：MMC）是一家全球性的提供风险、战略与人力资本咨询和解决方案专业服务的国际集团公司。达信公司是全球领先的保险经纪和风险管理机构；佳达公司是全球领先的提供风险和再保险中介服务的机构；美世公司是人才、健康、养老、投资等方面咨询的全球领导者；奥纬公司是全球领先的管理咨询机构。Marsh & McLennan Companies年收入逾130亿美元，在全世界范围内拥有大约60,000名员工，在全球130多个国家为客户提供分析、建议和交易处理。本公司致力于成为其业务领域中负责任的企业公民并发挥积极影响。

更多信息，请访问www.mmc.com网站，并加入我们的LinkedIn及Twitter @MMC_Global社交网站。