“Lord Kelvin有一句名言‘你不能改进你不能测量的东西’。计算机安全一直信守着这个令人遗憾的说法，为欺骗、恐吓留下了太多的空间。Andy的书补救了这个问题，他非常清楚地告诉我们度量是必要的，也是可能的。现在购买这本权威的书，有助于终止有关安全方面的许多废话。”

——Gary McGraw，Ph.D.，CTO，Cigital，《软件安全：内建安全》（“Software Security：Building Security In”）的作者

symantec. press

网络安全专家

安全度量

SECURITY METRICS

Replacing Fear,Uncertainty,and Doubt

——量化、分析与确定企业信息安全效能

[美] Andrew Jaquith 著
李冬冬 韦 荣 译
飞思科技产品研发中心 监制

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

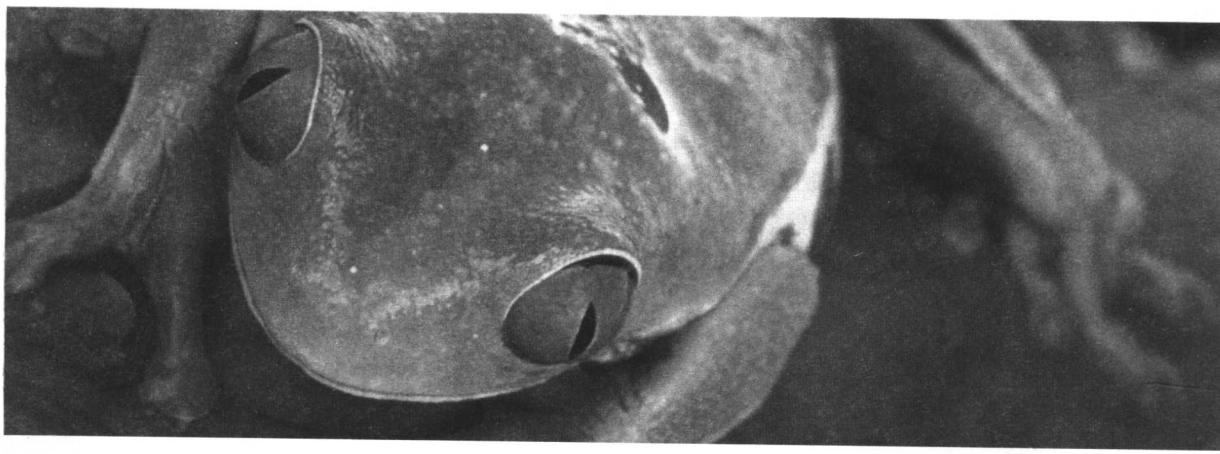
网络安全专家

安全度量

SECURITY METRICS

Replacing Fear, Uncertainty, and Doubt

——量化、分析与确定企业信息安全效能



[美] Andrew Jaquith 著
李冬冬 韦荣 译
飞思科技产品研发中心 监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

本书译自 Andrew Jaquith 编写的《SECURITY METRICS》。本书全面细致地介绍了在现代企业的环境下，如何量化、分类及度量信息安全操作。作者结合自己为软件、航空航天及金融服务等行业提供信息安全咨询过程中所积累的经验，通过图表、图形和案例的形式，准确而生动地说明了如何基于组织的特定需求来创建有效的度量、如何量化难以度量的安全事件、如何收集并分析所有的相关数据、如何确定企业的安全措施的效力，以及如何为高层管理者提供有用的消息。本书是企业定义、创建和利用安全度量的全面最佳指导，能够有效地帮助企业建立度量信息安全效力的解决方案。

本书题材新颖，内容翔实，适合于从事信息安全相关的工程技术人员、企业管理人员阅读，也可作为信息安全专业学生和科研人员的参考资料。

版权贸易合同登记号 图字：01-2007-3438

图书在版编目（CIP）数据

安全度量：量化、分析与确定企业信息安全效能 /（美）詹奎斯（Jaquith,A.）著；
李冬冬，韦荣译.—北京：电子工业出版社，2007.12
（网络安全专家）
书名原文：SECURITY METRICS：Replacing Fear，Uncertainty，and Doubt
ISBN 978-7-121-05405-1

