

<<信息安全风险管理方法及应用>>

图书基本信息

书名：<<信息安全风险管理方法及应用>>

13位ISBN编号：9787513000840

10位ISBN编号：7513000840

出版时间：2010-6

出版时间：知识产权出版社

作者：吕俊杰

页数：188

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>

<<信息安全风险管理方法及应用>>

前言

信息化现在逐步进入人们的生活，融入到人类社会的每一个角落，并不断推动着社会的进步和发展。然而，无处不在的信息孕育着随时可发生的风险。

伴随着社会经济对信息化依赖程度越来越高，各种恶意代码、黑客攻击、信息泄漏等安全事件时有发生，信息安全问题所导致的损失成倍增长。

面对日益增长的安全需求，单靠技术手段是不可能从根本上解决信息安全问题的。

绝大多数信息安全问题都是管理方面的缺陷，需要通过管理、技术、组织、物理等综合方法来解决信息安全问题。

由此，信息安全风险管理应运而生。

在信息安全领域，风险管理就是最大范围地保护信息资产，确保信息的保密性、完整性和可用性，在可接受的成本范围之内，识别、控制和降低或排除（可能影响信息系统的）安全风险的过程。

因此，掌握信息安全风险识别、风险评估和风险控制的方法，企业才能充分利用信息技术提供更便捷和更优质的产品或服务，同时又保障了信息的合理使用和安全。

目前学术界关于信息安全风险管理的研究，大多局限于某一个方面，鲜有对整个风险管理流程各阶段内容的研究。

同时，与信息安全风险管理相关的国际标准，对方法的介绍比较泛泛，企业在应用过程中往往无所适从。

因此，本书从信息安全风险管理的流程出发，研究各个阶段，即风险识别阶段、风险评估阶段和风险控制阶段的实施方法，并加以应用，对企业的具体实践提供理论指导，帮助企业建立合理的信息安全管理体系。

<<信息安全风险管理方法及应用>>

内容概要

本书从信息安全风险管理体系建立的流程出发，研究了各阶段的工作内容及方法，并引入博弈论进行分析以对信息安全管理提供决策依据，从而对企业的信息安全风险管理实践提供指导。

<<信息安全风险管理方法及应用>>

作者简介

吕俊杰，2007年6月毕业于北京航空航天大学管理科学与工程专业，师从于风险管理领域著名专家邱菀华教授，获博士学位。

2007年7月到北京工商大学商学院任教，主要研究方向为信息安全、风险评估、风险管理、决策理论等。

作为课题负责人，承担并完成了国家信息安全战略研究与标准制定工作专项项目“信息安全风险自评估理论研究”；作为主要研究者，参加了49国家自然科学基金项目，1项国家软科学研究计划项目以及多项省部级项目的研究工作；作为编写者，参与了国家信息中心2项信息安全相关国家标准草案的编写工作；作为项目负责人，承担了多项企业信息安全风险评估和风险管理项目。

