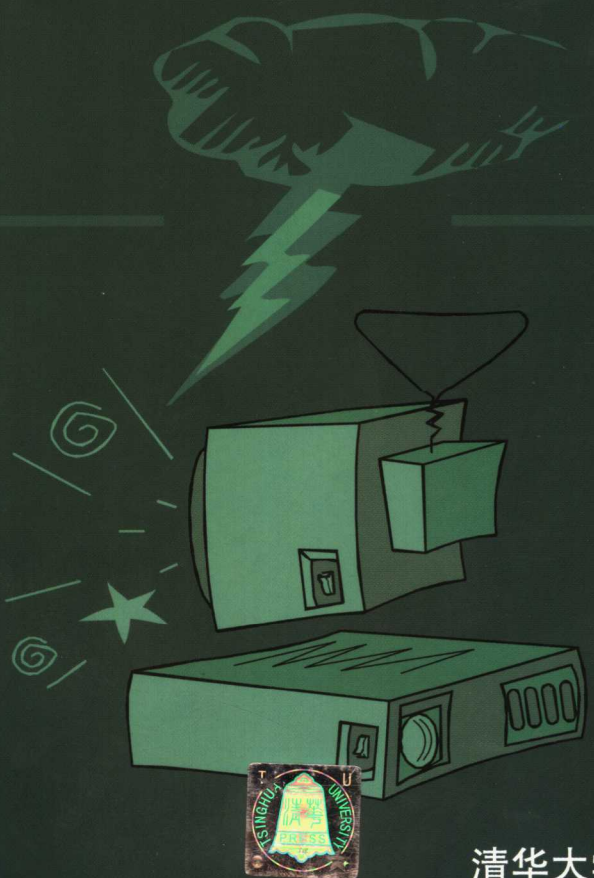
THOMSON

Disaster Recovery Planning

信息灾难恢复规划



Roopendra Jeet Sandhu 著

张瑞萍 等 译

清华大学出版社

信息灾难恢复规划

Roopendra Jeet Sandhu 著

张瑞萍　等 译

清华大学出版社

北京

Roopendra Jeet Sandhu
Disaster Recovery Planning
EISBN: 1-931841-98-5

北京市版权局著作权合同登记号 图字 01-2003-6413 号

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

信息灾难恢复规划/山德布(Sandhu. R. J.)著;张瑞萍等译. —北京:清华大学出版社,2004.7
书名原文: Disaster Recovery Planning
ISBN 7-302-08707-5

Ⅰ. 信... Ⅱ. ①山...②张... Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2004)第 050772 号

出 版 者: 清华大学出版社 **地 址**: 北京清华大学学研大厦
http://www.tup.com.cn **邮 编**: 100084
社总机: 010-62770175 **客户服务**: 010-62776969
责任编辑: 冯志强
封面设计: 付剑飞
印 刷 者: 清华园胶印厂
装 订 者: 三河市李旗庄少明装订厂
发 行 者: 新华书店总店北京发行所
开 本: 185×260 **印张**: 11 **字数**: 270 千字
版 次: 2004 年 7 月第 1 版 2004 年 7 月第 1 次印刷
书 号: ISBN 7-302-08707-5/TP·6233
印 数: 1～4000
定 价: 22.00 元

关于作者

Roopendra Jeet Sandhu 是 NIIT 公司知识解决方案事务部(KSB)的一名教学设计人员。在 NIIT 工作的两年中,她已经为 Course Technology、NetVarsity 和 ITT 这样的客户开发了基于计算机的培训、基于 Web 的培训和讲师指导的培训所用的内容。她独立地开发了几个基于 Web 的培训项目。此外,Roopendra 还一直在开发有关技术领域的内容,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。

前　言

人类一直在试图避开自然界的力量和它们造成的破坏。工业化和技术的发展带来了新的威胁，而且它们造成破坏的可能性也大大增加。因此，人们开发了各种策略来克服灾难或使灾难造成的影响最小化。人们的努力已经被引向制定灾难恢复计划。

要制定灾难恢复计划，必须了解它内在的要求和概念。为此，本书首先要回答“我为什么必须制定灾难恢复计划?”这个问题。除了详细说明制定计划的根据及其所需的组织结构以外，本书还将各种灾难及其后果区别开来。你将了解有关风险分析的详细信息，它们可以用于预防和控制风险。本书将论述避免和处理灾难的重要概念，如访问控制、反病毒和防火墙。利用规划所需的输入，本书将介绍创建灾难恢复计划的严密循环过程。本书还将介绍与测试和维护计划相关的重要信息。然后详细介绍恢复集中系统和分散系统的策略，你将了解系统恢复、网络及通信链接恢复和数据恢复。最后你将研究一个案例，了解与一个公司的恢复有关的步骤。

