Mc Graw Hill Education

IT SECURITY METRICS

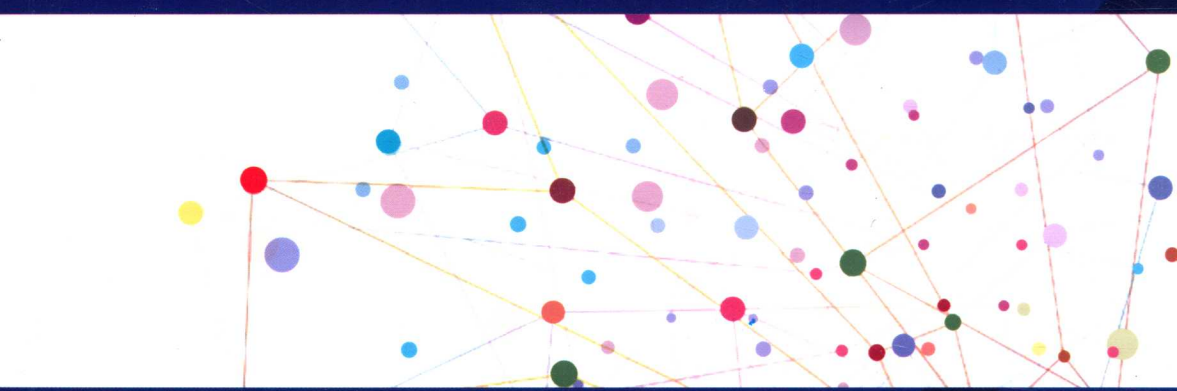
A Practical Framework for Measuring Security & Protecting Data

信息安全度量

用来测量安全性和保护数据的一种有效框架

〔美〕兰斯·海登（Lance Hayden）/著

吕 欣 王 标 于江霞 樊 晖 /译



北京大学出版社
PEKING UNIVERSITY PRESS

IT SECURITY METRICS

A Practical Framework for Measuring Security & Protecting Data

信息安全度量

用来测量安全性和保护数据的一种有效框架

〔美〕兰斯·海登（Lance Hayden）/著

吕 欣 王 标 于江霞 樊 晖 /译

北京大学出版社
PEKING UNIVERSITY PRESS

著作权合同登记号 图字：01-2013-4062

图书在版编目(CIP)数据

信息安全度量：用来测量安全性和保护数据的一种有效框架／(美) 海登 (Hayden，L.) 著；吕欣，王标译. —北京：北京大学出版社，2015.8

ISBN 978-7-301-26166-8

Ⅰ.①信… Ⅱ.①海… ②吕… ③王… Ⅲ.①信息安全－安全技术 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2015）第 185094 号

书　　名　信息安全度量：用来测量安全性和保护数据的一种有效框架
著作责任者　〔美〕兰斯·海登（Lance Hayden）著
吕　欣　王　标　于江霞　樊　晖　译
责任编辑　王　华
标准书号　ISBN 978-7-301-26166-8
出版发行　北京大学出版社
地　　址　北京市海淀区成府路 205 号　100871
网　　址　http://www.pup.cn　　新浪微博：@北京大学出版社
电子信箱　zpup@pup.cn
电　　话　邮购部 62752015　发行部 62750672　编辑部 62765014
印　刷　者　北京大学印刷厂
经　销　者　新华书店
720 毫米 × 1020 毫米　16 开本　19.25 印张　367 千字
2015 年 8 月第 1 版　2015 年 8 月第 1 次印刷
定　　价　58.00 元

致 Jayne 一直陪伴我患难与共的伙伴和朋友

致 Wyatt,你简直太酷了

序　言

如今，所谓的“没有测量就没有安全，”或类似像开尔文勋爵关于测量和结果之间的关系的最初宣言已成为老生常谈。不幸的是，很少有组织有效地遵从这一信条。在我看来，这是整个安全行业中最强有力的控诉之一；尽管控制框架、最佳实践以及指导在不断地扩大，但是似乎还没有人询问（引用风险分析测量专家道格拉斯·哈伯德的话），“我们怎么才能明白这个东西是否真的有用?!”

