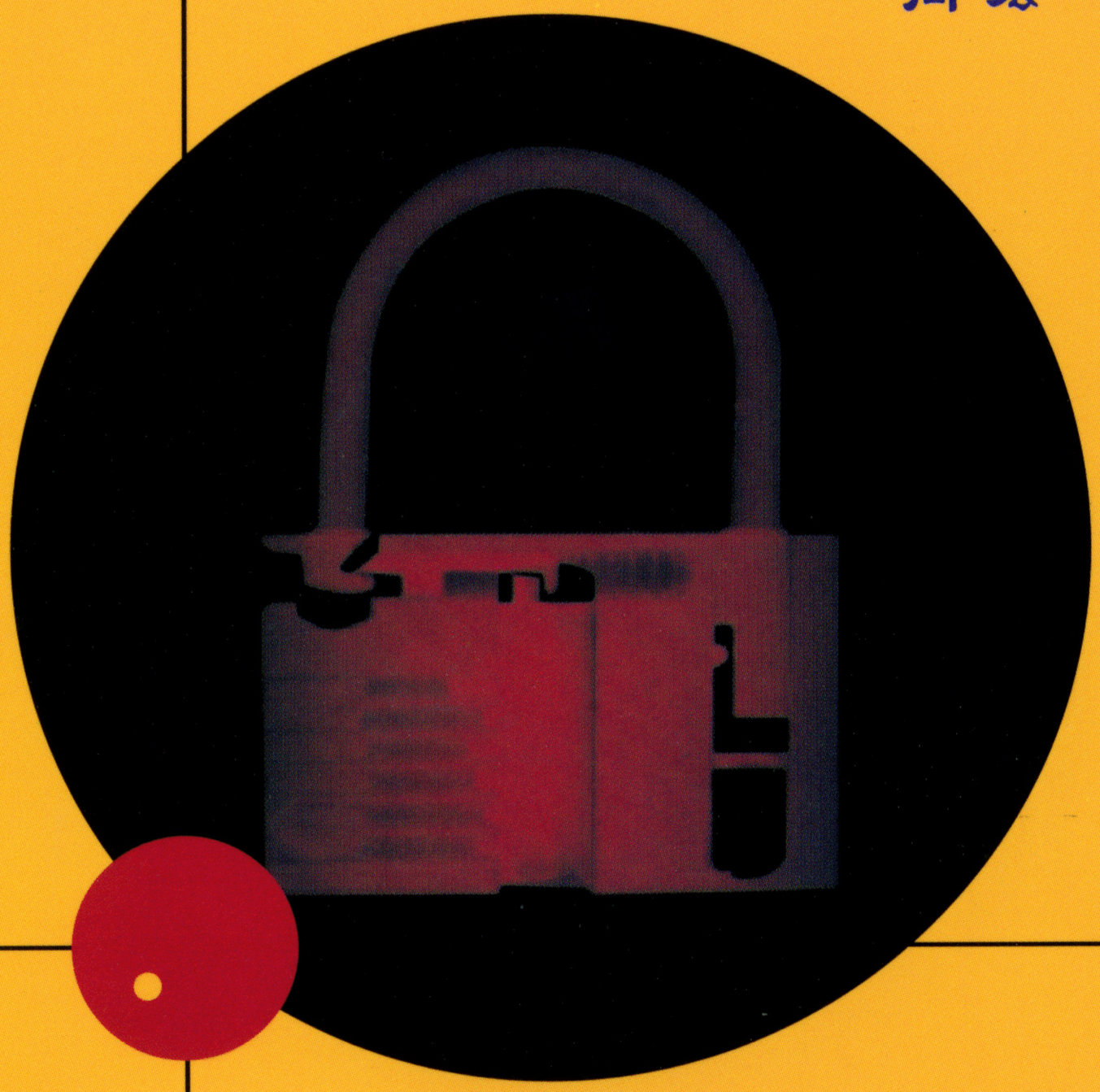
THOMSON

信息安全丛书

信息安全管理

[美] MICHAEL E. WHITMAN AND HERBERT J. MATTORD 著

向宏 傅鹂 主译



重庆大学出版社

信息安全管理

[美] 酡 著

向摇宏摇摇摇傅摇鹂摇摇主译

重庆大学出版社

前言

摇摇随着全球网络的持续发展，网际互联对于通信系统和计算系统的流畅运作变得愈发重要。然而，日益增多的病毒、蠕虫攻击网络的事件以及许多的黑客网络犯罪表明，当前的信息技术还存在诸多缺陷，因而有必要提高信息系统的安全。

