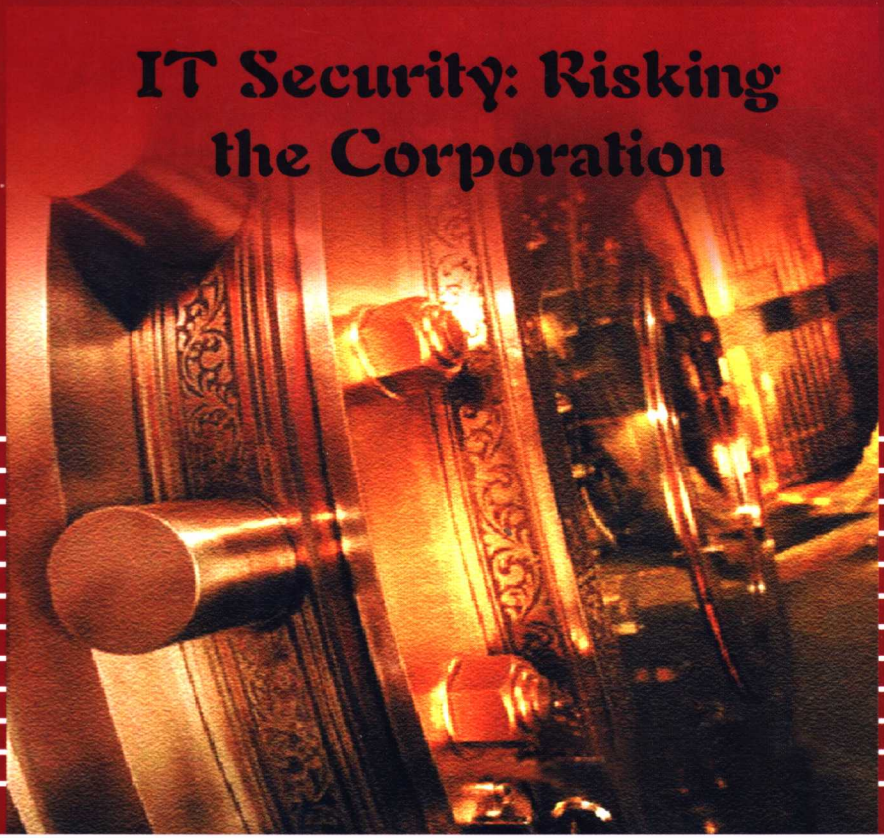
系统与安全丛书

PEARSON Prentice Hall

信息安全
——企业抵御风险之道



（美）Linda McCarthy 著
赵学良 译

您公司的信息暴露在危险之中，
本书指导您应对之策！

Pearson Education
清华大学出版社

系统与安全丛书

信　息　安　全

——企业抵御风险之道

（美）Linda McCarthy　著

赵学良　译

清华大学出版社

北　京

内 容 简 介

即使世界上最大和最为复杂的网络也容易受到攻击。本书中描述的情节暴露了操作系统、网络、服务器和软件中的致命缺陷，以及由于培训和公司方针不完善、管理层疏忽造成的漏洞。内容包括：对安全的破坏是如何发生的；典型对策以及它们的效果；应该预先采取什么预防措施等。

作者有着丰富的网络信息安全经验，本书为提高系统的安全性提供了一个明晰的规划。在本书中能找到可以立即应用的有用工具和预防性措施。另外，作者给出的检查列表和资源列表能够帮助您加强整个 IT 基础设施的安全性。

图书在版编目（CIP）数据

信息安全——企业抵御风险之道/（美）麦卡锡著；赵学良译. —北京：清华大学出版社，2003

（系统与安全丛书）

书名原文：IT Security: Risking the Corporation

ISBN 7-302-07201-9

Ⅰ.信… Ⅱ.①麦… ②赵… 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（2003）第 078832 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

