信息安全丛书

信息系统
安全策略

Disaster Recovery Planning

Preparing for the Unthinkable, Third Edition

灾难恢复规划

（第三版）

[美] Jon William Toigo 著

连一峰 庞 南 等译

- 9.11后的灾难恢复策略
- 高级存储技术和“数据恢复时间”准则
- Web服务和下一代灾难恢复业务外包的内涵
- 灾难恢复分析、规划、策略、测试和紧急决策
- 集中和分布式环境下网络和最终用户的灾难恢复

PRENTICE HALL PTR

PHEI

電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

信息安全丛书

灾难恢复规划

（第三版）

Disaster Recovery Planning

Preparing for the Unthinkable

Third Edition

[美] Jon William Toigo 著

连一峰 庞 南 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

随着信息技术在各个领域越来越广泛的应用，对信息安全的重视也和信息系统建设本身一样，已逐渐成为人们关注的焦点。信息系统灾难的恢复并不仅仅是针对信息系统的数据恢复和系统恢复，而是面向整个企业的生存规划，它将接受来自各个方面的威胁和挑战，包括火灾、洪水、飓风、地震、计算机病毒、网络入侵、电力故障、通信故障、人为失误，甚至是恐怖袭击。灾难恢复关注的不是灾难本身，而是预防灾难和应对灾难的方法。灾难恢复依赖于训练有素的人员，也依赖于合理完善的恢复规划。没有软件工程的开发项目将会陷入泥沼，没有恢复规划的灾难恢复则可能面临灭顶之灾。

本书可作为高年级本科生和研究生教材，对从事信息系统安全研究的科研人员和工程技术人员也是一本难得的参考书。

版权贸易合同登记号　图字：01-2003-1037

图书在版编目（CIP）数据

灾难恢复规划：第三版/（美）托伊戈（Toigo, J. W.）著；连一峰等译. -北京：电子工业出版社，2004.5
（信息安全丛书）
书名原文：Disaster Recovery Planning: Preparing for the Unthinkable, Third Edition
ISBN 7-5053-9889-X

Ⅰ. 灾...　Ⅱ. ①托... ②连...　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039001号

责任编辑：谭海平　许菊芳
印　　刷：北京市增富印刷有限责任公司
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：22　字数：563千字
印　　次：2004年5月第1次印刷
定　　价：38.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

译 者 序

虽然 Jon William Toigo 先生一直强调在灾难恢复领域中没有所谓的专家，只有经验才是最好的老师，但从 1990 年出版的《灾难恢复规划》第一版，到 2000 年出版的第二版，再到现在的第三版，作者为我们展示了灾难恢复领域各个方面的内容以及发展的历程和趋势。作为这一领域当之无愧的权威，Toigo 先生的谦虚为我们所称道。

由于信息技术领域较多地涉及到故障、崩溃、重建、恢复等专业术语，因此针对 IT 行业的灾难恢复更广泛地被人们所接受，这一点对于国内来说尤为明显。然而，灾难恢复并不仅仅是针对信息系统的数据恢复和系统恢复，而是面向整个企业的生存规划。它将接受来自各个方面的威胁和挑战，包括火灾、洪水、飓风、地震、计算机病毒、网络入侵、电力故障、通信故障、人为失误甚至是恐怖袭击。

灾难恢复关注的不是灾难本身，而是预防灾难和应对灾难的方法。灾难恢复依赖于训练有素的人员，也依赖于合理完善的恢复规划。没有软件工程的开发项目将会陷入泥沼，没有恢复规划的灾难恢复则可能面临灭顶之灾。

中国科学院研究生院信息安全国家重点实验室作为信息安全领域的研究机构，始终关注数据恢复、系统恢复、应用恢复等与灾难恢复相关的研究方向。电子工业出版社此次将这本经典的灾难恢复规划书籍交由本实验室负责翻译，也为我们提供了很好的学习机会。通过全书的翻译和整理，我们从中领略了灾难恢复这一领域广阔的发展前景以及对当前经济生活的紧迫性，希望本书能够为广大读者提供帮助。

参与本书翻译工作的包括实验室的研究生和工作人员，他们在翻译过程中付出了心血和努力，查阅了大量的相关文献资料，在准确表达原文含义方面可以说是不遗余力。在此对他们的辛勤工作表示深深的感谢。

本书的第 1 章和第 2 章由胡艳翻译，第 3 章由鲍旭华翻译，第 4 章由李闻和冯萍慧翻译，第 5 章和第 6 章由刘子锐翻译，第 7 章、第 8 章和本书的前言部分由庞南翻译，第 9 章由许一凡翻译，第 10 章、第 11 章、第 12 章和本书的专用术语部分由连一峰翻译。另外，许太平为本书的翻译工作也提供了帮助，在此表示感谢。全书的整理和审校工作由戴英侠和连一峰负责。

序　一

2001年9月11日，我刚刚到达自己位于世贸中心1号塔楼69层的办公室，准备开始一天的工作，对纽约及新泽西港务局的多种运输设备的收支情况进行总结。我打开我的Dell计算机，等待本地磁盘的引导和杀毒软件完成扫描过程，然后登录进入办公室的Novell网络。突然间，一切就发生了。

一声巨大的爆炸声伴随着嘈杂的噪音，整个建筑物发出隆隆的声响，并且开始摇摆。感觉就像是向一个方向移动了1米多，稍微停顿了一下，在相同的方向又继续移动了1米多。那时我深信大楼一定会倒塌，不知道是否有人能够从这场灾难中幸存（事后我得知是由于飞机的碰撞使得建筑物发生了2.5～3米的摇摆，而通常情况下的摇摆都不会超过0.3米）。

