<<信息安全管理与风险评估>>

图书基本信息

书名：<<信息安全管理与风险评估>>

13位ISBN编号：9787121105159

10位ISBN编号：7121105152

出版时间：2010-4

出版时间：电子工业

作者：张泽虹//赵冬梅

页数：173

字数：294400

前言

近年来，随着互联网的普及与应用，政府部门、金融机构、企事业单位和商业组织等对信息系统的依赖程度日益加深，信息技术几乎渗透到了人们日常工作与生活的方方面面。
置身高度开放的信息社会，计算机病毒、黑客入侵、信息失窃、物理故障……信息技术无处不在，安全事件时有发生，信息安全问题成为全社会共同关注的问题。
据有关部门统计，所有的计算机安全事件中，属于管理方面的原因比重高达70%以上，而这些安全问题中的95%是可以通过科学的信息安全管理来避免的。
因此，管理在解决信息安全问题中占重要作用，而管理的核心是信息安全风险评估。
目前，“信息安全管理与风险评估”已纳入我国普通高校信息安全、信息管理与信息系统、计算机科学与技术等专业的课程体系中，为使相关专业学生全面了解、掌握信息安全管理与风险评估理论与实践知识，我们组织编写了本教材，其教学目标是通过本课程的学习，使学生了解信息安全管理、信息安全风险管理、信息安全风险评估的基本知识、相关标准或指南，能够使用风险评估工具进行风险评估，能够对实际的企业、网站或单位进行信息安全管理、信息安全风险评估。
全书共分为8章。
第1章介绍信息与信息安全、信息安全管理、信息安全管理的目的，以及信息安全管理遵循的原则；第2章介绍国内外信息安全管理标准：BS 7799、ISO/IEC 13335、ISO/IEC 27001：2005、CC准则、GB/T 19715标准、GB/T 19716-2005；第3章介绍信息安全管理标准BS 7799实施中的问题及实施案例；第4章介绍信息安全风险管理概述及信息安全风险管理标准：AS/NZS 4360:1999、NIST SP800-30、The Security Risk Management Guide、GB/T 20269-2006；第5章介绍信息安全风险评估发展概况、信息安全风险评估的目的和意义、信息安全风险评估的原则、信息安全风险评估的概念、国内外信息安全管理标准：OCTAVE、SSE-CMM、GAO/AIMD-99-13、GB/T 20984-2007、信息安全风险评估方法，以及信息系统生命周期各阶段的风险评估；第6章介绍信息安全风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具、信息安全风险评估工具的发展方向和最新成果；第7章依据GB/T 20984-2007《信息安全技术 信息安全风险评估规范》，介绍信息安全风险评估的基本过程及各个阶段的主要任务；第8章依据GB/T 20984-2007《信息安全技术 信息安全风险评估规范》和第7章信息安全风险评估的基本过程，以某信息系统为例详细介绍信息安全风险评估的实施过程。
在编写上，根据当前高校相关专业课程体系设置情况，结合学生学习特点，力求保持内容的系统性、先进性和实践性，力求理论与实践相结合。

<<信息安全管理与风险评估>>

内容概要

本书以信息安全管理为主线，以信息安全风险评估为重点，对近年来国内外信息安全管理与风险评估的研究成果和应用实践，进行系统归纳和总结，全面介绍信息安全管理、信息安全风险管理、信息安全风险评估的基本知识、相关标准或指南，以及信息安全风险评估的工具、方法、过程等。

本书层次分明，结构合理，叙述严谨，重点突出，注重实验环节。根据章节内容，适量安排实验内容，并且将实验与习题分开，独立编写。

本书可作为高等学校信息安全、信息管理与信息系统、计算机科学与技术等专业本、专科学生的教材，也可作为从事信息化相关工作的领导、技术与管理人员的参考书。

<<信息安全管理与风险评估>>

书籍目录

章节摘录

插图：信息安全管理作为一个组织的整个管理体系中的一个重要环节，指导组织对其信息资源进行信息安全风险管理和控制。
只有建立统一、动态的安全管理，才能保证信息资源得以充分利用，发挥出系统的效率。
信息安全管理的目的，是通过对计算机和网络系统中各个环节的安全技术和产品实行统一的管理和协调，进而从整体上提高整个系统防御入侵、抵抗攻击的能力，使得系统达到所需的安全级别，将风险控制在用户可接受的程度，具体来说，信息安全管理的目的如下：（1）将政策、硬件及软件等方法结合起来，构成一个统一的分层防卫系统，阻击非法用户进入，以减少网络系统受破坏的可能性。
（2）通过非法活动的审计追踪，提供一种快速检测非法使用网络资源移迅速测定非法入口位置的方法。
（3）使网络管理者能够很快地重新组织被破坏了的文件或应用，使系统重新恢复到破坏前的状态，以最大限度地减少损失并促使系统恢复。
（4）使破坏者的一举一动均能在有效的监控之下，以便能被网络经营机构抓获，使其最终受到应有的惩罚。
1.4 信息安全管理遵循的原则信息安全管理应遵循以下原则。
1.规范原则信息系统的规划、设计、实现、运行要有安全规范要求。
要根据本机构或本部门的安全要求制定相应的安全政策，安全政策中要根据需要采用必要的安全功能，选用必要的安全设备，不应盲目开发、自由设计、违章操作、无人管理。
2.预防原则在信息系统的规划、设计、采购、集成、安装中应该同步考虑安全政策和安全功能具备的程度，以预防为主的指导思想对待信息安全问题，不能存在侥幸心理。

编辑推荐

《信息安全管理与风险评估》是由电子工业出版社出版的。

<<信息安全管理与风险评估>>

版权说明