那么，在经历了近十五年对财富 1000 强组织的安全咨询后，我在这里要告诉你们关于信息技术安全的一个可耻的鲜为人知的事实：防火墙、漏洞扫描、入侵检测/防御系统，数据泄漏预防、应用程序安全、补丁管理、加密、数据安全标准条例……没有人真正清楚这些东西是否有用。信息安全对以上所列举的各项投入越来越大，但是论及测量投资回报率时，他们仍然像躲避瘟疫似的避开这一话题。现在数量可观的资金开始投入到安全领域上（例如：据我所知就有信息技术安全年均消费超过五千万的机构），如今时机已经成熟，是时候迎接挑战并深入探讨实用、相关、有效的安全度量了。

走进你手持的这本书，兰斯开启了一段深刻且以事实为依据的旅程，去探寻谁提出安全度量、安全度量的意义，何时、何地、如何以及为什么去建立这个度量指标。他阐明原理，打破了神话，为信息技术在定义、实施以及说明安全活动与投资的价值上提供了更好的方法。

在这本书中，我特别欣赏兰斯务实的方法：他碰壁的次数足以使他理解和懂得对度量的专业化历史性尝试。（如年预期亏损）但是他也明确知道，到目前为止我们所做的还不能提供有用的决策支持，而且对于处于各组织问责制和监督逐渐加强的年代，我们也不能非常清晰地表述出安全活动的价值。

与其他我读过的书相比，这是此书的不同之处：书中暗藏着一种令人耳目一新、给人启示的逆向思维，但同时也提醒人们对其加以辨别。往往急于改革和挑战现状的想法在技术领域有些极端，会使我们脱离一些基本原则，而这恰是我们赖以工作的基础。此书并未忽视这些基本原则，而且鲜明地植根于风险管理、决策支持和基本经济学的基本概念中。与此同时，人们认识到，今天安全专家的许多实践是大打折扣的（借用第一章的一个表述），并且“炼金术”常常为那些想要走捷径的“懒虫”以及为使观众所想听的为结果增色的“套期保值者们”所采用。介于石器时代和发展最前沿之间，我们开始感到迷失和困惑；这本书是带我们回到中间地带的简明向导，它提出了一个更具有实证性的方法去思索信息安全和衡量它的进程。

虽然“中间道路”和“安全度量”可能听起来很乏味，但这本书却完全不会给我

们这种感觉。书中运用了大量丰富的实例、轶事、隐喻、对复杂概念的清晰描述、与其他行业的类比，此外作者近似纯娱乐化的写作风格不会使你感到枯燥乏味。这些东西读起来一点儿都不费力——像泊松分布和蒙特卡罗模拟法这样能用于当今信息世界解决实际问题的工具，书中对它们的描述并不是牙牙学语般的搪塞，例证中也应用了实际的数学法来阐述它们在实践中是如何运作的。

这本书的相关性、信息量以及可读性都是一流的，作为一个有十多年经验的技术作家，我是很郑重地说。在阅读章节时，我“抄袭”了许许多多的好点子来运用到我自己的工作中，这成为我自己的个人价值与实用性的指标。《信息安全度量》销量屡创新高，我强烈地把它推荐给任何一位本着热忱、严肃的态度，精确、高效地保护数字资产的人。

Joel Scambray

与人合著《黑客大曝光》，Consciere 公司首席执行官

2010 年 4 月 25 日

致　谢

完成这本书，我要感谢很多人，因为没有他们就没有这本书。我爱我太太和儿子，感谢他们在我研究和写作过程中给予我的坚定支持。我每次研究都要连续工作数小时，他们对我的理解仍然让我感动，我感到非常幸运，因为有他们在背后支持我。

我要真诚地感谢我所有的以这样或那样的方式促成了这本书的同事。Doug Dexter、Mike Burg、Caroline Wong 和 Craig Blaha，他们写了极好的研究案例，这本书对各行从业者投入上获益极大。我也感谢 Joel Scambray，他融入了自己的想法和见解写了一个非常宝贵的序言。作为技术报告审核专员，Caroline Wong 肩负双重任务，我要感谢她在我写作中为我提供了许多见解和建设性的建议。书中几个主题来自 Mike Burg 和我在不同项目共同工作中的经历，我感激他花费大量时间给我反馈。也感谢在思科水疗中心团队的 Pablo Salazar，很多想法都是从我们就各种主题多次交流中产生的，如：关于其他行业的测量、将学术界成果转化到现实世界中、人类安全行为、“圆形监狱”和钱币学。最后我想真诚地感谢我在思科的上司 David Phillips，他坚定的支持和鼓励使这本书的问世成为现实。

