CENGAGE Learning

安全技术经典译丛

信息安全原理

(第5版)

Principles of Information Security, Fifth Edition

[美] Michael E.Whitman
Herbert J.Mattord
著
王晓海
译

CENGAGE Learning 圣智学习

清华大学出版社

安全技术经典译丛

信息安全原理
(第5版)

[美] Michael E. Whitman
Herbert J. Mattord 著
王晓海 译

清华大学出版社
北 京

ISBN: 978-7-302-41703-3
北京市版权局著作权合同登记号　图字：01-2014-2799
Cengage Learning Asia Pte. Ltd.
151 Lorong Chuan, #02-08 New Tech Park, Singapore 556741

图书在版编目(CIP)数据

信息安全原理：第 5 版 / (美) 惠特曼(Whitman, M.E.) 等著；王晓海　译. —北京：清华大学出版社，2015
(安全技术经典译丛)
书名原文：Principles of Information Security, Fifth Edition
ISBN 978-7-302-41703-3

Ⅰ. ①信… Ⅱ. ①惠… ②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 237985 号

责任编辑：王　军　于　平
封面设计：牛艳敏
版式设计：牛静敏
责任校对：曹　阳
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：34　　**字　　数**：870 千字
版　　次：2015 年 11 月第 1 版　　**印　　次**：2015 年 11 月第 1 次印刷
印　　数：1～3000
定　　价：79.80 元

产品编号：063672-01

译 者 序

当今世界，信息安全已经是一个为人所熟知的概念，来自网络的攻击、病毒、黑客，使我们的信息无时无刻不处在威胁之中，攻击已经不再发生在一间电脑室中，而是分布在整个世界中，信息安全没有疆域，而且我们不知道对手是谁，在什么地方，在做什么，他们为什么这么做，并且他们在玩游戏的过程中总在悄悄地修改规则，对此我们必须时刻保持警戒和谨慎。

信息安全不是绝对的，它是一个过程，而不是一个目标。信息安全应在安全和可用之间保持平衡，在信息风险和控制之间保持平衡，是成功防御攻击、减少风险、克服弱点以提高安全性的安全机制、策略或过程。而且变化是不可避免的，因此必须制定相应的策略，以应对在信息安全计划的运行与维护过程中的变化。

要掌握如何保护信息安全，必须要具备大量的多学科知识，以及相关经验和技能。所幸本书的作者 Michael Whitman 和 Herbert Mattord，结合了他们各自在本研究领域内的理论知识以及商界的实际经验，联合创作了这部阐述信息安全原理的优秀教材，它面向信息安全专业的学生，均衡地介绍了安全管理和安全技术，作者自身丰富的实际经验也为读者提供了丰富的学习体验，使得本书成为广受欢迎的经典之作，一版再版。

作者作为专业人士，有意将信息系统安全专业人员的公共知识体系引入本书，这成为本书的一大特色。“NIST Special Publication(SP) 800-100，信息安全手册：经理的指南”提出了 13 个信息安全管理领域，其中信息安全的管理是作者特别强调的课题，并且全面、详细地介绍了系统开发生命周期(SDLC)如何通过多步骤方式(启动、分析、涉及、实现和维护)开发、实现、退出信息系统的整个过程。此外，作者还通过别出心裁地设计各种场景来介绍每个主题，带领读者理解和掌握各部分需要学习的知识。当然，作为一部优秀的教材，每一章的最后都会提出一些问题，让学生探讨故事内容所隐含的根本问题，能够进一步深入地领会和运用所学的知识，更深入地了解各种信息安全的主题。各章也都给出了要求学生研究、分析的小结、复习题和练习，帮助学生巩固学习目标，加深理解。作者在最后一章中提到了数字取证，作为新的热点领域，数字取证的目的是保护、识别、提取、记录、解释计算机媒体，找出证据和/或进行根源分析。最新的法律和行业趋势在本书中也做了介绍。这些都是本书的特色和亮点。