如何使用本书

第 1、2 和 3 章讨论灾难规划和灾难分类的初步知识，第 4、6 和 7 章讨论灾难恢复规划的不同阶段。第 5 章介绍基线措施。第 8 和 9 章介绍集中系统和分散系统的恢复。第 10 章介绍一个案例，以便了解一个公司如何实现恢复计划。

为了便于学习，本书使用了特定的辅助手段，如“注意”、“提示”和“警告”。所有与概念有关的附加或相关信息都包括在“注意”中；“提示”提供有用的信息或捷径，以便有效地执行任务；“警告”说明与过程或事实有关的警告。

目　录

第1章　灾难恢复规划:概览

随着IT(信息技术)领域的快速发展,公司越来越依赖IT以执行普通的以及关键的任务。当出现意外事件时,这种依赖性经常导致公司的正常运行中断。这些导致公司正常经营中断的事件称为灾难。

灾难大量存在于IT领域,其影响小到仅仅使人烦恼,大到完全破坏业务。幸运的是,在面临灾难时,可以通过实现适当的灾难恢复计划和过程,将它们的影响减至最小,并使操作继续进行。Booz Allen Hamilton最近进行的一项调查表明,自从2001年9月11日美国世界贸易大厦被攻击以来,年收入在10亿美元以上的公司中,90%的CEO亲自审查灾难恢复计划。

灾难恢复是在灾难发生时确保公司正常经营保持连续性的过程。这个过程不仅着眼公司主要功能和系统的恢复,而且强调在尽可能短的时间内恢复它们。要在最短的时间内达到最快的恢复,就需要制作一个路线图,详细说明在灾难之前、之中和之后应当采取的行动,这个路线图被称为灾难恢复计划。灾难恢复计划是一组内容广泛的声明,用于解决可能损害公司的任何灾难。

用以创建灾难恢复计划的过程称为灾难恢复规划。执行灾难恢复计划的目的在于不管引起灾难的原因是什么,都要确保快速、有效和划算地恢复营业。考虑到无法确切地预测灾难发生的时间、地点和方式,为意外情况制定计划就变得非常重要。艾森豪威尔总统所说的一句话恰当地强调了规划的重要性:"计划无关紧要,规划最为重要。"

本书建立在灾难恢复规划过程的重要性之上。本章将教会你正确评价灾难恢复规划的必要性,其内容包括实现规划过程的优点和策略,以及在制定灾难恢复计划时要牢记的事项。最后,本章将介绍灾难恢复规划的阶段和常用于灾难恢复规划的恢复目标。

1.1　灾难恢复规划的必要性

由于一个公司不能抵御灾难的冲击,所以它必须慎重地考虑灾难恢复计划。灾难发生以后,一个公司本身在没有关键系统、应用程序和数据的情况下可以支撑多久呢?会攻击一个公司的灾难可能有以下几种。

- **自然灾害**:包括洪水、飓风和地震等自然灾害。日本经历过一场可怕的地震,但是这个国家已经学会了使用精心设计的灾难恢复计划与这些灾难共处。极其恶劣的气候条件,如大雪或飓风,也会妨碍商业的正常运行。例如,1999年9月的佛洛伊德飓风使美国东部陷于停顿。这样的意外事故是非常重要的。
- **链接和电力故障**:链接和电力故障可以导致严重的商业损失。这些故障可能是自然灾害或人为的破坏活动(如罢工或恐怖活动)带来的副作用。想想世界贸易中心

受到攻击之后对商业和个人所造成的影响。电信和网络链接是所有商业机构的生命线，它们出现的任何中断都会使客户、股东和供应商感到不满。

- **犯罪活动和破坏活动**：网上恐怖主义和违法窃用都属于这一类。这些活动会导致机密数据或营销策略被盗或泄露。由于这样的灾难，公司可能不得不面临严重的窘迫境地。例如，如果一家电子商务公司存储机密客户记录（如信用卡信息）的数据库泄密，那么这个公司可能就会歇业。
- **国内动荡**：国内动荡、罢工或不稳定的政治环境都会妨碍业务的正常进行。2000 年在西雅图世界贸易组织会议上引起的骚乱就是国内动荡导致业务中断的示例。

