

赛门铁克 2010 灾难恢复研究报告

全球调查结果

2010 年 11 月

目录

摘要 3

研究方法.....4

调查结果 1：虚拟化和云使灾难恢复趋于复杂 5

调查结果 2：停机恢复时间差距 6

调查结果 3：灾难恢复测试的影响 7

建议 8

附录9

摘要

第六期赛门铁克年度灾难恢复调查研究报告显示了数据中心管理人员在管理单独的虚拟、物理和云资源时所面临的挑战。这些日益变化的资源加剧了企业保护和恢复关键任务应用程序和数据的复杂性。事实上，数据显示，由于资源和其他存储限制影响了备份，因此虚拟机未得到妥善的保护。

该研究报告还显示，企业认为能达到的恢复速度和实际的恢复速度之间存在着巨大的差距。此外，除了因系统升级、断电以及网络攻击等基本原因造成的停机事件外，企业还遭遇着其它情况造成的停机。

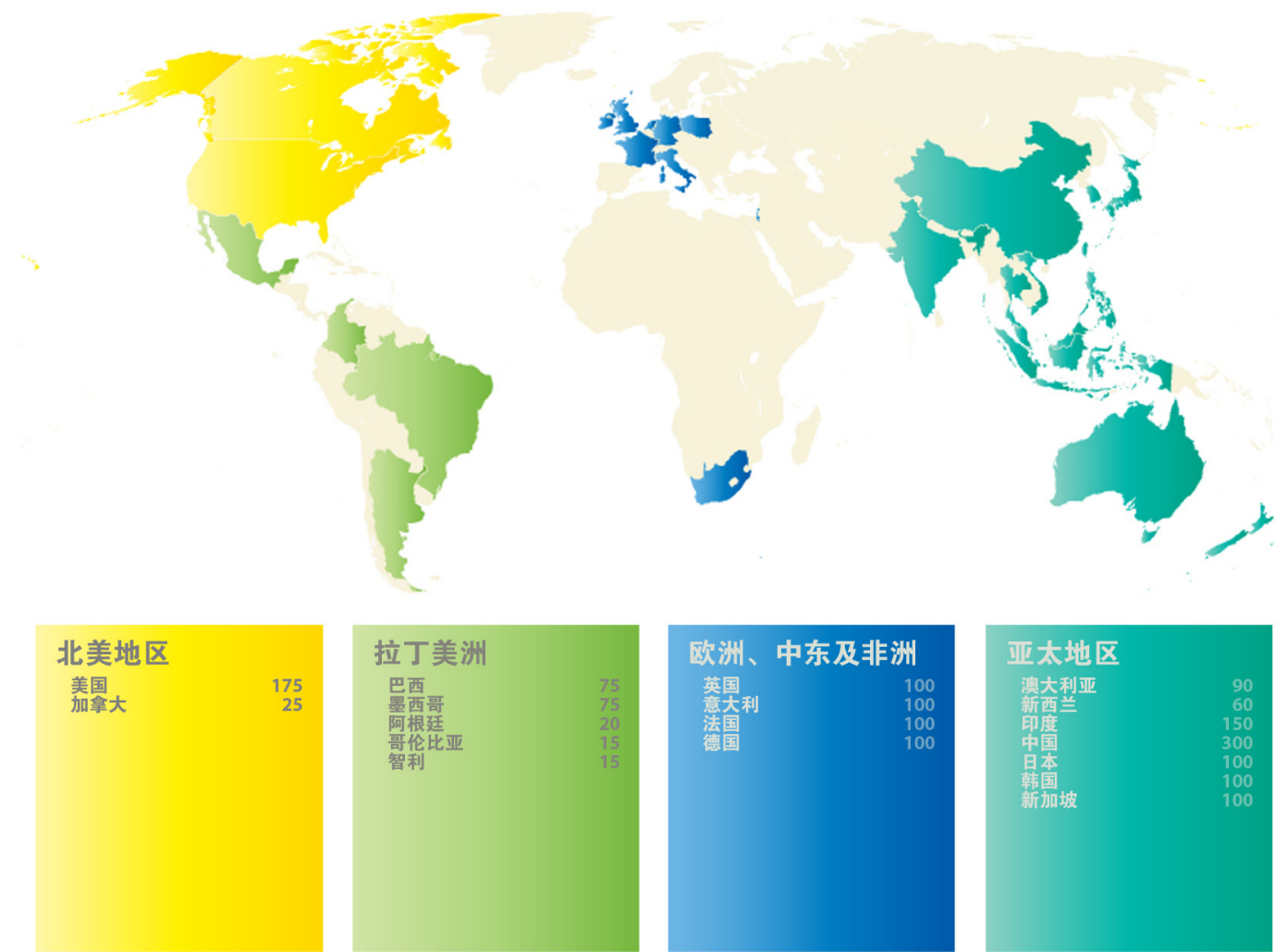
最后，该研究报告表明，灾难恢复测试频率大幅提升；但对员工、销售以及收入的影响仍居高不下。

