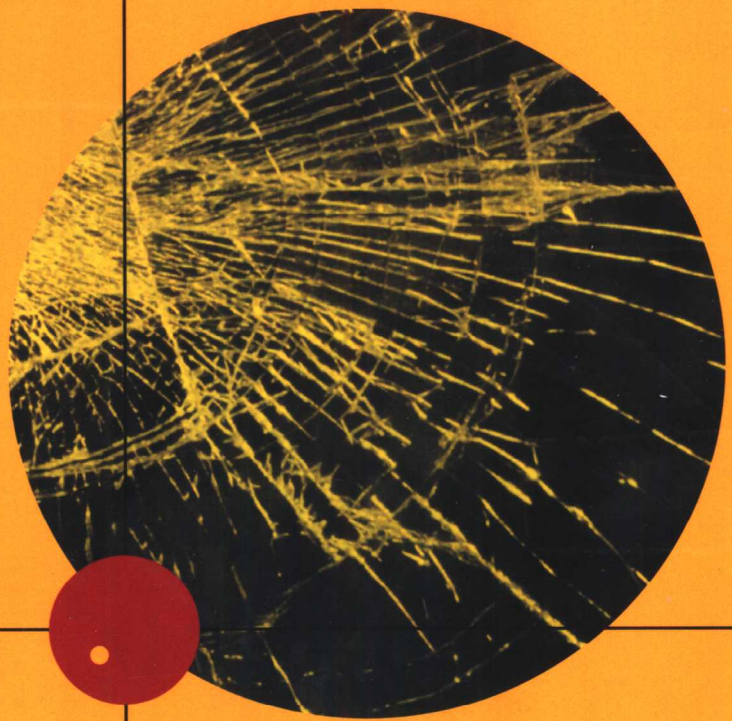
THOMSON

信息安全丛书

灾难恢复指南

[美] MICHAEL ERBSCHLOE 著　　杜 江 主译



重庆大学出版社

灾难恢复指南

原著:[美]MICHAEL ERBSCHLOE
主译:杜　江
译者:廖　斌　郭　坚　贺登科　张黎明　马宏亮

重庆大学出版社

Michael Erbschloe
GUIDE TO DISASTER RECOVERY
ISBN: 0-619-13122-5

Copyright © 2004 by Course Technology, a division of Thomson Learning.

Original language published by Thomson Learning. All Rights reserved.
本书原版由汤姆森学习出版集团出版。版权所有,盗版必究。

Chongqing University Press is authorized by Thomson Learning to publish and distribute exclusively this simplified Chinese edition. This edition is authorized for sale in the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.
本书中文简体字翻译版由汤姆森学习出版集团授权重庆大学出版社独家出版发行。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾)销售。未经授权的本书出口将被视为违反版权法的行为。
未经出版者预先书面许可,不得以任何方式复制或发行本书的任何部分。

981-265-277-9

版贸核渝字(2004)第43号

图书在版编目(CIP)数据

灾难恢复指南/(美)厄布施莱(Erbschloe, M.)著;
杜江等译. —重庆:重庆大学出版社,2004.12
(信息安全丛书)
书名原文: Guide to Disaster Recovery
ISBN 7-5624-3173-6

Ⅰ.灾... Ⅱ.①厄... ②杜... Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2004)第134796号

灾难恢复指南
Zainan Huifu Zhinan
[美]Michael Erbschloe(厄布施莱)著 杜江 主译

出 版 者:重庆大学出版社 **地 址**:重庆市沙坪坝正街174号重庆大学(A区)内
网 址:http://www.cqup.com.cn **邮 编**:400030
电 话:(023) 65102378 65105781 **传 真**:(023) 65103686 65105565
出 版 人:张鸽盛
责任编辑:王 斌 **版式设计**:王 斌
责任校对:邹 忌 **责任印制**:秦 梅
印 刷 者:重庆升光电力印务有限公司
发 行 者:全国新华书店经销
开 本:787×1092 1/16 **印张**:19.75 **字数**:398千
版 次:2005年1月第1版 2005年1月第1次印刷
书 号:ISBN 7-5624-3173-6
印 数:1—4 000
定 价:30.00元

序

随着世界科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息网络已成为国家和社会发展新的重要战略资源。与此同时，社会对信息的依赖程度越来越高，网络和信息系统的安全问题愈加重要。保障网络与信息系统安全，更好地维护国家安全、经济和社会稳定，是信息化发展中必须要解决的重大问题。

