2015 年数据泄露成本调研：
业务连续性管理对数据泄露成本的影响

基准调研，由 IBM 发起
波耐蒙研究所 (Ponemon Institude) 独立进行
2015 年 6 月

2015 年[1]数据泄露成本调研：

对企业业务连续性管理的影响

波耐蒙研究所，2015 年 6 月

第一部分：引言

《2015 年数据泄露成本调研：全球分析》由 IBM 发起，定量分析了数据泄露带来的经济影响，并且观察了过去一段时间的成本变化趋势。通过本调研，我们将深入了解数据泄露的成本、根源以及影响成本的因素，从而帮助各机构确定适当的投资金额和资源，防止或减少网络攻击带来的影响。

各个国家的人均数据泄露成本大不相同。这些成本差异主要归因于两点：机构所面临的攻击与威胁的类型不同，以及各国数据保护的法律法规不同。在今年的全球分析中，数据泄露的人均成本由 145 美元上升至 154 美元，而数据泄露的总成本也由 350 万美元上升至 380 万美元。[2]

今年的调研涉及了 16 个行业领域中的 350 家企业，它们分别来自以下国家：美国、英国、德国、澳大利亚、法国、巴西、日本、意大利、印度、阿拉伯地区，以及首次参与调研的加拿大。所有参与调研的机构都经历了数据泄露，泄露记录数量最少在 3,000 条左右，最多大约 100,000 条。[3]我们对泄露记录的定义是识别出数据泄露事件中个人信息发生丢失或被窃的记录。

本年度调研的一个重要作用就是更好地了解能够最大限度降低数据泄露财务后果的因素。该专题报告分析了业务连续性管理 (BCM) 对数据泄露财务后果和声誉后果的积极影响。[4]

许多公司都有 BCM 职能部门或团队来进行企业风险管理、灾难复原和危机管理。本调研中，有 50% 的企业在发生数据泄露时会寻求 BCM 专家的帮助。正因为有了 BCM 专家和相关流程，数据泄露才能够以更高效、更经济的方式得以解决。

业务连续性管理项目对数据泄露成本的影响

数据泄露人均成本下降 9%

识别数据泄露的平均时间减少 27%

控制数据泄露的平均时间减少 41%

未来两年内发生数据泄露的可能性降低 28%

有关 BCM 减轻数据泄露后果的重要结论：

数据泄露的成本与识别和控制数据泄露事件的平均时间呈线性关系。调研结果表明，BCM 能够大大降低识别和控制数据泄露事件的平均时间。没有采用 BCM 的企业平均需要 234 天来识别数据泄露事件，并且平均需要 83 天来控制数据泄露。相比之下，采用 BCM 的企业平均只需 178 天就能够识别数据泄露事件，并且平均只需 55 天就能够控制泄露事件。

[1]此报告标注日期为发表年度，而非实地考察完成日期。请注意，当前报告中研究的大部分数据泄露事件发生在 2014 年这个自然年度。
[2].本国货币转换成美元。
[3]此报告中，“每个被窃记录的成本”和“人均成本”这两个术语的意义相同。
[4]支撑事件响应过程的 BCM 团队包括具备灾难恢复能力的专业人员。

在数据泄露事件响应计划与执行过程中采用 BCM 十分重要。在参与此项全球分析的 350 家公司中，有 174 家自报在消除数据泄露后果的过程中采用了 BCM。这些公司中的大部分（占比 63%）认为采用 BCM 十分重要。

如果数据泄露事件响应计划和执行过程中不采用 BCM，数据泄露成本将更大。每项丢失或被窃记录的平均成本可能高达 161 美元。采用 BCM 后，平均成本可以降至 147 美元。

在事件响应计划过程中不采用 BCM，数据泄露的几率更大。调研结果显示，如果在数据泄露计划中不采用 BCM，未来两年里发生数据泄露的几率为 27.9%。反之，如果采用 BCM，几率将下降至 21.1%。

在德国和日本，BCM 团队协助进行数据泄露事件响应计划和执行的公司百分比最高。BCM 采用率最低的国家是巴西和阿拉伯各国。除意大利之外，所有国家都提高了在数据泄露事件管理流程中采用 BCM 的水平。

发生数据泄露时，BCM 能够最大限度减少业务中断。调研结果显示，在未采用 BCM 的公司中，有 80% 发生过实质性业务中断。而在采用 BCM 的公司中，仅有 55% 发生过实质性业务中断。

采用 BCM 能够提升 IT 运营的恢复力。在未采用 BCM 的公司中，有 74% 表示 IT 运营发生过实质性中断。而在采用 BCM 的公司中，仅有 52% 表示 IT 运营发生过实质性中断。

BCM 可以在发生数据泄露事件后保护公司声誉。在此项调研中，采用 BCM 的公司中有不到一半 (45%) 表示其声誉或品牌因为数据泄露受到了消极影响。但是，未采用 BCM 的公司中有 55% 表示其企业品牌和声誉受到了影响。

