IT 风险和声誉对经济的影响

业务连续性和 IT 安全对您的企业真正意味着什么

《IBM 有关 IT 风险对经济的影响全球调研》结果

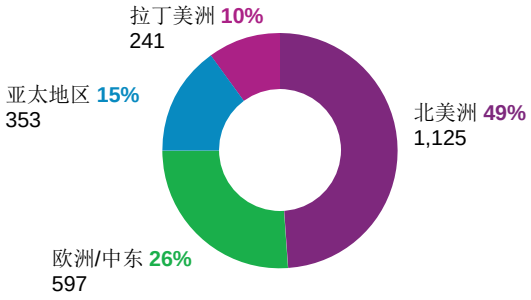
关于本调研

《IBM 有关 IT 风险对经济的影响全球调研》是迄今开展的最大的独立研究调研，旨在评估业务连续性或 IT 安全故障引起的业务中断所造成的财务和声誉影响。本次是 2013 年《IBM 声誉风险和 IT 研究报告》的后续之作，由 IBM 赞助，并由波耐蒙研究所® 于 2013 年 7 月独立执行。

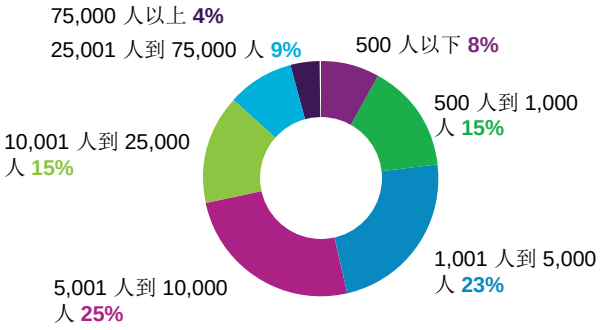
波耐蒙研究所调研了 1,069 名业务连续性专家和 1,247 名 IT 安全从业人员，涵盖 20 个行业和 37 个国家/地区。由 2,316 名受访者组成的联合小组中大部分来自 IT 企业，并直接向首席信息官或公司 IT 部门负责人汇报工作。经理层受访者占最大部分（33%），随后是总监层（23%）和主管层（19%）。超过半数的受访者服务于拥有 5,000 名以上全职员工的大型企业。

本次调研仅限工作重点为业务连续性、IT 安全或二者兼顾的 IT 专业人员，他们都具有决策制定或绩效相关职责。尽管大多数参与者仅关注其中一个 IT 领域，但其调研结果却惊人的相似，仅有少量存在轻微差异、但在统计上又具备一定相关性的情况。因此，为了分析和报告的目的，我们组合了来自两个抽样小组的数据。

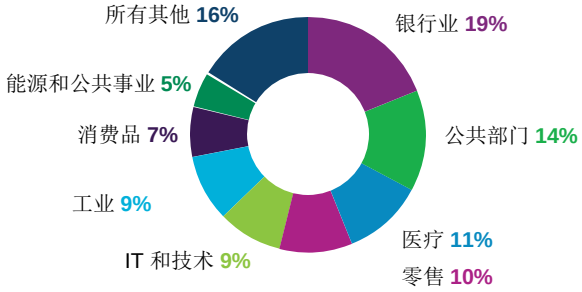
地点（37 个国家/地区）



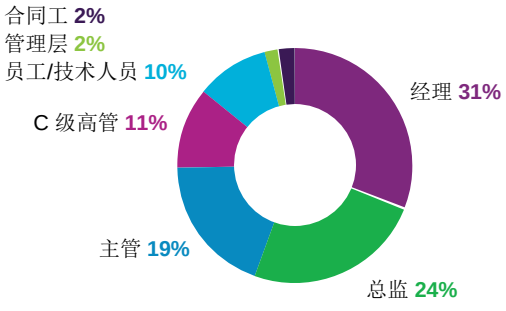
公司规模



行业



职位名称



《IBM 有关 IT 风险对经济的影响全球调研》由波耐蒙研究所单独执行，向全球范围的 2,316 名业务连续性和 IT 安全专业人员搜集信息。

目录

您将做什么？

如果您认为声誉和品牌很重要，那么就要将 IT 风险管理作为重中之重。

– 法国消费产品公司业务连续性管理主管

介绍

当 IT 系统故障和网络攻击中断正常业务运营时，经济和声誉方面的损失可能是毁灭性的。甚至短短几分钟的停机时间也可能给企业造成巨大的损失。在本文中，IT 风险是指与企业内的 IT 使用、所有权、运营和影响相关的风险。此类风险包括人为错误、系统故障、安全违规和数据中心运营中断，如电源故障和自然灾害等。

了解中断造成的财务影响对于确定应投入的资源有着重要意义，从而可以避免或最大限度减少此类突发事件。同时，它对于为 C 级高管制定业务案例，以评估业务连续性和 IT 安全活动的优先事项同样起着至关重要的作用。

企业在面对故障或正常运营挑战时，由于无法提供可接受的服务水平会造成财务影响或对“总成本”的影响。在本次调研中，我们对此影响进行了测量。我们还评估并量化了对声誉的影响，包括由于控制不佳、故障流程、IT 故障、数据被窃和违规对公司的形象和品牌价值造成的损失成本。

