

<<信息灾难恢复规划>>

图书基本信息

书名：<<信息灾难恢复规划>>

13位ISBN编号：9787302087076

10位ISBN编号：7302087075

出版时间：2004-7

出版时间：清华大学出版社

作者：桑德胡

页数：162

字数：270000

译者：张瑞萍

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>

## <<信息灾难恢复规划>>

### 内容概要

无论是自然灾害，还是技术灾难，二者都可以给公司带来严重损失。

每年各种灾难都会导致数亿美元的损失。

因此所有的公司都必须采取严格措施保护自己。

本书讲解实现简单的DRP（信息灾难恢复规划）的知识，帮助公司保护自己。

无论是地震、火灾，还是计算机病毒攻击，DRP都将帮助公司实现顺利运营，业务蒸蒸日上。

## <<信息灾难恢复规划>>

### 作者简介

Roopendra Jeet Sandhu是NIIT公司知识解决方案事务部（KSB）的一名教堂设计人员，在NIIT工作的两年中，她已经为Course Technology、NetVarsity 和ITT这样的客房开发了基于计算机的培训、基于Web的培训和讲师指导所用的内容。

她独立地开发了几个  
基于Web的培训项目。

此外，Roopendra还一直在开民有关技术领域内容，如操作系统、安全和数据库管理系统。  
并且她还开发了有关Netscape 6.0的项目，是Premier Press出版的NET Framework一书的合著者。

## &lt;&lt;信息灾难恢复规划&gt;&gt;

## 书籍目录

第1章 灾难恢复规划：概览 1.1 灾难恢复规划的必要性 1.2 灾难恢复规划的好处 1.3 灾难恢复规划的策略 1.4 规划事项 1.5 灾难恢复规划的阶段 1.5.1 启动阶段 1.5.2 风险分析 1.5.3 计划的创建和实现 1.5.4 计划的测试 1.5.5 计划的维护 1.6 组织规划结构 1.6.1 规划小组 1.6.2 恢复小组 1.7 恢复目标 1.7.1 RPO 1.7.2 RTO 1.8 本章小结 1.9 复习题 1.9.1 多选题 1.9.2 简答题 1.10 答案 1.10.1 多选题 1.10.2 简答题