第二部分：关键研究结果

下表列出了本调研中涉及的 11 个国家的名称、图例、样本大小和货币，并且展示了各国参与此年度报告的年数，最短的为只参与了 1 年的加拿大，最长的为参与了 10 年的美国。

表 1、全球分析一览

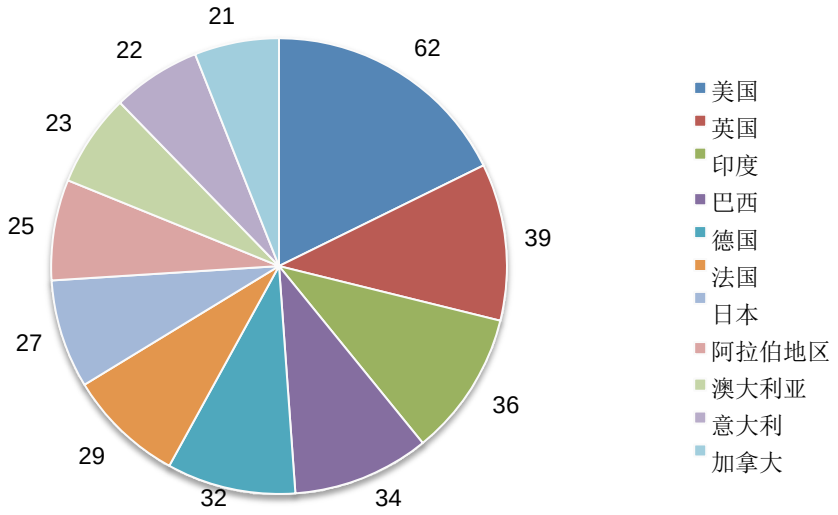
图例	国家	样本	百分比	货币	参与调研年数
AB	阿拉伯国家*	25	7%	阿联酋迪拉姆/沙特里亚尔	2
AU	澳大利亚	23	7%	澳元	6
BZ	巴西	34	10%	雷亚尔	3
CA	加拿大	21	6%	加元	1
DE	德国	32	9%	欧元	7
FR	法国	29	8%	欧元	6
ID	印度	36	10%	卢比	4
IT	意大利	22	6%	欧元	4
JP	日本	27	8%	日元	4
UK	英国	39	11%	英镑	8
US	美国	62	18%	美元	10
	总计	350	100%		

*AB 是沙特阿拉伯和阿联酋企业的组合样本。

下图展示了来自 11 个国家的 350 个参与企业的分布情况。如图所示，美国有 62 个企业参与调查，在下图中所占比例最大，而加拿大有 21 个企业参与调查，所占比例最小。

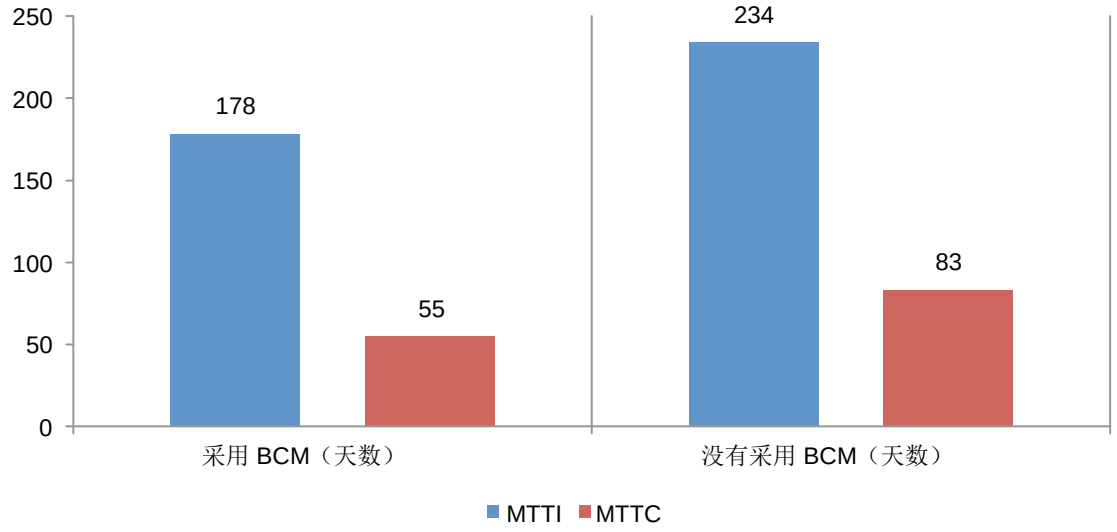
饼图 1、不同国家基准样本频率

合并统计 (n = 350)