我的窗口面向大楼的东面。从这里望去，我难以置信地看到玻璃和碎片从空中倾泻而下，大火在上面几层熊熊燃烧。我立刻意识到是上面的楼层发生了严重的爆炸，我们必须尽快从建筑物中撤离。

可能是紧张的缘故，一位同事紧紧抓住我的手大约有60秒钟，之后大楼停止摇摆并恢复到原来的位置。大楼稳定下来后，所有人都很有秩序地通过走廊走进楼梯。很可能当时有的电梯还能工作，但是平时大量的火警训练告诉我们，在这个时候最好不要使用它们。

1993年2月26日，我当时也在世贸中心上班，但是当恐怖分子的炸弹在地下室爆炸的时候，我并没有在建筑物内。那天，就在中午12:18爆炸发生前的几分钟，我离开办公室去参加一个午餐会议。那些1993年发生爆炸时在场的人们看来很清楚地知道现在到底发生了什么事情，不过事后证实1993年的爆炸事件给人们带来的震撼远远无法与9.11的冲击相比。

在我们跑向楼梯时获知，是一架飞机和大楼发生了碰撞。一位同事的办公室位于大楼北面，他看到了飞机逼近的过程。他后来说他知道这是一架干线飞机，而且在碰撞发生前他能够辨别出这是一架美洲航空公司的班机。

在下面楼层涌入的人们挤满楼梯间之前，我们还能够向下多走一些台阶。这就像陷入了一次保险杠挨着保险杠的大塞车，你能够向下走三四级台阶，然后停下来等待，再向下走三四级台阶，然后再等待。在楼梯间里有些轻微的烟雾，并且充斥着航空燃油的气味。

每个人都用上衣、领带或者餐巾掩住脸，而且大家都很关注为什么碰撞发生在上面的楼层，而我们还能够感觉到烟雾的存在。回想1993年的时候，烟雾是从地下室向上扩散的，使得人员的撤离非常困难。而且这次与1993年不同的是，在我们向下撤离的过程中，楼梯间的电灯一直亮着，这也是1993年爆炸后进行的安全改进措施。

下楼梯的过程有些超现实的感觉，我们开着神经质的玩笑来帮助自己放松心情，每一个人相对来说都还比较平静。当下撤到39层的时候，我们需要紧贴着墙排成一排，以便为从下而上的消防队员铺设消防设备腾出空间。

我只能够凭想像去揣摩那些消防队员的想法。他们清楚地知道情况的严重性，却依然在我们试图撤离的时候勇往直前。后来，我们从一个向上攀爬的气喘吁吁的消防员那里得知，第二架飞机也撞上了大楼。我们没有过多讨论这个事件，因为不想制造额外的紧张气氛，但是在我们头脑中已经意识到，一架飞机还可能是偶然事故，然而两架飞机相隔几分钟接连发生撞击事件，就一定是事先策划好的恐怖袭击了。

随着楼梯间里面情况的恶化，前面的人们会告诉我们有什么危险，而我们也要把这些传达给后面的人们。当我们到达大约30层的时候，楼梯由于潮湿和拥挤人群的汗渍而变得湿滑起来。到达25层时，我们脚下大约有5厘米深的积水，可能来自破裂的管道、喷淋系统或者上层的消防用水，我只能如此推测。下撤的速度慢慢变快起来，不过还是由于一些原因而显得比较缓慢，有的人因为虚弱必须在别人的搀扶下才能走完剩下的台阶。

大约在上午9:40，我们最终到达了大楼的第二层，也就是购物中心层。从楼梯间进入到宽敞的空间后，紧急和混乱情况发生了。我们从楼梯间内的缓慢下撤变成了四散奔逃，以离开建筑物到达足够安全的距离。消防员和警察护送我们经过购物广场一层时，那里的水像大雨一样从头顶喷洒下来，接着我们乘电动扶梯回到购物中心层。我曾经在购物中心参加过很多次曼哈顿的夏日午间音乐会，然而现在那里充斥着大堆的碎片：烧黑的碎石、燃烧的办公家具，还有那些一看就知道是遇难者的遗体。

为了躲避从天而降的碎片，我们迅速穿过街道。回过头去，我们第一次看到了袭击后的世贸中心双塔，它们已经被烈焰和翻滚的浓烟所包围。

街道上混乱不堪，我们一起继续向前穿过了四五个街区。我回过身来，想再看看眼前的世贸中心，但是同行的人们不希望站在那里旁观灾难，他们只想继续向前，远离商业区。

我们坐上了一趟突然停下的、离开商业区的地铁。我们在那里等了大约1小时，地铁才启动开往下一个车站，我们被告知在运河大街下车。

后来，我又重新回到这里的大街上，并试图寻找世贸中心，本来在我所在的位置应该很容易就可以看到，然而我却无法找到它。当我询问一个行人的时候，他的回答是，“它们不在了，它们在不久前都倒塌了”。我无法相信这是事实，无法想像这样的大楼会倒塌。

那时，我疯狂地想回家，想让我的家人知道我是安全的。我到下午1:00才和他们通上电话，晚上7:30才回到家里。那是一天中最艰难的时刻，我焦急地想回家，看到我的家人。他们都吓坏了，也不知道我是否安全。我8岁的儿子，那天没去学校待在家里，在电视中看到了所发生的事件。朋友和亲戚们来到我在新泽西的家里一起等待消息。当我终于回到家里以后，几乎每个人（包括我在内）都用了2天的时间才慢慢平静下来。

