抵御灾难的 90 天计划

企业的运作总是充满风险和不确定性。尽管基础设施陈旧不堪，经济形势极不稳定，政府管制严格，客户的信心也在丧失，但多数 CXO 仍满怀信心地（也许是没有理由地）表示，他们的数据中心、呼叫中心或网络中心在遭遇意外中断后能够恢复运作，但事实表明，这些公司中的五分之三并没有制定完善的业务连续性计划。

尽管客户希望他们在提交在线订单、进行转帐业务乃至社交活动时能够得到立即响应，但 Forrester Research 最近通过调查发现，去年只有十分之六的公司计划购买业务连续性服务或设备。因此，公司的高层管理人员对于公司能否经受全球、企业内部和财务危机的认识与现实差距很大。

以上发现有多重含义。随着 IT 管理人员角色的转换，即从传统的 IT 管理人员变为高级业务主管，他们必须了解企业面临的风险，并与业务部门一道对业务中断的影响进行量化分析。CIO 的职责包括考察投资于业务连续性规划的必要性、积极主动地开发适用的架构，并帮助实施销售计划。如果不能做到以上几点，可能无法使股东和董事会满意。

业务连续性规划不仅仅涉及如何在发生自然灾难时恢复业务运作，还涉及一些可能在多个地点突然间同时爆发的意外事件。该计划不是一种保险，而是用于实现收入、利润及成本目标的业务模式的有机组成部分。对于客户来说，高可用性是必须的，而不是可有可无的，他们对于故障越来越难以容忍。在发生中断时，他们会去寻找那些能够及时、稳定地满足其需求的供应商。

了解业务连续性参数

虽然为所有的应用和数据提供最强大的保护，令其免于中断或丢失是最理想的，但通常这样做的成本很高，或者很难做到。许多应用在短时间内停运不会产生很大的影响，只有一些特殊的关键任务应用可能需要保持 100％的可用性。为了系统全面地考察业务连续性计划，应该考虑 3 个业务连续性参数：

- **恢复点目标**（RPO）－确定企业能够承受的数据丢失数量，从零到几分钟或几小时
- **恢复时间目标**（RTO）－量化允许一个应用不可用的最高时间限制
- **恢复访问目标**（RAO）－确定将用户连接到被恢复的应用所需的时间

以上的三个参数为考察业务连续性计划提供了可衡量的标准，以及选择特定解决方案的系统化依据。结合 RPO、RTO 和 RAO 值以及距离要求，业务连续性管理人员能够将每一种应用与某种支持其业务职能的技术解决方案匹配起来。这些可能包括以下选项：

高可用性 SAN－SAN 解决方案能够在发生本机服务器故障时提供对备份或集群服务器系统的访问，从而确保业务的连续运作。一个共享的存储环境能够证明先进的存储系统在保证磁盘故障不影响应用运行方面的有效性。SAN 的优势在“SAN 的兴起”一文中有详细的阐述。

整合式备份 －定期备份是多数业务应用的标准操作规程的一部分。作为成本最低的解决方案，整合式磁带备份的恢复速度最慢，但它对于处理数据崩溃等故障是非常有效的。

远程异步复制 – 也就是将数据更改复制到另外一个地点的远程系统。根据数据的重要程度，可以选择在一天中的某个时刻对更改进行定点复制，或在出现更改时随时异步复制，复制时使用存储系统中先进的软件。数据复制可实现比磁带备份更快的恢复；但是，异步复制不能保证所有的数据均能被恢复。

抵御灾难的 90 天计划

同步磁盘复制与镜像 –对于需要以最快的速度恢复，同时又不能丢失数据的应用，同步磁盘复制与镜像是一种理想的解决方案，其中采用存储系统、主机上或集中在存储网络中的先进软件。所有磁盘写操作均在交易被确认之前通过一个高性能网络复制到一个远程地点，从而避免了任何交易的丢失。这种解决方案的局限性是延迟，这种缺陷限制了站点之间的实际距离。对于写操作密集应用和在线交易处理应用来说这种局限性尤其明显，例如企业资源规划和客户关系管理。

