CIO管理新知译丛

安全转型

——保护企业声誉和市场份额的数字防御策略

Security Transformation:

Digital Defense Strategies to Protect Your Company's Reputation and Market Share

玛丽·帕特·麦卡锡（Mary Pat McCarthy）
斯图亚特·坎贝尔（Stuart Campbell）　　/著
罗布·布朗斯坦因（Rob Brownstein）
胡春华 /译

中国人民大学出版社

CIO知译丛

安全转型

——保护企业声誉和市场份额的数字防御策略

Security Transformation:

Digital Defense Strategies to Protect Your Company's Reputation and Market Share

玛丽·帕特·麦卡锡 (Mary Pat McCarthy)
斯图亚特·坎贝尔 (Stuart Campbell) /著
罗布·布朗斯坦因 (Rob Brownstein)
胡春华 /译

CIO

New Managing Knowledge for CIO

中国人民大学出版社

图书在版编目（CIP）数据

安全转型：保护企业声誉和市场份额的数字防御策略/
（美）麦卡锡等著；胡春华译.
北京：中国人民大学出版社，2003
（CIO管理新知译丛）

ISBN 7-300-05228-2/F·1593
Ⅰ.安…
Ⅱ.①麦… ②胡…
Ⅲ.电子商务-安全技术
Ⅳ.F713.36

中国版本图书馆CIP数据核字（2003）第119191号

CIO管理新知译丛

安全转型

——保护企业声誉和市场份额的数字防御策略

玛丽·帕特·麦卡锡　斯图亚特·坎贝尔　罗布·布朗斯坦因　著

胡春华　译

出版发行	中国人民大学出版社		
社　　址	北京中关村大街31号	邮政编码	100080
电　　话	010-62511242（总编室）	010-62511239（出版部）	
	010-82501766（邮购部）	010-62514148（门市部）	
	010-62515195（发行公司）	010-62515275（盗版举报）	
网　　址	http://www.crup.com.cn		
	http://www.ttrnet.com(人大教研网)		
经　　销	新华书店		
印　　刷	河北涿州星河印刷有限公司		
开　　本	890×1240毫米 1/32	版　　次	2004年7月第1版
印　　张	6.875　插页 1	印　　次	2004年7月第1次印刷
字　　数	120 000	定　　价	18.00元

译者前言

10年前的今天，大多数中国人还根本不知道互联网为何物，更不用说与互联网相关的安全性了。然而，经过10年的发展，中国的互联网个人用户总数已经快成为世界第一了，企业用户总数同样也以迅猛的速度递增到了一个新的高度。企业之所以要融入到互联网中去，是因为互联网能给企业带来更大的利润，简言之，就是能够节约成本、提高效率、扩大市场。然而，在这样一个人人都可以自由使用的互联网中，由于安全问题造成的巨额损失每天都在发生，企业安全性的重要程度超过了以往任何时候。

人们对安全问题在认识上经常存在误区，以为只要技术足够先进，就能够保证足够的安全。其实远非那么简单，本书作者跳出了这样一种误区，从更高层次来看待安全问题，它不仅包括技术，还包括人员和过程，而且对企业安全问题影响最大的往往不是技术，而是企业内部人员。

本书是由玛丽·帕特·麦卡锡和斯图亚特·坎贝尔合著的，他们在信息风险管理方面有着多年的从业经验，曾为许多跨国高科技企业服务。他们在企业安全架构方面的长期经验为本书提供了很多素材，书中所列举的事例和假设的情形生动形象，讲述条理清晰，能让读者很快理解并着手去解决企业安全问题。

对于那些与企业数字化进程相关的人员而言，这是一本富有时代感的书，浅显易懂，技术性不强，专业术语使用得也较少，能让我们很快理解安全转型是什么、为什么以及该怎样做等这些困扰许多企业的大问题。

在目前已有的同类书中，像这样优秀的书并不多。相信本书一定能受到广大读者的欢迎，促进国内企业安全问题的解决，进而有助于加快企业数字化进程。

本书从多个角度分析了安全问题在现代企业正常运行中的重要地位，并提出了一些相应的措施应对安全转型带来的挑战。全书共九章，分为五个部分。第一部分从心理角度解释了安全转型的必要性；第二部分从利益角度说明