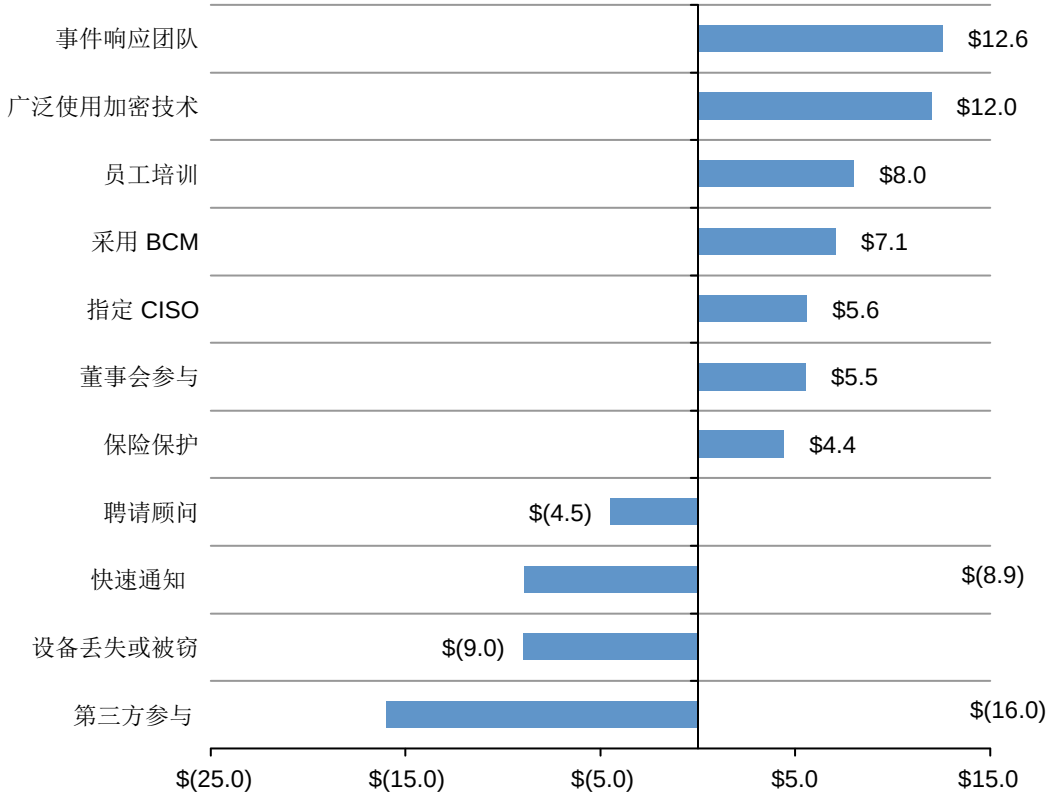
数据泄露的成本与识别和控制数据泄露事件的平均时间呈线性关系。在今年的调研中，我们展示了识别 (MTTI) 和控制 (MTTC) 数据泄露时间的平均时间与数据泄露的成本呈线性相关。图 1 则表明了另一种有趣的相互关系。对采用了 BCM 的机构来说，识别和控制数据泄露事件所用的天数要比没有采用 BCM 的机构少得多。MTTI 和 MTTC 的百分数差分别为 27% 和 41%。

图 1、在事件响应程序中采用或没有采用 BCM 的机构的 MTTI 和 MTTC。
MTTI 百分数差 = 27%；MTTC 百分数差 = 41%
合并统计（2015 财年 = 350，2014 财年 = 315）



影响数据泄露成本的因素。在此调研中，对于这 11 项因素，正数为增量成本节约额，负数为增量成本增加额。如图 2 所示，一个强大的事件响应团队能够最大程度地降低数据泄露的人均成本。业务连续性管理降低了人均数据泄露成本，平均降幅为每条被窃记录 7.1 美元。

图 2、11 项因素对人均数据泄露成本的影响
合并统计，单位为美元 (n = 350)



BCM 对事件响应计划的作用。图 3 提供了 BCM 参与数据泄露事件响应计划和执行过程的摘要信息。在参与此项全球分析的 350 家公司中，有 174 家（占比 50%）采用了 BCM。其余的 176 家公司没有 BCM 工作组或只在特殊情况下采用 BCM。去年的分析显示，有 45% 的企业在数据泄露事件响应中采用了 BCM。