当前，为了保护系统和网络的安全，许多机构必须吸收大量的信息安全从业者，这些机构还指望依靠具有熟练技巧和丰富经验的专业人才，来开发更为安全稳定的计算系统。网络安全技术专业的学生必须了解现有系统的缺陷和一些不安全因素，也必须学会去设计、开发应对这些威胁的系统软件。

本书的目的是为了满足对高质量的信息安全专业教材的不断增长的需求。虽然有许多信息安全的优秀出版物，但很少有相关教材去指导学生学习信息安全管理方面的知识。我们特别针对学习信息系统管理的学生编写此书，希望能弥补上述遗憾。有一点需要指出，如读者具有信息系统、刑事司法、政治科学和会计信息系统等学科的知识，就能更好地理解信息安全管理基础及其管理策略的发展状况。本书的宗旨是，现代机构中的信息安全是一个管理问题，而不只是一个技术问题。信息安全具有重要的经济意义，需要从管理的角度来认真把握。

本书特色

摇摇本书给读者提供了一个信息安全的管理视角，指导读者正确对待信息安全管理问题。本书既可用于信息技术专业学生以及 [illegible] 行业管理层的信息安全课程，也可用于商业或技术管理专业学生的信息管理和技术管理类课程。

因为作者是信息系统安全认证专家（[illegible]），虽尽量避免把本书写成一部 [illegible] 学习指南，但作者的学识背景仍然促使他在一定程度上把大量的 [illegible] 知识（特别是信息安全管理方面）并入了本书中。

章节情境（[illegible]）——每一章都以一个简短的故事开始，故事描述了一个虚构公司遇到的各种不同的信息安全问题。每一章结尾都有总结，并提出了相关的讨论问题，这些问题为学生和老师提供对某些相关内容进行讨论和交流的机会。

观点（[illegible]）——每一章中都有一篇信息安全技术的实践者或学者的短文，这些内容提供了一系列的评论来说明一些有趣的论题和个人的观点，拓宽了学生在这些论题上的知识面。

附加材料（[illegible]）——这一段强调了一些有趣的主题并对一些技术上的问题做了详细的阐述，允许学生就某些主题进行更深入的探究。每章包括一个威胁管理小节和所需的附加材料。

实践学习（[illegible]）——在每章末尾，有小结、复习问题以及习题和案例练习，为学生提供了课外练习的机会。通过练习，学生能研究、分析、总结以提高学习的成效并且能够加

深他们对课文的理解。借助案例练习，学生通过专业的判断、仔细的观察和初步的研究，找出简单的信息安全问题的解决办法。

作者简介

摇摇酝[illegible]一起撰写的这本教材将商业领域的实践经验和学术领域的学术研究结合起来。酝[illegible]博士是肯尼索州立大学（位于美国佐治亚州的肯尼索）计算机科学与信息系统系信息系统方向的副教授，他还是信息系统科学硕士导师和为信息安全教育与意识提升而设立的 运[illegible]战中心的主任。他和 [illegible]是《信息安全原理》（[illegible]一书的作者，该书由 悦[illegible]出版发行。宰[illegible]是信息安全、公正可靠使用策略、伦理计算和信息系统研究方法等领域的活跃研究者。他目前在教授本科生和硕士研究生信息安全、局域网和数据通信等课程。他在专业领域的许多一流杂志，如 [illegible]上发表了论文。他是信息安全协会、计算机安全研究所、机器计算协会和信息系统协会的活跃成员。宰[illegible]与人合著了一本实验手册《[illegible]》，该手册由[illegible]公司出版。他和 [illegible]教授还是大学课程研讨会的常客。