文稿编辑：潘旭燕

封面设计：付剑飞

印 刷 者：北京四季青印刷厂

发 行 者：新华书店总店北京发行所

开　　本：185×230　**印张**：18　**字数**：366 千字

版　　次：2003 年 9 月第 1 版　2003 年 9 月第 1 次印刷

书　　号：ISBN 7-302-07201-9/TP・5243

印　　数：1～4000

定　　价：35.00 元

国外读者对本书的评价

标题：令人惊慌失措的安全问题日志 **评级：★★★★★**

评论人：Charles Ashbacher（Amazon.com 顶级书评员），美国，爱荷华州，Hiawatha
日期：2003 年 5 月 28 日

读这本书时，您会感到毛骨悚然。本书总结了 McCarthy 所完成的安全审核，同时引入了一些其他安全破坏的实例，来进一步强化本书的重点。即：**计算机安全（甚至是在许多“重量级选手”那里）没有得到良好的组织，也没有采取充分的措施**。作者能够坐在终端前，轻易地获得公司（作者正在审核的公司）中最敏感数据的读/写访问权限。导致这种情况的原因可能是下列可疑项之一：缺乏安全培训；没有时间来应用已知的安全补丁；错误的观念——“这不是我的工作”；自大地以为有人知道如何修复一切问题；信任过时的安全软件——如防火墙；毫无根据地信任其他的系统和缺乏有效的管理指导。

解决方案也容易找到，基本上是所有可疑项的对立面。期望没有经过训练的人员能够实现复杂的安全方针是不切实际的，培训的花费远低于修复安全破坏所需的高昂费用。严格执行安全规程是雇员的责任，包括不要信任任何人，除非他们被证实值得信任。之后，只分配给他们（被证实值得信任的人）完成任务所必需的最小权限。我个人不想将任何时间浪费到 IT 行业中那些认为自己无所不知的人身上，许多人都认为自高自大是最为危险的安全错误。

在计算机安全的游戏中，面临的风险日益增长。随着我们日益依赖于计算机来管理每件事情，从信用卡到公共设施，重大安全事故的发生可能只是一个时间问题，此类安全事故可能会沉重地打击美国的经济，甚至会引起大量的伤亡。最令人害怕的故事就是，黑客试图访问加拿大水坝的泄洪控制装置。如果他们使用这些知识将其打开，则整个城市可能会被淹没。

实现有效的安全措施并非一个可选项，如作者指出，没有做到的话，可能会使您受到责任指控。因此，如果您参与制订公司的安全方针，您必须阅读这本书。它将会告诉您事情是怎样走向错误的，这也是正确处理它们的第一步。

标题：现实世界中恐怖的安全故事（来自一个安全专家）　评级：★★★☆☆

评论人：Ben Rothke（Amazon.com 一级书评员），美国
日期：2003 年 5 月 21 日

《信息安全：企业抵御风险之道》，基本上是来自于 Linda McCarthy 安全咨询生涯中的故事。

虽然本书并非针对安全专家，但对于管理人员来说，它是一个极好的资源。这本书详细讲述了许多忽视信息安全的故事，以及由此引发的可怕后果。

这本书用一种轻松明快的方式写就，能够在几个小时内读完。在每个故事之后，均给出了实用的解决方案，说明如何更好地处理所描述的情形。

总之，这本书是一系列不错的安全记事，其中没有太多的 FUD[①]和技术术语，适合于管理人员阅读。

虽然，任何对计算机安全感兴趣的人都可以从阅读本书中受益，但真正应该阅读本书的读者是那些在信息安全领域刚刚起步的人，以及那些经常意识不到信息安全重要性的人，即那些 CxO 们。

希望任何 CxO 们，在阅读本书后，能够了解信息安全的重要性，并采取相应的行动。

标题：给自己买一本，给老板买一本　评级：★★★★★

评论人：Rachel，美国，加利福尼亚州，Cupertino
日期：2003 年 4 月 28 日

从别人的错误中学习不但有价值，而且有趣。本书讲授的这些教训取材于真实生活中的经历，它们都发生在真实存在的公司之中。这种风格使得本书的教训

① FUD 是 Fear, Uncertainty, Doubt（惧、惑、疑）的缩写。其含义是在顾客的头脑中注入疑惑与惧怕，然后，你说什么他们就可能信什么，也称“心理恐怖战术”。——译者注