Ⅰ. 安… Ⅱ.①詹…②李…③韦… Ⅲ.企业管理－信息系统－安全技术 Ⅳ.F270.7

中国版本图书馆 CIP 数据核字（2007）第 178571 号

责任编辑：宋兆武　侯丽平
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1000　1/16　印张：18　　字数：302 千字
印　　次：2007 年 12 月第 1 次印刷
印　　数：5 000 册　　定价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

从 Kelvin 的“当你不能通过数字表达的时候，你的学识便是贫乏不足的”和 Maxwell 的“测量就是求知”到 Galbraith 的“度量激发”，都说明有必要讨论一下关于数字的话题。毫无疑问，你之所以拿起这本书，是因为对“安全需要数字”这一观点的支持。

但是需要什么样的数字呢？这正是问题之所在。我们所需要的数字要能够说明一些问题，不但能记录我们来自何处，而且能指明我们要去向何方。可我们不得不承认统计学家的核心信条：所有的数字都存在偏差，问题是你能否更正它。作为安全相关的从业人员，我们必须清楚我们的立场：安全是手段，而不是目的。我们要与倡导者、学者分享一个观点：“最好”绝不可能是“好”的敌人。所以，让我们从放下对本书及本书评论者的偏见开始吧。

在“The Book of Risk”一书中，Borge 提醒并教导我们：“风险管理的目的是改进未来，而不是解释过去。”不管是翻开了往日记录的文字，还是虔诚地立于墓地前缅怀往昔，过去都是一段美好的回忆。但是对于现在的我们及本书，都不能够沉湎于不能弥补的过去。我们需要管理风险，寻求最佳的切入点，一方面接受不可避免的风险，另一方面竭尽所能与之抗争。Borge 理解得更深刻：“风险管理意味着采取预防措施努力去影响事件发生的概率——提高有益事件发生的概率，降低影响恶劣的事件发生的概率。”这正是对你我工作的描述：努力去影响事件发生的概率。我们需要提醒自己的是：我们的对手也深明此理，他们也在努力地影响事件发生的概率。

为了改变概率，必须弄清楚这些概率到底意味着什么，我们应当能够检测在我们影响下概率的变化。为实现这一目标，就需要安全度量。对安全度量的描述如下：

> “风险管理是为做决策服务的，而安全度量是为风险管理服务的。所以，我们所感兴趣的安全度量是对管理风险所做的风险决策的支持。”

如果你对此有异议，那么本书将不适合你。我想不用问，Andrew 也会同意这一观点，他和我一样不愿浪费时间向与数字无关的人去解释数字是什么东西。在这里我说得比 Andrew 更直截了当一些，但是你也不要失望，恰恰相反：这只是

属于谁的任务的问题。生命中的失望与差异不是你所负担不起的奢侈品，让我称赞你的明智吧，不要争论上述的观点了，也许在某一方面你是对的。

现在我们明白了数字虽有所不足，但却是必不可少的。作为决策的前期参考材料，需要很好地理解它。我们要细心地定义所要测量的内容，以确保读者能够理解我们所测量的到底是些什么。数字不被理解会引起误导，它与安全一样是手段而不是目的，它展现了计算机系统的脆弱点，如计算机系统在远程或者本地因疏忽大意造成的误用等。数字就像是外科医生手中的解剖刀，能救人也能伤害人，但我们需要它。正如 Fred Mosteller 所说："用统计数据说谎很容易，可离开了统计数据，说谎就更容易了。"