常言道：防患于未然，“一分预防胜于十分治疗。”作为信息安全的专业人员，必须将安全纳入所有的阶段，确保选择、获得、使用合适的、性价比高的安全控制。此外，必要的评估和测试也是确保采取控制措施适当的重要环节。为了帮助人们保护信息的安全，必须确定了解他们需要保护什么，以及他们的安全性到底如何，因为用户是他们自己信息和系统的第一线防御者，当然，也要确保高层管理者和主管们理解你的工作本质和所受到的局限，这些对于信息安全从业人员也是十分重要的。

感谢清华大学出版社的编辑们，为本书的翻译投入了巨大的热情并付出了很多心血。没有她们的帮助和鼓励，本书不可能顺利付梓。

译者虽然本着“诚惶诚恐”的态度，在翻译过程中力求严谨和忠实作者意图，但是鉴于水平有限，错误和失误在所难免，如有任何意见和建议，请不吝指正。感激不尽！本书全部章节

由王晓海翻译，参与翻译的还有张曦、于学荣、白红军、孔祥亮、陈跃华、杜思明、熊晓磊、曹汉鸣、陶晓云、王通、方峻、李小凤、曹晓松、蒋晓冬、邱培强、洪妍、李亮辉、高娟妮、曹小震、陈笑等。

最后，希望这部经典之作能够成为引领读者深入领会和掌握信息安全的钥匙！

译者

前　言

全球网络使世界各地的信息系统之间的互连变得越来越广泛，顺畅的通信和计算解决方案因而也变得更加重要，但诸如恶意软件、钓鱼攻击以及各种犯罪攻击事件的频繁出现，说明当前的信息技术十分薄弱，需要加强对这些系统的安全保护。

为了保护已有的系统和网络，企业必须招收一定数量的信息安全专业人员。企业还期望具有丰富经验和技巧的下一代专业人士能开发出更加安全的计算环境，参与和管理肯定会出现的、复杂的信息安全问题。为此，技术类的学生需要在大学教师的指导下，学习更高深的内容以及相关的技术材料，认识已有系统中存在的漏洞和薄弱部分，学习设计并开发将来所需的安全系统。

本书是一本阐述信息安全原理的优秀教材。目前有许多面向从业人员的、关于信息安全的优秀出版物，但缺乏一本针对学生的、均衡地介绍安全管理和安全技术的教材。我们希望创作一本专门面向信息安全专业学生的教材来填补此空白。而且，显然本书需要包含犯罪立法、政治学、计算机科学、信息系统和其他相关学科的原则，以帮助读者更清晰地理解信息安全原则，并为系统漏洞形成跨学科的解决方案。本书的基本原则为：现代机构内的信息安全是一个需要管理层来解决的问题，而不是仅通过技术就可解决的问题。换言之，机构的信息安全具有重要的经济效益，管理层必须为之负责。

0.1　方法

本书全面介绍了信息安全的整个领域，其中包括许多相关元素的背景，以及理解该领域所需的足够细节。本书包含了该学科的术语、简史，并概述了信息安全计划的管理模式。

0.2　本书结构和章节内容简介

本书的结构遵循一种称为安全系统软件开发生命周期(或 SecSDLC)的模式。这个结构化方法可用于在几乎没有正式信息安全措施的企业中实现信息安全，也可以帮助改进已有的信息安全计划。SecSDLC 提供了坚实的基础架构，非常类似于在应用程序开发、软件工程、传统的系统分析与设计以及联网工程中使用的架构。本书使用这个结构化方法，提供了一条不超越主题的主线，此主线可指导教师和学生对信息安全领域的各个方面进行详细研究。为此，将本书分为 6 个部分，共 12 章。

第 I 部分——简介

第 1 章——信息安全简介

开篇章节讲述了理解信息安全各领域的基础内容。本部分定义关键术语，解释基本概念，并概述此领域的起源及其对理解信息安全的影响。

第II部分—— 安全调研阶段

第2章—— 安全需求

本章介绍商界对信息安全越来越感兴趣的原因。本章介绍了现代企业在信息安全领域的需求，强调并构建了第1章介绍的概念。一个原理性概念是：信息安全主要是一个管理问题，而不是技术问题。换言之，信息安全领域中的最佳实践过程是在考虑了商务需求后，才应用具体的技术。