面对复杂多变的国际环境和互联网的广泛应用，我国信息安全问题日益突出。加入世界贸易组织、发展电子政务等，对信息安全保障提出了新的、更高的要求。我国政府始终高度重视信息安全问题，将信息安全作为全面推进我国国民经济和社会信息化进程的重要环节，做出了一系列重要决策和部署。2003 年 9 月国家信息化领导小组研究提出了《关于加强信息安全保障工作的意见》，进一步明确了我国信息安全保障工作的总体要求、主要原则和重点任务；2004 年初又专门召开了全国信息安全保障工作会议，对信息安全保障工作做出了全面部署，为国家信息安全保障体系的建设注入了强劲的动力，将我国的信息安全工作推进到一个崭新的阶段。

有幸经历近 10 年来中国信息化进程的人都不会忘记，我国信息安全事业的发展、技术的进步和产业水平的提升从世界各国，特别是西方发达国家得益颇多。现代信息安全概念和技术的引入，给长期以通信保密为核心的中国信息安全界带来一股清新的风，它们的许多理论、观点、概念和方法对更新我们的安全观念、发展自主的安全技术、加强信息安全的管理等都发挥过相当积极的影响，进入新世纪后，在中国加入 WTO 和经济全球化的推动下，国内外在信息安全领域的学术交流和技术互动日益加深，信息安全国际化已成不可阻挡之势。在统筹考虑国际国内两个大局的背景下，中国信息安全界对于世界各国，尤其是西方发达国家的信息安全理念、法则、规范和实践经验的学习与研究正掀起新一轮热潮。

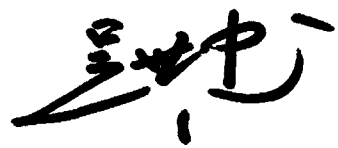
与过去相比，新一轮的学习与研究热潮在内容上已有本质的提高。几年前，西方的信息安全理论和技术让急于寻求解决方案和发展思路的中国信息安全界眼界洞开，我们曾以一种饥不择食的急迫心情将西方的信息安

全理论、概念和做法搬到国内来。但近年来，我们欣喜地看到，中国信息安全产业界和学术界已逐渐走向成熟，开始理性地审视国外的技术与方法，紧密结合中国的实际需要精心选择国外信息安全理论和实践的成果，并在研究、思考的基础上，努力探索适合中国国情的信息安全之路。生活在重庆的几位归国学人从众多的海外著述中精选了《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》和《灾害恢复指南》3本，细心译介给国内，就是众多的努力之一。信息安全意识、信息安全管理和安全容灾与恢复正是当下国内急需的知识与方法。从这3本书内容的深入浅出和方法的清晰实用，可以看出编译者的良苦用心，相信他们的愿望和努力会得到业界和学界的认可和尊重。

中国信息安全事业的发展需要更系统、更全面、更深入地翻译、介绍国外的经典著述，需要更迅速、更经济、更便捷地学习、掌握他人的实践经验。因此，我们十分乐见《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》、《灾害恢复指南》3本译著的出版，并乐于在其付印之前，将个人的观感和陋见附上，以示敬意。

兹为序。

中国信息安全产品测评认证中心　主任
中国信息产业商会信息安全产业分会　理事长
全国信息安全标准化技术委员会　副主任



2004年秋
于北京昆明湖畔

此为试读，需要完整PDF请访问：www.ertongbook.com

译者序

没有人能够忘记2001年发生在美国纽约的“9·11”恐怖袭击，它无疑是一场巨大的灾难，对现代社会政治、经济等各个方面都产生了深远影响。灾难发生后，所有位于世贸大楼内的公司和企业均遭受重创，关键性文档、客户档案、合同文本、票据等均毁于一旦，存储在计算机内的大量电子资料的也因损毁而无法恢复。公司和企业蒙受了巨大损失，有的甚至再无法进行以前的正常运作，从此一蹶不振直至倒闭。“9·11”使政府、公司和企业等各类组织更真切地认识到应对灾难，保证业务连续的重要性。

在中国，当2003年初“非典”SARS突然袭来，全国上下陷入一片恐慌，暴露出国家卫生防疫体系应对突发灾难的严重不足，其影响业已深入到社会的各个方面。事件过后，国内各大城市开始陆续制定各种灾难应急响应预案，以尽可能预防和降低灾难危害性，并使各种组织机构能够尽快从灾难中恢复正常运作。

近几年来，世界上各大知名企业也开始制定和实施灾难恢复计划。如IBM公司已经在中国北京和广州分别建立了“业务连续性与灾难恢复中心”，在上海外高桥保税区建立了“ETC灾难备份中心”，全面推出了完善的“业务连续性与灾难恢复”服务。然而，“灾难恢复计划”对绝大多数中国企业和各类组织来说还是一个全新的实践项目，需要参考和借鉴一些国外经验教训，以便能够更好、更快地制定和实施适合自己组织的“灾难恢复计划”，在未来可能不幸降临的灾难中求得生存。