图 3、BCM 如何促进数据泄露事件响应程序？
合并统计（2015 财年= 350，2014 财年= 315）

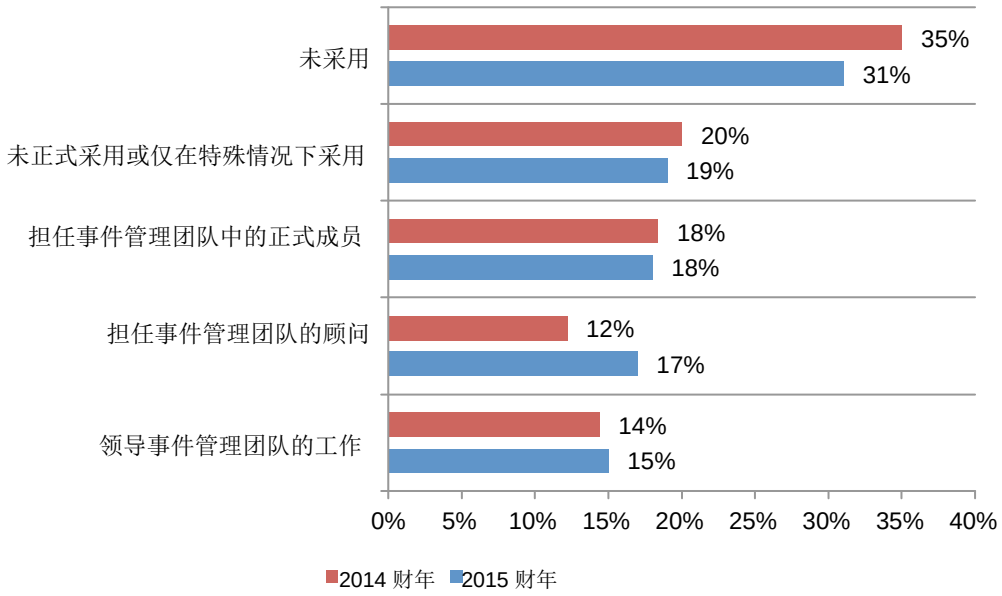
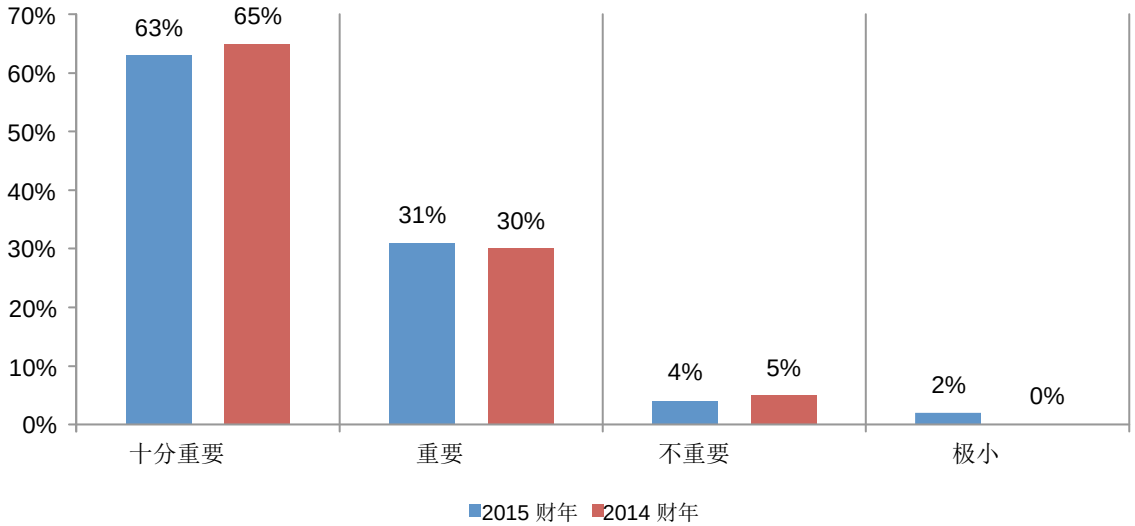


图 4 显示了在事件响应计划和执行中采用 BCM 的情况。在今年的调研中，有 63% 的公司认为采用 BCM 十分重要。有 31% 的公司认为采用 BCM 重要。而去年的调研显示，分别有 65% 和 30% 的公司认为采用 BCM 十分重要和重要。

图 4、什么是 BCM 对事件响应程序的作用的最恰当表述？
合并统计（2015 财年 = 350，2014 财年 = 315）



BCM 能够降低人均数据泄露成本。图 5 报告了过去两年在事件响应计划和执行过程中，有 BCM 工作组参与的公司人均数据泄露成本平均值和没有采用 BCM 的公司人均数据泄露成本平均值。采用 BCM 的公司遭受的数据泄露成本比那些没有采用 BCM 的公司要低。今年，采用 BCM 和没采用 BCM 的公司之间的人均数据泄露成本百分数差为 9%，而去年的百分数差为 13%。

图 5、采用 BCM 的和未采用 BCM 的公司人均数据泄露成本
2015 财年的百分数差 = 9%；2014 财年的百分数差 = 13%
合并统计（2015 财年 = 350，2014 财年 = 315）