这本书的许多概念和技术来源于我在得克萨斯大学奥斯汀分校做博士项目的经历，感谢论文委员会，尤其是委员会主席 Phil Doty 博士和 Mary Lynn-Rice Lively 博士，这些学者教我成为一名社会科学家和研究员。他们专注于定量或定性的研究方法，这种研究方法仅仅提出一个只有理解一半的问题，这让我印象深刻。得克萨斯大学信息学院是我多年来的学术之家，我想表达我对导师、同事、学生的感谢，他们一次又一次地拓宽了我的思想和经历。

我要感谢麦格劳-希尔的团队，这一团队使这本书顺利完成。感谢非常优秀的 Jane Brownlow 编辑和 Megg Morin 编辑，她们对本书满怀信心，并不断地提供建议和支持。项目协调员 Joya Anthony 为我们制定了严格的计划，保证我们如期完成目标。同时我还要感谢 Lisa Theobald 和团队里出色的编辑们，他们对章节编写的改进提供了敏锐的视角和很好的建议，感谢 Vasta Vikta Sharma 和在 Glyph 工作的每一个人，她们的付出保证了该书的出版。

最后，我想向给我启发的许多安全学者、从业者表达感谢之情，以及最终决定本书成功与否的读者们。我希望你们能对本书感兴趣并发现它的有用之处，使本书能作为另一种声音在以后关于测量和安全改进方面的讨论中发挥应有的作用。

译者序

中央网络安全和信息化领导小组第一次会议提出，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。如何去评判一个国家、一个行业、一个系统的网络安全态势，加强调控和能力建设，成为当前世界各国政府管理层、学术界和产业界关心的一个热点和难点问题。

安全度量是发现问题、判断形势、提出对策的基础，是加强网络安全管理的一项基础性工作。开展网络和信息系统安全度量需要解决三方面的问题：一是建立一个科学、可操作性强的指标体系，这些指标可以真实反映系统的安全态势；二是建立度量的方法学，以此为基础来推进安全度量的各个环节实施，以实现评价目标；三是度量结论可以服务于我们系统安全性能的改善和安全能力的提升，为决策层提供有效的信息参考。

网络安全度量的难点在于我们面对的网络信息系统的复杂性、不确定性和攻防双方信息的极大不对称性。正如本书作者兰斯·海登所说，尽管目前在网络安全领域已经建立了一些安全度量的方法，但很多度量都有其局限性并会导致某些安全性方面的问题。在本书中，作者系统阐述了什么是信息安全度量，谁来执行信息安全度量，如何设计有效的信息安全度量，以及如何用度量结果来支持决策。本书内容丰富，视角新颖，伴有相关应用案例，具有较强的实践应用价值。

我们在开展“信息安全保障指标及评价体系”专项课题研究过程中发现并认真学习了本书，并愈加认识到本书对于学习和开展信息安全度量具有重要的参考价值，深感翻译本书十分必要。因此，在北京大学出版社的大力支持下完成了本书的翻译。尽管翻译组的同志付出了大量的努力，反复讨论、认真论证，但基于水平限制，一定还存在一些不当之处，欢迎广大读者批评指正！