要确保一个公司持续地生存发展，就必须制定灾难恢复计划。要做到这一点，就要通过创建灾难恢复计划，解决 IT 环境中可能影响该公司的所有灾难。使灾难恢复规划成为必要的其他一些因素如下所示。

- **公司因灾难而出现的严重损失**：如前所述，当出现与 IT 有关的灾难时，对 IT 不断增加的依赖性可以引起严重的后果。基于工作的性质，每停工一个小时，一个公司可能就会损失相当大的一笔钱。由 IT 灾难引起的停工可能会损失收入、消费者、客户以及商业伙伴。要使消费者和客户相信因灾难发生后公司所处的情况是很难的。客户不愿接受这样一些不履行的借口。此外，长期的停工将减少公司的利润和市值，这最终可能会导致破产。
- **技术的快速发展同时带来了新的灾难类型的发展**：对产品和服务的全天候可用性的要求迫使公司在业务的每个方面都越来越依赖于 IT。因此，创新的营业方法正在按钟点被实现和更新。与分公司建立 24 小时远程连接的做法使公司极易受到外部攻击和灾难的影响。此外，数据跨越地理边界分散到站点和网络上，从而使数据容易受到未授权用户的攻击。而且，像地震这样的灾难可以损坏数据中心。在这样的情况下，一定不能忽视制定灾难恢复计划的必要性。
- **企业的生存取决于在尽可能短的时间内进行恢复**：在出现影响 IT 设置的灾难时，所有依赖 IT 的重要功能，如通信和交易，都将受到妨碍。虽然某个公司也许能够在缺少关键操作的情况下支撑一两天，但是长期的中断将断送这个公司。要防止这样的灾难，可以通过实现灾难恢复计划，准备策略和规程，确保在灾难发生时能够在尽可能短的时间内恢复公司。
- **契约义务**：直接向消费者或客户提供产品和服务的公司在履行义务时要受到 SLA（服务级别协议）的约束。供应商将在这些协议中保证，在出现灾难时，他们将不受阻碍地继续提供服务。当做出高可用性和高质量的承诺时，供应商要尽力兑现 SLA。这也只有通过灾难恢复规划才能达到。
- **恢复任务的有效协调**：在灾难恢复计划中，应当列出恢复规程，以确保公司能够在尽可能短的时间内恢复运行。由于这些规程是在灾难出现之前定义的，所以整个灾难恢复计划反映了公司迎接灾难挑战的效率和准备状态。因此，预先计划的恢复规程列表有助于公司轻松和有效地从灾难中恢复过来。

在分析了灾难恢复规划的必要性以后，你将更好地理解规划过程的好处。

关于 SLA

SLA 是一个合同，它规定一个公司向其消费者或客户提供的服务。这个合同列出了用于衡量供应商性能的参数以及不遵守该合同的后果。这个合同通常规定，无论供应商方面出现什么情况，都应当根据需要继续提供产品和服务。

1.2　灾难恢复规划的好处

在灾难恢复规划中，对于临时的技术不可用或无法访问，你要识别处理方法。灾难恢复规划对实现该过程的公司有什么好处呢？

灾难恢复规划的好处如下所示：

- **维护事务连续性**：实现灾难恢复规划的主要目标是确保事务的连续性以及关键资源和系统的可用性，以保证为消费者和客户提供连续的服务。
- **保护关键资源和活动**：要确保事务连续性，就需要识别和保护关键的资源和活动。这将增强公司的稳定性，从而保护商业伙伴的利益。此外，如果公司陷入停顿状态的话，公司的员工不必担心后果。
- **减少开支**：在灾难发生之前而非之后规划和识别恢复措施是明智的。通过有效的灾难恢复规划，可以将灾难引起的财务损失减小到最低限度。
- **识别单故障点**：灾难恢复规划中的一个重要活动是评估公司的业务功能。这样做的目的是为了识别单故障点。也就是说，你识别出高度依赖某个单个资源的功能和过程。从而，如果该资源受到灾难的影响，那么对依赖它的功能或过程的影响将是灾难性的。例如，如果一个公司将它的数据存储于单个数据中心，那么在发生影响整个数据中心的灾难时，数据将丢失。识别这样的故障点可以用来估计公司功能的风险大小。利用该信息，就可通过将数据备份在另一个地方来确保数据的高度可用性。
- **在灾难期间不要惊慌**：灾难恢复规划有助于减少灾难发生时的惊慌。在灾难发生之前，你就要确定在出现灾难时使公司恢复正常所需要执行的所有任务。这样，在出现灾难时，所有与决策有关的任务将大大减少。当公司受到灾难的影响时，就不必对灾难恢复进行规划和投资。这还意味着在灾难期间你不必等待关键人员的决定。因此，你将能够在最短的时间内实现顺利而有序的恢复。