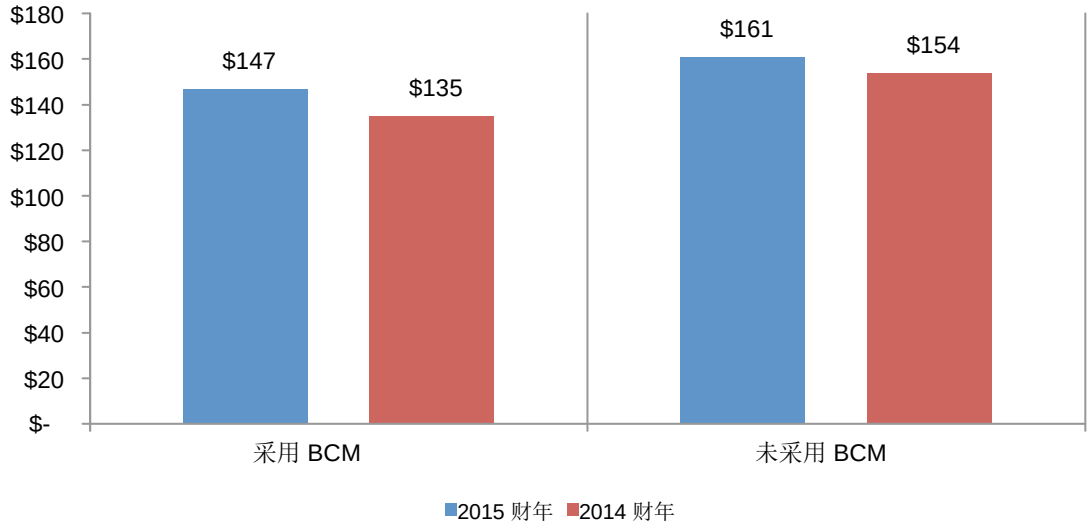


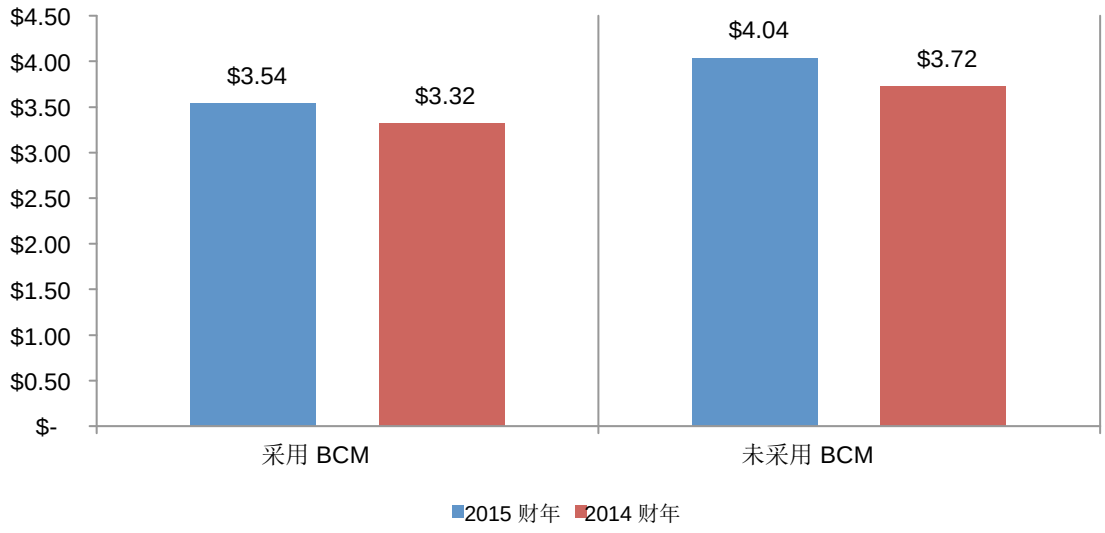
图 6 报告了在事件响应计划和执行过程中采用和未采用 BCM 工作组的公司过去两年里的数据泄露总成本。与上述情况类似，采用 BCM 的公司的数据泄露总成本比那些没有采用 BCM 的公司要低。采用 BCM 和未采用 BCM 的企业总成本百分数差为 13%。去年，这一百分数差为 11%。

图 6、采用 BCM 的公司和未采用 BCM 的公司人均数据泄露成本

2015 财年的百分数差 = 13%；2014 财年的百分数差 = 11%

合并统计（2015 财年= 350，2014 财年 = 315）

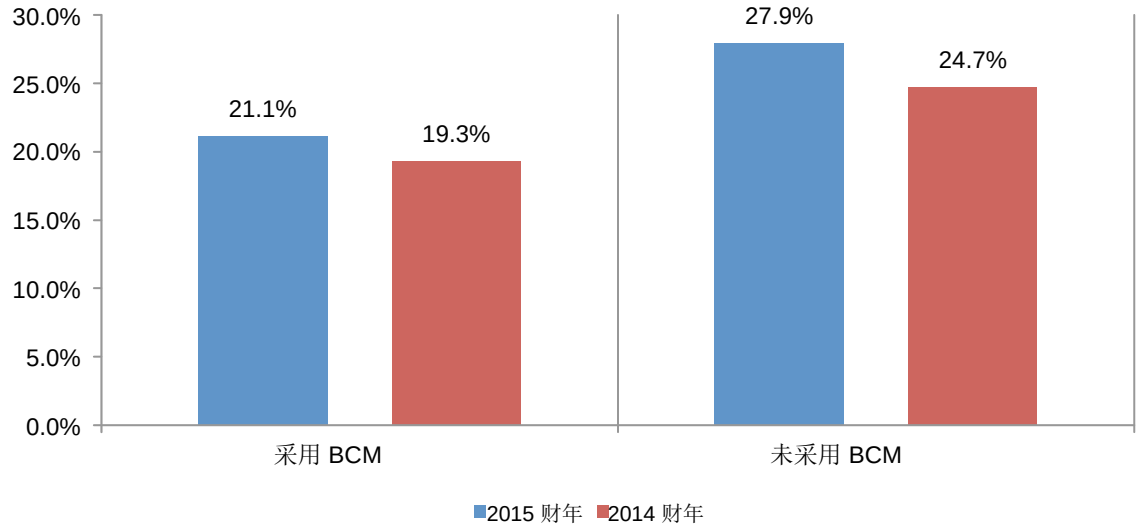
（百万美元）



BCM 降低数据泄露的可能性。图 7 报告了采用 BCM 工作组和未采用 BCM 的公司接下来 24 个月里数据泄露量至少达到 10,000 条或更多记录的平均可能性。