本章还介绍了企业面临的各种威胁，并给出对这些威胁进行分级的过程，以便在企业开始进行安全计划时利用相应的优先级。本章继续讲解上述威胁可能导致的各种攻击，以及它们对机构的信息系统产生的影响。本章进一步讨论了信息安全的重要原理，其中一些在第1章已经介绍过，如机密性、完整性、可用性、身份验证和标识、授权、责任和私密性。

第3章——信息安全中的法律、道德以及专业人员问题

除了SecSDLC调研过程的基本部分之外，本章对国家和国际条款中的现有法律、规章和公共道德进行了详细介绍，深刻阐述了商业交往中所遵循的规范。本章介绍了信息安全领域的几个重要法律，并详细描述了实现安全的人员必须遵守的计算机道德。不懂法律不是借口，但忽视法律(懂法但不守法)更危险。本章也介绍了现今企业中经常出现的几个法律和道德问题，以及可提升道德和法律责任的正规专业机构。

第III部分——安全分析

第4章——安全规划

本章给出了许多被广泛接受的安全模型和基础框架，还介绍了最佳商务实践方案以及合理注意、谨慎处理的标准，并扼要介绍了安全策略的开发。本章详细描述了安全策略每一层次的主要组成内容、范围和目标对象，还解释了军队和私人的数据分类模式以及安全教育培训和意识(SETA)计划。本章论述了支持业务持续、灾难恢复和事故响应的规划过程，描述了在发生事故时机构的作用，以及机构需要外部法律执行部门的时机。

第5章——风险管理

在开始设计一个新的信息安全方案前，信息安全分析人员必须首先要理解企业的当前状况以及它和信息安全的关系。企业目前有正规的信息安全机制吗？它们的效率如何？企业给安全管理人员和终端用户发布了什么策略和过程？本章描述了标识威胁和资产，并评定其优先级的过程，以及标识当前可用于保护这些资产免受威胁的控制措施的过程，进而介绍了实施基本的信息安全评估的方式。本章还讨论了各种可利用的控制机制类型，并指明进行最初风险评估所涉及的步骤。本章把风险管理定义为识别、评估风险，并将其降低至可接受的程度、实现有效的控制措施以维持此风险级别的过程。最后讨论了风险分析和各种可行性分析。

第IV部分——设计

本部分的内容为信息系统专业的学生介绍信息安全领域中使用的技术控制。如果读者不熟悉联网技术和TCP/IP协议，可能会觉得第6、7、8和9章的内容比较难理解。如果读者不具备网络协议的基础知识，在学习本部分的内容之前，应先学习联网教材中有关TCP/IP协议的一两章内容。

第6章——安全技术：防火墙和VPN

本章详细论述了如何配置和使用把企业系统和不安全的互联网隔离开来的技术。本章包含防火墙技术的许多定义和分类，以及可以部署防火墙的体系结构。接着讨论了防火墙的正确配

置和使用相关的规则。本章还阐述了远程拨号服务，以及为仍使用这种旧式技术的企业保护该访问点所必需的安全预防措施。之后介绍了过滤内容的能力和注意事项。最后讨论了通过虚拟专用网为授权用户提供远程访问权的技术。

第 7 章——安全技术：入侵检测防护系统和其他安全工具

本章继续讨论安全技术，介绍入侵的概念，防止、检测、响应入侵和恢复到入侵前的状态的技术。阐述了入侵检测和防护系统(IDPS)的特定类型：主机 IDPS、网络 IDPS 和应用 IDPS 及相应的配置和用法。本章继续论述专门的检测技术，将攻击者诱入诱骗系统(因而远离重要的系统)，或简单地把攻击者的入口指向这些诱骗的区域，这些区域称为蜜罐、蜜网或填充单元系统。本章还介绍跟踪系统，跟踪被诱入诱骗系统的攻击者的真实地址。之后详细论述重要的安全工具，信息安全专家可以使用这些工具检查企业系统的当前状态，标识出系统中已有的潜在薄弱区域或企业的整体安全态势中存在的潜在薄弱区域。最后讨论现代操作系统中广泛部署的访问控制设备，以及生物测定学中的新技术，对已有的实现方案提供强有力的身份验证。