2003 年 11 月，计算机研究学会（CRA）发起了数字安全领域的"重大挑战"，并得到国家科学基金会（NSF）为期 10 年的资助。其内容为：

- 杜绝未来的大规模流行病。
- 开发认证系统的有效工具。
- 完成低技能要求的安全必备设施。
- 量化信息风险管理达到金融风险管理的层次。

最后一点正是我们的目标。我们要把安全舞台从金融市场推向其他领域：我们要理解、量化、测量、记录、包装、折中数字安全风险，就像金融服务部门所处理的其他风险那样有效。

在金融界有"风险值"（VaR）这个概念，常用来表示一个银行可能受到损失的程度。风险值有其固有的缺陷，但其核心思想是对风险有一个控制目标，对你与该目标距离多远有一个度量。我有幸纵观了银行风险值的整个计算过程。那天最后，首席经济学家斜靠着他的工作台对他的同事说："现在你该问问自己为什么这一切都生效了。（耐人寻味的停顿）之所以生效是因为你了解了所有你面临的风险！"那一刻我灵光一闪，意识到什么人将承担什么风险这个问题。我们不能完成真正意义上的风险值计算，不能满足国家科学基金会所提出的重大挑战，除非我们找到一个为这场比赛打分的方式。

无论何种比赛，如果没有打分的方式，作为一个选手你就无法提高你的成绩。这就是我们今天所处的困境：没有打分的方式，没有提高的途径。这不单单是一个失败，其本身就是一个风险所在。如果我们不能在测量、打分、理解风险上取得长足的进展，不能通过支撑有关风险的决策来改变事件发生的概率，后果将不

堪设想。如果我们不能够测量风险、预测其后果，公众将通过立法简单地把所有的风险归罪于一些倒霉的家伙。如果指定的风险责任没有把倒霉的遭罪者置之死地，那么从此他们也将后继无人。坦白地说，数字领域及因特网本身的改革正是这里争论的问题。如果我们找不到测量安全问题的方式，恐怕我们的选择会变得更艰难。

有人也许会说需要的不是度量而是规范，也有人会说答案在于吸引安全投资的力量——即如果这像一场军备竞赛，实力雄厚的一方最终会取胜，因为相对于对手他们花费得更多。在物质的世界中，这也许是对的，不过这种想法在数字世界中便是种危险的错觉。在数字世界中，防御者成功的原因在于：总结到的攻击方法占攻击者所拥有的攻击方法的比例大，并且防御方法比攻击方法更复杂。攻击者成功的原因在于：在老的攻击方法失效之前发明新攻击方法，同时其复杂性必须能够保证新攻击方法层出不穷。

这种不对称性不允许“较对手投入更大”策略的存在。2001 年 10 月 23 日，即 911 事件 6 个星期后，美国首席经济学家 Morgan Stanley 在纽约时报（New York Times）上撰文分析说：“未来十年将需要全民公投来决定是否把整个生产力的增长都用于安全方面的花费。”这也许只有美国和某些国家能够承受得起，但是如果真的这样做，无论是我们自己还是我们的对手，安全都会成为创造财富的最大障碍而制约了财富创造。这一点是我们乃至任何人都无法接受的！

鉴于上述原因，数字安全的法则便是代价的有效性，以及在度量支持下的对代价有效性的分析，所涉及的度量包括输入与输出、状态与比率、前期与后期等方面。数字安全领域最大的需求就是定义好到底要度量什么内容，以及在此定义下的度量方式。但这也不会产生什么奇迹，人类的天性可以保证：单纯的计算处理会带来不安全，这是早已被理论和实践证明了的，但这些证明并不能改变人们的行为，公众消费者依然期望有技术性的设备，而这正中了设备销售者的下怀。但对于在此领域实践的我们，必须找到一种度量的方式，这样才能够管理身边日益增加的风险。朋友们，“逆水行舟，不进则退”。显然我们做得还不够，因为我们连现状都无法维持。

我热切地盼望 Andrew 能在此书中掀起一股有关度量的热潮，去完成定量信息风险管理的重大挑战，就像金融界的兄弟姐妹们所希望的那样，保护好每一台需要保护的计算机。也许这些要求对某些人会过于苛刻，但是对我来说，宁可在