了安全转型的巨大商机；第三部分阐述了解决安全问题的方法和步骤；第四部分论述了如何评估安全风险以及如何建立企业安全架构等内容；第五部分就未来安全转型的方向进行了展望。

本书适合那些与企业安全问题相关的管理人员和工程技术人员阅读参考。

在本书翻译过程中，得到了闻洁工作室熊妍妍、刘蕴莉等人的支持和帮助，在这里对她们表示衷心的感谢。

胡春华

2003 年 11 月

序言

自人类诞生之日起，安全性就是人类的一个基本问题。不久以前，关于安全问题的讨论还主要集中在物质安全方面：家人是否安然无恙，有没有可靠的食品来源，有无庇身之处等等。然而，随着计算机时代的来临，过去几十年中我们所有人都开始关心个人和企业信息的安全性了，互联网的出现更进一步加深了这种关心的程度。在这样一个看上去关于生活的每一个字节都只需要点击几下鼠标的时代，我们还能很自信地认为信息是安全的吗？

这种担心也许还会与日俱增，因为我们才刚刚处于互

联网时代的初始阶段。今天，我们在互联网上的主要活动只是简单的收发电子邮件或者浏览网页，而下一代互联网的出现则将使 2001 年看上去像数字“石器时代”。到那时，计算机基本不需要人进行控制，会在互联网上通过自动合作为我们收集数据。我们的家庭以及所有相关应用都将联机在线，随时对所需服务、订购或更换自动进行决策，并组织相关资源执行决策和支付报酬。当你决定去看病时，你的保险公司、医生以及个人日历等都会自动收到通知。在某种程度上，网络就是一个人生活的全部。

这不是科幻小说。对我们许多人而言，未来几年内生产率、效率和个人生活质量都会得到令人难以置信的提高，与此同时，由于我们越来越依赖于网上生活，因此，个人数据所面临的风险也就越来越大。风险的大小程度由我们用来保护自己的过程与技术的完善程度决定。我坚信，数字时代带给我们的好处要远大于风险带来的弊端，并且我们有能力对风险进行有效管理。

为了成功地进行风险管理，我们需要针对计算机系统及其关键的信息基础架构采取新的措施。计算机系统肯定会越来越复杂，规模越来越大，因而我们需要探索新方法来对这些系统进行分类、设计、执行、管理和审查——应该让计算机自身能更直接地融入到这些工作中，而不能仅仅像今天这样简单地“编码和管理”。

本书给读者带来一种考虑信息安全的全新方法，使读

者明确认识到信息基础架构的风险范围——从个人数据到国家金融、水资源和能源供应都可能受到安全威胁。该方法超越了传统的风险管理理念，对安全技术能带来的好处进行了探究，在提升客户价值、激活商业新机会、保护品牌、避免负债等方面能帮助企业制定发展战略。

微软公司的理想就是通过强大的软件推动人类进步——任何时间、任何地点、在任何设备上这些软件都存在，这样的目标使得我们在寻求创造性解决方案时，必须把眼光投向技术之外。本书还要求你在考虑信息安全的时候要有远见。除了技术，还应该包括远景、人力资源以及商业活动的全新方法等。

克雷格·蒙狄

微软公司先进策略部高级副总裁

2001 年 3 月

致 谢

在此我们要特别感谢下面这些企业领导者，他们接受了与本书内容相关的访谈，对本书的完成起到了重要作用。他们分别是 Michael Capellas，John Charters，Gary Dilts，Ellen Hancock，George Keyworth，Rhonda MacLean，William Malik，Terry Milholland，Craig Mundie，Peter Rosamilia，Richard Sarnoff，Howard Schmidt，Stratton Sclavos，Mark Walsh 和 Peter Weiss。他们针对安全性的富有洞察力的评论和观点使我们获益匪浅，也使本书质量得到了有力保证。应当感谢我们的同事 Brian Ambrose，Barbara

Carbone, Mark Carleton, Kevin Coleman, Clen Davison, James Devaul, Bradley Fisher, Carl Geppert, Larry Kelsey, Shahed Latif, Danny Le, Mark Lindig, Robert Litt, Gary Lord, Jack Miller, Tom Moser, Gene O'Kelly, Michael O'Malley, Tim Pearson, Gary Riske, Ed Rodriguez, Greg Russo, Ron Safran, Terri Santisi, Ted Senko, Frank Taylor, Henry Teng 和 Al Van Ranst，由于他们的努力和帮助，我们的想法才得以付梓成书。我们还要感谢本书的编辑 Marie Glenn，她为本书的出版做了大量工作；还有 Eric Fisch，也为本书提供了许多有价值的帮助。