第 8 章——密码学

本章详细介绍了现代密码系统的基础知识、体系结构和实现方案。本章首先概述了现代密码系统的历史，在该历史中有重要作用的各种密码，还论述了组成密码系统的一些数学技术，包括散列函数。接着，比较传统的对称加密系统和现代的非对称加密系统，非对称系统是公共密钥加密系统的基础。然后，本章概述在安全通信中使用的、基于加密技术的协议，包括 S-HTTP、S/MIME、SET 和 SSH。之后讨论隐写术，这是一个新兴的技术，是隐藏信息的一种有效方式。最后讨论信息安全中专门针对加密系统的攻击。

第 9 章——物理安全

物理安全是信息安全过程中的一个重要环节，关注的是物理设施的管理，物理访问控制的实现以及环境控制的监督。本章讲解了现代企业在面对各种物理安全威胁时应特别注意的事项：设计一个安全的数据中心，评估警卫和看门狗的相对价值，分析火灾抑制和电力调节的技术问题等。

第 V 部分——实现方案

第 10 章——实现信息安全

前面的章节介绍了企业设计信息安全计划的规则，本章介绍实现该设计所需的重要元素。本章主要实现了信息安全的靶心模型，讨论了企业是否应外包信息安全计划中的各种组件。此外，还讨论了变动的管理、程序的改进以及业务持续性工作的额外计划等内容。

第 11 章——安全和人员

实现阶段的下一领域解决的是人员问题。本章介绍了人员的两个方面：安全人员和人员的安全。具体内容有：人员问题、专业人员安全证书以及雇佣政策的实现和实践。本章还讨论了信息安全政策与顾问、临时工和外部商务伙伴之间影响和被影响的方式。

第 VI 部分——维护和改进

第 12 章——信息安全维护

最后也是最重要的一部分是对维护和改进的讨论。本章介绍了对信息安全计划的长期进行的技术性和管理性评估，企业必须执行该信息安全计划，才能维护其信息系统的安全。本章介绍了长期风险分析、风险评估和度量，这些都将保证风险管理计划的效率。然后探讨了现代企业中进行各种漏洞分析所需进行的特殊考虑(从互联网入侵测试到无线网络风险评估)。本章和

本书最后介绍了数字取证这个主题。

0.3 特色

下面是本书研究信息安全的一些特点：

信息系统安全专业人员的公共知识体系——因为本书作者是经过认证的信息系统安全经理(CISM)和信息系统安全专业人员(CISSP)，CISSP 的知识对本书的设计有一定的影响。虽然本书尽量避免成为一本认证学习指南类的书，但作者的背景导致了本书在介绍信息安全的知识时，在某种程度上结合了 CISM 和 CISSP 公共知识体系(CBK)。

每章场景——每章的开头和结尾都是一个小故事，讲述一个虚拟公司遇到某类现实世界常见的信息安全问题。每一章的最后都会提出一些问题，让学生和老师讨论故事内容所隐含的根本问题，并探讨这些问题的道德方面。

相关资料和技术细节部分——这部分内容穿插在整本书中，重点讲述一些有趣的主题和详细的技术问题，让学生更深入地了解各种信息安全主题。

强化学习——在每章结尾提供了该章的小结、复习题和练习。这些练习要求学生研究、分析和记录问题的答案，以巩固学习目标，并加深对本章内容的理解。这些内容便于学生在课堂外复习信息安全的内容。

0.4 本版中的改动内容

- 在每章末尾增添了一些讨论问题，以探讨该章内容的道德方面。
- 介绍了最新的法律和行业趋势。
- 关键术语框突出了行业中使用的术语。
- “更多信息”部分列出了一些网络地址，学生可在这些地方找到所介绍主题的更多信息。
- 增添了一些图片来介绍重要主题。

0.5 额外资源

在 www.cengagebrain.com 网站上可找到更多课程材料。查看本书封底的 ISBN，然后在 CengageBrain 主页顶部的搜索框中输入本书的 ISBN 进行搜索即可。