感谢何德全院士和国家信息中心有关领导对本书翻译工作给予的指导和支持。

本书的翻译工作得到了北京大学出版社陈小红主任，王华编辑的大力支持和帮助，在此表示诚挚的谢意。

本书所涉及的字母、公式和人名等，均沿用原著表示方法。

吕欣

2015 年 8 月

导　读

如果你想要一个好的测量问题，那么就去看《虎胆龙威》这部电影。这部电影的角色是由布鲁斯·威利斯和塞缪尔·杰克逊饰演的。杰克逊试图去阻止坏人，却发现自己置身于一个拥挤的公园之中，公园里有一个五加仑的塑料罐、一个三加仑塑料罐、一个喷泉还有一个威力巨大的炸弹。为了拆除炸弹，他们必须将四加仑的水（以不超过几盎司的误差）在一定的时间内放到称上，否则，每一个人都不得生还。当然，在他们意识到注重罐和规模是不够的，为实现必要的测量还需要一个精确的逻辑流程之后，他们才解除了这次危机。这一场景是壮观的，它包含一个测量挑战、一个可接受的误差、还有一个可能由于测量失败导致不可接受的后果。到最后，这个问题与度量关系不大（比如体积和重量指标），反而更多和探究决策制定的测量进程有关（是否冒着可能爆炸的危险把罐子放进去）。

信息安全性评估

这是一本关于测量过程的书，也是一本关于度量的书。越来越多的首席信息安全官以下的信息技术从业人员被指派去评估他们组织的安全和改善数据保护活动的效力。从对萨班斯—奥克斯利法案和数据安全标准的监管和产业规范到对由国家、跨国犯罪或恐怖组织构成的“高级持续性威胁”的讨论，信息安全显而易见正经历一场巨大的冲击，就连美国总统这样最具权威的人也参与进来了。回顾2009年美国网络空间政策，得出的结论是，美国的数字基础设施既不安全也不能防御持续的攻击。报告中给出的提高基础设施安全的一系列建议中，排列最靠前的就是需要实施更好的安全测量和度量。

这给我们提出了一个重要的基本问题：我们热衷评估的所谓的安全是什么？我们行业经常使用安全、风险、漏洞等词语，却并未首先定义一下这些术语的意义。我们常常听到这句口头禅，“要对自己的领域了解才能得心应手，”我同意这句话。但是如果你缺乏对所管控的现象进行定义或达成共识（例如，系统运行与人类行为），就直接进行度量，必然受挫或导致失败。如果数据是具体的且为每个人所接受，你对所测事物的理解也必须是具体的、一致的。

对岩石的理解

信息安全度量最难的工作源于努力去解释你想弄清楚的究竟是什么。毕竟，安全不是个有形的事物。让我们暂且先把安全抛在一边，考虑那些比较容易测量的事物如岩石。岩石测量似乎非常简单，岩石有高度、宽度和深度，你可以使用尺

子很容易地测量出来，把岩石放在秤上就能称出它的重量。如果安全测量有那么简单，并且一些安全维护人员所采用的测量方法正是你所想的，那么一切就太好了。但实际上岩石也具备复杂的测量特征，岩石有质量，它是不同于重量的，那么你该如何测量呢？岩石有化学成分和矿物学特征。岩石具有诸如碎石尺寸这样的特殊指标，它用于测量岩石个别颗粒的大小。并且测量岩石还有更多挑战性的指标。许多岩石兼具可以测量的社会价值和经济价值，尽管这些评估指标不能只从岩石的内在属性着手。

因此这印证了一个道理：即使是测量看似简单并且有形的物体都不是一个简单的事情。如果你不清楚你对岩石的哪一方面感兴趣，那么你在评估哪些指标将会增长你对岩石的了解或改进相应的决策时就会变得更加困难。这块岩石是掷向敌人更好还是把它擦亮打磨成一枚戒指更好呢？如果你为了保护自己的黄铁矿而向敌人投掷了一个 24K 的钻石，你可能会为此感到后悔。如果我们连测量岩石的过程和标准都难以达成一致的话——想象测量信息安全将会有多么的困难！

安全专家常常陷入这样一个陷阱里，即他们还没明白我们真正想要知道的是什么，就试图去评估安全。我们也许自以为知道，但往往我们的调查是过于简单的，只建立在我们的直接经验和先入为主的知识结构上。我们中有多少人在参与组织安全的讨论，结果后来（通常在方案实施的时候）却发现，每一位参与到讨论中来的人对安全的意义的想法千差万别。这一情况在企业安全经理与安全技术人员谈话时尤为常见。安全在业务上的定义不同于它在技术上的定义，因为一名财务分析师所熟悉和关注的事情常常与一名防火墙管理者所熟悉且关心的事情大不相同。