由Michael Erbschloe所著的《灾难恢复指南》一书，正符合了我们这样的需要。本书深入浅出地讲述了制定“灾难恢复计划”的8个步骤，其中每一个步骤都给出了清晰的目标和详细的策略，并编制了大量的用于灾难恢复计划的实用性表格。只需进行少许修改，这些表格就可以被用于任何一个组织。可以说，本书也是一个很好的“灾难恢复计划”工作手册，特别是为那些没有经验的计划制定者们提供了一个可快速参考的案头工具书。

虽然Michael Erbschloe本人是一个信息技术专家，但并没有局限于单纯信息领域意义上的灾难恢复研究，书中阐述的灾难恢复计划过程涵盖了IT技术、管理、政治、法律、社会学等多个领域，不单对普通的IT公司具有现实的意义，也对所有关注和需要准备制定实施灾难恢复计划的政府、企业等组织同样意义深远。本书的读者群不仅限于IT公司或者信息安全从业人员，更值得各类组织机构的管理人员、企业CEO、CIO等仔细研读。

在最初开始翻译本书时，原本是将它当成一本纯粹的IT信息安全专著，在随后深入翻译的过程中，才逐渐意识到其内容涵盖之广已远远超出了单纯的信息安全领域，

使我们自身对灾难恢复计划的认识有了一个新的飞跃。然而，由于译者本人主要从事计算机信息安全领域的研究，对于书中所涉及的管理、法律、社会学等领域的知识了解尚不够充分，所以在翻译中难免有很多不足之处，望读者在阅读本书过程中多提供宝贵意见，来信斧正。

本书的翻译和出版工作得到了重庆大学出版社的大力支持，特别是国际合作部的陈晓阳、方天瞳和王斌，是他们的远见和努力争取才从著名的 Thomson 出版公司取得版权。在整个翻译过程中，他们给予了很多指导和帮助，使得本书能够有缘与广大的读者见面，为提高国内灾难恢复水平做出一点贡献。

杜 江

2004.12

前　言

本书将告诉读者如何循序渐进地制定、执行和管理一项灾难恢复计划。曾几何时，灾难恢复计划还仅仅是一个美妙的商业构思，如今却成了一件关乎国家安全的大事情。世界贸易大厦和俄克拉荷马州联邦州政府大楼所遭受的恐怖袭击事件表明，很多组织即使不是恐怖袭击所针对的目标，也依然会受到灾难的影响。在俄克拉荷马州首府，爆炸使附近几个街区的建筑都受到了严重的毁坏；在纽约，至少 20 栋建筑毁坏严重，而不得不暂时疏散里面的大多数住户。

从 2001 年 9 月开始，美国政府开始着手成立国土安全部。联邦调查局、执法部门和情报机构警告说恐怖分子将对美国及其海外利益发动更多的袭击。如果不幸被言中，那么组织面临的最大灾难将会是人为而非自然力所造成。这种严峻形势使灾难恢复计划需求显得尤为迫切，这也是促成本书的原因。

为了详细阐述灾难恢复计划中的薄弱之处以及其前景，本书调查了 13 个行业的 254 位计划者和经理。调查的结果显示了灾难恢复计划中应受到特别关注的部分。例如，有些调查对象表示多数组织需要改进其灾难恢复计划和程序的文档编制工作。调查也同时表明，虽然对于计划和过程的测试与演练是很有价值的一个环节，但是并非所有的组织对此都给予了足够的重视。

本书读者

本书读者包括学生、管理人员以及任何负责灾难响应与重建灾后正常运作的工作人员。从第一章开始，读者就可以逐步地根据所给的材料，来制定灾难恢复计划以及程序。本书中每一章都包含了多个需要学生完成的基于该章主题的实践项目作业；另外每章还包含一个实例项目，要求读者作为一个解决问题的人，运用该章阐述的理论来解决真实工作环境中存在的问题。

章节概述

第一章 灾难恢复介绍

本章介绍组织灾难恢复的基本原则及如何建立灾难恢复计划。过程如下:组织计划小组、评估风险、制定并归档各种策略及程序、挑选并培训应急响应小组,以及在逼真的模拟环境中进行有效性测试。

第二章 准备制定灾难恢复计划

本章详述制定计划的第一步——组织如何组建灾难恢复计划小组。该小组应该是一个均衡的团队,由代表组织的各种职能的人员组成。

第三章 组织风险评估

本章详述灾难恢复计划的基本工作,即与组织内外各种关键人员合作以确保所有的风险都能够得到彻底的审查和评估。

第四章 划分系统和功能恢复优先级别

本章详述了各部门代表如何确定哪些业务活动对组织而言是最关键的。计划小组需要据此来制定灾难恢复程序,以便发生灾难时能尽快恢复组织运转。

第五章 制定计划和程序

本章详述了计划小组如何为组织的每一机构制定恢复程序。组织所有的机构都需要一些基础的程序,但是针对单一机构特殊的情况和模式,需要定制不同的程序。

第六章 灾难恢复中各组织间关系

从灾难中恢复,组织需要和不同的机构进行合作,如:执法部门、应急服务提供商、公共服务提供商、商业伙伴、供应商等;同时组织也需要和消费者、雇员以及他们的家庭、附近的社区进行交流沟通。