后来我才知道，其他一些人可没有这么从容。港务局的高级职员们在位于世贸中心Marriott酒店的应急指挥中心集合。当他们一起对状况进行评估的时候，世贸中心第二座塔楼在头顶上倒塌了。他们从废墟中爬出来，到达我们位于新泽西的办公室，重新调配能够利用的资源。那天傍晚，职员们已经开始工作，试图对灾难造成的损失和人员伤亡进行评估。

此时，港务局的其他一些工作需要得到尽快恢复。纽约地区的3个主要机场、隧道和桥梁、公交设施和火车，都属于港务局的管辖范围。在接下来的几天里，出于安全考虑，这些设施都保持关闭状态，但是增加安防和重新开放的计划已经开始酝酿。

恢复规划自始至终都处于执行状态，港务局的应急管理人员一直在忙于确定损失状况。那天我们一共失去了75名雇员，包括37名警务人员和38名普通雇员。我知道他们其中很多人的名字，有些是我在世贸中心的走廊中经常见到的，我甚至和其中一些人在港务局的不同岗位上共过事。

最重要的一点，是关键职能和业务的恢复。财务部门的恢复小组努力工作，以便完成文件和记录的定位，并且获得了那些保证薪资和账务处理正常进行的关键系统的访问权限。超过8000名雇员依赖于我们的部门，在这个困难时刻，必须确保他们能够获得支付供养和保护家庭所需的费用，同时能够支付众多的供应商，以便替换被毁坏的设备，使得公司的运作能够在其他的设施中继续进行。

我本人并没有参与及时的恢复操作，但毫无疑问我是它的受益者之一。事件发生在星期二，而在星期五我就收到了工资支票。部门的工作大约停滞了一周半，后来规划小组在新泽西州泽西城的Journal广场交通中心为我们建立了新的总部，我们又重新回到工作岗位。其他一些部门，也在包括港口设施和航空港办公室在内的一些分散办公室中重新开始工作。

我们试图通过接入网络来建立部分应用系统。幸亏港务局拥有分布式的办公室，能够接入在世贸中心之外运营的一个网络。通过路由变更并从异地保存的备份磁带中恢复数据，利用这个网络可以登录进入应用系统。

我们所面临的众多困难之一是难以找到可供使用的工作站和电话机。笔记本电脑变得非常普及，这是因为我们通常每天会在不同的工作站之间改变自己的工作位置。

开始的两个星期用于评估哪些文件还存在，而哪些文件已经丢失。存放在世贸中心内PC磁盘上的大多数文件永远丢失了。事实证明，电子邮件系统是一个找回丢失的计算机文件的有效来源。当我们逐渐进入无纸化办公环境的时候，如果文件被作为电子邮件发送给其他同事，那么就有一份拷贝仍然保存在收件箱、废件箱或者发件箱中，这样找回这个文件的机会就将大大增加。

危机管理咨询服务在此时可以很容易地获得。任何时候都可以找到咨询专家，而且他们给予我和很多同事非常大的帮助。他们和那些提供电话通信和局域网布线的技术人员一样重要，他们帮助我们恢复到一种正常的工作和生活状态。

除了港务局一直进行的恢复活动外，我还有责任重新组织会计管理协会的800多名会员，因为我是该协会纽约分会的主席。本来在袭击发生的那天，我们原计划举行一次午餐会议，由于事件的发生，这次会议也被取消了。我联系总部办公室，告诉他们丢失了位于世贸中心内的绝大多数分会财务记录。我让分会的信件和电子邮件都直接转发到我家中，我收到了全国其他分会主席发来的表示支持的电子邮件。

当我写下这些的时候，距离恐怖袭击已经过去两个多月了。今天，我环顾办公室，看到人们正在进入办公室，坐在他们的椅子上开始工作。我想这是人们平复创伤的一个标志，这与前几个星期形成了鲜明对比。在过去几个星期中，我们过不了几分钟就要停止工作，在一起聊天和谈论那天的悲剧。

虽然我们现在的办公室比以前拥挤了一倍，而且永久的办公地点和公司总部看来要在几个月之后才能建成，但是没有人对此有所抱怨。港务局同事们的信心并没有被打倒，而且我们正

在采取有效的步骤开始重建过程，这一点必须永远铭记。我们都知道很多人在恐怖袭击中遇难，但是这似乎是一个奇迹，在9.11悲剧的一天中，我们位于世贸中心1号塔楼69层的办公室中没有一个同事遇难。

Michael Shannon
纽约及新泽西港务局会计主管
会计管理协会纽约分会主席

序　二

“当我们回顾2001年，我们对于9.11事件充满了深深的悲痛和愤怒。我们之中有谁能够忘记那天所经历的震惊和恐怖呢？对摩根斯坦利家族来说，这次袭击恰好击中了我们的心脏——我们有3700名雇员在世贸中心工作。不幸的是，他们中有7个人以及6名合同服务的专业人员在那一天遇难。

但是，公司在被袭击时以及随后的几个星期中所做出的反应让我们感到骄傲。由于决心、纪律以及一些英勇的个人行为，我们绝大多数员工在北塔楼被击中后，执行了预先计划好并且经过反复演习的程序，立刻撤离了南塔楼。很多员工立刻前往备用地点来照顾客户和保护公司。我们相信，对于我们来说这是一个决定性的时刻——表明我们的坚定立场，并对极端环境的考验做出反应。”