对业务连续性和 IT 安全问题的回应

在本次调研中，我们提出了两个可选的开放式问题：
“贵公司或您所在的行业应采取哪些措施来降低 IT 运营带来的风险？”
“展望未来，IT 环境的哪些变化或趋势将最大程度地增加您企业的声誉风险？”

我们收到的调研者的回答均经过了深思熟虑，且发人深省，同时还出现了一系列共同主题。在全文中，我们将分享一些调研者的回答，它们反应了人们普遍关注的问题，呈现为以下两个主题：“您将做什么？”和“哪方面存在风险？”

量化业务和 IT 运营中断的经济影响

此次调研的一个非常重要的目标是，确定当业务流程或 IT 服务发生中断或受到损害时，企业要付出的代价。要求受访者基于三个独立的级别评估成本，包括轻微、中等和严重。

中断持续时间。根据停机时间，将业务中断分为轻微、中等和严重三类。如图 1 所示，轻微突发事件平均为 19.7 分钟，而严重突发事件为 442.3 分钟或者几乎全天 8 小时故障或停机。然而，有人预计严重中断可能持续两天以上。

可能性。根据图 2 所示，69% 的受访者预计在未来 24 个月内他们将会遇到至少一次或多次轻微中断，而 23% 的受访者预计在未来 24 个月内可能会发生一次或多次严重中断。换言之，受访者认为其企业遇到轻微中断的可能性比遇到严重突发事件的可能性高三倍。

成本。要求受访者针对以下六类成本，考虑所有直接现金支出、直接人工费用、间接人工成本、管理费用和丢失的业务机会：

- 由于停机或系统性能延迟而导致的用户停工时间成本和生产效率损失成本
- 确定中断或损害根源的取证成本
- 将系统恢复至运营状态的技术支持成本
- 声誉和品牌损失相关的成本
- 由于系统可用性问题而造成的收入损失
- 与不合规相关的成本

图 3 显示了每分钟轻微、中等和严重的业务或 IT 运营中断所造成的平均成本。每分钟轻微中断的成本比每分钟严重中断的成本要高得多（每分钟轻微中断的成本为 53,223 美元，每分钟严重中断的成本为 32,229 美元），这表明用户的停工时间、取证和技术支持成本在较少的停机时间（分钟）内进行分摊（也请参见图 5）。

图 4 显示了由于业务中断或 IT 运营中断可能造成的总平均成本。即使是轻微中断也会使企业付出超过 100 万美元的代价，严重突发事件可能导致超过 1,400 万美元的代价。然而，一些受访者表示，严重突发事件的影响可能会攀升至 1 亿美元以上。此预估基于上述 6 个成本类别。从经济影响角度来看，最严重的威胁是人为错误、网络攻击和数据丢失。