更为触目惊心，更容易记住，也使得阅读本书充满了乐趣。在每个故事之后，作者都给出实用的建议，说明如何处理与阻止特定的情况。

安全始终是计算机技术的一个重要方面，随着技术的发展，安全变得比以往任何时候都更为重要。这是一个必须解决的问题，不管您正在创办一个小型的公司，或者是为一家大型的公司工作，安全问题在您的公司中所涉及的领域可能比您能意识到的更为广泛。您或许以为购买一个安全软件包就可以解决一切问题。您或许以为电子邮件是一种安全的沟通方式。您或许认为公司的管理层高瞻远瞩，洞悉安全问题。请阅读本书，同时，最好给您的老板也买一本。

标题：实用的建议——完美的阅读体验 **评级：★★★★★**

评论人：Steve Larsen，美国，加利福尼亚州，旧金山
日期：2003 年 4 月 20 日

尽管这本书并不讲授如何侵入别人的系统，但是，从 Linda McCarthy 讲述的这些故事中，可以清楚地得出，侵入系统十分容易。McCarthy 以一种出色的格式将纷繁芜杂的信息组织起来，传达给读者。她根据从事安全审核员和顾问工作的经验，讲述了一系列的故事。这些故事都十分清新明快，易于阅读。她从每个故事都总结出一系列的教训，并分析采取什么措施才能避免在将来发生同样的问题，据此给出许多绝佳的实用观点。

最让我吃惊的是，和许多其他的事情一样，信息安全经常归结到人——他们的经验和培训、动力以及他们的组织与管理方式——技术处于第二位。我乐意将此书推荐给所有的人，从系统管理员、安全管理者，到 CIO、CEO 们。这本书的建议都是行之有效的。

译 者 序

从很小的时候开始，我们就接受“过马路左右看，要走人行横道线”等交通安全的教育。遗憾的是，在计算机领域却没有这样的传统。马路上开车的司机时刻注意着行人，避免交通事故的发生，而计算机黑客却是费尽心思要破坏计算机系统。这使得计算机安全现状远比交通安全更为严峻。

安全书籍也在逐渐走向成熟，从简单地介绍攻防技巧转而系统性地介绍防御措施。任何一个学科都是如此，就如同物理学从阿基米德的杠杆和浮力、伽利略的两个铁球同时着地，发展到牛顿的三大定律，直至爱因斯坦为之奋斗的统一场论。

计算机安全问题是随着计算机的应用而不断发展的。计算机从最初的单机系统，发展到今天的网络时代，各种联网的应用承载了至关重要的商业活动，随着应用的复杂性与连通性的增长，安全问题也日益严重。

安全之我见

安全首先需要意识上的转变。

“我们的网络没有连接到 Internet，所以没有安全问题。”

“我们的网络上没有什么重要的数据，所以不用考虑安全问题。”

“我们有最好的防火墙，所以安全不成问题。”

上面这些想法都是对安全的错误认识。要想维护计算机系统的安全，首先要意识到风险就在面前，只要使用计算机，就有计算机安全问题。

我们既不能对安全风声鹤唳、草木皆兵，也不能回避问题，采取“鸵鸟政策”。这两种态度都无助于问题的解决。

安全来源于“生于忧患、死于安乐”的意识，与一贯的谨小慎微、防微杜渐的态度。一曝十寒和侥幸态度都无助于安全。根据“木桶原理”，系统的安全取决于防护措施的最薄弱环节。

知道敌人是谁？“知己知彼，百战不殆”，但如果根本不知道敌人是谁，则这场战争没有什么悬念。

阅读本书的过程中，要注意这两个问题：我们的系统面临什么危险呢？我们的潜在敌人是谁？

安全问题实际上是黑客与安全人员之间的**“不对称”战争**。大家都知道，防御要比攻击困难，也复杂得多。伊拉克战争中“来福枪打下直升机”就是一例，虽然其真实性有待考证，但最起码大家没有否认其可能性。一个是集各种高科技于一身的、价值数千万的21世纪战争机器，一个几乎是古董级的“武器”，二者形成了鲜明的对比。所以，对计算机安全万不可等闲视之，一两个昂贵的产品或一两项完美的措施并不能从根本上改善系统的安全状况，只有系统地防御、有效地组织才能对抗日益增长的安全风险。

本书的大部分内容都是介绍如何防御。一个粗通电脑的人，到 Internet 上下载一些工具，看看说明就有可能侵入计算机系统，而防御则需要整套的理论、严密的思考、正确的意识与态度。双方在成本、知识、技能上都是一场“不对称”战争。