0.6 教师资源

配套网站

为支持本书内容，我们准备了许多教学工具，它们在多方面增强了课堂教学内容。

教师手册——教师手册包括使用本书的建议和策略，甚至还包括了讲座主题的提示。教师手册还包括每章结束处复习题的答案以及练习的建议方案。

答案——教师资源包含每章末尾所有材料的答案，包括复习题和练习题。

图形文件——图形文件允许教师利用本书的图形创建自己的演示文稿。

PowerPoint 演示——本书的每一章都提供了相应的 Microsoft PowerPoint 幻灯片。它们可以用作课堂演示，让学生在网络上回顾每章的内容，或打印出来，分发给学生。教师还可以为在课堂上额外介绍的主题加入自己的幻灯片。

实验室手册 —— Cengage Learning 出版了与本书和其他书配套的实验手册 *The Hands-On Information Security Lab Manual*, Fourth Edition (ISBN 13:9781285167572)。该实验室手册提供了跟踪痕迹、枚举和防火墙配置等安全性强化练习，以及诸多作为实验室组件或课堂项目的练习和案例，作为本书的补充材料。要了解详细信息，请与 Cengage Learning 出版社的销售代理联系。

Cognero——Cengage Learning Testing Powered by Cognero 是一个灵活的线上系统，允许：

- 编写、编辑和管理多个 Cengage Learning 解决方案的测试题库内容。
- 快速创建多个测试版本。
- 从 LMS、课堂或其他任意位置进行测试。

0.7 作者团队

本书由 Michael Whitman 和 Herbert Mattord 联合创作，结合了本研究领域内的理论知识以及商界的实际经验。

Michael Whitman 博士，是经过认证的信息系统安全经理和信息系统安全专业人员，是乔治亚州肯尼索州立大学 Michael J. Coles 商学院信息系统系的信息安全教授，他还是该大学信息安全教育中心(infosec.kennesaw.edu)的主任。Whitman 博士的主要研究领域有信息安全、公平可靠地使用策略、计算道德准则和课程编制方法等。目前他讲授信息安全和应急计划的大学课程和研究生课程。他还在其领域的顶级刊物“Information Systems Research”、“Communications of the ACM”、“Information and Management”、“Journal of International Business Studies”和“Journal of Computer Information Systems”等发表了一些文章。Whitman 博士也是“Information Security Education Journal”的主编。他是信息系统安全学会、计算机学会和信息系统学会的成员， Whitman 博士还与他人合著了 *Management of Information Security*、*Principles of Incident Response and Disaster Recovery*、*Readings and Cases in the Management of Information Security*、*The Guide to Firewalls and VPNs*、*The Guide to Network Security* 和 *The Hands-On Information Security Lab Manual*，这些图书都由 Cengage Learning 出版社出版。在 Whitman 博士开始其学术生涯之前，他是一名美军的装甲骑兵队军官。

Herbert Mattord 是 Ph.D.、CISM 和 CISSP。他曾经做过应用程序开发人员、数据库管理员、项目经理和信息安全专业人员。他在结束了 24 年的 IT 职业生涯之后，于 2002 年进入肯尼索州立大学。Mattord 教授是信息安全与保证学位管理学士协调员，以及 KSU 信息安全教育和意识中心(infosec.kennesaw.edu)的副主任。他也是“Information Security Education Journal”的副编辑。在 IT 从业期间，他已经是肯尼索州立大学、乔治亚州玛丽埃塔市南方理工州立大学、得克萨斯州奥斯汀市奥斯汀社区学院以及得克萨斯州立大学圣马科斯分校的副教授。目前他讲授信息安全、数据通信、局域网、数据库技术、项目管理、系统分析和设计以及信息资源管理与

策略等大学课程。他曾是 Georgia-Pacific 公司的公司信息技术安全部门的经理。本书包含了他的诸多实践知识。Mattord 教授还与其他人合著了 *Management of Information Security*、*Principles of Incident Response and Disaster Recovery*、*Readings and Cases in the Management of Information Security*、*The Guide to Firewalls and VPNs*、*The Guide to Network Security* 和 *The Hands-On Information Security Lab Manual*，这些图书都由 Cengage Learning 出版社出版。