通过《信息安全度量》提高安全性

随着安全行业（职业）的成熟，以及安全被视为业务流程的核心，人们对这一流程的有效评估的需求在与日俱增。为了满足这一需求，信息安全技术的度量运动也在逐渐加强。这本书试图继续探讨安全测量，帮助你理解如何在组织环境中有效地使用度量指标。为此，我提出了一个框架，有助于在业务流程改进的背景下确定安全和安全度量，同时我希望能给你们提供一些信息安全测量的新方法，这些方法也许会有别于你在其他度量书中可能会读到的方法。

本书的组织结构

本书共分为四个部分，体现了全书的整体内容及各个章节的写作目的。我并没有把这些部分或章节作为独立的模块去写，而是自始至终以叙事的方式把各部分串联起来（当然，你不用非得从头到尾顺着去阅读，但这是我整本书的结构编排）本书的结构围绕着安全过程管理（SPM）框架展开，它是创建内聚性的信息安全度

量项目的通用方法，而这一度量项目将测量项目的战术和战略因素都考虑在内。因此，在其他条件相同的情况下，我建议你从头到尾地读完这本书，对于有些章节的概念介绍，如果你已经熟练掌握，就可以跳过。

我也诚邀了几名对度量的某个方面或多个方面颇有经验的行业从业者，他们的研究构成了此书的案例部分。每一部分都以案例的研究为结尾，多多少少都与特定章节的内容相关。这些案例研究用来说明我所讨论的是如何在不同情境和环境下呈现的，希望它们在测量安全上对你有所启发。

部分

本书由四个部分构成。

第一部分：介绍安全度量

第一部分讨论了信息安全度量的现状，批判了一些现存的安全度量以及关于应如何进行安全测量的偏见，提供了思考安全度量的新方法。这部分还介绍了数据的概念，这些数据在理解如何进行安全测量中发挥着重要作用。

第二部分：安全度量的实施

第二部分介绍了安全过程管理（SPM）框架和讨论了安全度量数据的分析策略。这一部分还探讨了安全测量项目（SMP）的概念—作为一个度量实践，这是上述框架的重要组成部分。

第三部分：探索安全度量项目

第三部分从目标、数据、到分析来讨论安全测量方案具体实用的实例。这些项目范例为读者提供了先前章节中所提及的概念的具体介绍，并说明如何去实施这些项目。

第四部分：安全度量之外

第四部分探索如何开展一个安全度量项目，并战略性地将其应用到不同的组织情景和环境下，其目标是实现持续性的安全改进。

章节

这本书的每一章节涵盖了与理解和开发信息安全度量和安全过程管理框架密切相关的具体材料。我尽力使章节的内容变得切合实际：我力图为我们正在谈论的问题提供具体的、可操作的例子，而不仅仅只是描述概念。我的目的是为了使读者能够形成这样的思想，即他们如何在自己的实践和组织的范围内实施这些概念。为此，各个章节都包含了方法、使用案例和工具的描述，同时它还能够展现模板和组织方面的因素。每一章节还包括总结以及就各章概念和主题相关的扩展阅读。

结束语

这本书终于诞生了。当我完成我的博士课程时，我越来越清晰地意识到——

我的同行可能受益于许多社会科学研究方法和技术，而这些方法技术我已经探索了好几年。我论文的题目本身并不重要，在社会科学方面写一篇论文是一个有趣的、有意义的想法，而且，深入的挖掘探索之后，它不仅仅只适用于自己。但是，在写论文的过程中所得到的实践大于所获得的启示。当我从研究过程中醒过来时，我意识到，虽然我的特定课题不会改变安全实践，但是我学会的技术和工具很可能改变安全实践。我开始阅读他人关于安全度量的想法，并且意识到因为科学探索的开始，安全领域是行业和研究领域的旅程的开始。我们是新人，有很多需要学习。但测量不是新的手段，也不是测量完成后调查和观察经验的方法。我希望能在这本书中与大家分享一些方法。如果我的研究完成得很好，你可能对其中一些方法不熟悉。如果我把我作为一个作者的工作做得很好，你就应该可以用这些方法来理解和改进你的安全操作。我希望这两个工作我都完成得很好。

目　录

第二部分 安全度量的实施

第三部分　探索安全度量项目