截至2007年4月，已在国际学术会议以及国内一级学术期刊上发表并被录用学术论文20余篇，相关论文已被EI、ISTP检索20余篇次。

<<信息安全风险管理方法及应用>>

书籍目录

第一章 绪论 第一节 选题背景 第二节 信息安全风险管理的发展历史 第三节 信息安全风险管理标准概述 一、BS7799 / ISO27001&ISO27002 二、CC / ISO—IECI5408 三、ISO / IECI3335 四、OCTAVE 五、SSE . CMM 第四节 信息安全风险管理方法研究 一、风险管理理论发展历程 二、风险管理主要内容和方法 三、信息安全风险管理方法研究现状 第五节 本书的工作概要第二章 基于流程优化的信息安全风险识别方法 第一节 信息安全风险与风险管理 一、信息安全的含义 二、信息安全风险与风险管理的内涵 第二节 信息安全风险识别 一、资产识别 二、威胁识别 三、脆弱性识别 四、资产 / 威胁 / 脆弱性映射 五、已有的安全控制措施识别 第三节 基于流程优化的信息安全风险识别方法 一、信息流的特征以及信息流的优化方法 二、多因素设计结构矩阵方法 三、多因素结构矩阵的优化方法 第四节 层次化的资产识别与评估方法 一、问题描述 二、作业一资产识别模型 三、层次化的关键资产评估模型 四、应用举例 第五节 本章 小结第三章 基于三角模糊数的信息安全风险评估方法 第一节 风险评估方法介绍 第二节 模糊集以及三角模糊数 一、模糊集的相关定义 二、三角模糊数及其相关性质 第三节 基于三角模糊数的信息安全风险评估方法 一、语言评价条件下的信息安全风险评估矩阵 二、信息安全风险评估短阵集结方法 三、基于三角模糊数的信息安全风险评估方法 四、算例 第四节 本章 小结第四章 信息安全风险控制及安全措施排序方法 第一节 信息安全风险控制的内容 一、选择风险控制方式 二、选择风险控制措施 三、对控制措施的评价第五章 信息安全风险管理的运行与有效性测量第六章 信息安全风险管理机制设计第七章 多主体信息安全风险管理策略模型第八章 基于安全控制模型的信息安全风险评估及风险控制参考文献附录后记

章节摘录

插图：标准化组织采纳为国际标准，编号为ISO15408。

这个期间英国自己还研发了基于风险管理的BS7799信息安全管理标准，澳大利亚和新西兰制定了共同的风险管理标准AS / NES4360。

1997年12月，美国国防部发表了《信息技术安全认证和批准程序》（DITSCAP），成为美国涉密信息系统的风险评估和风险管理的重要标准和依据。

3.2 0世纪90年代末至今，国际范围的风险管理实践与理论进入第三个阶段，即全球化阶段由于20世纪90年代以来互联网、移动通信和跨国光缆的高速发展，各国原本局限于本国内的信息网络迅速跨越国境连成一片。

与此同时，信息安全也成为世界各国面临的共同挑战。

2002年，美国通过了一部联邦信息安全管理法案（FISMA）。

根据该法案，美国国家标准和技术委员会（NIST）负责为美国政府和商业机构提供信息安全管理相关的标准规范。

NISTSP800系列已经出版了近90本同信息安全相关的正式文件，形成了从计划、风险管理、安全意识培训和教育以及安全控制措施的一整套信息安全管理体系。

其中，正式发布的此类标准主要有：SP80026信息技术系统安全自评估指南（2001年）、SP800-30信息技术系统风险管理指南（2002年）、SPS00-51CVE使用和漏洞命名法（2002年），等等。

后记

20世纪90年代以来，随着经济全球化和世界科技革命，信息技术、信息产业和信息网络的蓬勃发展，社会信息化程度不断加深，信息对国家、组织和个人发展的影响日益增加、日益突出。

国家、企业和个人对信息安全性要求也变得越来越来高。

与此同时，各种黑客利用系统安全弱点不断地开展新型攻击，网络攻击群体的规模迅速扩大，攻击水平飞速提高，攻击所造成的影响也不断严重，信息系统所面临的安全风险和威胁日趋严重。

信息系统安全问题单凭技术是无法得到彻底解决的，管理与技术相结合的观点也日益被学术界和实业界所接受。

由此，信息安全风险管理应运而生。

在信息安全领域，风险管理是指最大范围地保护信息资产，确保信息的保密性、完整性和可用性，在可接受的成本范围内，识别、控制和降低或排除（可能影响信息系统的）安全风险的流程。

本书就从这一流程出发，注重可操作性，分别研究了风险识别、风险评估、风险控制的方法，对企业信息安全实践提供指导。

然而，由于时间和个人能力有限，书中的瑕疵纰漏在所难免，有待同行专家批评指正。

本书的完成仅仅我一个人的力量是远远不够的。

在此，我由衷地感谢我的恩师邱菀华教授，是在她对我的悉心指导、帮助、支持、鼓励下，本书的研究才得以顺利完成！

邱老师聪慧博学的头脑、敏锐深刻的洞察力、勤奋严谨的科学作风、严肃认真的治学态度和高尚的学术道德，都使我受益匪浅。

<<信息安全风险管理方法及应用>>

编辑推荐

《信息安全风险管理方法及应用》是由知识产权出版社出版的。

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>