——摘自给股东的一封信
摩根斯坦利2001年度报告

将日历翻到2002年1月1日是种很特别的感觉。继续我们的生活，并且将2001年发生的事情抛在脑后，这是人类的天性。我们经常听到关于9.11悲剧事件是如何永远改变了我们生活的说法。我觉得我们应该暂时停留，回顾一下那天中发生的事情，这是非常重要的，虽然这件事做起来非常困难。

我们中的许多人毫无准备地失去了家庭、朋友和同事。我们在努力接受这样一个无情和野蛮的事实，可以看到周围的很多人也在努力这样做。恐怖分子利用了我们的聪明才智和自由，并且用来对付我们。

生命中第一次不用再去想像我们的父母和祖父母们在1941年12月7日那天的感受。我们中的很多人回到家里，面对孩子们困惑的表情，试图帮助他们理智地面对我们自己都无法面对的事情。在我们的记忆中，白宫由于害怕袭击而紧急疏散好像还是第一次。自从1929年的崩溃以来，纽约股市第一次连续关闭了3天。纽约市完全置于一种停顿状态，对于我们这些无法理解9.11事件的人们来说，曼哈顿大街上近乎空荡荡的景象，只有一车车的国民警卫队和武装车辆，这是我们无法忘怀的场景。全国的空运也第一次停顿了大约一周时间。

棒球大联盟和橄榄球联赛也暂停了安排好的赛程，历史上第一次将世界职业棒球大赛推迟到11月，将总决赛推迟到了第二年的2月。很多电视台和广播电台在袭击后的几天中暂停了正常安排的节目和广告。好莱坞颁奖仪式在历史上第一次被取消。

Patrick Witty是一位很有远见的摄影师，他在2号塔楼开始爆炸的时候，将摄像机转向了相反的方向。当其他所有人都在拍摄塔楼倒塌的景象时，他拍摄到了大街上数百人被恐怖袭击后的反应，这肯定会成为9.11的一个经典画面。现在，我想遵照Witty先生的做法，将我的镜头转向另一个方向——从消极转向积极。

是的，我敢这么说，9.11事件带来了并且还将一直带来很多积极的东西。我们中的很多人都将重新考虑生活中最重要的是什么，也从家庭、朋友和信仰中发现了新的慰藉。一些我们一直关注的小事情，在生活中已经显得不那么重要，有些像过时的时尚。至少在一段时间内，我们之间不再有政治观点、种族和宗教的隔阂。只有美国人联合在一起，相互支持、相互鼓励、共同向前。我们向自己、向世界证明了美国依然是一个伟大的国家，能够在关键时刻团结起来，没有什么能将我们分开。我们在艰难的环境中依然能够拥有坚定的信念，并为之不断奋斗。

总统和政府部门坚持不懈地工作，在打击全球恐怖主义方面获得国际的一致赞同。纽约市的前市长及其内阁、纽约市警察局和消防部门，也被认为在工作岗位上每天都做出了无法估量的贡献。确实，美国在2001年9月11日经历了一次严峻的挑战，我们每个人都是其中的一员。

我们为很多无私的勇敢和英雄主义感到惊讶，我们为全世界汹涌澎湃的激情所感动，我们为军队的迅速果敢而重获信心。每一个身处其中的人都是英雄，大家都是英雄。

但是，在我看来，还有一件更加不可思议的奇迹。美国的经济被直接击中了要害，经受了最严峻的考验，虽然非常不稳定，但是最终却没有崩溃，这要归功于很多应该被大家了解的无名英雄。

他们是那些每天早晨醒来以后，照顾孩子上学、吻别爱人、将才智和想像力分享给美国的每一个工作岗位上的人们；他们是那些没有接受过应对危机的正规培训，然而却做得很出色的人们；他们是那些每天早晨出门上班、乘坐飞机或者面对新的不确定事件时会心跳加速的人们；他们是那些人类历史上最强大的经济机器的设计者和管理者。他们，我可爱的人民，是千百万像你一样在阅读本书的人们。美国经济的坚韧不拔，以及我们克服灾难重新投入战斗的能力，是最让人感到妙不可言的故事。

如果没有从中吸取经验教训，没有相应地调整我们的行为方式，这样的结果只能是无法彻底了解事情的本质。是的，我们的生活方式和商业运作的模式已经永远地改变了。我们恢复关键功能的能力不再被看做是一种反应过程，必须被看做是一种主要的操作风险。我们恢复关键任务数据的能力是最重要的因素。如果没有它，诸如物理位置的多样化和工作区域恢复等其他的策略都不可能实现。

引用一句古老的中国谚语：祸兮，福所倚。我们现在就面临着大量的机遇。团结在一起，我们可以建设一个新的、充满活力的美国，充满希望、力量与和平。让我们开始努力吧。

我想把这篇前言献给我的姐夫Stephen P. Dimino，Cantor-Fitzgerald的合伙人，他在2001年9月11日的世贸中心袭击事件中不幸遇难。

Gregory Ferris
执行主管
全球业务连续性计划（机构安全）
摩根斯坦利

第三版前言

在阅读本书序的时候，所有人都会被感动，甚至产生敬畏之情，因为它包含了2001年9月11日发生在世贸中心的恐怖袭击事件中的真实记录。

除了9.11造成的损失和悲痛之外，我们也被那些在灾难发生后致力于拯救生命和恢复组织运作的人们所表现出的惊人的坚毅和英雄主义所吸引和折服。谨以本书追忆逝者，并献给那些灾难中幸存的人们。