研究方法

Applied Research 于 2010 年 10 月对来自 18 个国家或地区 1,700 家企业的 5,000 多名员工进行了电话调查。本次调查涉及各行各业。

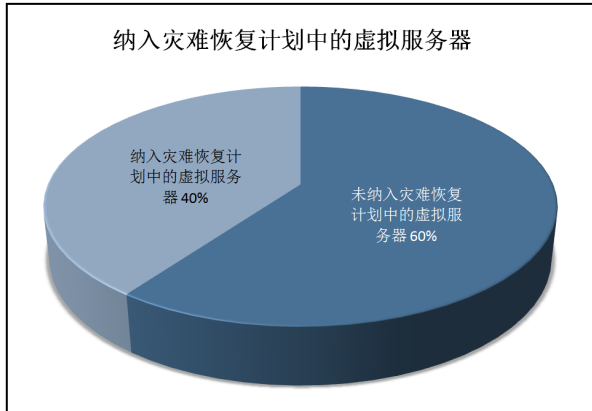
本调查报告的确凿度达到 95% +/- 2.4%。

此外，赛门铁克与很多 IT 专家组成了电话讨论焦点小组，以便更深入地了解他们的反馈和经历。



调查结果 1:

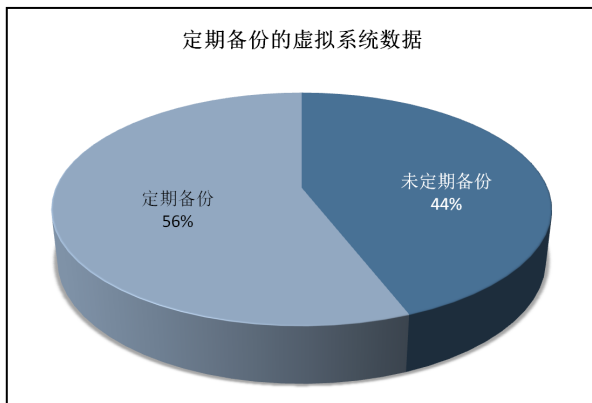
虚拟化和云使灾难恢复趋于复杂



虚拟和云环境中的应用程序和数据量与日俱增，这使得数据中心管理人员难以开展保护、控制和管理的工作。资料显示，这些环境的复杂性增加会导致其得不到应有的保护。

调查对象称，四分之一到三分之一的应用程序都位于虚拟环境中。84% 的调查对象表示，虚拟化使他们对灾难恢复计划进行了重新评估。

尽管越来越多的应用程序和数据都位于虚拟环境中，但是，60% 的虚拟服务器并未纳入现行的灾难恢复计划中。赛门铁克还发现，虚拟系统上略过一半 (56%) 的数据进行了定期备份。82% 的备份只是每周进行一次或频率更少，而不是每天都进行。