此领域中奋斗，也不愿忍受那些纷繁复杂的竞赛，而那些不必要的复杂性都是刻意制造出来的陷阱。我们要管理风险，用最小的代价换取最高的安全控制，而不是等待那些可怕后果的到来。

亲爱的读者，你的机会来了，就算不积极参与，至少也要当一名被动的消费者吧。Andrew 写这本书的时候已经料想到你所要说的“不可能做到”甚至是“根本没人会做这些”。在本书面世之时，所有的这些借口及极端的偏见都将终止。我们不能在空想上浪费时间。从这里开始吧，我们已经无法用语言来形容了，怎么说都是不够的。如果你想要做一个英雄，让一些书来做你的奠基石吧，本书正是你所需要的！

马萨诸塞州剑桥大学
Daniel E.Geer，Jr.，Sc.D
2006 年 11 月

前　言

本书内容

本书讲的是安全度量问题，即在现代企业的环境下，如何量化、分类，以及度量信息安全操作。

本书来源

每个顾问都会通过积累一些暗喻、类比及巧妙表述来显现他们的价值。这有助于解释和说明顾问们为使咨询事项得以顺利进行而所做的简单事情。我所喜爱的且与所说的话题相关的一点是：

任何美好的事物都会有缺陷。

简单地说，就是付出努力的同时也会伴随着很多意想不到的（往往是不想要的）结果。这句话同样适用于“安全度量”领域。正如你所想，我将要告知你的是我坚定的信念：安全度量应该是一个非常严肃的研究领域，但其本身也带有固有的缺陷。

几年前，我和几个同事对应用安全的课题进行了一系列详尽的实验研究。我们严格地采集和筛选了大量的原始材料，集合并分析了结果数据，建立了特殊的数学模型，撰写了此课题的研究论文，完成了一些可视的图表。这项工作得到了消费者和媒体的认可。此后，我受一些出版行业的邀请，通过因特网简单地介绍了我们的研究结果，该网络版的资料包括一些演示文稿和录音说明。主办者给我选定的听众包括 CSO（首席安全执行官）、技术专家和决策者。

这听起来很棒，本书的出版将给全世界无数喜欢在网上冲浪的人留下深刻的印象，我很高兴有机会参与其中。另外，我的内心非常希望大部分听众都能给我发 E-mail 或者信件，使我们从中得到所需要的分析技术、广泛的数据，以及许许多多闪光的观点和看法。可是我错了，我不但没有得到学术界的赞许，而且收到一些类似这样的信件：

“好棒的介绍啊，但是我还是希望能看到更多的‘投资回报率’度量。你也该明白，我真的很需要说服我老板让他帮我买些小部件_____（填空）。”

还有一些更让人烦恼的评论，例如：

“我们没有资金投入我们的安全规划！可怜我吧，我需要更多的投资回报率（ROI）。帮帮我！”

坦白地说，这里我有一点点添油加醋，我所提到的第二封 E-mail 没有那么可怜。但是主题已经很清楚了，听众把“安全度量”当做是投资回报率（ROI）了！我们神奇的度量是一个好事物，但是无法实现听众的期望是其固有的缺陷。

本书目标

可惜的是，“安全投资回报率”追随了 Macarena（20 世纪 60 年代一个流行音乐组合）的道路。但是，绝对可以肯定的是：你的期望是可以管理的（为你提供更多的咨询）。这就是本书的目的所在。

本书的首要目的在于从数量上分析信息安全行为。以下章节提供了如何使用度量来阐明一个组织安全行为的方式。

- **测量安全：**度量传统意义上难以测量的行为事件。
- **分析数据：**都存在些什么类型的安全数据源，你怎么让它们为你所用。
- **得出结果：**整合经验数据使其形成连贯的信息集合的技术。