[illegible]（酝[illegible]认证专家）在 [illegible]领域已经有 圆[illegible]年的工作经验，他做过应用程序开发员、数据库系统管理员、项目经理，并作为信息安全的实践者加入了肯尼索州立大学的教师队伍。他和 酝[illegible]合作编写了《信息安全原理》一书。在他作为 [illegible]从业者的职业生涯中，他曾经是美国肯尼索州立大学、州立南方工业大学（[illegible]位于佐治亚州的玛丽埃塔）、奥斯汀通信学院（位于美国德克萨斯州的奥斯汀）以及德克萨斯州立大学（位于圣马科斯）的兼职教授。现在他讲授的大学课程包括信息安全、数据通信、本地局域网、数据库技术、项目管理以及系统分析与设计。同时，他也是信息系统安全与保障中心认证部门的协调人，信息系统安全协会以及计算机协会的活跃分子。他曾经是[illegible]公司中信息安全技术部门的前任主管，这本书以及他以前著作中的很多应用知识都出自于该公司。

结 构

摇摇本书按照计划、策略、人员、项目以及保护机制等内容分为 员[illegible]章和 员个附录。

第 员部分摇简介

第 员章摇信息安全管理简介

作为全书的起始，本章为理解信息安全奠定了基础，揭示了信息技术的重要性并指出谁应该负责保护机构的重要信息。读者可在本章中了解信息安全的定义和重要特点，以及信息安全

管理与普通管理的区别。

第 圆部分摇计划

第 圆章摇安全计划

本章阐明了计划的重要性,并讲述了组织计划和信息安全系统实施计划的主要内容。

第 猿章摇应急计划

本章讲述了应急计划的必要性,形象地介绍了怎样根据业务影响分析建立一系列简单的应急计划,以及怎样测试这些计划。

第 猿部分摇策略和项目

第 源章摇安全策略

本章定义了信息安全策略,并讲述了它在一个成功的信息安全项目中的中心地位。研究表明,有 猿类主要的信息安全策略 :本章解释了每一类安全策略的内容,并对怎样开发、实施和维护各种类型的信息安全策略做了示范。

第 缘章摇制定安全项目

本章探索了信息安全的各种不同组织方法,并且阐述了信息安全项目的各个功能组件。读者将学习怎样按照机构的规模去规划和配置机构的信息安全部门人员,也将学习怎样评估影响机构及其活动的内外部因素。本章也鉴别和描述典型的工作职务,并且阐述了它们在信息安全计划中所扮演的角色。最后,讲述安全教育、培训和意识提升项目的设立和管理。

第 远章摇安全管理模型与实践

本章介绍了几个主要的信息安全管理模型的组件(包括经美国政府同意的模型),还讨论了怎样实现这些模型以适应某个具体机构的需求。读者将学习怎样实现信息安全管理关键操作的基本要素,并理解美国联邦 隐系统认证和鉴定中出现的新趋势。

附录——[illegible]信息技术系统的安全性自我评估指南,人工防火墙委员会安全管理索引概览。

根据美国国家标准与技术研究院([illegible]文档和人工防火墙委员会安全管理索引,本附录介绍了基本的安全管理模型。

第 源部分摇保护机制

第 苑章摇风险评估

本章定义了风险管理及其在机构中的作用,描述了怎样使用风险管理技术以鉴别信息资产的风险因素,并对其按重要性次序进行区分。风险管理模型根据不利事件的可能性及其发生时

对信息资产的影响对风险进行评估。最后，简单讨论了怎样记录风险鉴别的结果。

第 愿章摇风险管理和控制

本章介绍了基本的风险缓解策略选择，并对如何控制风险进行了讨论，包括鉴别风险控制分类，使用已有的概念框架对风险控制进行评估，并提出了成本效益分析法。读者将学习怎样实施和坚持风险控制。除了在本章前面部分介绍的方法外，还介绍了 剖猪跨玉风险管理方法。

