

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<信息安全管理与风险评估>>

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，其教学目标是通过对本课程的学习，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

第1章 信息安全管理概述	1.1 信息与信息安全	1.1.1 信息	1.1.2 信息安全	1.2 信息安全管理
1.3 信息安全管理的目的	1.4 信息安全管理遵循的原则	习题1	第2章 信息安全管理标准	2.1 国
信息安全管理标准	2.1.1 信息安全管理标准BS 7799	2.1.2 ISO/IEC 13335	2.1.3 ISO/IEC	
27001:2005	2.1.4 CC准则	2.2 我国的信息安全管理标准	2.2.1 我国的信息安全管理标准概述	
2.2.2 GB/T 19715标准	2.2.3 GB/T 19716—2005	习题2	第3章 信息安全管理实施	3.1 信息安
管理标准BS 7799实施中的问题	3.1.1 企业信息安全管理的现状	3.1.2 信息安全管理标准实施的	3.1.3 信息安全管理标准实施的	
误区	3.1.3 灵活使用BS 7799	3.2 BS 7799信息安全管理实施案例	3.2.1 信息安全管理体系认证实	
施案例	3.2.2 BS 7799框架下安全产品与技术的具体实现	习题3	第4章 信息安全风险管理	4.1 信
安全风险管理概述	4.1.1 信息安全风险管理的概念	4.1.2 相关要素及概念	4.1.3 信息安全风	
险管理各要素间的关系	4.2 AS/NZS 4360:1999	4.2.1 AS/NZS 4360:1999简介	4.2.2 AS/NZS	
4360:1999的内容	4.2.3 AS/NZS 4360:1999风险管理流程	4.3 NIST SP800-30	4.3.1 NIST SP800-30	
简介	4.3.2 NIST SP800-30的内容	4.3.3 NIST SP800-30风险管理流程	4.4 The Security Risk	
Management Guide	4.4.1 The Security Risk Management Guide简介	4.4.2 The Security Risk		
Management Guide的内容	4.4.3 微软风险管理流程	4.5 GB/T 20269—2006	4.5.1 GB/T 20269	
—2006简介	4.5.2 GB/T 20269—2006的内容	4.5.3 GB/T 20269—2006风险管理	习题4	第5章 信
安全风险评估概述	5.1 信息安全风险评估发展概况	5.1.1 国外信息安全风险评估发展概况	5.1.2 我国信息安全风险评估的发展现状	5.2 信息安全风险评估的目的和意义
5.1.2 我国信息安全风险评估的发展现状	5.2 信息安全风险评估的目的和意义	5.3 信息安全风险	5.4 信息安全风险评估的原则	5.4.1 信息安全风险评估的概念
5.4 信息安全风险评估的相关概念	5.4.1 信息安全风险评估的概念	5.4.2 信息安全	5.4.3 信息安全风险评估的两种方式	5.4.4 信息安全风险评估的分
风险评估和风险管理的关系	5.4.3 信息安全风险评估的两种方式	5.4.4 信息安全风险评估的分	5.5 国外信息安全风险评估标准	5.5.1 OCTAVE
类	5.5.1 OCTAVE	5.5.2 SSE-CMM	5.5.3	
GAO/AIMD-99-139	5.6 我国信息安全风险评估标准GB/T 20984—2007	5.6.1 GB/T 20984—2007简介	5.6.2 GB/T 20984—2007的内容	5.6.3 GB/T 20984—2007的风险评估实施过程
5.6.2 GB/T 20984—2007的内容	5.6.3 GB/T 20984—2007的风险评估实施过程	5.7 信息安全风险	5.7.1 概述	5.7.2 典型的信息安全风险评估方法