要想打赢这场战争，就必须聚合各方之力：获得管理层在资金与人力上的支持、培训计算机的使用者、严密而完美的规章制度……

几点说明

公司名与人名的译法

在本书正文中，我将人名和大部分公司的名称都译成了中文。

请看下面两个句子：

1. “我和约翰一起去看曼联队的比赛。”
2. “我和 John 一起去看 Manchester United 队的比赛。”

我觉得第一个句子好一些，都是汉语，读起来流畅。读者可以十分流畅地从中得到所要表达的意思。而第二句虽然意思相同，但在阅读时，遇到 John，我们不得不临时切换到

英文发音，并联想这是一个男子的名称，而遇到 Manchester United 更是要费一番脑筋才能知道原来就是曼联。

但在本书的序、致谢等内容中，我基本上采用原名，如果在正文中出现过，则后面加上括号，注上在书中用的汉语名字。如：Linda McCarthy（琳达·麦卡锡）。

用词的考虑

Internet 按照国家规范应译为“因特网”，但更常应用的可能还是英文单词 Internet。所以本书中一般使用 Internet（某些特殊情况除外）。

procedure 用在工业生产中应该译作“程序”，在计算机编程中用作“过程”，但用在计算机书籍中，“程序”容易与 program（程序）混淆，为了翻译更为准确，我将其译作“规程”，规程一词能够十分准确表达出“规定的程序”之义，同时不会引起歧义。所以本书中将 policy and procedure，译为“方针与规程”。

incident，既用作“事件”，也用作“事故”。便为了和 event（确定无疑应译为“事件”）区分，我采用了“事故”的译法。这样表达起来更为准确，同时带有些许贬义，表达是人们不愿意发生的事情。

另外，比如本书中用“坐着的鸭子”来比喻对即将发生的事情没有准备的人，可能有人会觉得“趴着的鸭子”或“卧着的鸭子”更为合适，但我觉得用“坐”字会有更多一层意思，即“坐以待毙”，所以就采用了“坐”，至于实际的效果，只能见仁见智了。

上面这些细微的调整，在阅读过程中可能根本不会体察到，但是，希望读者能够在阅读本书的过程中享受到流畅、轻松的体验。

译者注

文中“译者注”稍多，这和作者的行文有关。作者是一个长期从事审核的专业人士，既不能像编写科技论文一样用词艰涩严谨，又要能够清楚生动地将问题表述清楚。在本书中，她（Linda McCarthy）采用了比较明快与形象的表达方式。书中较多出现的“译者注”主要是为了使意思更为明确，多说一点终究没错。

譬如去问路，您希望听到下面哪个回答：

1. “往前，大概走 50 米，约一分钟不到的路，有一个十字路口，那有红绿灯，路边正好有一家小商店，卖一些水果、饮料，然后向右拐，也就是向西，再向前 100 米就到。”

2. “向前，右拐”。

致谢

清华大学出版社所出版的图书在读者中拥有良好的口碑，也是我最喜欢的出版社之一。在合作过程中，我认识到，这和出版社拥有一批优秀的编审人员是分不开的。我深深为他们那种专业、敬业和认真的精神所感动与折服。一本图书就是在他们的精雕细琢下变得更趋完美，换来读者更为流畅的阅读体验。

感谢本书的策划编辑尤晓东和文稿编辑潘旭燕，他们对语言文字敏锐的把握，以及开放的态度，对本书的行文有莫大的帮助，也使本书很好地展现出原书的风格。另外还要感谢在我成长与工作过程中一直帮助我的家人、同学和朋友。

序

请注意——本书不同于您能买到的其他有关安全的书籍。本书中既没有服务器中缺陷的详细信息及它们使用的 IP 端口列表，也没有详细注解的病毒源代码清单。作者既没有列出突破脚本的目录，也没有列出可以下载这些脚本的 WWW 站点。本书中也没有耸人听闻的第一人称故事，展示如何轻而易举地解密人们的密码。因此，如果您希望寻找这些内容，那么您会失望的，请及早将本书放下。