这类书要叙述些什么已经清晰起来了。安全是需要管理的少数领域之一，而这些管理不能为度量提供便于理解的技术手段。例如，在后勤学中，“每公里的运费”、“仓库货物流转的总量”可以帮助操作人员理解运输消耗和仓库运转的效率；在金融学中，“风险值”是在历史价格波动的基础上，计算一个公司未来某个时间点可能损失的资金量。相比之下，安全具有……实际上一无所有。对安全的关键指标并没有达成一致的认识。

安全度量方面缺少一致的认识，部分归咎于与安全相关的文化。例如，遭受黑客攻击的公司不会公开讨论安全事件；同样，部署了正确安全措施的公司也不说话，以免窥探的目光出现在他们的防火墙堡垒外。只有在保密协议（NDA）下或者内部小团体范围内才会发表一些言论。所以，本书的第二个目标，是记录一些肩负起严格度量安全行为事件责任的公司所做的有效实践。

非本书目标

本书首要内容是量化安全行为，它确定了度量大多数企业很看重的安全过程的方式。我所提到的度量法和分析技术部分来自于我的设计，提炼于我为软件、航空航天及金融服务等行业提供咨询过程中所积累的案例。我遇到很多已经开始编写他们自己的度量程序或者对安全度量法充满热情的人们，并和他们进行了交流。最低程度，我希望你能把本书看做是对当前安全测量实践的综合。

“实践”一词是至关重要的。我小心地挑选了这个词是因为它无形中与其反义词“理论”形成对比。在本书中，你会看到许多案例、度量列表及测量安全事

件的方式等。但我只用很小的一部分篇幅涉及安全风险建模——它是用来找出哪个风险或者威胁是需要担心的。风险评估是众多学者所关注的领域。聪明的人们花费大量的精力去研究威胁建模、安全策略效力建模，以及模拟周边防御。

所以非本书目标的内容首先是企业风险建模和评估。这是每个企业都要努力承担的，但其特定技术不是本书所涉及的范围。风险评估是组织的具体行为，我可不想花费大半的篇幅去否认某些事情，因为“这些事情取决于组织本身觉得哪些是最重要的风险”。此外，我也不想为已经非常丰富的风险建模和评估工作再添砖加瓦。

我还要添加三项意义重大的非本书目标的内容。缺乏可被广泛接受的安全度量意味着不谨慎的销售者们可能要大出血了，中层管理者为了其自身的目的，也会迅速决定利用这些度量。所以，本书与下列内容无关。

- **预算理由：**怎样说服你的老板在安全上花钱。如果你所在的公司还没有计划在安全上面花费资金，这可能存在着比缺乏统计更深层次的问题。
- **恐惧、不确定与疑虑（FUD）：**怎样滥用、误用数据制造安全恐怖事件。我对此没有兴趣，这让我感到低级庸俗。
- **有趣的金钱：**与“安全投资回报率”相关的所有话题。除了安全效力不确定的度量之外，ROSI（安全投资回报率的缩写）和经验式的安全度量是不相关的。

当然，人无完人，本书也有考虑不周的地方。但是正如安全分析学者所说，那是值得一试的风险。

读者

本书面向的是两类截然不同的读者：安全从业者和听取他们汇报的领导。从业者需要清楚度量的方式、内容及时机；而他们的老板需要知道该期待什么。安全领域之所以抵制度量不为别的，正如一家普通金融服务公司的安全管理者跟我说的：“我的老板都不明白我每天所做的工作，他能够理解的只是数字。”在从业者与管理层之间的鸿沟上架设桥梁，这就是本书致力完成的任务。