当编辑在9.11事件余波未平之际就要求我开始写本书的第三版时，我的第一反应就是犹豫不决。在此时出版本书的新版本真的合适吗？抑或只是为了迎合9.11事件所唤醒的人们对于灾难恢复和风险管理的关注，以获取商业利益为目的而设计的市场策略？为了将这些问题弄清楚，我迅速整理了一下思路：

问题：9.11事件是否确实改变了我们对于灾难恢复的理解？

答案：当然没有。最近的9.11事件给组成灾难恢复规划的方法论、规程以及最佳实施方法所带来的改变，并不比Andrew飓风或者Kobe地震带来的改变更大。如果有什么不同的话，那么可以说9.11证实了恢复规划的功效，而且再次显示了如果缺乏预先的灾难恢复规划，成功理解“恢复”的内涵是很困难的。

问题：对于那些需要新的预防方式的组织来说，恐怖主义是否是一种新的威胁？

答案：还是否定的。恐怖分子的潜在威胁，很多年来在私立和公立机构的灾难场景中都是一种灾难性的混合，在美国或者其他国家都是如此。另外，灾难恢复规划较少关注造成灾难的根本原因（除非这些知识可以有助于在一开始就避免灾难的发生），而是主要致力于处理灾难造成的后果。从灾难恢复的观点出发，9.11到底是由基地组织的人员、拉登的狂热信徒，还是其他政治和宗教派别的疯狂劫机犯所制造的，这并没有什么区别。灾难可能只是一个电火花或者其他点火装置造成的结果。

对于灾难恢复规划人员来说，最重要的事情就是如何使得位于世贸中心和五角大楼中的关键资产（特别是经过培训的人员以及数据）能够得到保护，并且在灾难之后能够迅速有效地恢复工作。无论灾难本身的代价是什么，如果不能以一种合理的方式对事件做出响应，将使得付出的代价大幅增加。

问题：9.11事件是否改变了灾难恢复规划执行的环境？

答案：也许。这个事件不是自然力量的表现，也不是某种随机状况造成的结果。它是敌对势力策划的有预谋的行动，激起了越来越大的反响，并且带有战争的特征。作为结果，它将特定的社会和政府机构置于战争的立场，这会给灾难恢复规划需要执行的环境造成深远的影响。

毫无疑问，新的法令将考虑9.11事件。其中一些将引入“强硬立场”和对公共基础设施的保护。在能源和交通部门中，安全方面的投入已经得到增加。信息和通信系统正在经受详细调查，这些调查致力于发现恐怖分子是如何获得机构脆弱性的详细信息，以及他们如何能够如此轻而易举地建立虚假的身份。

当环境发生变化时，需要重新测试灾难恢复规划。与灾难恢复有关的书籍也应如此，所有书中的假设都需要被重新审视和验证。

问题：除了9.11事件之外，有没有其他的技术变化对本书内容的更新有所裨益？

答案：是的。《灾难恢复规划》的第一版（1989）和第二版（1999）之间相隔了10年的时间。在此期间，信息技术在众多的应用环境中开始从数据中心向部门和工作组的分布式环境演变。本书的第二版致力于将前一版的内容进行更新，以反映新的挑战和由此创造出的机遇。

从1999年到2002年这个相对较短的时期内，技术同样发生了重要的变化，许多指标都证实了这种说法的真实性。

数据增长：根据美国加州大学伯克利分校进行的一项研究，到1999年，所有的人类社会组织中积聚并且以电子方式存储的数据量总计达到12 EB（12 000 000 000 000 000 000字节），研究者们认为这个数目到2002年中将会翻倍，这是更多数量的个人产生更多数量的信息的结果。

由个人所产生的数据，大约55%保存在个人计算机中，这些计算机通常没有包括在灾难恢复规划的安排中。这是灾难恢复的一个潜在弱点，很多9.11恢复计划都强调了这一点。

新的存储技术：对上述的爆炸数据进行管理，为其提供安全的、可以访问的存储业务，成为IT业界在21世纪面临的中心挑战。如今，我们见证了新生的网络化存储技术的出现，它们预示着切断存储阵列与服务器之间的连接。这种技术被用于改进数据的可访问性，并且能够提供不会造成混乱的可测量性。供应商们声称他们的软件产品还能够改善数据存储的弹性，并且能减少关键业务过程恢复的时间延迟，这种特性被“时间数据关系”的量度所描述。这些断言的正确性还需要进一步证实，而且互操作性问题还在困扰着不同厂家，由于互操作性问题而导致的灾难比它们所能防止的灾难还多。

支持业务过程解构的新应用范例：目前，业界已经看到了基于XML的Web服务这类新技术的涌现，能够为不同公司完全不同的系统之间提供全新级别的互操作性和可集成性。同时，新的服务托管范例（例如应用服务提供或者ASP）也被采用以降低商业成本，提高公司的业务能力。

这些技术需要能够支持向“商业过程解构”转变的大趋势。公司可以通过这种手段，将更多的后勤任务外包给供应链和价值链上的合作伙伴，以改进业务过程的效率。现在的问题是，相对它们能够避免的灾难，这些正在发展中的技术是否会导致更多的灾难？使用ASP是否会增加业务过程的灾难脆弱性，还是能够使之有所降低？Web应用系统是否能带来更低成本和更安全的B2B操作，或者只是造就了比以前更加不稳定的多层客户端/服务器平台？