赛门铁克认为，虚拟服务器不断增加、服务器杂乱无章以及缺乏工具可能是引起这些变化的原因。

此外，调查对象表示，他们企业虚拟环境中 20% 的数据和关键任务应用程序都是以复制的方式进行保护的。调查对象还表示，同样有 20% 的数据是以高可用性故障转移和全球/广域故障转移的方式进行保护的。

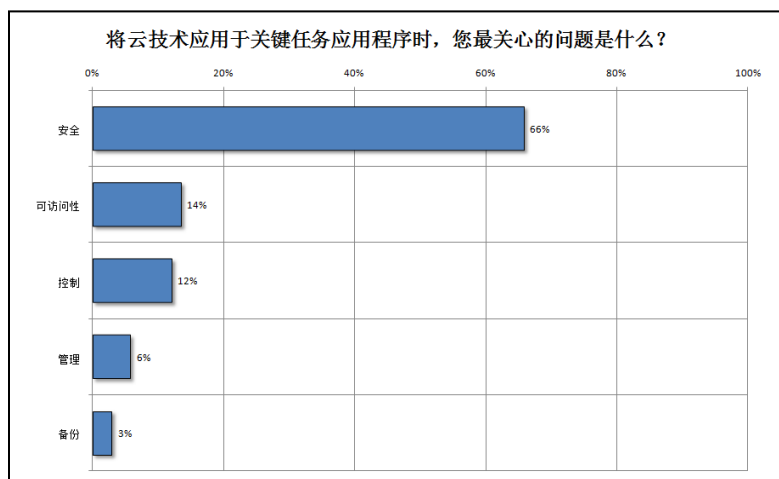
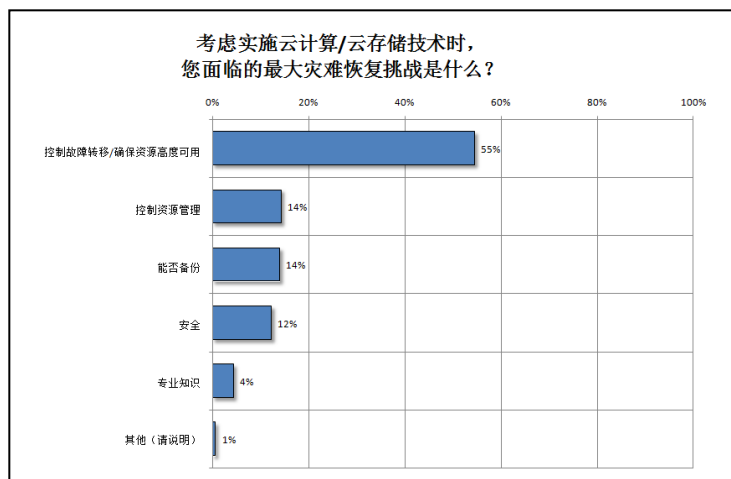
在主要调查对象小组中，调查对象说，企业经常为图省事而没有实施复制技术。一位数据经理说道，“现在，我们缺乏复制计划。这是我们当时要实施的计划。但由于公司发生变故，复制计划就半途而废了。因此，谈到灾难恢复时，正是我们会下定决心实施的计划。我们住在加利福尼亚州，将经历一场地震，我们已经将磁带存放到另一栋大楼里，但是，我们确实希望把磁带存放在另一座城市。在这种情况下，我们缺少的正是这一计划”。

企业还将云技术应用到大约半数的关键任务应用程序和非关键任务应用程序中，但问题在于无法对云环境进行控制。企业需要更有效的工具来管理虚拟和云环境。

虽然三分之二 (66%) 的调查对象称,将云技术应用于应用程序,安全问题是主要的顾虑,但他们认为,考虑实施云计算/云存储技术时面临的最严峻的灾难恢复挑战,是能否控制故障转移以及能否使资源可用 (55%)。