内容简介

本书共分为 8 章。

第 1 章，“绪论——摆脱无尽的困扰”：今天，安全度量的现状总是围绕着漏洞的检测与消除打转，就像实验室的老鼠围着轮子转一样没完没了。把安全看做

一个循环的零和博弈[①] 削弱了我们清晰思考的能力。本章提倡用度量这一指标代替“仓鼠轮子”，来测量关键安全行为事件的有效性。

第 2 章，“定义安全度量”：本章描述了度量法的原理，说明了迫使人们接受它的商业压力，推荐了一些评估度量法好坏的标准，并提醒我们不要转移注意力，使用不好的度量。

第 3 章，“诊断问题和测量技术安全”：不同企业测量安全行为事件的差异，在于不同的需求和内容。本章罗列了企业常用做诊断安全问题的各种测量类型，包括对各种主题的实际度量法，如覆盖与控制、基于口令的漏洞管理、隐藏路径、得分基准及业务调整风险等。

第 4 章，“度量计划效力”：除了纯粹技术上的安全测量，组织机构需要测量战略安全行为事件的方法，来追踪安全回报和执行效果，以及测量当前安全组织的效力。本章列出了一些应用 COBIT 框架作为组织原则的计划层面的度量法。

第 5 章，“分析技术”：为创建度量，分析者需要把原始的安全数据转换成语义丰富的数据。本章描述了排列、集合和分析数据以抓住主要语义的基本技术。本章也描述了先进的分析技术，如交叉分析法和四分位数分析法。

第 6 章，“可视化”：如果不能有效地被展示出来，即使是最有说服力的数据也会变得毫无意义。本章展现了众多的可视化技术，从最简单的表格到二维栅格，再到复杂的“小型多重（small multiple）”图表。

第 7 章，“自动度量计算”：大部分企业有很多安全数据可用，但是他们常常会陷入专用工具和信息孤岛的陷阱中。本章提出要找到合适的数据来源，包括防火墙日志、杀毒软件日志和第三方审计报告。本章还描述了一些技术，用来把获得的数据转换为便于汇聚和报告的格式。

第 8 章，“设计安全记分卡”：一个组织收集并分析了其安全度量之后，就剩下最后一个步骤了，创建一个记分卡记录所有的事情。本章列出了几种可选的方法来设计安全“平衡记分卡”，这些卡能够简捷地、全面地展现组织的安全效力。

除这些主题以外，本书还包含了一些我个人经历过的或者采访获悉的奇闻轶事和战争故事。

感谢你购买本书。希望你能像我享受其创作过程一样享受阅读过程。

---

①原文为 zero-sum game，零和博弈。又称零和游戏，是博弈论的一个概念，属非合作博弈，指参与博弈的各方，在严格竞争下，一方的收益必然意味着另一方的损失，博弈各方的收益和损失相加总和永远为“零”。双方不存在合作的可能，零和博弈的结果是一方吃掉另一方，一方的所得正是另一方的所失，整个社会的利益并不会因此而增加一分。——编者注

致　谢

那是个风雨飘摇的夜晚，回想在 2006 年的感恩节，我所写下这些文字的时候，记忆里是一片狂风骤雨。可这天气算不了什么。上天赐予了色氨酸、馅饼和调料等食物，使我不用关心窗外的大雨！

用食物来打比方似乎很适合现在的状况——不单是因为场合，而是因为它让我想起了有关安全度量方面的一些无奈。努力地去完成这本书，夸张地说，就像是要吃掉一头大象，唯一的方式就是一点点地啃。

初次接触这头“大象”是在我就职于@stake 公司的时候，@stake 公司是一家创建于 1999 年的网络安全顾问公司。我有一个快乐的小个子女同事叫 Heather Mullane，她是市场部的事务策划。Heather 是一个完美的同事——准时、高效、细心，她的工作总是按时完成，她的桌子总是十分整洁。我和一些爱开玩笑的同事总喜欢把她的订书机和录音带藏起来捉弄她。当然，她总是能发现什么东西不见了，并向我们兴师问罪。