显而易见，采用 BCM 的公司发生数据泄漏的可能性比那些没有采用 BCM 的公司要低。2014 财年和 2015 财年的调查都显示了这样的结果。采用和未采用 BCM 的公司未来发生数据泄露可能性的百分数差今年为 28%，去年为 25%。

图 7、采用 BCM 的公司和未采用 BCM 的公司实质性数据泄露可能性
2015 财年百分数差 = 28%；2014 财年百分数差 = 25%
合并统计（2015 财年 = 350，2014 年 = 315）

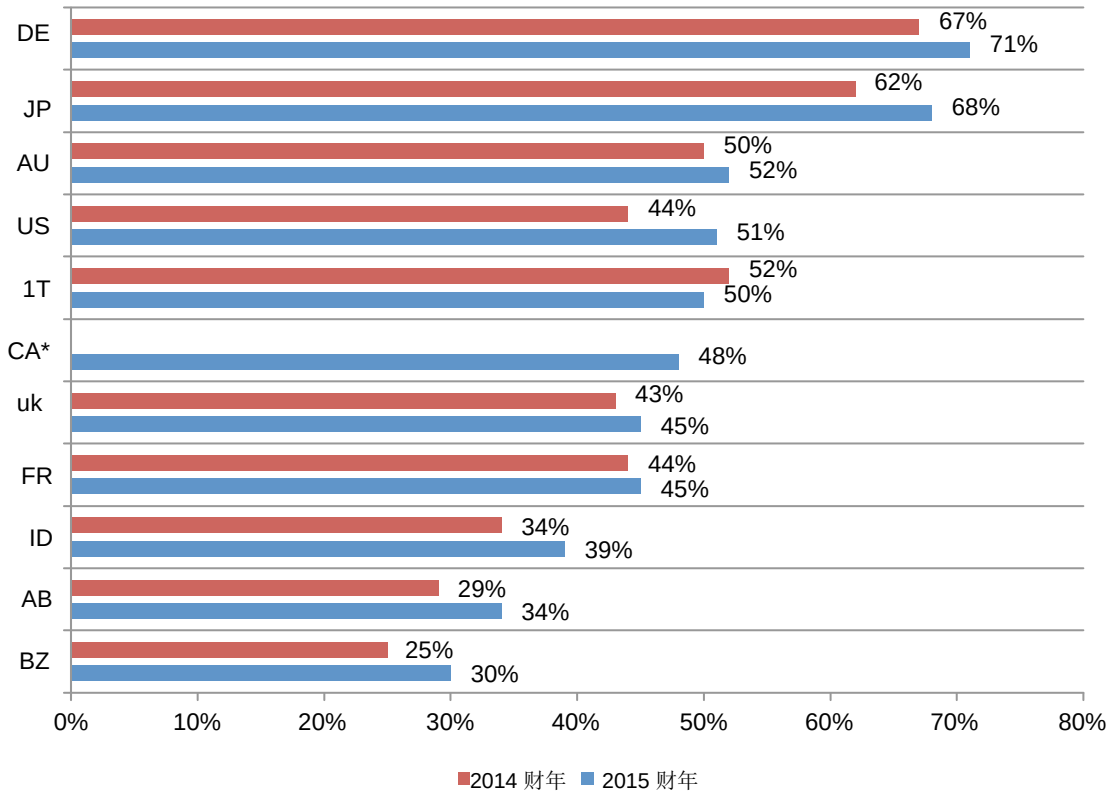


在处理数据泄露事件时，德国和日本最倾向于采用 BCM。图 8 显示了 11 个抽样国家在事件计划和执行过程中采用 BCM 工作组的百分比。与去年相似，德国 (DE) 的 BCM 采用率最高，有 71% 的德国公司报告说拥有 BCM 工作组。相比之下，仅有 30% 的巴西 (BZ) 公司采用 BCM。有趣的是，除意大利之外，在过去一年中所有国家的 BCM 采用率都出现了净增长。