及时了解管理和保护这些应用程序的各种工具,是企业面临的一项挑战,这在虚拟和云环境中的应用程序和数据不断增加的情况下显得尤为突出。

加利福尼亚一家汽车业制造商的数据中心管理人员说,“如果我知道有一种工具可以为我们代劳一切,我是很乐意了解一下的”。



调查结果 2:

停机恢复时间差距

有句老话说，任何 IT 项目所花的时间至少比想象中多 1 倍。在调查企业需要多长时间从停机中恢复时，本研究报告发现这是正确的。

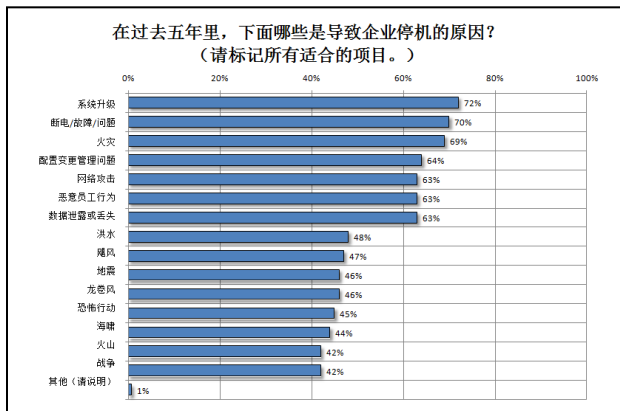
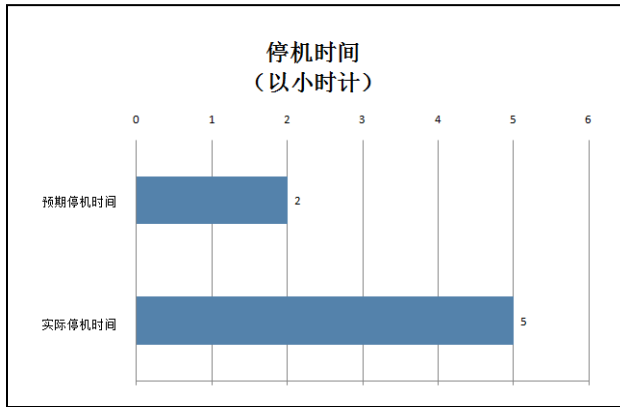
从中断中恢复所需的实际时间与企业想象的时间存在着很大的差距。当被问及需要多久才能从毁掉主要数据中心的严重灾难中恢复时，调查对象表示，只需两个多小时即可恢复正常运行。但是，调查对象表示，在过去的 12 个月中，每起事件的平均停机时间是 5 小时。

造成该差距的部分原因可能是中断期间出现了情况不明的需求。一位数据中心管理人员说，“我认为，很多公司在灾难来袭时会不知所措。他们的首要任务是满足紧急服务的要求 - 消防局、医院以及所有这样的服务。因此，虽然我不知道我们中会有多少家企业面临这样的情况，但是我认为，它对我们的影响是相当大的。”

在过去五年里，系统升级 (72%) 是导致企业停机的最主要原因。企业还因系统升级平均历经 50.9 小时的停机时间，因而无论是从停机小时数还是事件数来衡量，系统升级都是造成停机的最主要原因之一。

提及单向系统升级对灾难恢复测试的影响，一位数据中心管理人员说，“未来三个月内，我们安排了数次升级，在这三个月期间的一些时候，甚至是升级完毕后，我保证不了系统始终就像今天一样运行良好，因为很多事情始终是变化的”。