第 怨章摇保护机制

本章通过介绍访问控制方法，向读者展示了技术上的风险控制方法：包括认证、授权以及使用生物特征测量的访问控制；定义并识别防火墙和常用的防火墙实施方法；另外，该章还涉及了拨号访问、入侵检测系统和密码学等技术控制方法。

第 缘部分摇人与项目

第 员园章摇员工与安全

本章进一步阐述了第 缘章介绍的信息安全职位的要求和技术。探讨各种信息安全专业认证，以及每种认证包含的具体技巧。在本章后半部分，探讨了在机构人力资源配置方面对信息安全约束条件的实施状况，机构用这些约束来控制员工的行为，防止对信息的误用。

第 员员章摇法律和道德

在本章中，读者将了解到与信息安全相关的法律环境以及它们之间的关系。这一章讲述影响信息安全实施的主要国内国际法，以及文化在信息安全道德规范中所起的作用。

第 员圆章摇安全项目管理

最后一章覆盖了信息安全领域里的项目管理，提供了基本的项目管理技术，还介绍了如何把项目管理原则应用到信息安全计划中。

教师资源

摇摇我们为本书准备了多种教学工具，并提供了提高课堂教学效率的多种资源。教师只须填写书末的教辅材料申请表，寄给 栽葬藻遭司公司北京办事处就可以索要如下资料。

教师电子手册——该教师手册包括使用本教材的建议和方法（例如对讲课要点的建议），也包括复习题的答案，并且对每章的练习题给出了参考答案。

图形文档——老师可以利用取自本书图片的文档对所讨论的问题给出自己独到的阐述。

幻灯片——本书为每章提供了 孕葬糟辩酝藻灯片。作为课堂教学辅助工具，可供学生用于网上复习，也可打印出来在课堂上分发。教师也可以把补充的附加论题做成他们自己的幻灯片。

实验手册——栽课考驶士蒸酬醒公司已专门出版了一本与本书匹配的实验手册，该手册由

本书的一位作者所著。

信息安全和保障研究计划课程设置——除了本书外，在肯尼索州立大学的信息安全教育和意识提升中心，你还可以获得信息安全和保障研究计划课程设置文档。该文档详细介绍了如何设计和实施安全课程，并且从作者的角度给出了指导意见。

考试大观——是满足客观、公正测试需要的最佳工具，是一个强大的客观公正的考题生成器。它使教师能够根据专门设计的 [illegible] 课本题库编制试卷，或组织网上考试，在不到 缘分钟的时间里，教师就可根据 [illegible] 题库，利用高效快速的测试向导编制考卷，也可由教师自己组合题目来制定考卷。

鸣 谢

摇摇笔者要感谢家庭的理解与支持，因为在本书编写过程中，耗费了大量的时间，特别是许多时候占用了家庭活动的时间。特别感谢乔治亚州大学英语博士生 [illegible] 她对本书的初稿作了评审，并且建议本书的编写以学生为潜在的读者，这些都使得本书更具可读性。

几位肯尼索州立大学的学生也参与了本书的编写准备工作，感谢他们为此所作出的努力。在第 愿章的威胁管理小节中列出了他们的名字。

向以下对本书做出贡献的人员表示感谢。他们对本书的初步方案、项目大纲提出各自有力的见解，并对每一章都进行了评审。

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇感谢 [illegible] 出版社的编辑和出版人员，他们的勤奋工作和专业知识使本书水平大为提高：

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

此外，一些专业和商业机构人士也通过提供信息与灵感来帮助本书的编写，在此也感谢他们所做出的贡献：

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇 [illegible]

摇摇悦[illegible]

摇摇月[illegible]

摇摇远[illegible]

摇摇栽[illegible]

摇摇为编写威胁管理小节而做出努力的众多学生

摇摇[illegible]

摇摇悦[illegible]

摇摇肯尼索州立大学计算机科学与信息系的同事们

摇摇肯尼索州立大学计算机科学与信息系的[illegible]

笔者以满足读者需要为己任，非常愉快和荣幸地恭候关于本书及其相关材料的反馈意见，您可以通过悦[illegible]出版社的以下电子邮件地址联系我们：[illegible]。

序

悦[illegible]