图 8、各国采样 BCM 采用率

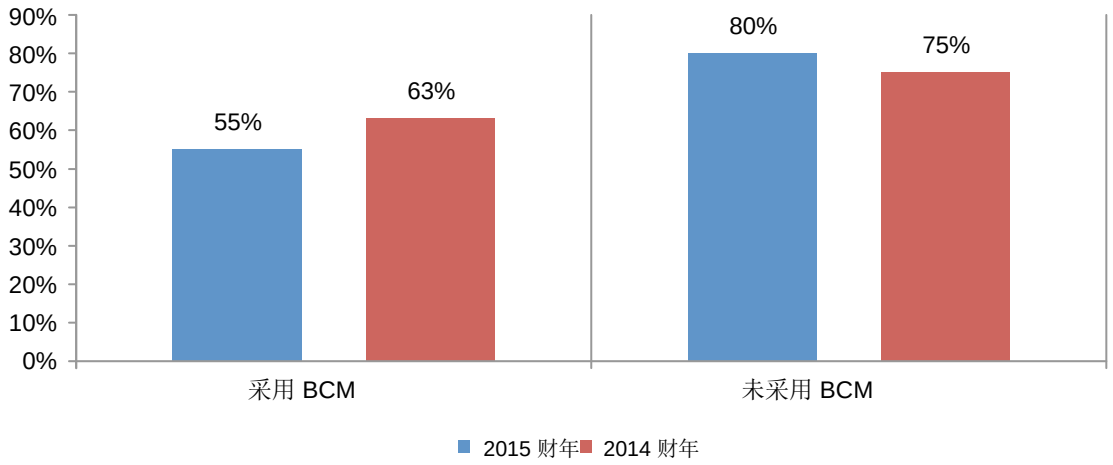
*无历史数据

（2015 财年 = 350，2014 财年= 315）



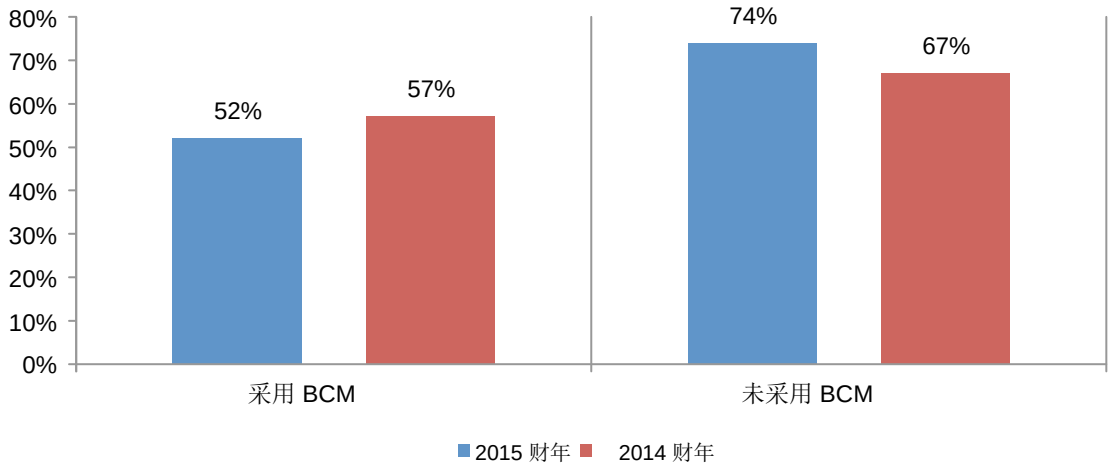
发生数据泄露时，BCM 能够最大程度降低业务运行中断。图 9 显示了采用 BCM 和未采用 BCM 的公司之间在业务程序实质性中断方面的差异。正如 2015 财年报告所示，未采用 BCM 的公司中有 80% 表示数据泄露事件引发了业务程序的实质性中断。然而，采用 BCM 的公司中仅有 55% 发生过实质性中断。这一结果与 2014 财年相似。

图 9、数据泄露事件是否会导致业务程序的实质性中断？
合并统计（2015 财年 = 350，2014 财年= 315）



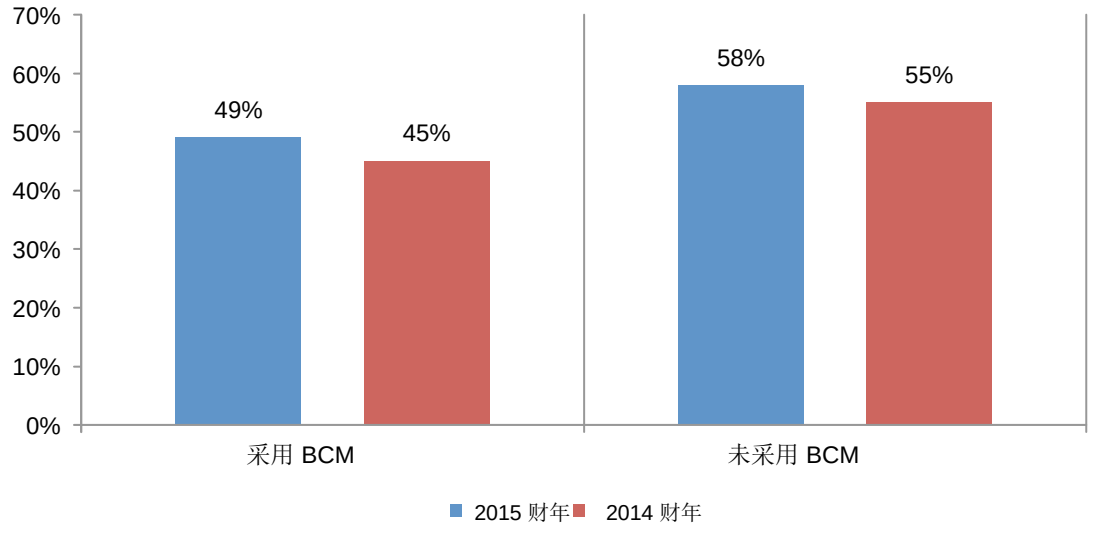
采用 BCM 能够提升 IT 运营的恢复力。与上图类似，图 10 显示了采用 BCM 和未采用 BCM 的公司之间在 IT 运营出现实质性中断方面的差异。正如 2015 财年的报告所示，未采用 BCM 的公司中有 74% 表示数据泄露事件引发了 IT 运营的实质性中断。相比之下，采用 BCM 的公司中仅有 52% 表示事件引发了实质性中断。这一结果与 2014 财年相似。

