灾备大师

具备高度灾备能力的企业如何脱颖而出

IBM Center for Applied Insights
ibm.com/ibmcai | ibmcai.com

云、移动、社交及物联网等技术正在重塑业务模式，促进我们不断提高生产力、灵活性、连通性及响应性。但是，随着我们越来越严重地依赖 24/7 全天候可用的基础架构，致使我们在灾难来袭时面临更大风险。

为何有些企业能够更好地掌控灾备、从而满足当今“业务永续”的期望？
因为他们制订了利用先进技术与健壮性测试的一体化战略。

在当今的企业 IT 环境中，每一个组成单元均已提高了连通性、均需确保全天候可用性、并且都是由数据驱动的。您的员工、客户及合作伙伴都希望他们所需的信息、产品和服务“永续”—随时随地以他们希望的方式提供。

为满足这些需求，系统的集成性、分散性及相互依赖性不断增强—从而带来大量的潜在安全漏洞。如果将更多的关键系统链接在一起来满足更高期望，将会加剧灾备和安全保护的复杂性。只要这条链子中有一条链路断裂或遭遇攻击，影响将波及整个企业。

通过对 310 名业务连续性 (BC) 与灾备 (DR) 专业人员展开调查，我们发现近 60% 的企业会在服务中断时执行灾备计划。约 40% 的企业仅在最近两年被迫开展过这项工作，但这种做法不仅没有帮助他们缩短恢复时间，而且宕机的业务影响还在不断加剧，不禁令企业倍感压力。[1]

业务中断时有发生。提前预测问题至关重要。但是，即便运行着最完善的预防性措施，您仍然需要制定基于实战的灾备计划。

问题是：从容驾驭灾备比任何事情都更加具有挑战性。

近 40% 的企业仅在最近两年因服务中断而被迫开展过灾备工作。

SOCIAL SIGNALS

在为期 6 个月的调查期间，我们发现关于灾备与业务连续性的社交媒体讨论超过 9.9万 次。[2]

关于本次调查

为洞悉当今最有效的业务灾备战略，IBM 应用洞察中心对美国和加拿大的 310 名灾备与业务连续性专业人员开展了调查。受访者主要由高级 BCDR 主管组成，其中超过 60% 是 IT 总监或首席信息官 (CIO)。受访者来自 19 个行业中各种规模的企业 — 有些企业不到100 名员工，有些则超过 1 万名。

关于 IBM 应用洞察中心

ibm.com/ibmcai | ibmcai.com

IBM 应用洞察中心洞悉全新思维、工作和领导方式。中心旨在通过实证调查给领导者提供实用指南与案例，从而推动他们实施变革。

业务连续性团队面临棘手问题

现在，灾备与业务连续性专家所工作的业务环境比以往任何时候都更加苛刻和复杂。约 55% 的受访者指出，他们所面临的首要挑战是如何将越来越多的关键业务系统整合到灾备计划中。例如，已有越来越的企业开始考虑将移动应用作为关键工具使用。这意味着这些应用需要与后勤、呼叫中心或电子邮件工作负载等更加传统的关键系统一样得到相同级别的保护。

关键应用和工作负载数量的增长推动 IT 集成水平不断提高，导致灾备团队必须管理的潜在故障点越来越多。而企业与供应商和业务伙伴之间连接点数量的增加只会令问题变得更加复杂。

近半数的灾备主管指出，手段越来越高明、范围越来越广的数据泄露与网络犯罪是公司业务连续性团队所面临的另一个严峻挑战。显然，许多企业已因此遇挫，近半数的业务连续性主管承认他们并未准备好应对网络攻击造成的服务中断。

但也有一些企业脱颖而出，展示出卓越的灾备能力。他们是如何做到的？

灾备任重道远

业务连续性专家需克服各种艰难险阻才能满足“业务永续”的期望。

*恢复时间目标(RTO)和恢复点目标(RPO)

精英们脱颖而出

尽管面临严峻挑战，仍有一些具备高度灾备能力的企业凭借包含一体化计划与健壮性测试的灾备策略脱颖而出。不足 1/3 的 BCDR 专业人员有幸跻身精英行列，成为灾备“大师”(Master)。相比之下，约 44% 的 BCDR 专业人员属于“专家”(Specialist)，剩下的 26% 只能算“谋士”(Tactician)。