但……，请注意，您放下的可是一本讨论真实安全隐患的书，它提供基本和永远的教训——其中一些内容强烈建议每个接触计算机的人都要学习。

请考虑这些情况——本书出版后一年左右的时间内，Internet 上的 e-Commerce 将会超过每年 1 万亿美元的关口。以前，对网络的商业应用是不允许的，在 1993 年之前并没有真的启动，所以其增长率十分惊人。但是，在我们看到这些数字时，需要意识到这只不过是一个开始——世界人口中只有一少部分人当前连接到网络，企业对企业的商务只有一小部分开始联机进行。

大家都听说过摩尔定律（Gordon Moore），该定律最早见于 1965 年，它预言处理器的性能每 18 个月就会提高一倍。现实印证了这个预言，并且预期会在下一个 10 年中依旧生效。在存储领域也有类似的增长，在最近几年中，联机资源的容量大约每 14 个月就会翻番。通过光纤与无线前所未有的增长，通信带宽也得到了显著的提高。所有这些日用品（它们已经确实成为了生活必需品）的成本在下降，而总容量在上升。

越来越多的重要信息放到了网上，引起 IT 基础设施投入的增长，同时 IT 基础设施的增长又刺激了网上重要信息的增长。形形色色的银行、证券代理公司、会计与财务公司都使用计算机和网络来运作它们的业务。没有网络的话，美国联邦政府和州政府就不能运转。重要的基础设施，如：电力和运输，要依赖于联网的传感器和控制器件。法律的执行与国家的防务要依赖 IT 设施存储它们的数据并提供支持。健康记录、医疗参考和诊断越来越计算机化。驱动当今大部分商务运转的智力财产——包括芯片设计、新的软件、医药配方、石油勘探、音乐、电影、文学以及众多的其他事物——都在网络上，它们可能会被窃取、更改和毁坏。几乎所有的商务形式都会有重要部分在网络空间中（或很快就会有）。

现在，请看知名的银行抢劫犯威利·萨顿的名言：当被问及他为什么抢劫银行时，萨顿回答说："因为钱就在那里。"您认为未来比较突出的犯罪会集中在什么领域？恐怖分子？激进的活动家、蓄意的破坏者、无政府主义者？让我们面对这个现实吧——信息技术将成为各种攻击形式的目标之一。实际上，这种事情已经发生，有团体估计每年由病毒、入侵和联机欺骗所造成的损失可能会达到数千万美元。

造成这些损失的主要原因是信息、安全工具和人员的长期缺乏，加上设计欠佳的产品充斥市场。一般的在线系统是由于设计时根本没有考虑安全因素的软件构建而造成，而为了与早期的软件兼容，这些软件变得更为不安全，这些软件的编写人员都没有经过安全方面的培训，软件编写完成后，仅仅进行简单测试，为了满足上市日期的要求而不顾存在的已知缺陷，匆匆推向市场。之后，此类系统被对安全一无所知的人们购买，作为附加软件安装到一个不安全的基础之上，被那些寻求最低安全措施的人们使用，他们的在线活动存在安全隐患。所有这一切都极为常见，管理层需要依赖于那些自称是专家所提供的服务与报告，而这些"专家"所有的经验都来自于下载和运行其他人编写的突破工具。发生如此之多的计算机事故并不奇怪——相反，奇怪的是为什么没有更多的事故发生。

即使到了20世纪80年代，相比于其他专业，如图形、网络和人工智能，信息安全依然是计算世界中一个十分艰深、有限的领域。我记得，当时从事一般计算的用户只能买到很少的几种介绍信息安全的书籍。由于当时一般的用户仍未面临实际的IT安全威胁，所以人们也不真正关注它。Internet和日用计算的发展已经改变了这种状况。最近，我们看到，美国市场上现已出版的安全方面的书籍超过了数百种。但是，在这些书籍中，只有一小部分值得购买——其余的书籍只不过是一些研究成果的改头换面、很快就会过时的漏洞列表、以及如何向已经不稳定的基础构架应用更多补丁的信息。