0.8 致谢

作者感谢他们的家人一直给予的支持与理解，作者在写作这本书期间投入了大量时间，甚至于错过了一些家庭活动。特别要感谢 Carola Mattord 博士。她对本书的草稿进行了审订，提出了一些建议，使作者将注意力集中在学生需要上，让最终成稿易于阅读。

贡献者

一些人士和组织为本书提供了材料，感谢他们的贡献。例如，本书中的许多引用、表格、图形和其他内容都来自美国国家标准与技术研究院(NIST)。

评审者

感谢以下人士对本书的最初提议、项目规划和逐章评审所给出的反馈：

- Paul Witman, 加利福尼亚路德大学
- Pam Schmelz, 印第安纳常春藤技术社区学院
- Donald McCracken, 弗吉尼亚 ECPI 大学
- Michelle Ramim, 佛罗里达诺娃东南大学

特别致谢

作者要感谢 Cengage Learning 的编辑和制作团队。他们勤奋而专业的工作大大提升了成稿的质量：

- Natalie Pashoukos, 高级内容开发编辑
- Dan Seiter, 开发编辑
- Nick Lombardi, 产品经理
- Brooke Baker, 高级内容项目经理

另外，一些专业组织、商业组织和个人为作者提供了信息和灵感，帮助了本书的创作。作者感谢他们的贡献：

- Charles Cresson Wood
- Donn Parker
- 我们在 KSU 信息系统系和 Coles 商学院的同事们

作者的承诺

作者承诺以本书选用者和读者的需求为己任。我们很乐意收到读者对本书及其辅助材料的反馈。读者可通过 Cengage Learning 联系作者，电子邮件地址为：mis@course.com。

0.9 序

信息安全更像是艺术而非科学。掌握如何保护信息安全，要求具备大量多学科知识，以及相关经验和技能。本书作者将通过真实场景介绍每个主题，带领读者理解安全系统开发生命周期，所以通过学习本书，读者可掌握大部分需要的知识。作者实际经验丰富，并运用学院式方法，为读者提供了丰富的学习体验。读者选择这本书是正确的决定。

选择阅读本书，说明读者很可能想要以信息安全作为职业，或者至少对信息安全有浓厚的兴趣。有一点在心理上必须做好准备：几乎每个人都讨厌安全性给他们的工作带来的约束。好人和坏人都是如此，不过恶意黑客是个例外，他们喜欢把我们安装的安全措施视为要击败的挑战。我们把注意力集中在阻止有意作恶的人们身上，因为此时采取的措施也会防止其他人在无意间做坏事。针对无意间犯错的人们设计安全保护措施不足以防御有意作恶的人们。

工作 40 年的时间里，我使用计算机，与心怀恶意的人们斗智斗勇。这是一个令人兴奋且回报颇丰的领域，读者也会发现如此。安全控制和实践包括登录和注销、使用密码、加密和备份关键信息、锁住门和抽屉、激励利益关系人支持安全性，以及安装防病毒软件。只有在困境出现的少数时候，这些保护措施才会提供收益。没有问题出现，良好的安全性就发挥了作用，但是当没有问题出现时，谁又需要安全性？现如今，除了丢失记录，我们仍然需要安全性，因为这是法律、规章和审核者的要求——当我们处理其他人的私人信息、电子货币、知识产权以及保持领先竞争对手时尤其如此。

知道雇主的信息和系统比较安全，并且自己得到了可观的报酬，在发生紧急情况时成为焦点人物，把自己的才智用在对抗坏人上，这会带来极大的满足感。所以虽然安全工作存在缺点，这些满足感足以补偿。但是这份工作不适合完美主义者，因为我们几乎从不会做到彻底成功，总是会存在我们不知道或者坏人们先于我们发现的漏洞。敌人们相比我们具有巨大优势。他们只需要在已知位置(电子位置或物理位置)找到一个漏洞和一个目标，在他们选择的时间进行攻击，而我们则需要防御针对资产和漏洞可能发生的数百万次攻击，而这些攻击已经不再发生在一间电脑室中，而是分布在整个世界中。就好像我们在打一个游戏，但是我们不知道对手是谁，在什么地方，在做什么，他们为什么这么做，并且他们在玩游戏的过程中总在悄悄地修改规则。我们必须遵守道德，保持警戒、秘密和谨慎。夸耀自己的安全措施多么出色可能会向敌人泄露信息。享受自己经历的少量成功时刻，因为有一些成功你甚至不会知道。