大师采取全企业灾备策略，测试活动更加频繁和严格。

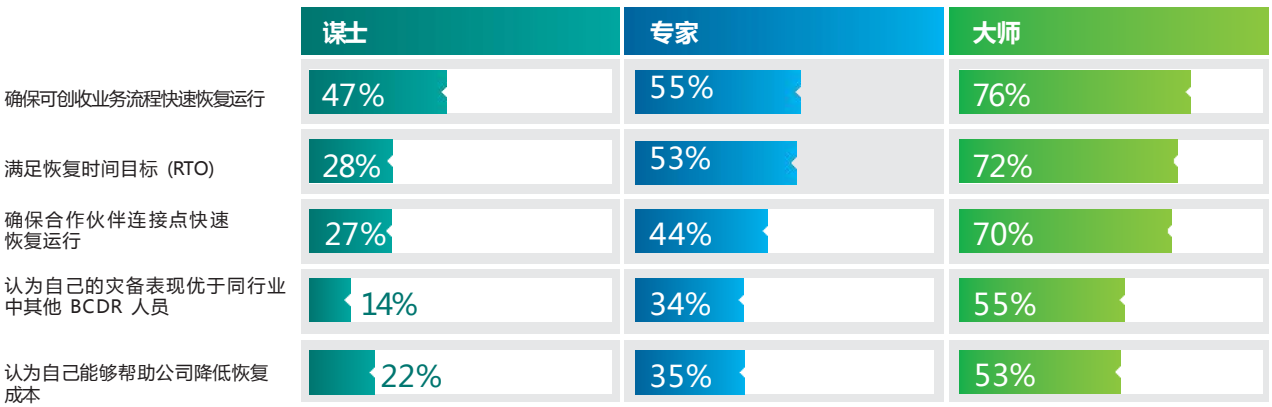
专家已经开始着手改进测试和安全保护机制，但距离全面的一体化方法还有相当一段距离。

谋士仍停留在独立系统测试阶段且频率较低，仍将灾备作为 IT 问题进行处理。

调查结果几乎毫无疑问地证明“大师”比其他同行表现更为卓越。他们的各项主要灾备指标表现均占据显著优势。例如，在确保可创收业务流程快速恢复运行方面，“大师”比“谋士”快 1.5 倍—在业务中断时，这是维护客户关系的关键。

此外，“大师”在满足恢复时间目标及控制恢复成本方面的成功率约是其他同行的 2.5倍，这些成就均可证明灾备团队能给公司取得成功贡献巨大力量。

总体而言，“大师”的灾备能力是同行业中“谋士”的 4 倍。



谁在灾备能力提升竞赛上独占鳌头？

面对迎头而至的挑战，一些具备高度灾备能力的企业凭借一体化 BCDR 计划与频繁开展健壮性测试活动脱颖而出。

抵达业务连续性的巅峰

“大师”预测并规划灾备活动。他们会在 IT 与业务部门之前建立合作文化，他们在制订灾备计划时会考虑到新技术、业务优先级和风险等诸多因素。

“大师”开展测试与评估活动，通过反复实践与改进来加快响应速度并扩展业务连续性计划的覆盖范围。

“大师”还能加快响应与恢复速度。他们能够巧妙地利用适当的技术来确保关键业务流程的快速备份和运行。

Textron 将灾备提升到新高度 [3]

作为生产 Bell Helicopter 及 Cessna 等著名产品的多种经营公司，Textron 知道必须倾尽全力确保业务连续性。

某些企业的灾备方法并未总是将关键基础架构和安全服务包含在内，或者在决定首先恢复哪些资产时并未全面考虑到此类资产与业务的关联性。而 Textron 则采用了更加全面的灾备规划方法。首先，他们针对关键资产以及此类资产与业务之间千丝万缕的关系制定路线图。 Textron CIO Diane Schwarz 表示：“以前，我们主要是考察‘哪些应用对于保持业务运行是不可或缺的？’。我们会评估 ERP、生产和库存系统，但不会去考虑支持业务运行所需的更加广泛的系统。企业还应考虑网络中的关键资产，而不仅仅是从财务的角度去关注重要资产。”