需要指出的是，尽管相对于严重突发事件，轻微突发事件的平均成本相对较低，但轻微中断的出现频率高，这可能意味着，随着时间的推移轻微中断会造成严重的财务影响。

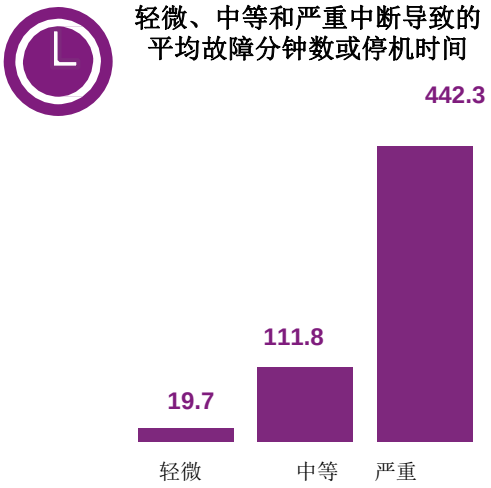


图 1. 轻微、中等和严重中断导致的平均故障分钟数或停机时间

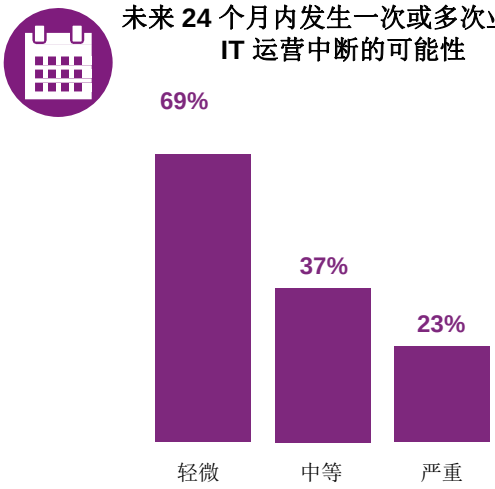


图 2. 未来 24 个月内发生一次或多次业务和 IT 运营中断的可能性

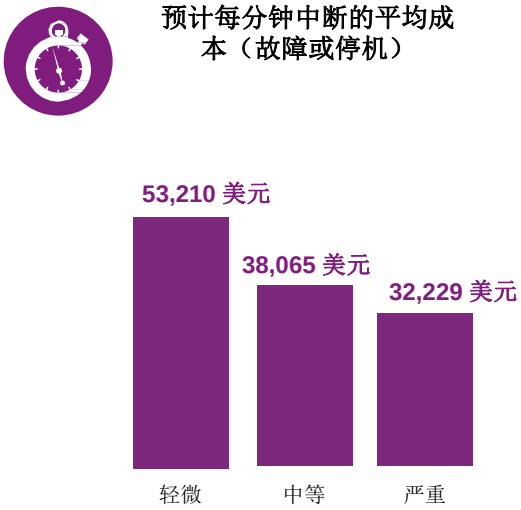


图 3. 预计每分钟中断的平均成本（故障或停机）

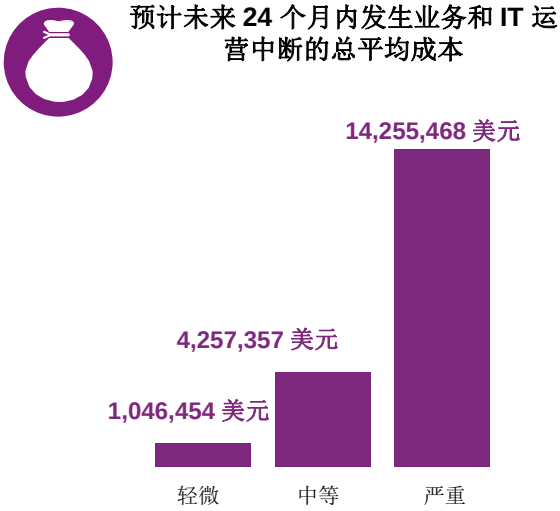


图 4. 预计未来 24 个月内发生业务和 IT 运营中断的总平均成本

声誉风险和 IT 连接

如果您对于有效的业务连续性或 IT 安全计划的重要性有任何疑问，那么请考虑业务中断对企业声誉和品牌价值可能造成的财务影响。图 5 是成本分配图，该分配图通过为轻微、中等和严重中断分配 100 分制值确定。如图所示，声誉和品牌损失的相关成本与突发事件的严重程度成比例增加。相应地，声誉损失在轻微业务中断和 IT 运营中断中仅占 2 个百分点，而在严重中断中占到 37 个百分点。

所有三种中断综合来看，排名前三项的成本为：
(1) 用户的停工时间成本
(2) 取证成本
(3) 技术支持成本

值得一提的是，尽管领导层最担心的是由系统不可用问题而导致的收入损失，但在 IT 专业人员眼中，这一方面却几乎排在所分配成本的最末位。

您将做什么？

“我们应该从被动转向主动，制定出更成熟的风险管理战略。”

– 德国技术公司 IT 安全总监

总成本的分配

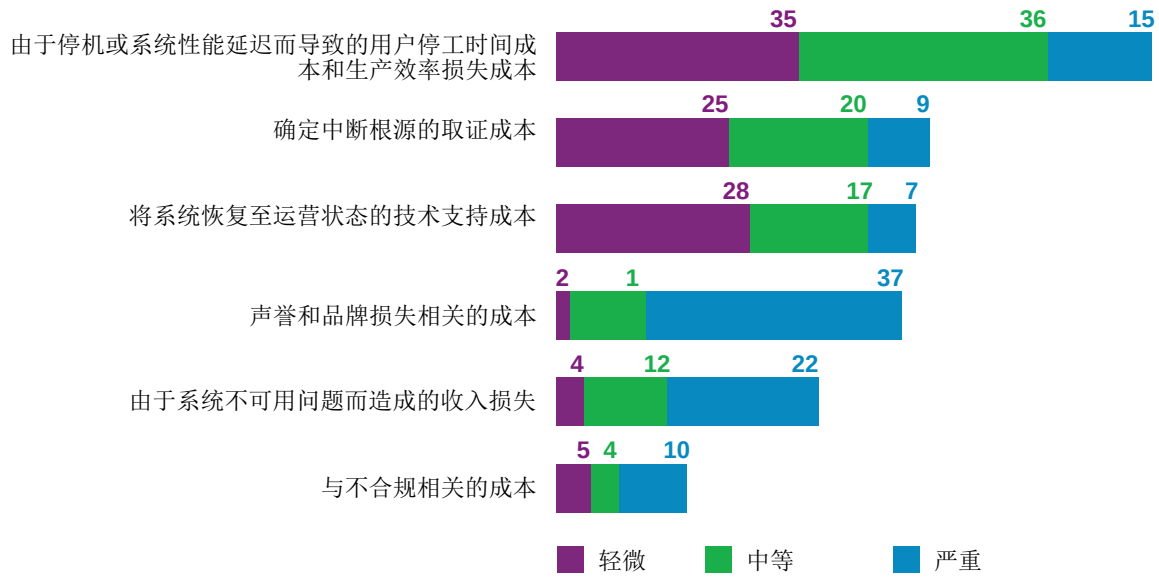


图 5. 对于这三种中断级别中的每个级别（轻微、中等和严重），要求受访者使用 100 分制将总成本分摊到这六个成本类别中。

根据前面得出的轻微、中等和严重成本分配结果，我们预估了所有三个级别中断造成的声誉和品牌相关损失。图 6 显示严重中断相关的声誉成本为近 530 万美元。相比较而言，轻微中断相关的声誉成本相对可以忽略不计。

声誉威胁：感觉与现实

对企业声誉面临的 IT 威胁来源方面，界定比较模糊。我们请受访者对影响其企业声誉的七种常见威胁进行排名。如图 7 所示，数据破坏和灾难在威胁排名中最靠前，
受访者认为这两项会造成最大的声誉风险，IT 系统故障排在第三位，人为错误排在第六位。