在@stake 公司的一个低潮时期，Heather 被裁员，之后她去 Addison-Wesley 当了一名编辑助理。但她还和我们保持联系，有时候她还穿过 Charles 河来看望我们。几乎每次她都鼓励我去写作，经常问“你什么时候开始写本关于度量的书呢”，还把我介绍给一些编辑认识。这样持续了两年，我终于投降了，开始为您所拿着的这本书工作。Heather 最终还是离开了 Addison，结婚并移民到西部去了。我跟她失去了联系，但她推荐了我，真是想得太周到了。谢谢了，Heather，谢谢你好心的“纠缠”。

本书是几年来努力观察和反思如何将数字融入信息安全的结果。主要是在开始和修补上取得一些进展，大部分是修补上的进展。虽然我的名字写在了封面上，但这本书并不是我独立完成的。我特别要感谢 Betsy Nichols 所做的贡献，她是第 7 章“自动度量计算”的主要作者。她的公司 Clear Point Metrics 在自动度量定义、收集、汇聚和报告实例等方面做了大量工作，我本人极力推荐他们的产品。此外，第 2 章“定义安全度量”的前半部分，受益于 IEEE 的文章“The Future Belongs to the Quants”，这是由 Dan Geer、Kevin Soo Hoo 和我联合撰写的。

第 3 章“诊断问题和测量技术安全”和第 4 章“度量计划效力”所提到的众

多度量法得益于平时和我一起讨论的专家们。他们是 Jayson Agagnier, Jerry Brady, Rob Clyde, Mark Curphey, Dennis Devlin, Royal Hansen, Mark Kadrich, John Kirkwood, Pete Lindstrom, Rhonda MacLean, Tim Mather, Besty Nichols, John Nye, Gunnar Peterson, Tom Quinn, Kevin Soo Hoo, Andrew Sudbury, Phil Venables, Phebe Waterfield, Bob Westwater 等。他们都很耐心地接受我的拜访，告知我大量的信息，或者用他们的经历来启发我。2006 年 8 月，我参加了在温哥华举行的 MetriCon 1.0 发布会，与会的有 securitymetrics.org 250 位正式成员，他们也充当了我的智囊团。

吃掉一头大象的后果就是消化不良。我有幸与一个编审团队共事，从大量地收集文献资料到消化这些文献资料，他们帮我把关并整理我即兴写出的零散文稿。当我弄错一些事情的时候，他们会加以改正并就如何使材料更加易于理解方面提出宝贵的意见。他们是 Olivier Caleff, Alberto Cardona, Anton Chuvakin, Fred Cohen, Mark Curphey, Dennis Devlin, Alex Hutton, John Leach, Dennis Opacki, Jon Passki, Adam Shostack 及 Chris Walsh。真是谢谢你们了！

第一次从事写作的我在创作过程中往往会喋喋不休并有点神经质。为他们的耐心和包容，我要感谢 Addison-Wesley 的全体员工：Jessica Goldstein, Romny French, Karen Gettman, Kristin Weinberger 及 Chris Zahn。另外，我还要感谢一直给我支持的 Linda McCarthy（Symantec），Steve Mulder（Muldermedia），Becky Tapley，容易忘记的 Catherine Nolan，以及我的父亲和兄弟 Russ。虽然 Russ 的工作与安全行业毫不相干，但是他试读了我某一章的手稿，还边看边赞不绝口。这可让我放心了，书上的错误，大部分读者都会发现但不会介意的。

最后我要感谢一位特别的朋友 Dan Geer。他长发络腮、能言善辩、熟悉度量、充满活力，是位出色的诗人，而且很仁慈。他就像一位好老板：把我放到能让我成功的位置。我要感谢他激发我对安全度量的兴趣。我希望本书能够得到读者的支持。

马萨诸塞州波士顿

Andrew Jaquith

2006 年 11 月

作者简介

Andrew Jaquith 是 Yankee Group's Enabling Technologies Enterprise 组的项目经理，是合规、安全和风险管理方面的专家。Jaquith 建议企业客户如何在其环境下管理安全资源。他也帮助安全销售者开发影响企业客户的策略。Jaquith 的研究方向有安全管理、风险管理，以及基于网络的打包和定制应用。