上面的问答列表还可以继续下去，但是作为一个简要的结论，我认为确实有必要出版本书的新版本。出版新版本并不只是直接源自9.11事件，还源自于支持关键业务流程的信息技术基础设施的变化，以及执行灾难恢复规划的组织和外部环境的变化。这些变化要求传统的灾难恢复规划方式也发生变化。

不能够总是被动地做出反应，灾难恢复规划人员需要在工作中变得主动一些。他们需要着手与应用程序设计者们保持交流，开始在应用系统、存储以及IT基础设施的最初设计阶段就考虑它们的可恢复性。灾难恢复规划不再被认为是一种事后的想法，它必须成为系统开发过程中一个完整的部分。

当然，要进入这个角色，规划人员自身需要在技术方面更加敏锐。由行政秘书来进行规划的日子已经远去了。要与IT设计者这样的技术人员直接面对面交流，要求规划人员对前沿技术领域的概念和术语更加精通。现在的规划人员需要熟悉面向对象编程、中间件技术、可扩展标记语言、存储区域网络以及其他很多比较冷僻的信息技术。要以IT设计者的方式工作，规划人员必须首先学会以他们的方式交谈。

规划人员还需要更加具有商业头脑。虽然9.11的确增加了商业界对于灾难恢复需求的了解程度，但是历史告诉我们，商业界对于灾难恢复的兴趣有随着时间减弱的趋势。这是一个很自然的现象，就像当前的事件会成为历史书籍中的脚注一样。灾难事件过去的时间越长，业务经理们处理灾难恢复而进行准备的紧迫性就越低。事实表明，公司会更乐意投资于那些促进利润目标实现的项目。这样，具有商业头脑的规划人员会使用更加具有说服力的商业价值建议而不仅仅是“降低风险”来阐述他们工作的价值。引入灾难恢复解决方案的价值包括降低风险和保证每天正常的业务操作，这必将成为灾难恢复策略发展的终极目标。

最后，灾难恢复规划需要成为业务运作和IT决策过程的一个完整部分。开发新的业务过程，以及在技术基础设施中选择元素和组件来支撑这个业务过程，应该将可恢复性作为一个关键的衡量标准。

当以上这些都能够实现时，关于灾难恢复规划是否是一门独立学科的争论将会结束。灾难恢复规划不会是某个人或者某类相同的规划人员组织的任务，它是组织内部每个人的工作，从最高级的经理到最低级的雇员，从业务专业人士到IT专业人士。

当然，如果有这么一天的话，那么对本书新版本的需求也将慢慢减弱（我乐于看到这一结果）。

但是，在这一天来临之前，灾难恢复规划的新版本将会继续推出，以解决商业、技术以及我们所处的机构和文化背景的变化所提出的挑战。

第二版前言

本书被安排在西元的新千年前夜出版。其实，在过去的5年中，“2000年问题”（Y2K）在从商业界到政府的每一个层次中都成为主要的讨论议题，至少在世界上的发达国家中是这样的。到1999年底，这种渐强的趋势达到了顶点，各个主要出版社有关Y2K的书籍厚度累积超过了数万米，从而给这个本来很普通的日子蒙上了一层神秘色彩。

2000年1月1日被看做是人类历史上的分水岭。然而，它不仅仅标志着一个决定农业繁荣的季节轮回中冬季的结束，也不仅仅是一个从前天晚上庆祝活动的过度狂欢后开始休养生息的元旦日，也不仅仅是一个在院子里工作，或者在家看电视，或者参加宗教活动的星期六。

对很多人来说，这个日子有着重要的象征意义。2000年使得我们认真去总结过去的10个世纪，快速的技术革新永久地改变了我们的社会和文化。仅仅在过去的100年中，我们就见证了利用电子、原子、微波、光子来满足人类日常生活的需求。工业革命已经成熟，并且让位于目前以全球因特网、万维网、无所不在的Web浏览器为特征的计算机时代，将模拟现实转变为信息时代的数字现实。

毫无疑问，我们有理由选择一天做短暂停留，来反思过去，考虑现在，准备将来。心理学家认为，人类的精神需要书签、里程碑以及某些“终止的事件”，以保持自信和健康状态。有人认为2000年元旦这一天和其他日子一样，是个不错的选择。

然而，Y2K还具有第二重的象征意义，这层意义与20世纪80年代的心理学革命关系不大，那场革命带给我们梵蒂冈二世，无过错的离婚，以及很多自勉自助的书籍。对很多人来说，千年是一个神秘的事件，触动了根深蒂固的迷信层面，这种因素似乎从人类诞生开始一直到现在都存在于人类的精神世界中。出于很多原因，Y2K被看做是世界末日的预兆，是一些大灾难正在酝酿之中的信号。

好莱坞能够理解这种现象，并且在20世纪90年代即将结束的时候推出了一系列的灾难电影。这些最近非常风靡的电影，借助于灯光、魔术和其他的计算机图形效果技术，使得观众能够“体验”那些由于自然、人为甚至是宇宙中的灾难所造成的恐慌和毁灭。这些电影中的表演和情节并不能充分解释它们的成功，也许这样说对于Bruce Willis和其他演员有些不公。这些电影真正吸引人的地方看起来在于灾难本身：飓风袭击、火山爆发、地球与其他星球的碰撞、病毒肆虐、核子恐怖主义以及基于计算机入侵的基础设施的崩溃。它们满足了观众想要面对死亡的需要，哪怕只是一种间接的感觉。