预计未来 24 个月内因业务和 IT 运营中断而造成的声誉相关成本

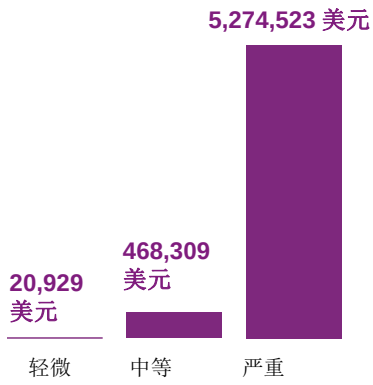


图 6. 预计未来 24 个月内因业务或 IT 运营中断而造成的声誉相关成本

按声誉影响排列的常见威胁

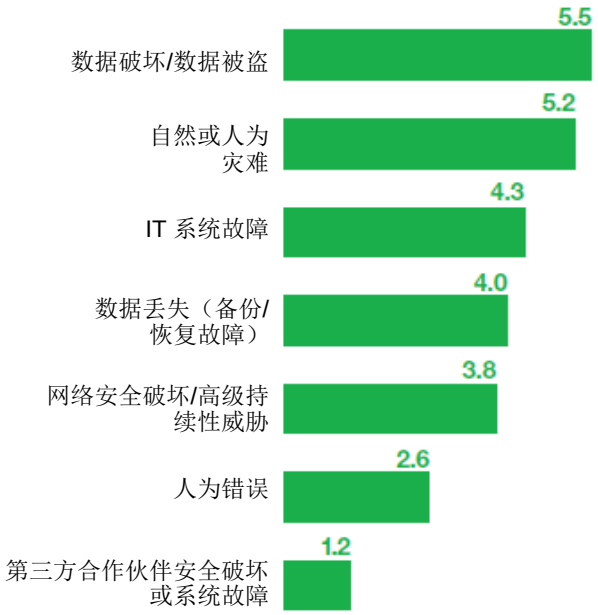


图 7. 按声誉影响排列的常见威胁

您将做什么？

“制定一项能够将信息风险与企业风险关联起来的战略。”

– 加拿大金融服务公司业务连续性总监

当受访者被问及其企业是否真的遇到了声誉或品牌价值损失，以及具体的原因时，威胁的排名出现了很大不同。如图 8 所示，基于过去两年的经历，最严重的声誉威胁是涉及 IT 系统故障和人为错误的突发事件，其次是网络安全破坏。自然或人为灾难造成声誉或品牌损失的可能性要小得多。

在过去 24 个月遇到的影响声誉和品牌价值的威胁

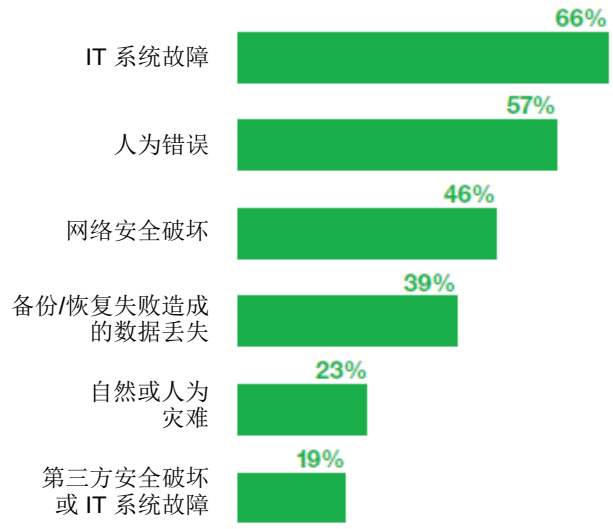


图 8. 在过去 24 个月造成声誉和品牌价值影响的威胁（回答“是”的百分比）

了解威胁环境

我们的调研还更广泛地探讨了威胁环境，以确定 IT 从业者*认为*会发生的事件与其实际经历之间的关联有多紧密。总体而言，受访者关于威胁发生的可能性的看法与所报告的事件情况基本一致，其中在可能性、遇到的中断次数和预计的财务影响方面，人为错误排第一位。

图 9 显示了受访者从其企业发生威胁的可能性方面对七种常见威胁的排名。业务连续性和 IT 安全专业人员将人为错误列为最主要的潜在威胁。同时， IT 系统故障、数据破坏和第三方合作伙伴安全破坏或系统故障也是主要的威胁，彼此几乎不分上下。