停电和断电 (70%) 是导致停机的第二大原因。考虑到将停电和断电视为一项主要停机原因的企业数量，难怪仅有 26% 的企业执行了停电和断电影响评估。

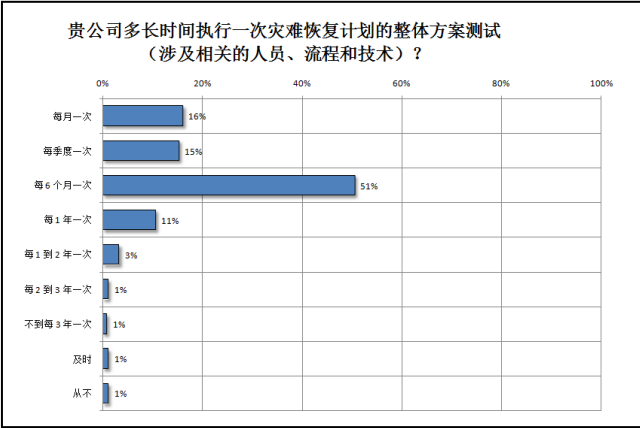


调查结果 3:
灾难恢复测试的影响

该研究报告还表明，灾难恢复测试频率大幅提升；但对员工、销售以及收入的影响仍居高不下。

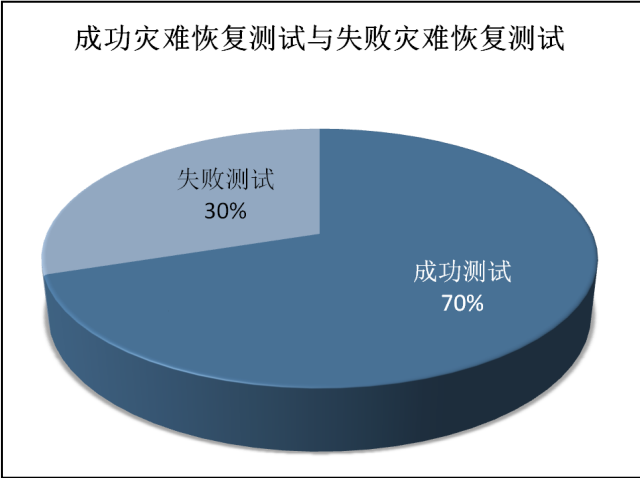
据调查对象报告，超过四分之一 (26%) 的年度 IT 总预算都安排给了与灾难恢复相关的计划，因此将被视为业务开展基本基础架构的一部分。从预算方面来讲，在过去 12 个月里，企业在灾难恢复测试方面的平均支出是 606,948 美元。

加利福尼亚一家汽车业制造商的数据中心管理人员说，“灾难恢复支出是保持业务应急运行所必需的。它就是开展业务的一种成本”。赛门铁克观察到，提高灾难恢复计划测试频率的企业有所增多。大约 82% 的企业每年至少对其灾难恢复计划测试一次。这与去年 66% 的调查结果相比，有了大幅提升。



40% 的灾难恢复测试未能在 RTO 和 RPO 内恢复关键数据和应用程序。在这些失败的灾难恢复测试中，企业主要将其归因于灾难恢复站点的 IT 基础架构不够完善。

对于企业为何不测试更多内容，最频繁提及的原因包括：资源，预算方面 (60%)；对员工的影响 (59%)；对客户/销售和收入流的影响 (24%)；以及资源，人员时间方面 (26%)。



赛门铁克的建议

- **所有环境同等对待：**在灾难恢复评估和计划方面，确保采用相同的方式对所有环境（虚拟、云、物理）中的关键任务数据和应用程序进行处理
- **使用集成工具集：**由于减少了管理物理、虚拟和云环境所使用的工具量，因此可以帮助企业节省时间，降低培训成本，更好地自动执行流程
- **简化数据保护流程：**采用影响小的备份方法和去重技术，确保备份并高效异地复制虚拟环境中的关键任务数据
- **通过计划和自动执行最大限度缩短停机时间：**对自动执行流程的计划活动和工具划分优先级，这样可最大限度缩短系统升级期间的停机时间
- **尽早发现问题：**实施检测问题、减少停机时间以及加快恢复速度的解决方案，以便与预期更相符
- **勿走捷径：**企业应实施中断时提供保护的基本技术和流程，而不应走捷径，以防出现灾难性后果。