第七章 计算机攻击响应程序

灾难的产生更有可能是因为计算机遭到网络或黑客攻击,而不是自然的事故。处理这种情况需要对重要的数据进行备份和分析,还要和执法部门进行合作。

第八章 特殊情况的程序制定

本章讨论了一些在灾难中如何保护特殊资产的技巧。这些资产包括有毒材料、管制物质、历史文献和商业秘密等。

第九章 灾难恢复计划实施

本章详述了组织如何实施灾难恢复计划,包括制定实施计划、评估缓解灾难损失步骤的价值、实施过程中的职责分配、制定计划实施进度表和训练雇员。

第十章 测试与演练

本章讨论如何进行测试演练以确定灾难恢复计划的实际工作性能。计划小组将观察整个过程并对计划做相应的修改。

第十一章 对需求、威胁和解决方案的持续评估

本章讨论在灾难恢复计划小组制定、实施和测试计划程序后,组织如何过渡到日常的维护模式。计划小组需要制定能长时间监控和管理该计划的方法。

第十二章 度过灾难

本章讨论组织如何在灾难中获取知识和经验。管理人员和计划制定者必须认识到灾难不管对单个的雇员还是整个组织都有着长时间难以消除的影响。

附录 A 和 B

总结有关本书主题的调查结果,同时列举了一些非常好的网上资源。

特 点

本书具有如下特点:

- **章节目标** 本书在每章开头均详细列出了需掌握的重要概念,有助于快速了解本章的内容。
- **章节总结** 本书在每章末尾附有总结,有助于回顾本章的内容。
- **关键术语** 每章中以黑体字标识的术语均收录于章末的术语表中,有助于对新术语的理解。
- **复习题** 本书每章也提供了许多复习题,以加深对重要概念的理解。
- **实践项目** 每章均附有一定数目的实践项目,可以从里面学习一些实际的解决方案和经验。
- **实例项目** 每章末均附有一些实例项目,需要运用一些常识以及本书涉及的知识来完成这些练习,这些问题与将在实际中遇到的类似,你的目标就是找到它们的解决方案。

图标介绍

为了能更好地理解本书的内容，本书在每一个适当的地方都插入了附加说明和练习。这些附加材料旁边都加了图标以提醒您的注意，以下是对图标含义的解释：

“注释”图标，提示关注与本主题相关的补充资料。

“实践项目”图标，指示本书的实践项目及其练习内容。

“提示”图标，显示依据作者经验给出的关于实际情况中如何把握和处理问题的方法。

“警告”图标，指示有可能出现的错误和问题以及避免的办法。

“实例项目”图标，基于现时的实例项目。在这些更具广泛意义的实例中，读者要独自运用所学知识来解决问题。

教师资源

当本书用于教学时，教师可以利用补充资料。教师若需要这些资料，可以填写书末附表后，直接与 THOMSON 公司联系，索要如下资料：

电子版教师手册：与本书配套的教师手册中包括各种备课所需的辅导资料，如课堂活动开展建议、讨论话题和一些附加项目。

问题解答：包括本书所有章节后面的复习题、实践项目和实例项目的解答。

测试检查软件：本书附带一套功能强大的测试检查软件，可帮助教师进行笔试和网上考试（局域网或互联网）。该套软件储存了大量涵盖本书各个主题的问题，可为学生提供详细的学习指导和复习参考。其中网上考试功能使得学生在自己的计算机上考试成为现实，通过自动评分还可以节约教师的时间。

此为试读，需要完整PDF请访问：www.ertongbook.com

Power Point **演示文稿**:本书的每章均带有 Microsoft Power Point 幻灯片,用于辅助教学。教师也可以自由地向里面添加一些内容。

图形文件:本书中所有的图形均以 BMP 格式存储在教师资源光盘中。与幻灯片一样,所有的图形都可用于辅助教学,可网络共享供学生下载或者打印后分发。

致 谢

首先要感谢我的朋友们,在我写作本书的过程中他们给予了我许多鼓励和支持;感谢产品经理 Amy Lyon;感谢 Randy Weaver 给予本书的富有创见的技术审核和质量保证;感谢开发经理 Dan Seiter;还要感谢编辑 Danielle Power 和 Brooke Booth。

感谢以下评审者给予我许多有益的意见:Barbara Belon (Vorwalk Community College), Faebod Karimi (Heald College), Michael Nicholas (Davenport University), Randy Nichols (George Washington University)

目 录

此为试读，需要完整PDF请访问：www.ertongbook.com