如何将移动设备纳入灾难恢复计划 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022__E5_A6_82_E4_BD_95_E5_B0_86_E7_c100_259054.htm 将移动设备纳入灾难恢复计划中，这是被很多IT管理员们忽略的地方，然而，这已经成为了灾难恢复中重要的一部份。 在过去的几年里，移动设备被认为是一项“ 令人叹息 ”的技术，因为它并不非常适合充当公司必需品，因而无法成为商业关键设备。所谓的商业关键设备指的是一种上至行政官员，下至底层库房人员都不可或缺的设备。问题是，要整合这些随处可见的移动设备，需要对灾难恢复计划做一些什么?当然，每个组织针对问题的答案都会不同，以下的步骤将指导你制定符合你公司需求的完美的灾难恢复计划。 1. 确定移动设备的位置。 2. 决定移动设备数据和应用程序的重要性。 3. 了解你能以多快的速度从一个灾难中恢复。 知道去哪里寻找你的移动设备 暂时抛开安全问题不谈，在公司内部确定移动设备的安放位置是极其困难的一件事。开始时，最好根据业务进程流来决定具体的位置。这些用户级别的进程流通常会提示你用户与公司系统是如何相互作用的。如进程流可能会提示如下信息：“ 循环计数之后，用户输入需要传输到ERP上的数据。 ”类似于这样的提示信息能帮助你启动确认进程。除了定义业务进程之外，对于那些在很大程度上依赖移动设备的销售人员、管理者和实际操作的用户来说，这也是相当重要的。除了那些手动操作之外，通常，还会有一系列的第三方产品，用来跟踪用户身份模块，即SIM卡。它能帮助控制移动设备的库存和位置。 数据?应用程序?或者是两者兼有? 确定移动设备的

位置之后，你就可以开始将它们整合到你的灾难恢复计划中。为了达到合理的整合效果，你必须确定这些设备上最有价值的是什么，是其所承载的数据?还是其上运行的应用程序?移动设备最大的价值在于，无论在什么地方都能够对重要的数据进行快速的访问。然而，这也成为了组织最大的危机，所以应该被列入灾难恢复计划中。另外，你还不得不考虑移动设备的意外损害和被盗，以及雇员辞职对其所造成的影响。 在整个移动设备的发展过程当中，掌握数据情况一直都是相当困难的。幸运的是，你能够使用Windows Mobile 5.0，结合Exchange Server 2007来保护你的组织远离各种大大小小的灾难，如手持移动设备丢失或被盗，或者手持设备需要那些由于错误操作导致被删除的敏感数据。 除了标准的功能之外，如设备锁和增强型密码，Windows Mobile中提供的device wipe应该算的上是灾难恢复计划中的关键一项。device wipe使组织具备远程删除所有数据的能力，包括设备上的数据和任何可移动存储卡上的数据。 由于移动设备数据存储天生存在的不可避免的问题，它们通常仅用来运行应用程序，以便收集数据并将数据传回中央服务器。在这种情况下，你的灾难恢复计划应该更集中于设备供应或者是在某种级别上重新部署硬件和软件的能力。 尽管你可以计划准备每月都重新部署设备，但是，你还必须考虑在过度的压力下将设备重新部署成为一个完整站点的能力。在这些情况下，可移动存储上的无线通讯按钮或填充装置是最通用的备用方案。你也可以使用活动目录(AD)来促进和维护内部的安全。 决定灾难恢复速度 一旦你对移动设备的位置以及公司如何使用这些设备的情况有了一个清晰的认识和了解之后，接下来，决定这些设备在整

个“ 食物链 ”中的位置。不管这些设备位于哪个位置，你都需要考虑灾难恢复速度。因此，可以从以下几方面考虑：● 标准的设备：对于哪些移动设备允许访问数据，哪些允许运行应用程序的标准把握得越清晰，灾难恢复过程就会越简单。标准化设备还要考虑到图像包以及将设备从一个位置重新部署到另一个位置的能力。● 标准的方法：要求用户对邮件、数据和应用程序的活动目录进行认证。这确保类似微软的device wipe这样的选项能用来保护你的组织。● 失策的地方：你是否已经计划好如何接替300甚至3000台手持设备?掌握硬件部署如同配置软件一样难。事先了解配置和重新分配策略使你能够冷静地面对大规模的设备替换。 帮助高层管理者理解如何将移动设备整合到灾难恢复计划中，这将为你制定设备标准提供坚强的后盾。记住，只求速度不求质量只会使情况更糟糕。测试你的部署策略是不可忽视的。 随着移动设备在各行各业的广泛应用，从医疗到制造业，IT管理员们需要意识到它们确实支撑着这些行业。如果在你的灾难恢复计划中忽视它们，很有可能就是你还没有完全理解这些设备对业务的重要性。不管情况是否如此，移动设备已不再只是单纯的玩具，它们需要得到同样的尊重和注意，就像你对待膝上型电脑一样。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com