5.7.1 概述	5.7.2 典型的信息安全风险评估方法	5.8 信息系统生命周期各阶段的风险	5.8.1 规划阶段的信息安全风险评估	5.8.2 设计阶段的信息安全风险评估
5.8.1 规划阶段的信息安全风险评估	5.8.2 设计阶段的信息安全风险评估	5.8.3 实	5.8.3 实	5.8.4 运维阶段的信息安全风险评估
5.8.3 实	5.8.4 运维阶段的信息安全风险评估	5.8.5 废弃阶段的信息安全风	5.8.5 废弃阶段的信息安全风	5.8.5 废弃阶段的信息安全风
5.8.5 废弃阶段的信息安全风	习题5	上机实验	第6章 信息安全风险评估工具	6.1 风险评估与管理工具
6.1 风险评估与管理工具	6.1.1 MBS		6.1.2 COBRA	6.1.3 CRAMM
6.1.2 COBRA	6.1.3 CRAMM	6.1.4 ASSET	6.1.5 RiskWatch	6.1.6 其他风险评估与管理
6.1.3 CRAMM	6.1.4 ASSET	6.1.5 RiskWatch	6.1.6 其他风险评估与管理	6.1.7 常用风险评估与管理工具对比
6.1.4 ASSET	6.1.5 RiskWatch	6.1.6 其他风险评估与管理	6.1.7 常用风险评估与管理工具对比	6.2 系统基础平台风险评估工具
6.1.5 RiskWatch	6.1.6 其他风险评估与管理	6.1.7 常用风险评估与管理工具对比	6.2 系统基础平台风险评估工具	6.2.1 脆弱性扫描工
6.1.6 其他风险评估与管理	6.1.7 常用风险评估与管理工具对比	6.2 系统基础平台风险评估工具	6.2.1 脆弱性扫描工	6.2.2 流光 (Fluxay) 脆弱性扫描工具
6.1.7 常用风险评估与管理工具对比	6.2 系统基础平台风险评估工具	6.2.1 脆弱性扫描工	6.2.2 流光 (Fluxay) 脆弱性扫描工具	6.2.3 Nessus脆弱性扫描工具
6.2 系统基础平台风险评估工具	6.2.1 脆弱性扫描工	6.2.2 流光 (Fluxay) 脆弱性扫描工具	6.2.3 Nessus脆弱性扫描工具	6.2.4 极光远程安全评
6.2.1 脆弱性扫描工	6.2.2 流光 (Fluxay) 脆弱性扫描工具	6.2.3 Nessus脆弱性扫描工具	6.2.4 极光远程安全评	6.2.5 天镜脆弱性扫描与管理系统
6.2.2 流光 (Fluxay) 脆弱性扫描工具	6.2.3 Nessus脆弱性扫描工具	6.2.4 极光远程安全评	6.2.5 天镜脆弱性扫描与管理系统	6.2.6 渗透测试工具
6.2.3 Nessus脆弱性扫描工具	6.2.4 极光远程安全评	6.2.5 天镜脆弱性扫描与管理系统	6.2.6 渗透测试工具	6.2.7 Metasploit渗透工具
6.2.4 极光远程安全评	6.2.5 天镜脆弱性扫描与管理系统	6.2.6 渗透测试工具	6.2.7 Metasploit渗透工具	6.3 风险评估辅助工具
6.2.5 天镜脆弱性扫描与管理系统	6.2.6 渗透测试工具	6.2.7 Metasploit渗透工具	6.3 风险评估辅助工具	6.3.1 调查问卷
6.2.6 渗透测试工具	6.2.7 Metasploit渗透工具	6.3 风险评估辅助工具	6.3.1 调查问卷	6.3.2 检查列
6.2.7 Metasploit渗透工具	6.3 风险评估辅助工具	6.3.1 调查问卷	6.3.2 检查列	6.3.3 人员访谈
6.3 风险评估辅助工具	6.3.1 调查问卷	6.3.2 检查列	6.3.3 人员访谈	6.3.4 入侵检测工具
6.3.1 调查问卷	6.3.2 检查列	6.3.3 人员访谈	6.3.4 入侵检测工具	6.3.5 安全审计工具
6.3.2 检查列	6.3.3 人员访谈	6.3.4 入侵检测工具	6.3.5 安全审计工具	6.3.6 拓扑发现工具
6.3.3 人员访谈	6.3.4 入侵检测工具	6.3.5 安全审计工具	6.3.6 拓扑发现工具	其他：评估指标库、知识库、漏洞库、算法库、模型库
6.3.4 入侵检测工具	6.3.5 安全审计工具	6.3.6 拓扑发现工具	其他：评估指标库、知识库、漏洞库、算法库、模型库	6.4 信息安全风险评估工具的发展方向和最