现实情况是，只有少数专家极为突出，因为他们真正了解信息安全的"全貌"。Linda McCarthy（琳达·麦卡锡）就是这样的一个人，仔细阅读本书就会明白，为什么她写的图书第一版一经推出就立即上了教育专家和从业者的书架。琳达并不是提出一些局部的解决方案或临时的补丁，她凭着自己的工作经历——作为安全审核员、顾问、经理、开发人员、教育专家和执行人员——标识并说明了驱动安全计划与执行的下层结构和态度。她了解，计算机安全并不主要依赖于计算机，而是取决于购买、部署和操作这些计算机的人。这需要对经济学、心理学、法律和围绕计算应用的商业实践（正是这些应用决定了总体的安全状况）都有相当的了解。本书中除了琳达的许多小插曲之外，各章节的标题本身就指出了对安全应该着重注意什么：从组织的最高级别着手。当从正确的级别来审视信息安全时，它远不止是"系统管理与黑客"的对抗——它是整个企业生存能力的保障。如本书中所述，信息安全的职责和方针必须由高层来驱动，要主动而非被动，并且一贯地保证维持信息安

全所需的资源。仅仅知道如何运行一个漏洞扫描程序是不够的。

在我们大踏步地向信息时代迈进的同时，信息安全也变得前所未有的重要，我们需要清醒地意识到，在所有情况下，我们所涉及的都是“信息”而不是“计算机”。对于每一个人，重要的是要知道如何保护我们的信息资源，不管它们可能的形式是怎样的。我们考虑的重点不应该是一台特定的计算机或某个版本的操作系统，而是支撑它们运转的下层结构——社会、经济和法律结构。我们都应该明白，单单靠人员或技术对于解决人们所面临的安全问题是远远不够的，否则，信息安全也就不是什么大不了的问题。当然，技术很重要，但它并不是惟一——或最重要的因素。琳达多年前就了解这些基本的真理，并在她的职业生涯中身体力行。本书中，她将自己的经历在之后的章节中做了充分的总结，并进行了详细说明，几乎所有人都能够从她的经验中得到一些有价值的东西。

本书的第一版并不是我书架上惟一一本深度探讨信息安全的书籍。然而，当我的学生和同事们找寻深度介绍安全的书籍时，我总是将这本书推荐给他们，他们都觉得本书有教育意义。并且，和那些罗列基于万维网（WWW）的黑客工具站点、提供含糊不清建议的“大部头”书籍相比，本书的突出点在于：本书能够根本性地改变人们对信息安全的思考方式。故而，如果您正在寻找此类图书，我的建议是您不要放过本书……至少，在您读完之前。

Eugene H. Spafford
2002 年 12 月

致　谢

特别感谢我的编辑 Denise Weldon-Siviy。没有她的帮助我不可能完成本书的编写工作。她的意见、鼓励和热情都为本书增色不少。还要感谢 Randall Millen 鼓励我开始了本书的写作，并始终支持我的工作。

我还深深地感谢我的出版商及其职员，包括 Sun 微系统公司的 Rachel Borden、SunSoft 营销部门的 John Bortner、Prentice Hall 的编辑 Greg Doench。我十分感谢他们的支持，以及为了本书的出版而做的具体协调工作。

Dan J. Langin 编写了第 11 章的 11.2 节“保护信息与网络的法律责任”。

当然，我还要感谢我的前任雇主，Sun 微系统公司。特别感谢 Sun 的首席信息官（CTO）Eric Schmidt，是他营造了一种宽松的环境，鼓励创造力和才能的发挥与成长。在 CTO 的组织中，尤其要感谢 Humphrey Polanen。

许多计算机安全专家排出时间来教授我职业技巧，并与我分享有价值的信息。在这里，我要特别感谢 Matthew Archibald、Casper Dik、Dan Farmer、Alec Muffett、Brad Powell 和 Marcus Ranum。

还要感谢其他有关专家从他们繁忙工作中挤出时间来编写评论意见、建议和支持。这些慷慨的人是（以字母顺序列出）：Dianna Browning，Dr. Tom Hafkenschiel, Susan Larsen, John McCarthy, Tim Murphy, Michele Parry, Richard Power, Bob Shotwell, Steve Smaha, Gene Spafford, Keith Watson, 以及 Deborah Yarborough。

最后，我想问候所有为我提供无尽支持与灵感的朋友和家庭。

谢谢！

关于作者

Linda Ann McCarthy（琳达·安·麦卡锡）是安全技术领域中知名的权威，同时也是作家和行业发言人。McCarthy 是赛门铁克公司 CTO 办公室的执行安全顾问。之前，McCarthy 是 Recourse Technologies 系统工程部门的副总裁，该公司开发检测、捕获和跟踪黑客的软件。