Textron 还发现，基于业务需求的变化灵活调整灾备策略非常重要。为此，公司需要值得信赖的技术合作伙伴来帮助他们在云、共享平台与混合解决方案之间灵活切换。

实践出真知。公司每年都会对其恢复计划开展三次测试。通过对全企业灾备计划开展频繁测试，公司经常能够从容应对日常工作中遇到的形形色色的小问题。

Textron 认为刻板的人事架构并不可取。Schwarz表示：“人才储备是经常被忽略的重要问题。我们不仅需要高度灾备能力的战术架构，而且还需要构建高度灾备能力的工作团队。”

Textron 的测试人员包括业务部门员工、应用支持部门员工、基础架构支持部门员工、项目经理、重要用户、以及来自服务供应商的支持团队。

像大师一样扩大灾备范围

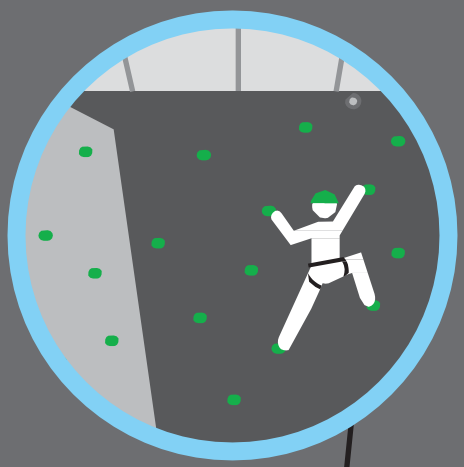
大师在灾备的四个主要领域均领先于其他同行。

从战略的角度规划灾备活动

集成安全机制

利用新技术

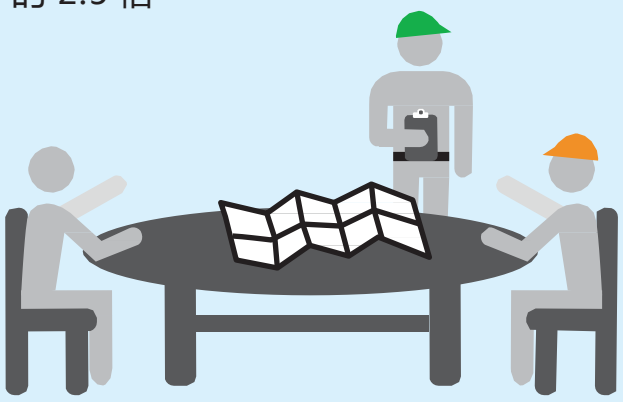
开展严格测试



大师会从战略的角度规划灾备活动

2.5 倍

采用一体化灾备计划的“大师”比例是其他同行的 2.5 倍



采用一体化灾备计划的“大师”比例是“谋士”的两倍多。参与制订灾备方案的这些大师中不乏企业高管。面对如此高风险的活动，董事会岂能允许出现半点纰漏。“大师”对此心知肚明，因此会积极邀请董事会参与投资规划活动，给最关键的业务需求优先安排投资。

高管的介入给灾备计划下达了明确命令。高达 71% 的受访者指出，业务主管希望在制定灾备计划时能将信息安全风险考虑在内。约半数的受访者指出，公司要求灾备投资必须生成丰厚的 ROI。此外，大师中还包括频繁参与公司灾备评估活动的值得信赖的外部合作伙伴—生态系统合作伙伴及灾备规划专家。

SOCIALSIGNALS

在为期 6 个月的调查期间，我们发现关于灾备策略与端到端规划的社交媒体讨论高达 **9,000** 次。

	谋士	专家	大师	*大师 vs. 谋士*
邀请董事会参与灾备规划	34%	47%	73%	20 倍
制订一体化的、全面的灾备计划	19%	26%	46%	2.5 倍
邀请外部专家参与灾备规划、执行与评估活动	21%	34%	44%	20 倍
邀请供应商参与总体测试活动	9%	12%	39%	4.5 倍

大师会与风险和安全专家进行合作

针对潜在安全漏洞构建全企业视图能够提高灾备计划的针对性和有效性。“大师”会将企业安全和风险管理机制作为关键部分写入灾备与业务连续性计划中。在邀请公司的 CISO 及 CRO 参与灾备规划方面，“大师”的比例分别是“谋士”的 3.5 倍和 5 倍。此外，“大师”在开展灾备测试、执行灾备计划以及运行安全保护机制时都会应用安全策略。