6.3.5 安全审计工具	6.3.6 拓扑发现工具	其他：评估指标库、知识库、漏洞库、算法库、模型库	6.4 信息安全风险评估工具的发展方向和最	新成果
6.3.6 拓扑发现工具	其他：评估指标库、知识库、漏洞库、算法库、模型库	6.4 信息安全风险评估工具的发展方向和最	新成果	习题6
其他：评估指标库、知识库、漏洞库、算法库、模型库	6.4 信息安全风险评估工具的发展方向和最	新成果	习题6	上机实验
6.4 信息安全风险评估工具的发展方向和最	新成果	习题6	上机实验	第7章 信息安全风险评估的基本过程
新成果	习题6	上机实验	第7章 信息安全风险评估的基本过程	7.1 信息安全风险评估的过程
习题6	上机实验	第7章 信息安全风险评估的基本过程	7.1 信息安全风险评估的过程	7.2 信息安全风险评估的准备
上机实验	第7章 信息安全风险评估的基本过程	7.1 信息安全风险评估的过程	7.2 信息安全风险评估的准备	7.2.1 确定信息安全风险评估的目标
第7章 信息安全风险评估的基本过程	7.1 信息安全风险评估的过程	7.2 信息安全风险评估的准备	7.2.1 确定信息安全风险评估的目标	7.2.2 确定信息安全风险评估的范围
7.1 信息安全风险评估的过程	7.2 信息安全风险评估的准备	7.2.1 确定信息安全风险评估的目标	7.2.2 确定信息安全风险评估的范围	7.2.3 组
7.2 信息安全风险评估的准备	7.2.1 确定信息安全风险评估的目标	7.2.2 确定信息安全风险评估的范围	7.2.3 组	7.2.4 进行系统调研
7.2.1 确定信息安全风险评估的目标	7.2.2 确定信息安全风险评估的范围	7.2.3 组	7.2.4 进行系统调研	7.2.5 确定信息安全风险评估的依据和方法
7.2.2 确定信息安全风险评估的范围	7.2.3 组	7.2.4 进行系统调研	7.2.5 确定信息安全风险评估的依据和方法	7.3 组
7.2.3 组	7.2.4 进行系统调研	7.2.5 确定信息安全风险评估的依据和方法	7.3 组	7.3.1 识别资产
7.2.4 进行系统调研	7.2.5 确定信息安全风险评估的依据和方法	7.3 组	7.3.1 识别资产	7.3.2 资产分类
7.2.5 确定信息安全风险评估的依据和方法	7.3 组	7.3.1 识别资产	7.3.2 资产分类	7.3.3 资产赋值
7.3 组	7.3.1 识别资产	7.3.2 资产分类	7.3.3 资产赋值	7.3.4 输出结果
7.3.1 识别资产	7.3.2 资产分类	7.3.3 资产赋值	7.3.4 输出结果	7.4 识别并评估威胁
7.3.2 资产分类	7.3.3 资产赋值	7.3.4 输出结果	7.4 识别并评估威胁	7.4.1 威胁识别
7.3.3 资产赋值	7.3.4 输出结果	7.4 识别并评估威胁	7.4.1 威胁识别	7.4.2 威胁分类
7.3.4 输出结果	7.4 识别并评估威胁	7.4.1 威胁识别	7.4.2 威胁分类	7.4.3 威胁赋值
7.4 识别并评估威胁	7.4.1 威胁识别	7.4.2 威胁分类	7.4.3 威胁赋值	7.4.4 输出结果
7.4.1 威胁识别	7.4.2 威胁分类	7.4.3 威胁赋值	7.4.4 输出结果	7.5 识别并评估脆弱性
7.4.2 威胁分类	7.4.3 威胁赋值	7.4.4 输出结果	7.5 识别并评估脆弱性	7.5.1 脆弱性识别
7.4.3 威胁赋值	7.4.4 输出结果	7.5 识别并评估脆弱性	7.5.1 脆弱性识别	7.5.2 脆弱性分类
7.4.4 输出结果	7.5 识别并评估脆弱性	7.5.1 脆弱性识别	7.5.2 脆弱性分类	7.5.3 脆弱性赋值
7.5 识别并评估脆弱性	7.5.1 脆弱性识别	7.5.2 脆弱性分类	7.5.3 脆弱性赋值	7.5.4 输出结果
7.5.1 脆弱性识别	7.5.2 脆弱性分类	7.5.3 脆弱性赋值	7.5.4 输出结果	7.6 识别安全措施和输出结果
7.5.2 脆弱性分类	7.5.3 脆弱性赋值	7.5.4 输出结果	7.6 识别安全措施和输出结果	7.6.1 识别安全措施