按发生可能性排列的常见威胁

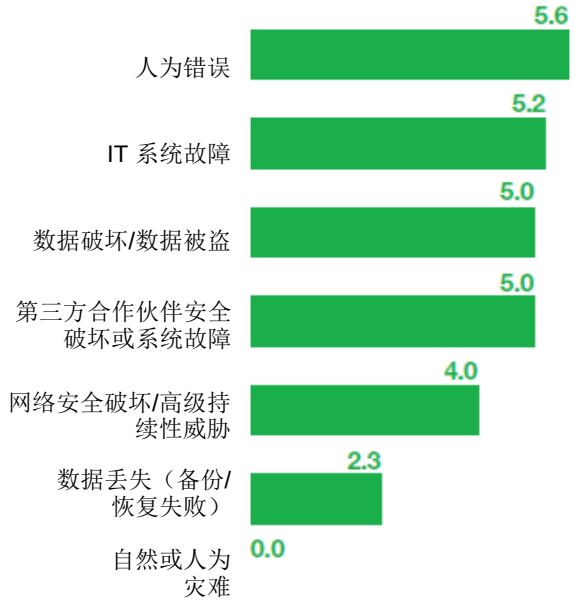


图 9. 按发生可能性排列的常见威胁

总体而言，对于一般威胁环境的了解，IT 专业人员的把握都非常准确。根据图 10 所示，受访者报告在过去两年里，他们平均遇到了超过 9 次由于人为错误而导致的业务中断，正好与业务和 IT 运营及 IT 安全的主要潜在威胁排名相吻合。事实上，人为错误造成的突发事件的实际发生次数远远超过预测。由于备份/恢复失败造成的数据丢失也比预计的更常见，并且略微比网络安全破坏更频繁。

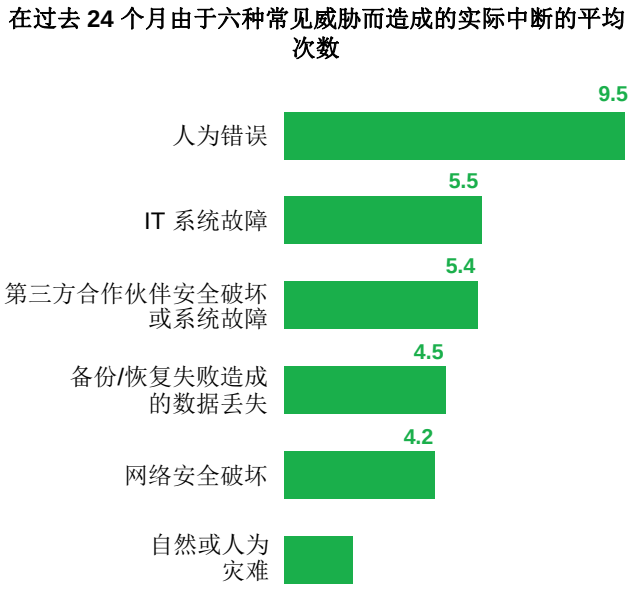


图 10. 在过去 24 个月由于六种常见威胁而造成的实际中断的平均次数

从对企业的潜在经济影响方面来评估威胁时，图 11 显示受访者在将人为错误列为最主要威胁方面很一致。然而参与者认为，网络安全破坏和数据被盗在经济影响方面的风险远大于声誉影响方面的风险（也请参见图 7）。

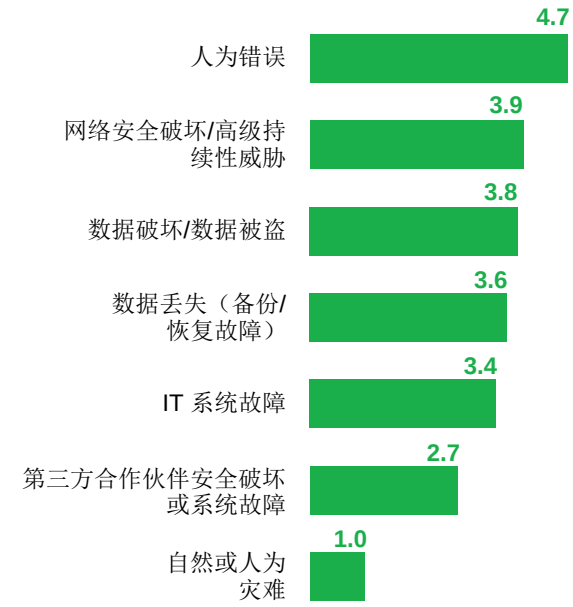


图 11. 按经济影响排列的常见威胁

第三方合作伙伴的角色：进一步观察

供应商和第三方会对受访者的公司造成多大的威胁？41（21+20）% 的受访者（图 12）表示，在过去 24 个月发生的业务和 IT 运营中断中，供应商相关的事故为主要原因。

其中一个原因可能是标准的问题。根据图 13 所示，并非所有供应商和其他第三方都被要求遵从受访者公司遵守的同一业务连续性和 IT 安全要求。31% 的受访者表示，其公司并不要求供应商和其他第三方遵守其业务连续性要求，40% 的受访者表示其公司不要求合作伙伴遵从其 IT 安全标准。