有一个故事描述了我们所踏入的战场。有一个小国家征召了一个年轻人入伍，但是军队装备紧缺，没有足够的枪支，所以在培训这个新兵时给了他一个扫把。在基本训练中，年轻人问："我拿这个扫把做什么？"

指导员把他带到射击场，告诉他假装这个扫把是一把枪，然后瞄准目标说"砰，砰，砰"。他照做了。然后指导员带他进行刺刀练习。新兵问："我拿这个扫把做什么？"

指导员说："想象它是一把带刺刀的枪，然后说，'刺，刺，刺'。"

新兵仍然照做。后来战争爆发，军队仍然没有足够的枪支；新兵上了前线，敌军朝着他冲过来。他只有一个扫把，所以能做的就是指导员在训练中教导他的。他把扫把瞄准敌军，说："砰，砰，砰。"敌军的一些士兵倒下，但是仍然有很多在继续前进。一些士兵冲到了他身边，他只能说："刺，刺，刺。"更多的敌军士兵倒下了。但是，仍然有一个顽固的敌军士兵(这样的故事中总会有这样一个士兵)朝着他冲过来。新兵说："砰，砰，砰"。但是没用。敌人不断

接近，新兵说："刺，刺，刺"，但是仍然没有用。敌军士兵把他撞倒在泥地上，折断了他的扫把。在敌军士兵冲过他身边时，新兵听到这个敌军士兵在喃喃低语："坦克，坦克，坦克"。

我在许多讲解计算机犯罪和安全性的课程最后说过这个故事，目的是让听众深刻认识到，如果我们要战胜罪犯，就必须知道规则，而罪犯在进行犯罪行为时制定了他们自己的秘密规则。这让我们战胜他们变得十分困难。

我在里约热内卢讲课时，面对着几百位带有耳机的听众，一位年轻的女士负责同声传译，把我讲的内容翻译成葡萄牙语。在这种情况中，我不知道我的听众听到的是什么。我讲了那个笑话，但是没人发笑。他们只是坐在那里，一脸莫名其妙的样子。课后，我问这位翻译发生了什么情况。原来，她把"坦克、坦克、坦克"翻译成了"水箱、水箱、水箱"。那一次，新兵和我都被欺骗了。

三周后，我在巴黎的乔治五世酒店给一群法国银行家讲课。我的一位精通双语的朋友听了我讲课内容的翻译。里约热内卢的事件再次发生。没人发笑。后来，我问我的朋友发生了什么。他说："说出来你不信，那个翻译把'坦克、坦克、坦克'翻译成了'谢谢'。"就算是在讲笑话时，我也和那个新兵一样，不知道游戏的规则是什么。

记住，在安全行业工作，我们就像在一个虚拟的军队中，保护雇主和利益关系人不受敌人侵害。从我们的角度看，敌人在思考和行动时很可能没有理性可言，但是从他们的角度看，他们是非常理性的，通过破坏我们的安全措施来解决严重的个人问题并获得收益。我们不只是负责在系统和网络上安装技术控制的技术专家。我们的主要工作应该是帮助潜在受害者避免陷入信息困境，以及对抗狡猾但是常常无理性的敌人，尽管我们很少见到甚至辨别出他们。我在安全行业的职业生涯中，大部分时间用到了找出计算机罪犯并对他们和他们的受害者进行采访，试图得到一些深刻的认识，以更好地防御他们的攻击。类似地，读者应该利用每个机会来找出计算机罪犯并了解他们。这种经历能使你作为一个真正的、独特的专家收获声望，即便你只接触到了很少的敌人。