在我从事信息安全工作的[illegible]年中，曾经为世界上[illegible]家不同的组织机构做过风险评估。不论该组织的规模多大，不论它的影响力多强，也不论公众认为它的科技水平有多高，我发现管理层都并未足够慎重地看待信息安全这个问题。一方面是因为信息安全还是一个相对较新的领域，而我们对它还知之甚少；一方面是因为高层管理对信息系统的技术了解不多，也不屑于去深入了解；还有一方面是因为高层管理做出的是传统的权衡决策，他们考虑较多的是诸如低成本、研发速度、贴近用户、新产品投放市场的时间等因素，而忽略了安全。

当今时代已经发生了翻天覆地的变化，但在大多数情形下，决策层还没有意识到随之而来的问题。以安达信（[illegible]）公司为例，它曾是世界上最大最负盛名的公共会计公司之一。安达信曾为安然公司提供审计和咨询服务。但现在，安然公司已经信誉扫地，大多数业务已经停止。美国证券交易委员会对安然的会计状况进行了调查，安达信的某些雇员为此毁掉了许多文档，而这些文档有可能与这些调查有关。安达信的雇员以及安然公司的会计销毁文档，主要是由于他们曲解了公司的文件销毁规定。当安达信公司某些雇员销毁成千上万镑重的安然公司文件时，他们还觉得自己所做的是正确的。当然，文件销毁是信息安全领域的一个重要组成部分。如果这些雇员在文件销毁规定方面能预先接受更好的培训，那么安达信公司今天可能仍然存在。因此，对信息安全的曲解和缺乏这方面的培训，就导致了一个世界上最优秀会计公司的倒闭。然而直到现在，决策层仍然错误地认为，信息安全相对来说不是很重要，不值得给予太多重视。

另外，请注意最近一次由[illegible]公司搞的民意测验。调查显示，整整[illegible]的美国公众认为，在没有经自己允许的情况下，他们的个人信息也会被其他组织共享。很明显，美国公众不相信商业机构和政府机构，即使他们出台了个人隐私保护政策。美国人认为这些政策只不过是“窗口装饰”，或者说是取悦审计员的某些东西。在此，我们可以看到这主要是一个信任问题，顾客不相信商业机构和政府机构对个人数据保护的陈述，表明了这些机构在此问题上的严重失败，他们没法让顾客相信他们会负责任地尊重个人隐私权。同时，一个由类似机构（那时

称为 [illegible] 更早完成的一项研究报告指出，当客户的隐私得到充分的保障，电子服务（如因特网业务）的使用率将成倍增加。也就是说，如果客户觉得他们的个人信息得到充分保护，他们将有可能成倍增加在线定单。

然而，决策层很少为信息安全分配足够的资源，比如设置一个“ 首席个人隐私保护官员 ”，致使客户觉得，网上交易是件痛苦的事。通常，决策层并没有意识到做好信息安全工作会给企业带来怎样的诸如竞争优势这样的切实利益。对决策层来说，如果能够成倍增加交易额这样的事都不重要，那么什么才是重要的呢？

如今，需要把信息安全作为一个机构的常规工作。人们在自己的工作中有必要考虑信息安全，部门在任务说明中也需要考虑信息安全，而且外购公司在签合同时也应考虑信息安全。每台个人计算机都有必要安装病毒检测软件包、防火墙以及相关软件，最终用户也有必要接受信息安全培训。例如当计算机感染病毒时，他们应当知道怎么做。如今，最终用户处在信息安全战争的前沿。信息安全战争是一种新的、比以往更复杂、更具攻击性的战争，它能威胁信息系统的安全，并且每天都在向前发展。

信息安全不仅仅只是信息技术部门以及技术人员的职责。例如，那些电话采访者或所谓的调查者，他们往往试图通过所谓的‘ 社会工程 ”（[illegible]，即欺骗或电子欺诈技术来获得信息。这种技术包括诱导客户相信来电者的虚假身份。访问者可能说他们来自 [illegible] 部门，他们为了改正网络中的问题而需要拥有用户的用户名和固定密码，虽然可能听起来难以置信，但研究却显示大部分用户会轻易地泄露他们的用户名和密码，除非用户事先意识到不能泄露这些敏感的个人数据。