在这一节中，你了解了灾难恢复规划的益处。将不同的策略应用于规划过程就可以获得这些益处。这些策略都是为了使灾难的消极影响最小化，下一节将对它们予以介绍。

1.3　灾难恢复规划的策略

灾难恢复规划的主要目的是有效地响应灾难并从灾难中恢复过来。要达到这一目的，灾难恢复规划将通过实现 3 个策略，着重把公司所面临灾难的影响减小到最低限度。这些策略包括：

- **预防策略**：正如它的名字那样，在这个策略中，所有工作都是为了防止灾难的发生。要达到这一目的，你应当具备基本的措施，保护公司赖以生存的活动和系统。此外，你要使用工具和技术来消除故障、配置错误和硬件故障。换句话说，你要尽力减少与 IT 有关的并且在你控制之下的灾难发生的可能性。在第 5 章“基线措施”中将介绍预防策略。
- **预测策略**：在预测策略中，你要识别出响应灾难并从灾难中恢复的规程。为此，你要预测可能导致灾难的情况、它们发生的可能性以及它们的影响。你可以根据经验以及与部署在公司中的系统有关的信息获得这些信息。利用这些系统的配置和有可能影响它们的问题，你可以获得可能导致灾难的情况以及它们的影响的信息。在第 4 章“风险分析”和第 6 章“恢复计划”中，你将详细地了解这一策略。
- **缓解策略**：当你规划缓解策略时，你要采取措施，使不可避免的灾难的影响最小化。在第 6 章以及第 8 章“集中系统的恢复计划”和第 9 章“分散系统的恢复计划”的实现部分中，你将详细地了解这一策略。

要实现这 3 个策略，你必须确保你的灾难恢复规划遵循面向项目的方法。在你实现灾难恢复规划策略时，你需要牢记某些事项。下一节将介绍这些事项。

1.4 规划事项

在制定灾难恢复的计划时，必须牢记所有灾难响应规程和从灾难中恢复的选择方案。此外，你必须了解灾难恢复的所有假定，以帮助你创建全面的灾难恢复计划。下面是在制定灾难恢复计划时要牢记的其他一些事项。

- **规划结构的创建**：规划结构的创建对灾难恢复规划的成败至关重要。这是因为灾难恢复规划的过程包括多个个体和相当大的支出。规划结构应当是多层次的，这样才能保证公司的不同层次和不同部门之间的协调性。在后面的“组织规划结构”一节中，你将了解灾难恢复规划的规划结构。
- **管理人员的支持**：在规划过程中以及计划的整个创建和维护过程中，寻求管理人员的支持和参与是非常重要的。管理人员的帮助不仅在于提供财务支持，而且在于允许员工集中时间成功地完成规划过程。管理人员应当协调灾难恢复计划的实现和维护，以确保它在整个公司中的有效性。灾难恢复规划的内在支持需要公司部门和员工的必要参与作保证。

获得管理人员支持的关键在于与其沟通计划过程的必要性和好处。为了获得管理人员的支持，你可以采取各种不同的方法。例如，你可以说明与灾难有关的事实，使管理人员意识到有可能蒙受的损失和其他影响。

- **使灾难恢复成为组织过程的一部分**：要确保从灾难恢复计划中获得最大的好处，你需要使灾难恢复成为一个有组织的过程。为了在不确定环境中保持计划的有效性和相关性，你还必须保证灾难恢复规划是一个不断前进的过程。换句话说，你应当把公司中的所有变化都合并到灾难恢复计划中。这需要采取适当的措施来减少灾难的影响。

- **时间事项：**了解灾难恢复实施的时间是非常重要的。灾难恢复是在灾难发生之后恢复公司操作的最后努力。通常情况下，当公司的重要活动或功能受到威胁的时间无法接受时，公司将会决定创建和实现灾难恢复计划。这一决定取决于公司的类型、营业状况和它对 IT 的依赖程度。此外，IT 设置承诺的服务级别决定应当实施灾难恢复计划的时间。例如，IT 部门向你保证将在规定的时间内恢复中断的营业。但是，如果营业中断的时间超过了规定的时间，你就需要实施灾难恢复计划。
- **评估现有的应急计划和规程：**在制定灾难恢复计划之前，你必须检查和评估公司中设置到位的所有计划和规程——如备份计划、归档规程和安全规程。你还应当评估不同类型灾难的应急规划。执行这样一个评估的目的是为了确定可以直接合并到灾难恢复计划中的现有计划和规程。