SOCIAL SIGNALS

与安全相关的灾备话题在社交媒体上被讨论多达 8,000 次。

	谋士	专家	大师	*大师 vs. 谋士*
邀请 CISO 参与灾备规划	16%	36%	57%	3.5 倍
将企业安全和风险管理融入到灾备计划中	21%	32%	52%	2.5 倍
制订安全策略并在灾备测试期间执行安全策略	4%	16%	47%	12.0 倍
邀请 CRO 参与灾备规划	6%	19%	30%	5.0 倍

大师擅长利用新技术

这些领跑者经常喜欢利用云、分析和移动等创新技术来快速恢复关键业务流程。他们在中断期间更有可能提供实时移动更新并使用云技术开展恢复活动。

由于宕机影响收入，“大师”还比其他同行更有可能部署虚拟网络、复制和存储系统，以便提高灾备能力，加速实现系统备份与运行。

最后，“大师”不会选择坐以待毙。使用诊断分析工具去主动发现风险和安全漏洞的“大师”比例高达“谋士”的 15 倍。此外，他们还更有可能使用预测性分析工具来洞悉潜在宕机。他们部署这些工具不仅仅是为了诊断潜在问题的根源，而且还希望借此来预测风险、从而防止业务中断的真实发生。

SOCIAL SIGNALS

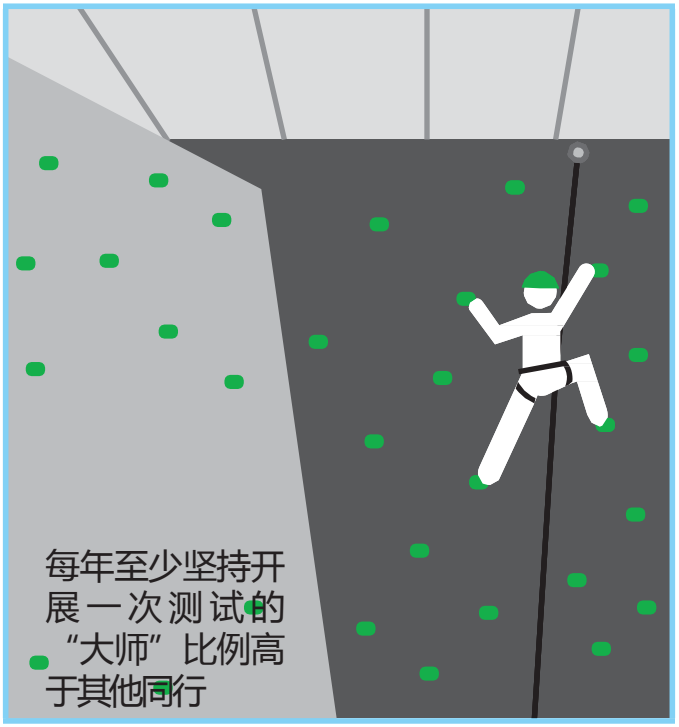
在与灾备有关的社交网络讨论中，约有 1/5 以技术为核心。

而在这些被讨论的技术中，又有 67% 以云计算为主。

	谋士	专家	大师	*大师 vs. 谋士*
在业务中断期间提供实时移动更新	16%	34%	51%	3.0 倍
使用诊断分析工具来发现灾备风险	3%	18%	46%	15.0 倍
部署云计算来支持灾备（如灾备即服务）	12%	23%	25%	2.0 倍
使用预测性分析工具来预测服务中断	0%	5%	22%	–*

** 因分母是零而无法计算 — 没有任何“谋士”指出他们使用过预防性分析工具*

大师坚持开展严格测试



这些精英们会通过频繁开展全面测试来不断优化他们的灾备计划。例如，每年至少坚持对灾备计划开展一次测试的“大师”比例是“谋士”的 2.5 倍。许多情况下，他们都是每月甚至每周测试一次。他们会基于测试结果酌情更新未来计划。