在这之前，McCarthy 是 NETSEC 的高级副总裁，该公司提供受控的入侵检测和响应服务。再往前，她还曾是 Sun 微系统公司负责安全研发的经理，并设立了网络防卫基金（Network Defense Fund）。

应他们的要求，McCarthy 曾入侵过公司网络的许多系统，向执行经理们演示访问公司机密、关闭生产制造系统，甚至破坏全球计算机运转是多么容易。相应地，她运用她的知识启发执行经理们如何去避免这些灾难。

作者在 Sun 微系统公司曾教授过多门课程，有硬件构架、系统管理和 UNIX 安全等。

绪　论

互相联通的时代已经到来。随着信息纵横交错地自由流动，电子商务不断敲开新领域的大门，网络安全已经变得十分复杂，远不止仅仅使用一个好的防火墙连接到 Internet 那么简单。

我在审核分布式网络的安全上投入了大量的时间。在很多案例中，我都发现数据能够被轻易地修改、窃取或毁坏，甚至不会留下任何痕迹来标志事故曾发生过。系统管理员和其他掌握权力的人了解系统没有配置好安全措施。他们所不知道的是，他们所面临的风险有多高。执行经理们同样没有意识到这些风险。

这本书让您能够从他们的错误中得到有益的教训。如果您是一位执行经理、经理、系统管理员——或任何负责网络安全的人——您必须对安全采取一种积极的方式。不要犯和这些公司同样的错误。犯错误的代价有可能是您的整个公司倒闭。

关于本书

您将读到的内容并非虚构，而是真实安全审核的汇编。每一章都集中在一个审核上，每次审核都是我为真实存在的、运转正常的公司实施的。如果我使用真实的公司名称，您也许会发现，您曾与其中的一些公司发生过联系。

当然，由于明显的法律和道德原因，我不会使用公司、雇员或其他各方的真实名称。但每个案例中风险的实际情况和我的审核方法都是真实的。

请仔细阅读，尤其当您是执行经理、一线经理、系统管理员、律师或专业执法人员时。本书中所描述的风险是您需要了解的风险。

在每个案例中，真正的风险并不只是操作系统自身的风险。严重的风险在于系统的安装、配置、支持和管理方式。这些因素很大程度上决定了公司的风险。

在指出这些风险的同时，我希望负责网络数据的人对安全开始采取一种积极、认真的方式。

本书的组织方式

尽管这些审核都是真实的，每一章，我都会以一个第一人称的虚构剧本开始。在我为公司工作的过程中，我发现很多人只有在他们的系统、数据以及他们的公司发生了什么事故之后，才开始认真地对待安全问题，这也是此类问题屡见不鲜的因素之一。我将每个剧本做了个人化，将“您”——读者，放入故事中，以此来传递这个信息：这种事情真的会发生在您的数据和您的公司身上。

每章的大部分篇幅描述我在审核过程中揭示出来的实际安全风险。在这一部分中还解释了这些风险的后果。您不会在一天早上醒来时突然发现您的网络安全漏洞百出。对安全的破坏一般发生在疏忽或不完善的规划执行了较长一段时间之后。这些段落解释了问题可能发生的一些方式。

每章的“我们不能步其后尘”一节说明如何预先避免这些问题。我希望您仔细阅读这些章节，并牢记这些指导方针。

关于黑客

我使用术语“黑客”贯穿全书来表示那些获得对系统和信息未经授权访问的人。而有些专家使用术语“黑客”表示喜欢自称黑客的一些编程人员，实际上他们是出色的代码编写者，并不倾向于犯罪活动。但是我还是决定使用“黑客”这一称呼，因为在安全圈子以外它的应用十分广泛，几乎每个拿起本书的人都会知道我用它的意思。

我还在大多数案例中将“这个黑客”或“该黑客”统称为“他”。我们都知道黑客既可以是男性，也可能是女性，但是一次又一次地读“他或她”十分麻烦。

本书的内容与黑客有关，但并不是为他们所写。如果您希望成为一名黑客，您从本书中学不到如何入侵系统。明智的做法是您现在立即将本书放回书架上。