数据中心镜像 – 为了实现最高的业务连续性，企业越来越倾向于运行双重的主用数据中心，在这两个站点间运行庞大的服务器集群。虽然有些企业只让一个数据中心处于运行状态，另外一个只在发生中断时启用，但更常见的是同时将两个数据中心作为“热”或主用数据中心运行，其中一个数据中心的所有交易均同步镜像到另外一个。这种解决方案有两种运行模式。第一种模式是，两个数据中心共担相同应用的流量负载，并且完全同步化，同时利用全局负载均衡机制在站点间分布用户流量。镜像的主用数据中心可确保任何一个数据中心的中断恢复流程对用户都是透明的。这种模式还能更好地利用昂贵的资源，提高投资回报。在第二种模式中，每个数据中心用作不同的应用群的主用主机，同时镜像另外一个数据中心的交易。如果一个数据中心出现故障，另外一个将代替其支持站点上所有的应用。在这两种模式中，数据中心镜像实现了最高水平的业务连续性。

连续的用户访问与连接 – 业务连续性计划中必须包括的一个 RAO 战略是使用户能够在环境条件不断变化的情况下始终保持与应用的连接。接入方法可能对用户透明，也可能需要手动重新配置，这取决于灾难的严重程度。对用户透明的技术包括镜像数据中心之间的全局负载均衡、针对故障链路的自动重路由以及发生故障时向备用组件或设备的自动切换。

简单的 90 天灾难抵御计划

第一个月：获得高层管理人员的支持

- 利用风险管理模型和技巧初步表达你的观点和立场
- 与风险管理方面的主管人员合作，开始解决差距问题
- 将 IT 目标与企业及其业务部门的目标统一起来。为业务连续性计划铺垫一种政治氛围。
- 确定努力的方向和可衡量的目标，以确保成功。
- 制定一个包括抵御战略的风险计划，但应准备随时予以更新。

第二个月：基本工作

- 建立一个跨部门团队，其中业务部门的人员占多数，而不是 IT 部门。
- 收集并查看以前类似项目的资料、部门要求以及相关规定。
- 设立目标和“当前”模型。
- 对“当前”模型进行差距/重叠分析。
- 对数据源、使用情况、要求和监管人员进行初步核查。

第三个月：制定行动计划

- 利用差距和重叠分析与管理委员会确定下一步的优先任务。
- 制定一个跨机构计划，以确保成功执行。
- 将计划分成易于管理的多个分计划，每个分计划包含一系列独立的项目
- 将这些分计划提交给项目管理办公室，以便于跟踪和管理。
- 从大处着眼，小处着手。要把每一步细节的工作踏踏实实做好。

抵御灾难的 90 天计划

总体说来，企业的业务连续性解决方案应该包括 7 个关键的要素：

- 确保系统中没有单故障点；
- 可在 10 公里的范围内对重要数据进行远程存储/镜像；
- 规划实施高可用性；将对性能的影响降到最低；
- 在发生中断时，确保系统能够自动进行路径选择/故障切换；
- 改进负载均衡功能，确保即使网络的某些部分停运，数据流量仍正常传输；
- 保护您的高优先级业务应用和目标。
- 最后，最重要的是，您的所有工作的核心应该是将收入、客户、竞争地位方面的损失降到最低。

最根本的是，CIO 必须能够回答一个可能涉及几十亿美元的恢复问题：如果企业没能满足客户、董事会以及法规部门对业务连续运作的要求，那么这是因为发生了不可控制的事件还是因为缺乏对企业生存能力的关注？CIO 如果不能给出一个令公司的利益相关者满意的回答，那么他们将自己承担后果：责任追究。

请点击以下链接，了解思科怎样帮助您部署 业务连续性和存储联网解决方案。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街 1 号东方广场东方经贸城东一办公楼 19-21 层
邮政编码：100738
电话：(8610) 85155000
传真：(8610) 85181881

上海
上海市淮海中路 222 号力宝广场 32-33 层
邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

广州
广州市天河北路 233 号中信广场 43 楼
邮政编码：510620
电话：(8620) 85193000
传真：(8620) 38770077

成都
成都市顺城大街 308 号冠城广场 23 层
邮政编码：610017
电话：(8628) 86961000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn

2005 年 4 月翻译