

<<移动商务风险管理研究>>

图书基本信息

书名：<<移动商务风险管理研究>>

13位ISBN编号：9787030371171

10位ISBN编号：7030371178

出版时间：2013-3

出版时间：科学出版社

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>

<<移动商务风险管理研究>>

内容概要

《移动商务风险管理研究》从风险现状、风险要素、风险评价及风险控制等方面对移动商务风险进行了较为全面深入的研究。

全书共四篇，13章。

第一篇是移动商务风险管理理论与现状，通过大量案例介绍了移动商务风险的背景和起源，对研究现状进行了综述总结；第二篇是移动商务风险要素分析，对移动商务的风险要素、风险要素关联性和交易风险问题进行了实证调研和总结；第三篇是移动商务风险度量与评价，对湖北省移动商务现状、移动商务成熟度、移动商务交易风险等问题设计了度量指标和评价模型；第四篇是移动商务风险控制与规避，探讨性地解释了移动商务组合对冲策略、基于实物期权风险分担策略和控制决策方法。

<<移动商务风险管理研究>>

书籍目录

总序 前言 第一篇移动商务风险管理理论与现状 第1章移动商务风险管理概论 1.1移动商务背景介绍 1.2移动商务风险的起源 1.3相关案例 1.4本章小结 第2章移动商务风险研究现状 2.1移动商务行业特征分析 2.2企业风险管理理论综述 2.3移动商务经营风险研究现状 2.4移动商务交易风险研究现状 2.5本章小结 第二篇移动商务风险要素分析 第3章基于Delphi法的移动商务风险要素分析 3.1Delphi法风险要素识别方法和过程 3.2风险要素调查结果排序比较 3.3与安永风险调查报告对比分析 3.4风险要素分类与对应管理方法分析 3.5本章小结 第4章基于模糊认知影响图的移动商务风险要素关联分析 4.1结合认知图的模糊影响图推理过程改进研究 4.2移动商务风险要素关联分析 4.3基于模糊认知影响图的移动商务风险控制有效策略分析 4.4本章小结 第5章移动商务交易风险因素识别 5.1移动商务交易风险因素辨别 5.2移动商务交易风险因素分类 5.3本章小结 第三篇移动商务风险度量与评价 第6章湖北省移动商务现状分析 6.1概述 6.2湖北省移动商务发展现状 6.3本章小结 第7章移动商务成熟度评价模型设计 7.1能力成熟度模型及其应用价值 7.2移动商务成熟度评价模型的构建 7.3移动商务成熟度的综合评价方法 7.4湖北省移动商务成熟度计算 7.5本章小结 第8章移动商务交易风险评估指标构建 8.1移动商务交易风险评估的基本步骤 8.2移动商务交易风险评估指标的设计原则 8.3移动商务交易风险评估指标体系设计 8.4本章小结 第9章基于证据理论的移动商务交易风险评估 9.1概述 9.2证据理论及其发展 9.3指标权重与风险状态评语值的设定 9.4基于证据理论的移动商务交易风险评估模型 9.5应用举例 9.6本章小结 第10章不完全信息下移动商务交易风险评估证据推理法 10.1概述 10.2模糊隶属度函数 10.3Mass函数决策矩阵的转换 10.4基于证据理论的移动商务交易风险模糊评估模型 10.5应用举例 10.6本章小结 第四篇移动商务风险控制与规避 第11章基于投资组合理论的移动服务风险组合对冲策略 11.1风险组合对冲理论的提出和应用 11.2移动服务分类与风险差异分析 11.3移动服务风险对冲投资组合策略 11.4算例验证 11.5本章小结 第12章基于实物期权的移动服务风险管理帕累托改进 12.1实物期权理论的提出和应用 12.2运营商与服务提供商的风险分担及合作模式背景 12.3移动服务风险管理模型与实物期权应用效果分析 12.4实物期权协议应用效果算例验证 12.5本章小结 第13章移动商务交易风险控制决策 13.1移动商务交易安全技术 13.2移动商务交易安全措施方法库的建立 13.3移动商务交易风险控制的策略 13.4移动商务交易风险控制模型 13.5本章小结 参考文献

章节摘录

版权页：插图：来自运营商核心网内部的安全威胁容易得到有效的管理，而对于从接入网接入核心网的移动设备而言，其安全管理相对困难得多，小的移动台因为资源有限因而防御能力较低，一旦其操作系统出现漏洞或安全应用未及时更新，则很容易导致病毒入侵；而且移动终端数量众多，分布范围广泛、移动性强等特点，使得移动终端一旦感染病毒并成为病毒的源头时，运营商从网络上很难保证安全地为用户提供高质量的服务。

移动通信运营网络包含用户子系统（终端和卡）、接入网、IT支撑系统、核心网、业务网和传送网等。

用户到业务网服务器、用户之间、用户到互联网和PSTN或其他PLMN端到端的访问都会经过移动通信网络中不同部分的网络，而不是单独完成的。

运营网络的关键系统中任何一个区域出现安全问题都可能引发其他区域的安全问题，甚至导致整个链路安全性的丧失。

由于移动通信网络是一个公众使用网络，其开放程度较高，因此黑客容易对该网络进行攻击。

移动通信网络中存在较丰富的数据资源，给黑客带来了较强的攻击动机。

移动通信网络中的设备、协议、服务庞杂，这些设备、协议和服务在设计上容易产生脆弱性，黑客容易利用这些脆弱性实施攻击。

目前，大多数安全防范工具都是针对已知威胁和攻击手段。

然而，运营商网络用户众多、业务协议复杂，很可能存在未知的脆弱性，被黑客所利用并产生新的攻击手段。

移动通信网络中运行着各种各样的信息系统，它们具有不同的安全基线。

因此，在构建面向3G移动通信网络安全框架时，必须充分考虑这些不同的安全基线并满足其需求。

移动运营商的信息系统十分复杂，存在相对封闭的网络环境，如计费系统和网管支撑系统等；也存在相对开放的网络环境，如与互联网相连接的部分、用户接入系统部分、应用业务部分等；以及半开放的网络环境，如承载系统PS域等。

这些存在于不同开放程度的网络环境下的信息系统拥有不同的安全基线。

另外，不同运营商之间、运营商与不同用户之间、运营商与不同服务提供商之间，甚至是运营商内部网络之间都存在不同的信任程度。

3G移动通信网正向全IP网络方向发展，所面临的威胁也逐渐增加，包括过去仅仅出现在互联网上的威胁。

这些威胁都包含这样一些要素，即攻击者、攻击者的动机、攻击者所利用的资源 and 脆弱性以及威胁的类型和影响等。

公众运营网络所面临的攻击者可能是黑客、内部人员、敌对国家政府、其他运营商、恐怖分子等。

<<移动商务风险管理研究>>

编辑推荐

《移动商务风险管理研究》可供信息管理、信息安全、电子商务、网络营销等领域的研究人员研究参考，也可供与该领域相关的管理人员、工程人员、研究所和高等院校高年级学生阅读参考，还适合作为研究生教材。

<<移动商务风险管理研究>>

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>