凡是接触到敏感、有价值或重要数据的人员，都必须了解数据安全的重要性。这意味着垃圾清理工需要知道应该如何解决那些可能被扔到垃圾箱中的机密文档。同样，正在前台接电话的临时职员需要知道可以把什么信息告诉给外人。这也意味着外包公司必须知道如何回击闯入的黑客，以便把损失降到最低，维护公司的良好声誉并使公司的业务能够不被中断。换句话说，信息安全必须依靠团队精神，团队上下一致使用相同的安全策略，让每个人在各自的领域发挥作用，只有这样，才能保证机构的信息安全。

在此，我以此书来告诫未来的领导者们，在商业领域和政府机关工作的每一个人都应该了解一些信息安全知识。如果他们完全不关注信息安全，那么现在大学的很多信息安全课程将陷入泥潭。尽管这类技术是有趣的，但这只是一个观念。领导者们需要了解一些信息安全的实用信息，如此他们才能理解信息安全的重要性和使用方式。信息安全领域规律多变、部门众多、结构复杂，未来的商业领导者们必须考虑信息安全是如何与他们将来的工作相联系的。

当今社会，对信息安全知识的需要比以往更加紧迫。美国联邦调查局和计算机安全委员会每年都会相互合作进行关于计算机犯罪的调查。最近的一次调查显示，计算机犯罪造成的损失比上一年上升了 [illegible]（显然，这一状况还不足以引起决策层的注意 ）。然而，仍然有 [illegible] 的受调查者连应该向哪里报告违规和事故那样简单的规定都不知道。如果一个机构的工作人员不知道应该在什么时间、向谁汇报违规和事故，那么当发生信息安全问题时，管理者就不能知道到底发生了什么。如果管理者不清楚情况，那么他们就不可能及时、合理地处理安全问题。为了合理地解决这类问题，本书探讨了如何帮助管理者及时地掌握所发生事件，确定处理问题的最佳方式和最好途径。

—— [illegible]

独立信息安全顾问

写于 [illegible]

苑

序

摇摇随着世界科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息网络已成为国家和社会发展新的重要战略资源。与此同时，社会对信息的依赖程度越来越高，网络和信息系统的安全问题愈加重要。保障网络与信息系统安全，更好地维护国家安全、经济命脉和社会稳定，是信息化发展中必须要解决的重大问题。

面对复杂多变的国际环境和互联网的广泛应用，我国信息安全问题日益突出。加入世界贸易组织、发展电子政务等，对信息安全保障提出了新的、更高的要求。我国政府始终高度重视信息安全问题，将信息安全作为全面推进我国国民经济和社会信息化进程的重要环节，做出了一系列重要决策和部署。[illegible]年 [illegible]月国家信息化领导小组研究提出了《关于加强信息安全保障工作的意见》，进一步明确了我国信息安全保障工作的总体要求、主要原则和重点任务；[illegible]年初又专门召开了全国信息安全保障工作会议，对信息安全保障工作做出了全面部署，为国家信息安全保障体系的建设注入了强劲的动力，将我国的信息安全工作推进到一个崭新的阶段。

有幸经历近 [illegible]年来中国信息化进程的人都不会忘记，我国信息安全事业的发展，技术的进步和产业水平的提升从世界各国，特别是西方发达国家得益颇多。现代信息安全概念和技术的引入，给长期以通信保密为核心的中国信息安全界带来一股清新的风，它们的许多理论、观点、概念和方法对更新我们的安全观念、发展自主的安全技术、加强信息安全的管理等都发挥过相当积极的影响，进入新世纪后，在中国加入 [illegible]和经济全球化的推动下，国内外在信息安全领域的学术交流和技术互动日益加深，信息安全国际化已成不可阻挡之势。在统筹考虑国际国内两个大局的背景下，中国信息安全界对于世界各国，尤其是西方发达国家的信息安全理念、法则、规范和实践经验的学习与研究正掀起新一轮热潮。