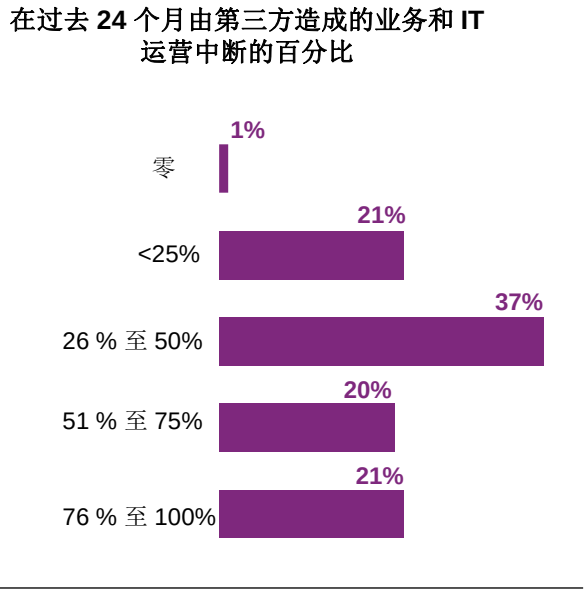


图 12. 在过去 24 个月由第三方造成的业务和 IT 运营中断的百分比

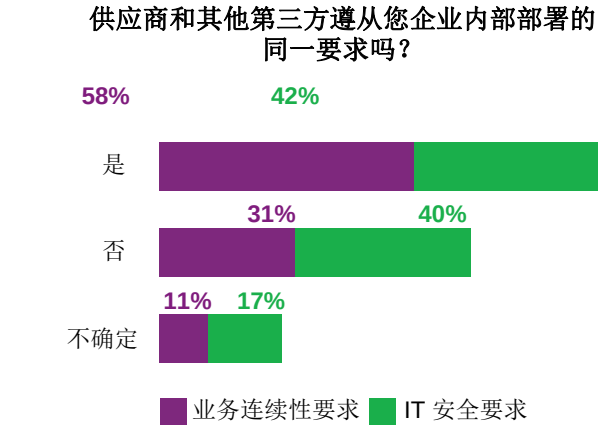


图 13. 供应商和其他第三方遵从您企业内部部署的同一要求吗？

建立业务连续性和 IT 安全投资案例

业务连续性和 IT 安全专业人员坚信，其领域对企业的成功起着重要作用。图 14 显示了这一研究的一个意外发现：89% 的受访者表示，保护知识产权是其 IT 角色的一个非常重要的目标。我们认为，这反映了知识产权本身日益数字化的性质，以及面对网络攻击或 IT 故障导致的丢失时，知识产权显示出的脆弱性。

最大限度地提高员工生产效率（72%），最大限度地减少违反法规或法律情况（70%），以及提升品牌价值和声誉，是业务连续性和 IT 安全活动推进的前四项非常重要的目标。基于以往的 IBM 调研，2013 年 65% 的受访者将提升品牌价值列为“非常重要”，这一事实证明，越来越多的 IT 专业人员认识到 IT 风险与声誉风险之间的关系。

哪方面存在风险？

“最令我感到害怕的是，社交媒体的使用不断增加，这会泄露公司知识产权并损害声誉。”

– 美国专业服务公司 IT 安全主管

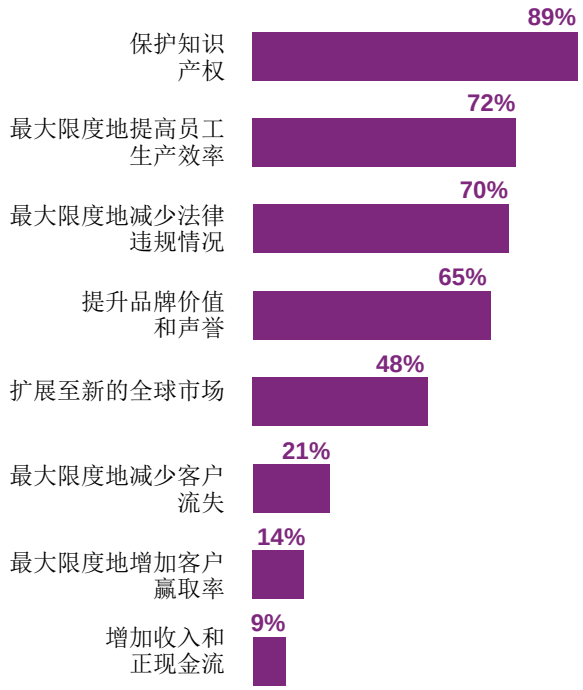


图 14. 业务连续性和 IT 安全管理活动推进的业务目标

现在，防止声誉和品牌价值的潜在损失，也成为企业投资业务连续性和 IT 安全计划的一个动机。图 15 显示，防止生产率损失、系统故障损失、违规损失及声誉损失，是确保预算承诺的主要因素。

确保业务连续性和 IT 安全预算承诺的主要因素

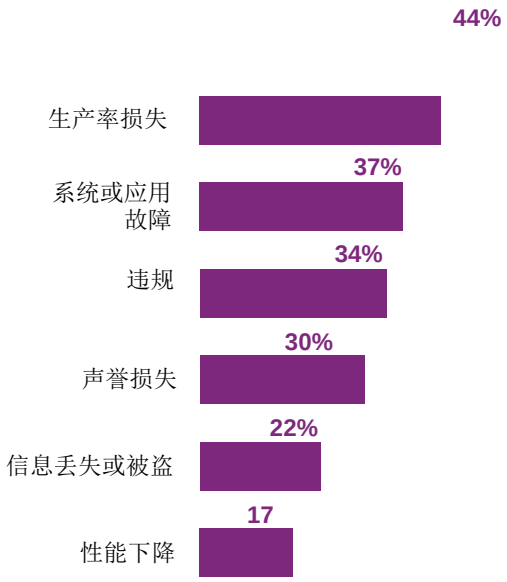


图 15. 确保业务连续性和 IT 安全预算承诺的主要因素

哪方面存在风险？

“升级 IT 风险管理问题需要 C 级高管的支持，而且这很难完成。”