一些电影植根于现实生活中的灾难事件，它们在一些人看来与世纪末的临近有潜在的连带关系。

- 世贸中心和俄克拉荷马城联邦大楼的爆炸案，为迄今为止一直没有接触过恐怖事件的北美民众们强调了恐怖主义的现实存在性。

- Saint Helens火山在沉睡了128年之后于1980年的喷发，以及加州的强烈地震，包括1989年10月Loma Prieta/旧金山的地震和1994年1月Northridge/San Fernando山谷的地震，刺激了人们对于地质灾害及其发生频率的关注。美国地质测量局的国家地震信息中心很快就指出“虽然看起来我们还会经历更多的地震，震级为7级或者超过7级的地震在本世纪一直持续发生，然而根据我们的记录，这些地震在最近几年中有减少的趋势。”
- 20世纪90年代还发生了北美历史上损失最惨重的飓风袭击。1969年的Camille飓风是当时最为猛烈的飓风，然而1992年的Andrew飓风造成了260亿美元的损失，这是当时有记录的自然灾害所造成的最高损失。当本书行将出版之际，专家们还在忙于统计1999年的Floyd飓风所造成的损失，这个数量可能刷新Andrew飓风所创造的记录。在这些毁灭性的风暴之间，还发生过很多相对弱一些然而也具有很强破坏性的龙卷风事件。
- 有些人可能会说，生活总是在模仿艺术。由于电影《龙卷风》的成功，俄克拉荷马的Bridge Creek在1999年5月真实地遭遇了5级龙卷风，这场风暴还被称做“上帝的手指”[1]。这场风暴以及其他很多严重风暴使得1999年成为1992年以来龙卷风活动最为频繁的一年。部分是由于电影的原因，这些风暴引起了媒体的全面关注，人们将过去10年中的龙卷风、飓风、洪水和冰雹归因于人类对自然和环境的破坏活动所遭到的报复。在一些报告中，龙卷风被错误地与厄尔尼诺/南方波动效应相联系[2]。根据官方龙卷风观测人士的观点，在世纪末的时候龙卷风的数量有所增加，但是没有任何有意义的统计手段能够说明，这种增加与厄尔尼诺/厄尔尼娜现象有关联。
- 自从20世纪50年代科幻小说这一流派进入黄金时代以来，近地轨道的天体和彗星与地球相撞的可能性就一直是科学幻想小说的一部分。当千年临近，对此类威胁的关注由于几次相关的事件而有所提高。一次是1994年Shoemaker-Levy 9号彗星与木星发生碰撞，美国宇航局的哈勃太空望远镜在强光下拍摄到这一场景，照片刊登在了世界范围内多家报纸和杂志上。另一次是关于1997年XF_{11}的说法，XF_{11}星体最早被认为将会与地球发生碰撞，然而后来被确认没有任何威胁，它将在2028年以一个安全的距离掠过地球。最初的错误估计使得很多观测者进入地下避难所，也使得美国宇航局要求天文界的权威来审查这些前提条件，直到它们能够被合理地证实。
- 当千年临近之际，一个快速增长的、潜在的人为灾难就是计算机病毒。它们通常冠以看似无害的名字，例如美丽莎、切尔诺贝利、ExplorZIP等。1999年病毒所造成的损失比以往任何一年中恶意代码所造成的损失更为严重。专家们预计这种趋势还将继续，有以下3点原因：首先，广泛地使用因特网用于电子邮件和文件的传输为病毒的扩散提供了一种有利的机制；其次，编程工具日益增加的功能正在使得新手也能创造出强有力的病毒程序；第三，通用桌面应用程序日益增长的复杂性，例如文档处理、电子表格、浏览器等，为黑客和其他恶意代码作者提供了一个“丰富的应用环境”[3]。
- 根据联邦调查局和计算机安全机构提供的数据，与病毒有关的破坏只是计算机和网络犯罪趋势的一部分。针对关键的基础设施系统，例如电力网络、电信、航空控制系统等，恶意的程序和计算机恐怖主义可能潜在地造成与核武器同等程度的破坏。

在很多人的意识中，认为当千年临近的时候，灾难将会大量发生，因此很容易理解Y2K是如何与世界末日如此紧密地联系在一起。然而，经过更加认真和细致的分析，没有什么证据能

够显示在1月的第一个星期六，人类的存在会遭遇灾难性的结束。这一天将会平静地到来，然后平静地过去，不会造成海水沸腾或其他噩梦中见到的场景。

我们展望2000年1月1日（以及接下来的几个月），所能看到的可能是一系列由信息系统和网络所支撑的服务发生令人气恼的，有时候又是非常危险的中断。这种中断与大自然的愤怒和审判日无关。它们只与简单的、基于软件的数据计算错误有关。

Y2K漏洞存在于很多旧的软件程序中。在编写这些软件的时候，没有考虑当日历从99变到00的时候，这些程序将如何进行处理。一些软件被编译在计算机系统上执行，另外还有一些软件被嵌入到微处理芯片中，这些芯片被安装在计算机和网络设备之中。

显然，政府和业界了解Y2K问题已经有一段时间了。关于Y2K代码的补救工作在20世纪90年代中期就在一些发达国家中开始了。然而在1998年，由第三方主持的对这些工作的检查和验证显示，在已经修改过的代码中依然存在大量的错误。这些持续存在的错误，是由于早期的Y2K代码补救工具的弱点和对修改过的代码进行充分测试工作的组织不当等原因造成的。很多公司付出了大量的努力，以3种方式来解决这一问题：