“大师”时刻保持警惕，包括将测试需求写入服务水平协议中。他们还心思缜密，会努力保持灾备测试环境与生产环境之间的一致性。

SOCIALSIGNALS

调查期间，我们发现以灾备测试为核心的社交媒体对话多达 2,500 次。

	谋士	专家	大师	*大师 vs. 谋士*
至少每年进行一次测试	34%	68%	89%	2.5 倍
将测试需求写入 SLA	33%	43%	64%	2.0 倍
维护灾备测试与生产环境之间的一致性	13%	19%	55%	4.0 倍
基于测试结果制订未来方案	21%	34%	45%	2.0 倍

贵公司如何轻松实现灾备？

制订战略性的一体化灾备方案

- 同时与内部领导者（包括董事会）及外部的供应链合作伙伴和业界知名专家一起开展工作。
- 待充分了解合规需求之后再合理制定战略。
- 同时考虑到业务部门及其客户的需求。

设计健壮性测试计划

- 每年至少开展一次测试，培养实时测试能力，可使用任何设备开展特殊查询。
- 将之前测试获得的洞察融入灾备计划中，从而持续改进测试方法。
- 扩展测试覆盖面，使其覆盖整个内部基础架构、全新的移动和云应用、以及供应链合作伙伴连接点。
- 参照业界的灾备领导者开展自我评估，从而发现需要改进的方面。

与安全和风险主管展开合作

- 与风险团队展开合作，以便提高灾备的合规与治理能力。
- 与内部安全团队展开合作，以便将网络安全需求写在灾备计划中。
- 考虑邀请内部审计团队参与灾备规划，以进一步确保满足规章制度的要求。

将新技术融入灾备计划中

- 尝试利用云、高级分析和移动技术来提高响应活动的效力并预防未来服务中断。
- 社交技术不仅可用于实时通报系统状态和负面事件，而且还能监控可能造成业务中断的经济、环境或其他外部事件。

本文作者

Mike Errity 现任 IBM 全球信息技术服务部附属 IBM 连续性服务部北美分部副总裁，负责带领咨询、销售和交付团队与各行各业的客户展开合作，帮助他们通过评估、设计和实施适当的解决方案来控制技术与运营风险。Mike 在业务连续性领域拥有二十多年的专业经验，曾在英国主管业务连续性工作，亲眼见证了美国及全球市场中客户需求朝向“业务永续”的发展演进。如想联系 Mike，您可致函 merrity@ us.ibm.com 或访问他的微博 @MikeErrity。

Rasheq Rahman 现任 IBM 应用洞察中心北美主管，负责以数据为依据针对连续性、安全性及客户转型提供洞察。加入 IBM 之前，他曾从事能源技术商品化工作，花费了近十年的时间给多家跨国投资银行开发贸易运作程序。如想联系 Rasheq，您可致函 rsrahman@us.ibm.com、访问他的微博 @rasheqrahman、或者访问他在应用洞察中心博客上的个人主页。

Kelly McKenna 现任 IBM 应用洞察中心高级分析师，负责提供思维领导力来帮助领导人在数字时代开展睿智的对话。在这个工作岗位上，她主要负责围绕着新兴技术趋势开展数据驱动的调研工作，以便给前瞻性的思维领袖和业界先锋提供支持。加入洞察中心之前，她是 IBM 全球信息技术服务部的一名顾问。如想联系 Kelly，您可致函 mckennak@us.ibm.com、访问她的微博 @k_mck120、或者访问她在应用洞察中心博客上的个人主页。

本文其他贡献者

Angie Casey
Laura DeLallo
Anurag Goyal
Tyler Kettle
Lindsey Reichelt

注释与信息来源

1 “2015 Cost of Data Breach Study: Impact of Business Continuity Management,” Ponemon Institute, 2015 年 6 月。
www.ibm.com/security/ data-breach/

2 《Social Signals》中提供的统计数据是我们于 2015 年 6 月至 11 月期间在全球范围内的英文博客、论坛和微博上针对灾备与业务连续性征求社会意见时获得的。
如想阅读有关各类业务主题的其他《Social Signals》，请阅读 IBM 应用洞察中心系列博文。

3 摘录自 “Case study: Building resiliency into disaster recovery,” Forbes Insights, 2016 年 1 月。
http://www.forbes.com/forbesinsights

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国出品
2016 年 1 月

BUE03004-CNZH-01