– 阿根廷服务公司 IT 安全经理

尽管受访者认识到了最大限度地降低由潜在的声誉和品牌威胁造成的 IT 风险的重要性，但是他们不相信其领导者也持有相同的看法。图 16 显示仅 32% 的受访者表示其公司的领导者认识到了 IT 风险会影响品牌形象，35% 的受访者表示其公司的领导者认识到了 IT 风险会影响声誉。半数（50%）的受访者认为其企业的领导者没有认识到 IT 风险会影响收入。

企业领导者强烈同意或同意，业务和 IT 运营中断会造成经济和声誉影响

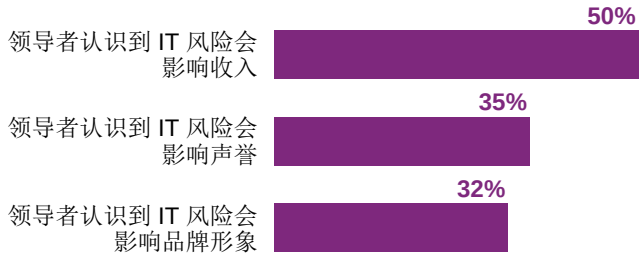


图 16. 企业领导者是否认识到了业务和 IT 运营中断造成的经济和声誉影响？（图为表示强烈同意和同意的组合）

取得成功的阻碍因素

受访者表示，实现高效业务连续性和 IT 安全管理计划的最显著阻碍因素是资金不足、颠覆性技术的出现、缺乏经验丰富的员工和业务流程的复杂性（图 17）。

尽管仅有 17% 的受访者提到了规划、准备、数据孤岛思维，对另外两个问题的回答表明，这些因素对于业务连续性和 IT 安全计划的成功与否可能确实起到更重要的作用。根据图 18 所示，大多数受访者表示其公司针对整个企业的业务连续性或 IT 安全管理没有制定正式的战略（而且这会影响这些 IT 运营的效率）。

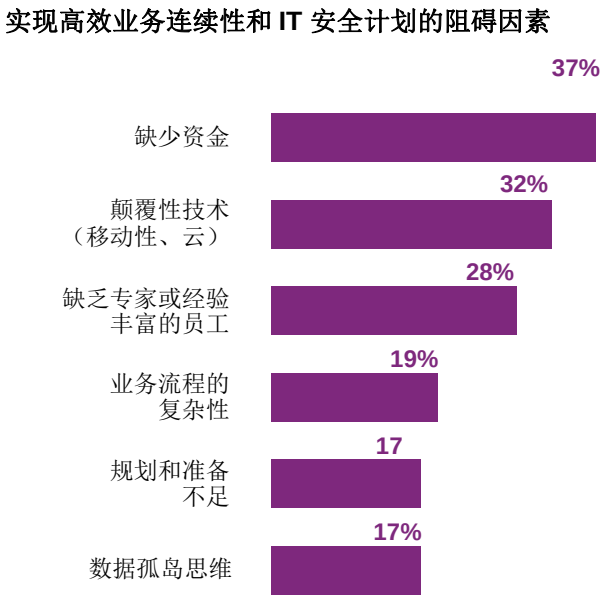


图 17. 实现高效业务连续性和 IT 安全计划的阻碍因素

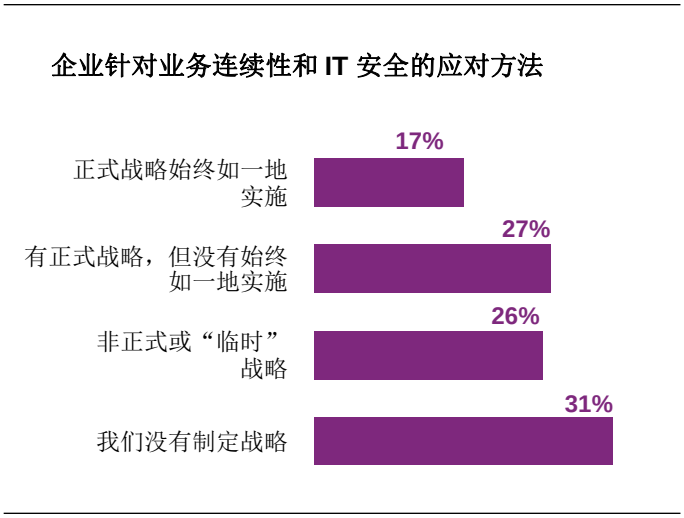


图 18. 企业针对业务连续性和 IT 安全战略的应对方法

图 19 中总结的结果表明，受访者无法实现高水平的协作。44% 的受访者认为其部门与其他业务或 IT 部门之间的协作很差或者不存在协作，这表明数据孤岛思维严重阻碍了实现高效业务连续性和 IT 安全管理计划，而 IT 专业人员却不愿承认这一点。