是他们，证明了安全性问题普遍存在，因而本书的主要内容就是围绕安全性而展开的。再一次对他们表示感谢！

玛丽·帕特·麦卡锡

斯图亚特·坎贝尔

2001 年 3 月

导言

对电子交易和电子商务而言，互联网安全吗？显然，这很难说。谁都知道，无论在哪里，房子和汽车的安全性总是有好有坏，惯偷一般喜欢偷那些防护措施少、安全性能差的。即便是第一次偷东西的小偷，也会避开那些明显有防护措施的目标，转而去偷方向盘没有加锁的汽车，或者既没有报警系统也没有看家狗的房子。

因此，问题不在于互联网是否安全，而在于企业及其网络赖以存在的基础是否安全，这是一个很有挑战性的问题。企业环境的安全包括两方面问题——网络环境和物理

环境。如果一个人很容易就能进入企业里面，并从一台联网计算机上下载敏感数据，这种情况下即便网络安全系统再好又有什么用呢？而这种事件发生的可能性要远比你想象的大得多。

从另一个角度来说，企业到底需要多高的安全级别才行呢？对需要进行电子资金转账的企业和通过网络销售图书的企业，解决方案不可能完全一样。对需要通过网络进行患者病历记录交换的医疗机构和医药中心而言，需要注意保护个人隐私；对拥有客户信用卡信息的信用卡公司来说，则需要防止信用卡信息被盗。另一方面，对于大型汽车制造企业来说，如果想通过一种通用网络对供应商之间的关系进行整合，又该如何进行呢？这种通用网络应该具备多高的安全性才能保护其知识产权、竞标信息以及其他对竞争至关重要的信息呢？

显然，每家企业都有自己的特殊情况，同一领域的企业也是如此。它们所处的地理位置不同、员工不同、品牌不同、知名度不同、产品不同，客户群也不一样。Amazon 或 eBay 能在安全性得不到保证的情况下就投入运营吗？E*Trade 能行吗？英特尔或思科公司的客户和供应商在没有安全保证的情况下会加入它们的电子商务转账业务吗？在这种情况下，安全性是保证这些公司扩展业务和降低操作成本的“激活器”。

什么东西对企业构成的威胁最大？企业的缺陷是什

么，它们会影响企业的哪些资产？企业的哪些部分可能面临风险？对这些问题的回答就构成了企业的风险分布轮廓。要建立适当的企业安全环境，首先必须弄清楚风险是什么。

本书主要讲述与企业安全相关联的所有问题，对评估安全漏洞的一些现有方法和工具进行了详细描述，并引导读者学会在现有安全环境中寻找解决方法，使企业现在和将来的安全需求能得到满足，并具有最大可升级性和最小分离性。

如果不限定时间，不限制预算，谁都可以构建滴水不漏、完美无缺的安全环境。可是用相对较短的时间和有限的预算，我们也一样可以构建一个适度的安全环境。本书将使你在构建企业安全环境的时候清楚自己需要做什么样的工作。

没人愿意让自己的企业“倒退”，我们都喜欢“前进”。但有些时候，恢复原状是我们惟一可做的事，不过这不是我们要讨论的主要问题。如果你能够对系统进行安全检查，毫无疑问，企业肯定已经被“攻击”了。许多攻击没有引起重视，被简单地忽略了，可是这些攻击就像是窃贼在你房门把手和在窗户上进行的试探性敲打，是攻击者对企业网络安全性能的试探。一项调查报告显示，在过去的12个月里，90%的被调查企业在它们的系统中发现了计算机攻击事件，其中273个被调查企业的经济损失总

数高达2.65亿美元。如果你的企业安全系统从未被黑客攻破，那你和你的企业很幸运，可是你能保证它将来也不可能被攻破吗?

你需要建立防御系统阻止外部和内部的入侵，需要提高入侵检测的效率和速度，并使用可靠人员来进行技术管理，同时你还需要制定一套有效方案以减少系统崩溃或毁坏带来的损失，并尽可能进行补救。如果所有工作都做了，而且做得很好，这时一旦有人问你："企业的网络系统安全吗?"你就可以回答："很安全!"

目录