Jaquith 有着 15 年的 IT 从业经验。在加入 Yankee Group 前，他创办了被 Symantec Corporation 誉为 2004 年安全顾问先驱的@stake 公司，并担任其项目主管。在此之前，Jaquith 曾在 Cambridge Technology Partners and FedEx Corporation 公司担任项目经理及业务分析员。

他的应用安全和度量研究收录在 CIO，CSO，Information Week，IEEE Security and Privacy 和 The Economist。此外，Jaquith 对一些安全相关的开源项目也做出过贡献。

Jaquith 拥有耶鲁大学颁发的经济政治学的硕士学位。

目 录

第 1 章 绪论——摆脱无尽的困扰

1.1 风险管理的混乱……1
1.2 度量替代风险管理……5
1.3 本章小结……6

第 2 章 定义安全度量

2.1 安全度量业务驱动……10
2.1.1 数据共享的障碍……11
2.2 安全度量建模……12
2.2.1 模型 VS 度量……13
2.2.2 质量保证理论……15
2.2.3 公共卫生术语和报告结构……15
2.2.4 证券管理……16
2.2.5 加速失效测试……17
2.2.6 保险业……18
2.3 怎样才算好的度量……19
2.3.1 “度量”定义……20
2.3.2 一致的度量……22
2.3.3 易于采集……22
2.3.4 以数值或者百分比的形式表示……23
2.3.5 最少使用一个度量单元来表达……24
2.3.6 特定的前后关系……24
2.4 怎样才算不好的度量……25
2.4.1 不一致的度量……25
2.4.2 不能廉价地采集……26
2.4.3 不能用基数和度量单元来表达结果……26
2.5 什么不是度量……27
2.5.1 安全分类的误用……27

2.5.2 年损益预算……30
2.6 本章小结……35

第 3 章 诊断问题和测量技术安全

3.1 使用度量来诊断问题：案例学习……39
3.2 定义诊断度量……41
3.3 安全和威胁边界……43
3.3.1 电子邮件……45
3.3.2 反病毒和反恶意软件……46
3.3.3 防火墙和网络边界……46
3.3.4 攻击……47
3.4 覆盖和控制……48
3.4.1 反病毒和反间谍软件……53
3.4.2 补丁管理……53
3.4.3 主机配置……56
3.4.4 脆弱性管理……59
3.5 可用性和可靠性……62
3.5.1 正常运行时间……63
3.5.2 系统恢复……64
3.5.3 变更控制……65
3.6 应用程序安全……66
3.6.1 黑匣子缺陷度量……68
3.6.2 定性过程度量和指标……69
3.6.3 代码安全度量……75
3.7 本章小结……79

第 4 章 度量计划效力

4.1 使用 COBIT、ITIL 和安全框架……82
4.1.1 框架……83
4.1.2 没有作用的事情：资产估价……86
4.2 计划和组织……89

4.2.1 评估风险 90
4.2.2 人力资源 91
4.2.3 管理投资 92
4.3 获得和实施 94
4.3.1 确定解决方案 94
4.3.2 安装和鉴定解决方案 96
4.3.3 开发和维护步骤 100
4.4 交付和支持 100
4.4.1 教育和培训用户 102
4.4.2 确保系统安全 105
4.4.3 确定和分配费用 107
4.4.4 管理数据 109
4.4.5 管理第三方服务 111
4.5 监视 112
4.5.1 监视过程 113
4.5.2 监视并评估内部控制 114
4.5.3 确保制度合规 115
4.6 本章小结 116

第5章 分析技术

5.1 平均值（平均数） 121
5.2 中值 122
5.3 标准差 123
5.4 分组和聚合 125
5.4.1 记录和属性 125
5.4.2 分组 128
5.4.3 聚合 128
5.5 时间序列分析 130
5.6 交叉分析 132
5.7 四分位数分析 134
5.7.1 四分位数汇总统计 135