与过去相比，新一轮的学习与研究热潮在内容上已有本质的提高。几年前，西方的信息安全理论和技术让急于寻求解决方案和发展思路的中国信息安全界眼界洞开，我们曾以一种饥不择食的急迫心情将西方的信息安全理论、概念和做法搬到国内来。但近年来，我们欣喜地看到，中国信息安全产业界和学术界已逐渐走向成熟，开始理性地审视国外的技术与方法，紧密结合中国的实际需要精心选择国外信息安全理论和实践的成果，并在研究、思考的基础上，努力探索适合中国国情的信息安全之路。生活在重庆的几位归国学人和青年学者从众多的海外著述中精选了《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》和《灾害恢复指南》猿本，细心译介给国

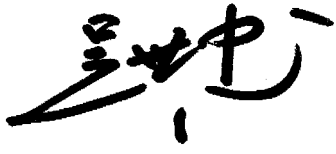
员

内，就是众多的努力之一。信息安全意识、信息安全管理和安全容灾与恢复正是当下国内急需的知识与方法。从这三本书内容的深入浅出和方法的清晰实用，可以看出编译者的良苦用心，相信他们的愿望和努力会得到业界和学界的认可和尊重。

中国信息安全事业的发展需要更系统、更全面、更深入地翻译、介绍国外的经典著述，需要更迅速、更经济、更便捷地学习、掌握他人的实践经验。因此，我们十分乐见《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》、《灾害恢复指南》猿本译著的出版，并乐于在其付印之前，将个人的观感和陋见附上，以示敬意。

兹为序

中国信息安全产品测评认证中心摇摇摇主摇任
中国信息产业商会信息安全产业分会摇理事长
全国信息安全标准化技术委员会摇摇摇副主任



圆猿园园猿年秋
于北京昆明湖畔

译者序

摇摇提到信息安全，人们往往会将它与高深莫测、正邪难辨、技术高超的“黑客”和五花八门的计算机病毒联系起来。随着人类社会进入全球信息时代，层出不穷的 IT 技术正在冲击和改变着我们的日常工作、生活，甚至思维方式，从而进一步加深了人们对 20 世纪的“技术迷思”，不知不觉中形成了“信息时代 = 信息技术 = 西方信息技术”的惯性思维，仿佛以美国为代表的西方信息强国只是沉湎于纯技术的研发，并以此为利器引导着世界潮流的发展。

事实上，在各种令人眼花缭乱、晦涩深奥的 IT 技术、IT 规范、IT 解决方案后面，处处可以看到西方文化的烙印和科学管理、控制的思想。如果说信息像一只看不见的手渗透于社会各行各业之中，那么信息管理科学和信息控制方法则是指挥着这只手的大脑中枢神经。

信息安全作为信息科学的一个有机组成部分，是一个开放的、复杂巨大的系统，它所涉及到的知识囊括了自然科学和社会科学的各个领域，在这浩瀚的知识海洋里，管理与控制同样是信息安全领域的核心思想。然而目前我国出版界在筛选有关信息安全领域的学术专著中，通常将重心放在了国外技术专著的翻译上。而事实上，在信息安全这一高技术领域西方学者同样倾注了大量科学管理的心血。为此我们组织力量将 [illegible] 等人编写的《信息安全管理》一书翻译出来，“他山之石，可以攻玉”，希望此书的出版能对正在从事信息安全管理和技术工作的我国科技工作者有所裨益。

此书的翻译出版，得到了重庆大学出版社国际合作部的大力支持，重庆大学软件学院信息安全研究所的研究生董长青、罗蜀燕、陈京浩、夏晓峰、马涛等同学也积极参与了本书的翻译工作，在此一并表示衷心的感谢。由于时间仓促、能力有限，在翻译过程中仍有不少缺陷，希望能够得到广大读者的批评指正。

向宏　摇傅　鹂

[illegible] 年冬摇于重庆大学

目　录

第 员部分摇引摇言

第 圆部分摇计摇划

第 猿部分摇策略和项目

第 源部分摇保摇护

第 缘部分摇人与项目