第2章 构成灾难的因素 2.1 什么是灾难 2.2 灾难的原因 2.2.1 自然灾害 2.2.2 人为灾难 2.3 灾难及其后果 2.4 本章小结 2.5 复习题 2.6 答案第3章 分类灾难 3.1 灾难的影响及严重级别 3.2 分类灾难：影响的严重性 3.2.1 硬盘子系统故障 3.2.2 服务器故障 3.2.3 电力危机 3.2.4 关键数据的意外删除/更改 3.2.5 盗窃或破坏 3.2.6 病毒攻击 3.2.7 网络故障 3.2.8 系统软件故障 3.3 本章小结 3.4 复习题 3.4.1 多选题 3.4.2 简答题 3.5 答案 3.5.1 多选题 3.5.2 简答题第4章 风险分析 4.1 风险的定义 4.1.1 有意的和无意的风险 4.1.2 固有的和后天的风险 4.1.3 保险的和保险不保险的风险 4.2 定义风险分析的过程 4.3 风险分析的好处 4.4 执行风险分析 4.4.1 执行风险分析的指导原则 4.4.2 风险分析的方法 4.4.3 风险分析的阶段 4.5 风险分析的输入 4.6 本章小结 4.7 复习题 4.7.1 多选题 4.7.2 简答题 4.8 答案 4.8.1 多选题 4.8.2 简答题第5章 基线措施 5.1 访问控制 5.1.1 身份验证 5.1.2 许可 5.1.3 加密 5.2 反病毒 5.2.1 病毒的类型 5.2.2 反病毒软件 5.3 防火墙 5.3.1 防火墙的功能 5.3.2 防火墙的类型 5.3.3 使用防火墙时要考虑的事项 5.4 IDS 5.4.1 IDS模型 5.4.2 选择IDS 5.4.3 分析IDS 5.5 数据备份 5.6 本章小结 5.7 复习题 5.7.1 多选题 5.7.2 简答题 5.8 答案 5.8.1 多选题 5.8.2 简答题第6章 恢复计划 6.1 灾难恢复计划的目标 6.2 创建灾难恢复计划的步骤 6.2.1 识别恢复策略 6.2.2 选择恢复策略 6.2.3 创建初稿 6.2.4 灾难恢复计划的组件 6.2.5 创建定稿 6.3 实施灾难恢复计划的步骤 6.3.1 进行培训 6.3.2 进行练习和演习 6.4 本章小结 6.5 复习题 6.5.1 多选题 6.5.2 简答题 6.6 答案 6.6.1 多选题 6.6.2 简答题第7章 测试和维护恢复计划 7.1 测试和维护计划的必要性 7.2 计划测试 7.2.1 计划测试的目标 7.2.2 计划测试的预备措施 7.2.3 测试的类型 7.2.4 计划测试中的主要步骤 7.2.5 计划测试文档 7.3 计划的维护 7.3.1 变化管理 7.3.2 变化管理的方法 7.3.3 定期和不定期维护 7.3.4 维护循环检查点 7.4 本章小结 7.5 复习题 7.5.1 多选题 7.5.2 简答题 7.6 答案 7.6.1 多选题 7.6.2 简答题第8章 集中式系统的恢复计划 8.1 制定数据恢复的计划 8.1.1 分析和分类信息 8.1.2 检查现有的备份策略 8.1.3 选择和评价备份策略 8.1.4 实施备份策略 8.2 制定系统恢复的计划 8.2.1 识别关键应用程序和硬件 8.2.2 next box off the line策略 8.2.3 互惠备份策略 8.2.4 冷站点 8.2.5 热站点 8.2.6 服务局 8.2.7 冗余系统策略 8.3 制定建筑物恢复的策略 8.4 制定通信链接恢复的计划 8.4.1 计算机外国设备和终端网络的恢复 8.4.2 恢复WAN和数据网络链接 8.5 制定员工恢复的计划 8.6 本章小结 8.7 复习题 8.7.1 多选题 8.7.2 简答题 8.8 答案 8.8.1 多选题 8.8.2 简答题第9章 分散式系统的恢复计划 9.1 制定数据恢复的计划 9.1.1 分类数据 9.1.2 对数据进行基于策略的管理 9.2 制定系统恢复的计划 9.2.1 使用复制 9.2.2 谨慎选择中间件 9.2.3 鼓励清楚地定义应用程序的分区设计 9.2.4 鼓励容错配置 9.2.5 鼓励支持Web的应用程序 9.3 制定建筑物恢复的计划 9.3.1 next box off the line策略 9.3.2 热站点和冗余系统 9.3.3 服务局 9.3.4 应用程序合并 9.3.5 集中策略 9.4 制定通信链接恢复的计划 9.4.1 LAN恢复 9.4.2 内部音频通信 9.5 制定员工恢复的计划 9.5.1 “不工作”方法 9.5.2 备用方法 9.5.3 商业恢复设施 9.5.4 远程访问 9.6 本章小结 9.7 复习题 9.8 答案第10章 实施灾难恢复计划 10.1 案例分析 10.2 灾难恢复计划的启动 10.3 成功恢复的因素 10.3.1 灾难前的阶段 10.3.2 规划阶段 10.3.3 灾难后的阶段 10.4 本章小结附录A 最优方法附录B 常见的问题与答复附录C 幕后情况附录D 攻击和入侵检测系统的常见模式 D.1 常见的攻击模式 D.1.1 IP哄骗 D.1.2 嗅闻 D.1.3 DoS攻击 D.2 入侵检测产品 D.2.1 选择有效的入侵检测产品 D.2.2 入侵检测产品附录E 评估可用的防火墙产品 E.1 路由器（无状态的基于数据包过滤器的）防火墙 E.1.1 Cisco 2500系列 E.1.2 Livingston FireWall IRX E.1.3 The Security Router E.2 有状态的基于数据包过滤器的防火墙 E.2.1 BorderManager E.2.2 Firewall-1 E.2.3 PIX防火墙 E.2.4 GNAT Box Firewall E.2.5 NetScreen Firewall E.2.6 Guardian Firewall E.3 应用程序代理防火墙 E.3.1 Firewall Server E.3.2 Raptor Firewall E.3.3 Sidewinder

<<信息灾难恢复规划>>

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>