业务连续性、IT 安全与其他业务或 IT 职能部门间的协作

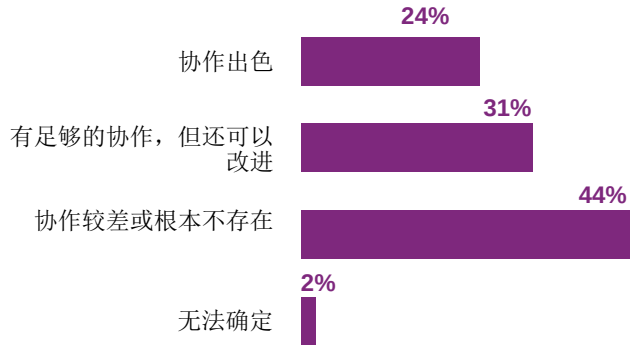


图 19. 业务连续性、IT 安全与其他业务或 IT 职能部门间的协作程度

我们的研究结果还表明，在防止 IT 运营中断的总负责人方面，目前还没有明确的最佳实践。尽管最可能的责任人是首席信息官（CIO），但仅有 28% 的受访者持此观点（图 20）。接下来占最大比例的是不属于 IT 部门范畴的业务部门领导。排第三的选项是“没有一个人全面负责”，占比 11%。缺乏明确的职责履行者，也可能成为我们取得成功的障碍。

全面负责指导工作以确保 IT 运营不被中断的总负责人

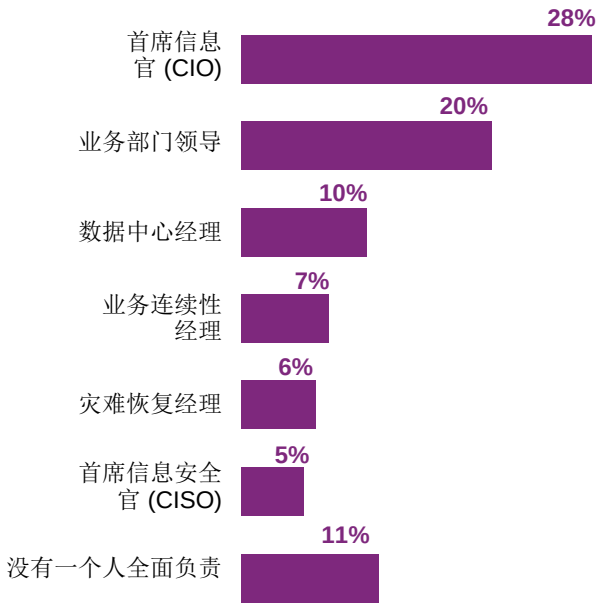


图 20. 全面负责指导工作以确保 IT 运营不被中断的总负责人

结论和意见

业务连续性和 IT 安全故障产生的经济影响可能非常显著，范围涵盖从平均造成 100 万美元损失、持续 20 分钟的轻微中断，到造成超过 1,400 万美元损失、持续近 8 小时的严重中断。轻微中断比严重中断发生的可能性更大，但一次轻微事件造成的代价就可能超过预防成本。

业务连续性和 IT 安全专业人员认识到，由于严重事件造成的声誉和品牌损失相关的成本也非常可观。平均而言，他们估计在未来 24 个月，仅声誉损失相关的成本一项将会超过 500 万美元。尽管 65% 的调研受访者认为业务连续性和 IT 安全管理能够提升品牌价值和声誉，但只有不到 35% 的受访者认为高级管理层认同这一观点。

这意味着，业务连续性和 IT 安全专业人员需要建立一个更强大的商业案例，以推动企业投资 IT 控制，进而避免停机、数据丢失、网络安全破坏和由此造成的生产率损失和声誉损失。IT 人员可以从严格评估企业内部实际根源着手，然后关联支出与可避免的潜在财务风险。这种方法能够为建立业务相关指标奠定基础，进而衡量有效性并提供进一步的预算根据。

将 IT 风险防范与成本效益分析关联起来，这不仅有助于提升这一讨论的影响力，而且还有助于领导者了解风险的来源。这一点特别重要，因为造成业务中断和经济影响的一个最重要的原因是人为错误，这不是 IT 部门凭一己之力就能够解决的问题。尽管 IT 部门可以投资业务流程，例如通过变更管理或自动化数据备份等措施来减少人为错误，然而，教育终端用户以及建立安全意识和合规文化需要整个企业范围的努力和自上而下的领导推进。

了解更多信息

如需了解 IBM 如何通过加强 IT 风险管理，帮助您保护企业声誉，请联系您的 IBM 代表或 IBM 业务合作伙伴，或者访问业务连续性服务中文网页：**http://www-935.ibm.com/services/cn/zh/it-services/business-continuity/index.html**

加入业务连续性对话

加入 IT 安全对话

局限性
本调研研究存在内在的局限性，从以上呈现的调研结果中得出结论之前，需要谨慎考虑。下列各项是与大部分基于调研的研究密切相关的具体局限性。

不回应产生的偏差：目前的研究结果基于调研反馈的样本。我们从众多国家/地区的业务连续性管理人员、IT 和 IT 安全从业人员中抽选抽样代表，并将调研问卷发送给他们。我们收到了大量有效的反馈。尽管本调研测试属于非回应性测试，但始终存在这样的情况，即没有参加本调研的个人，其基本观念与那些完成调研的个人存在显著不同。

抽样范围偏差：相对于选定国家/地区抽样的业务连续性管理人员、IT 和 IT 安全从业人员，我们的抽样范围是否具有代表性，这决定了调研结果的准确性。

自陈报告结果：调研研究的质量取决于受访者保密反馈信息的完整性。虽然我们的调研评估过程中融入了某些制衡因素，包括完整性检查，但始终存在一些受访者不提供真实反馈的可能性。

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10504

美国印刷
2013 年 9 月

RLW03022-USEN-00