在真正进行防御时，全面性是一个重要方面，因为敌人会找出最简单的方式来攻击我们尚未彻底保护或者甚至不知道存在的漏洞和资产。例如，危害资产是在威胁列表中很少看到的一个威胁，也就是让信息资产存在风险。危害资产也是安全专业人员最常见的违反安全的行为；当他们透露关于自己的安全措施和灭失记录的过多信息时，就会发生危害资产。

我们必须做到彻底而细心，记录所有相关信息，这是萨班斯-奥克斯利法案的要求，同时在有人质疑我们的能力时使我们能够提供反驳的证据。把文档记录锁好。文档很重要，这样当敌人进行攻击而我们输掉战斗时，我们就有证据说明尽管发生了损失，但是我们已经尽力。否则，我们的职业生涯可能受到冲击，至少我们的效率会降低。例如，如果发生损失的原因是管理层没能为我们知道需要的安全性提供足够的预算和支持，那么在损失发生前，我们应该已经记录下这种问题。不要吹嘘我们的安全措施多好，因为再好的安全措施都可能被击败。用一个清单记录下所有事情，并不断补充这个清单。清单中记录的内容包括威胁、漏洞、资产、关键的潜在受害者、恶行嫌疑人、安全支持者和不支持者、攻击、敌人、司法正义资源、审核者、监管者和法律顾问。为了帮助利益关系人(他们是自己的信息和系统的第一线防御者)，必须确定他们必须保护什么，以及他们的安全性到底如何。确保高层管理者和你的主管理解你的工作的本质和局限。

我们自己应该使用最佳安全实践来建立一个好的示范。在完成工作时，我们会知道大量敏感的密码。把它们写下来，然后把这个单子安全地放到钱包中，和信用卡放一起。尽可能深入

地了解组织的系统和网络，并知道如何联系其他问题的专家。与本地和国家司法正义官员、组织的律师、保险风险经理、人力资源、设施经理和审核员建立良好关系。审核是组织具备的最强大的控制方法之一。记住，人们讨厌安全措施，必须通过惩罚和奖励措施来恰当地激励他们实施安全。寻找一些方式来让安全性对利益关系人透明，同时仍然使之有效。不要推荐或者安装利益关系人不会支持的控制或实践，因为他们会表现得好像控制措施生效，但其实并非如此，这种情况要比没有安全性更加危险。

这份工作最令人激动的地方之一是我们能够深入理解组织的内部机制和秘密，以及组织的业务和文化。作为一名信息安全顾问，我有幸了解到250多家全球性的大公司的文化和秘密。同样幸运的是，我有机会采访权力极大的公司执行官们，并为他们提供建议，尽管他们的时间十分宝贵，这个过程可能只用了几分钟。我们总是应该准备好一个“银弹”，以便在与公司高层交流的短暂时间中，为公司安全性带来最大收益。认真了解管理层对安全需求的限制。了解业务的本质，知道这是一个政府部门还是一个竞争激烈的公司。有一次，我参与了一个会议，与某公司的董事会成员激烈讨论如何保护他们最大的商业秘密——新的一次性尿布的制造过程。

最后一点重要的建议。一定要信任同行，与他们建立互信的关系。我们最重要的目标不只是降低风险，增加安全性，还包括努力避免疏忽和危害，遵守所有法律和标准，并且当安全成为一个竞争或者预算问题时使其可以实施。为了实现这些目标，我们必须与同行以彼此信任的方式交换最敏感的安全信息，这样就能够知道自己的组织相对于其他企业处在一个什么样的位置上。但是与此同时，一定要保持谨慎小心。我们需要知道普遍接受的最新的安全解决方案。如果交换的信息被公开，就可能会危害自己和他人的职业生涯，并且为自己的组织带来灾难。我们的个人和道德表现必须无懈可击，并且我们必须竭尽全力来保护自己的声誉。要特别关注本书介绍道德的部分。我建议读者加入信息系统安全协会，并成为其中活跃的一员，当自己合格后进行专业认证。我最喜欢的认证是国际信息系统安全认证协会的信息系统安全专业人员认证(CISSP)。

Donn B. Parker, CISSP
加利福尼亚洛斯阿尔托斯

目　录