7.5.3 脆弱性赋值	7.5.4 输出结果	7.6 识别安全措施和输出结果	7.6.1 识别安全措施	7.6.2 输出结果
7.5.4 输出结果	7.6 识别安全措施和输出结果	7.6.1 识别安全措施	7.6.2 输出结果	7.7 分析可能性和影响
7.6 识别安全措施和输出结果	7.6.1 识别安全措施	7.6.2 输出结果	7.7 分析可能性和影响	7.7.1 分析可能性
7.6.1 识别安全措施	7.6.2 输出结果	7.7 分析可能性和影响	7.7.1 分析可能性	7.7.2 分析影响
7.6.2 输出结果	7.7 分析可能性和影响	7.7.1 分析可能性	7.7.2 分析影响	7.8 风险计算
7.7 分析可能性和影响	7.7.1 分析可能性	7.7.2 分析影响	7.8 风险计算	7.8.1 使用矩阵法计算风险
7.7.1 分析可能性	7.7.2 分析影响	7.8 风险计算	7.8.1 使用矩阵法计算风险	7.8.2 使用相
7.7.2 分析影响	7.8 风险计算	7.8.1 使用矩阵法计算风险	7.8.2 使用相	7.9 风险处理
7.8 风险计算	7.8.1 使用矩阵法计算风险	7.8.2 使用相	7.9 风险处理	7.9.1 现存风险判断
7.8.1 使用矩阵法计算风险	7.8.2 使用相	7.9 风险处理	7.9.1 现存风险判断	7.9.2 控制目标确定
7.8.2 使用相	7.9 风险处理	7.9.1 现存风险判断	7.9.2 控制目标确定	7.9.3 控制措施选择
7.9 风险处理	7.9.1 现存风险判断	7.9.2 控制目标确定	7.9.3 控制措施选择	7.10 编写信息安全风险评估报告
7.9.1 现存风险判断	7.9.2 控制目标确定	7.9.3 控制措施选择	7.10 编写信息安全风险评估报告	习题7
7.9.2 控制目标确定	7.9.3 控制措施选择	7.10 编写信息安全风险评估报告	习题7	第8章 信息安全风险评估实例
7.9.3 控制措施选择	7.10 编写信息安全风险评估报告	习题7	第8章 信息安全风险评估实例	8.1 评估准备
7.10 编写信息安全风险评估报告	习题7	第8章 信息安全风险评估实例	8.1 评估准备	8.1.1 确
习题7	第8章 信息安全风险评估实例	8.1 评估准备	8.1.1 确	8.1.2 确定信息安全风险评估的范围
第8章 信息安全风险评估实例	8.1 评估准备	8.1.1 确	8.1.2 确定信息安全风险评估的范围	8.1.3 组建适当的评估管理与实
8.1 评估准备	8.1.1 确	8.1.2 确定信息安全风险评估的范围	8.1.3 组建适当的评估管理与实	
8.1.1 确	8.1.2 确定信息安全风险评估的范围	8.1.3 组建适当的评估管理与实		
8.1.2 确定信息安全风险评估的范围	8.1.3 组建适当的评估管理与实			
8.1.3 组建适当的评估管理与实				

<<信息安全管理与风险评估>>

施团队 8.1.4 进行系统调研 8.1.5 评估依据 8.1.6 信息安全风险评估项目实施方案
8.1.7 获得最高管理者对信息安全风险评估工作的支持 8.2 识别并评价资产 8.2.1 识别资产
8.2.2 资产赋值 8.2.3 资产价值 8.3 识别并评估威胁 8.4 识别并评估脆弱性 8.5 分析可能性
影响 8.5.1 分析威胁发生的频率 8.5.2 分析脆弱性严重程度 8.6 风险计算 8.6.1 使用矩阵
阵法计算风险 8.6.2 使用相乘法计算风险 8.7 风险处理 8.7.1 现存风险判断 8.7.2 控制目标
确定 8.7.3 控制措施选择 8.8 编写信息安全风险评估报告 上机实验 参考文献

<<信息安全管理与风险评估>>

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，将风险控制用户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。

<<信息安全管理与风险评估>>

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。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>