明智的做法是向过程所有者或这些计划和规程的创建者寻求帮助，以获得更有价值的输入。此外，你可以使用文档（部门的过程流图和组织图表）来收集灾难恢复规划的有用资源。

- **公司所有部门的参与：**某个灾难不可能只影响一个部门。因此，要成功地实现规划过程，所有部门在其中发挥积极作用就变得非常必要。管理人员的支持肯定会推动员工参与到规划过程中。通过向员工讲授灾难恢复规划的目的及其重要性，可以达到各部门之间的协调。此外，你可以用一些事实来说明灾难如何影响员工和公司。考虑一些创新性的方法，使员工参与到规划过程中来。例如，奖励所有成功地完成灾难测试训练的员工。

另外，你必须分析每个部门执行的活动和功能，以确保在灾难恢复计划中恰当地表示风险和可能的灾难。为了分析每个规划步骤对不同部门及其活动的影响，各个部门都派代表检查规划小组做出的决定是很重要的。这样，灾难恢复计划才是现实和有效的。后面的“规划小组”一节将介绍这个小组。

- **有关灾难的知识：**要使创建灾难恢复计划的整个活动取得理想的效果，准确和深入地了解灾难是非常重要的。在进行规划时，你应当考虑其中全部设施都被破坏的最差情况场景，并将你的计划集中于这样的不测事件。

注意

虽然明智的做法是对所有的灾难进行规划和准备，但是时间和财务限制也许只能使你规划其中的一些灾难。灾难恢复规划背后的驱动力是平衡业务要求和公司面临的现实。

- **外部专家的作用：**公司经常聘请公司外部的专家（如顾问或提供商）收集用于创建灾难恢复计划的信息。你可以利用顾问的专业技能来创建灾难恢复计划。一个公司只有在缺乏独立执行灾难恢复规划或系统审计时，才会聘请外部专家。在这种情况下，外部专家可以执行有助于灾难恢复规划的活动。经过培训的灾难恢复顾问可以确定一个公司的薄弱点和风险。基于收集的信息，顾问可以确定执行灾难恢复所需的活动。此外，他们还可以确定执行灾难恢复所需的人员、预算和时间。这些专家可以定义灾难恢复计划的范围、评估现有的计划并指导灾难恢复工作，以便获得管理人员的批准。

注意

为了完成任务，外部专家要评估公司现有的灾难恢复计划和规程。这些专家在确定和收集有关公司、公司的功能和资产等信息时，一个重要的来源就是该公司的关键人员。此外，这些专家通过查询本地的公众服务机构，以确定该地区的自然灾害。

除了前面描述的规划考虑事项以外，还可以使用不同的方法实现灾难恢复。这些灾难恢复的方法因公司的不同而有所变化，不过有两种方法最为常用。

在第一种方法即程序格式方法中，你要把规划过程的细节记录成完整的句子。在第二种方法即清单方法中，你要以着重点的形式记录规划细节。这两种方法都有优点。因此，具体使用哪种方法，还是使用两者的组合，这完全由你决定。

尽管不同公司使用的方法有所不同，但是规划过程的阶段对于所有方法都是通用的。

1.5 灾难恢复规划的阶段

灾难恢复规划项目是按阶段进行研究的，一定要牢记项目涉及的时间和资源。分阶段方法确保可以考虑到灾难可能影响到的公司的所有关键区域，还确保规划过程既有系统又简单。

注意

在此，阶段和活动只作为指导原则。你可以更改它们，使之满足公司的要求。同样，你可以自行决定是否对每个阶段中执行的活动进行分类。

在规划过程的每个阶段中，都要寻找问题的答案，然后利用这些答案进行及时的恢复。例如，一个公司或部门的关键活动是什么？类似地，当前公司对付灾难的准备级别是什么？

每个阶段都把前一阶段的输出作为输入。灾难恢复规划过程的各个阶段如下所述：

- 启动阶段
- 风险分析阶段
- 计划的创建和实现阶段
- 计划的测试阶段
- 计划的维护阶段

接下来的章节将依次介绍各个阶段。

1.5.1 启动阶段

启动阶段是对灾难恢复规划项目进行概念化的阶段。在这个阶段中，要成立规划小组。小组创建后，就要决定规划过程的目的和目标。这个小组要在规划项目的假定上达成一致意见。为此，该小组要分析公司的不同方面，如要求、环境和所受灾难的影响。例如，小组可