- 继续对存在的数据计算错误进行修补。
- 提高对意外事故和灾难恢复规划的关注，以减小未解决的错误所造成的影响。
- 当中断发生的时候，针对那些可能陆续发生的与Y2K有关的诉讼案件，寻求法律手段确定相关责任。

依据目前的实际情况，Gartner集团在给美国参议院的陈述中预言[4]，25%的Y2K代码问题会在2000年1月1日之前的数月中暴露出来，55%会在新千年的第一年中暴露，15%会在2001年暴露。在嵌入到芯片的软件中，未修改的错误很可能会在1999年12月31日晚上11:59日期转变的时候立刻暴露出来。

根据分析，在与Y2K漏洞有关的故障中，只有10%会在2000年的前2周中发生。在所有这些故障中，只有10%会造成超过3天的服务中断。每100 000个芯片中只有1个会因为Y2K漏洞发生故障。

Gartner集团的调查结果得到了其他业界分析家的拥护，也有一些批评认为该结果太过保守，以至于人们感觉良好。这些数字是否确切，这并不是我们所讨论的范围。分析家们都认同，无论对问题有多么深入的了解，很多公司在1998年之前并没有努力推动日期计算问题的解决，从那时开始它们已经落后了。因此，这种形势改变了灾难恢复规划原先所处的IT系统服务员这样一个不被重视的地位，并且在很多公司中将其提升到具有最高优先权，在管理上需要特别关注的程度。

在某种意义上，Y2K做到了其他通常意义的灾难恢复论点所做不到的事情。它明确了需要对业务过程依赖信息系统和网络的程度进行管理。而且，它还提高了管理层对那些不仅仅针对商业运作，而且针对公司利润的灾难威胁的感知能力。

政府立法以限定公司的责任，由Y2K中断造成的经济诉讼案件也肯定会发生，这些都经过了很多的激烈辩论。其中一个广为关注的问题是将“克尽职守”调整为企业责任的重要性。

“克尽职守”要求商业公司如果了解当前形势中存在的潜在危害，就必须采取行动以修正当前形势，缓和其可能造成的结果。对于其他潜在的灾难，例如洪水、火灾、飓风以及地震，由于潜在灾难转变为真实灾难相对来说概率较小，可以限定大多数公司在诉讼案件中需要承担

的责任。法律要求必需拥有的灾难恢复规划，以及对这些规划进行测试的案例（例如金融部门）则是个例外。实际上，如果由于飓风影响了业务运作，造成了正常操作发生一段时间的中断，公司的股东和客户通常都会对此表示出宽宏大量的态度。

在有关Y2K漏洞的案例中，很难获得来自股东和客户的谅解。美国的立法者决定了股东和客户更倾向于责备和起诉某些人。他们会质问，如果公司管理者了解灾难可能会发生，为什么不采取任何措施来避免灾难？如果Y2K漏洞不能及时地从代码中清除，为什么公司不制订意外事件计划，将无法避免的潜在灾难所造成的影响减至最小？这些问题都与公司是否克尽职守密切相关，也是政府关于Y2K责任限定的中心议题。

在本书出版后不久，Y2K（包括漏洞和日历的改变）都将成为历史。由于Y2K漏洞造成的中断将验证众多灾难恢复规划人员一直持有的看法：这只是又一种由于软件原因造成的业务过程的中断。

然而，对于一些灾难恢复规划人员来说，Y2K虽然具有危险，但也提供了一个机会。所有关于千年和Y2K漏洞的观点（无论是实际的还是带有迷信色彩的），都使得人们关注业务过程对信息系统的依赖程度，以及业务对于意外中断的脆弱程度。现在，灾难恢复协调员已经开始参与公司的管理工作。如果合理地加以利用，这种认知程度的提高可以培养成企业文化的一部分。

由于目前广受关注，灾难恢复规划人员能够有效完成他们的专业工作，并且使用所有的技能、知识和经验来协助高级经理处理Y2K的漏洞问题（以及他们所持有的任何其他有关千年的迷信观点）。一个完善的规划可以针对众多的灾难恢复场景提供保护，然而，通过强调Y2K问题作为规划的目标，灾难恢复规划人员可以向管理层表明，他们是用来支持商业目标可信赖的资源（包括智力方面和能力方面）。这一优势使得灾难恢复规划人员能够在保护更广泛的业务流程方面发挥更大的作用。

欢迎进入灾难恢复规划的世界。

尾注

[1] 按照龙卷风分类的Fujita等级标准，第5级或F5龙卷风有时称为“上帝的手指”，是极少见的。

[2] 尽管电影和大众传媒有将龙卷风和厄尔尼诺联系起来的趋势，但这种联系经不起推敲，见“The Relationship Between El Nino, La Nina, And United States Tornado Activity,” Joseph T. Schaefer, Storm Prediction Center, Norman, OK, and Frank B. Tatom, Engineering Analysis Inc., Huntsville, AL, Preprints, 19th Conf. Severe Local Storms, Minneapolis, MN, October 1999。

[3] Daniel Sforza, “New Terror Lurks in Computer Mailboxes”, *The Record*, June 12, 1999 and Robert Gebeloff, “On-Line Perils, Pitfalls Growing for the Unwary,” *The Record*, June 12, 1999。

[4] Lou Marcoccio, “Year 2000 International State of Readiness: Expert Testimony of Lou Marcoccio, March 5, 1999 to the U.S. Senate Special Committee on the Year *2000* Technology Problem, Washington, D.C.,” GartnerGroup, 1999。