图 10、数据泄露事件是否导致 IT 运营出现实质性中断？
合并统计（2015 财年= 350，2014 财年= 315）



发生数据泄露事件后，BCM 能够保护公司声誉。图 10 也显示了采用 BCM 与未采用 BCM 的公司之间的差异。在本年度的调研中，未采用 BCM 的公司中有 55% 表示数据泄露对声誉和品牌存在实质性的负面影响。相比之下，采用 BCM 的公司中仅有 45% 表示数据泄露事件对企业声誉和品牌存在实质性的负面影响。这一结果与 2014 财年相似。

图 10、数据泄露是否对企业声誉存在实质性的负面影响？
合并统计（2015 财年= 350，2014 财年= 315）



第三部分：如何计算数据泄露成本？

为了计算数据泄露成本，我们采用了“基于活动的成本核算” (ABC) 方法。该方法识别活动后，根据实际利用情况分配成本。
要求参加此项基准调研的公司估算为解决数据泄露而进行所有活动的成本。

发现和立即响应数据泄露的典型活动包括以下内容：

- 进行调查研究和取证，确定数据泄露的根本原因；
- 确定数据泄露的可能受害者；
- 组成事件响应工作组；
- 进行沟通和公共关系外伸；
- 准备向数据泄露受害者和监管机构发出的通知文件及其他要求披露的内容；
- 实施呼叫中心程序和专门培训。

以下是发现数据泄露事件完结后进行的典型活动：

- 提供审计和咨询服务
- 提供防范法律服务
- 提供合规性法律服务
- 向数据泄露受害者提供免费服务或打折服务
- 提供识别保护服务
- 计算客户流失或营业额以确定损失的客户业务
- 支付客户获取和忠诚度方案费用

一旦公司估算出这些活动的成本范围，我们就根据如下定义将成本划分为直接成本、间接成本和机机会成本：

- *直接成本*——完成规定活动的直接费用支出。
- *间接成本*——付出的时间、努力及其他组织资源，但不作为直接现金支出。
- *机会成本*——在向受害者报告（和向媒体公开披露）数据泄露之后，因负面声誉影响导致业务机会损失而产生的成本。

我们的调研还考察了与带动大范围的企业数据泄露检测、响应、防范和补救的核心程序相关的活动。各项活动的成本参见“关键研究结果”部分（第二部分）。四个成本中心如下：

- 检测或发现：使公司能合理检测个人数据泄露风险（存储）或动态的活动。
- 上报：在给定时间内向相关人员报告受保护信息泄露情况的必要活动。
- 通知：使公司能够采用函件、出站电话、电子邮箱或一般通知的方式通知数据对象有关个人信息丢失或被窃情况的活动。
- 数据泄露后处理：帮助数据泄露受害者与公司沟通询问其他问题，或获得建议以实现潜在损害最小化的活动。数据泄露后活动也包括信用报告监测或重新开设账户（或信用卡）。

除以上程序相关活动之外，大多数的公司产生了与数据泄露事件相关的机会成本，结果导致现在和将来客户的信任或信心减少。相应地，我们研究所的研究显示，对数据泄露事件的负面宣传会影响声誉，这可能会导致营业额异常或费用流失，并可能会降低新客户获取率。

为了推断这些机会成本，我们采用了依赖于为各参与企业定义的平均客户“终生价值”这一成本估算方法。

- 既有客户营业收入：因数据泄露事件很可能会终止业务关系的客户的估计数量。损失扩大来自数据泄露事件造成的营业收入异常。所提供的数字为年度百分比，根据基准访问程序过程中管理层提供的估算值得出。[5]

- 客户获取率下降：因数据泄露而不会与企业发生业务关系的目标顾客的估计数量。所提供的数字为年度百分比。

我们证实，非客户数据损失，例如雇员记录，不会导致企业的客户流失或营业收入损失。[6] 在这种情况下，数据泄露不涉及客户或客户数据（包括付款交易信息）时，我们预期企业成本会更低。

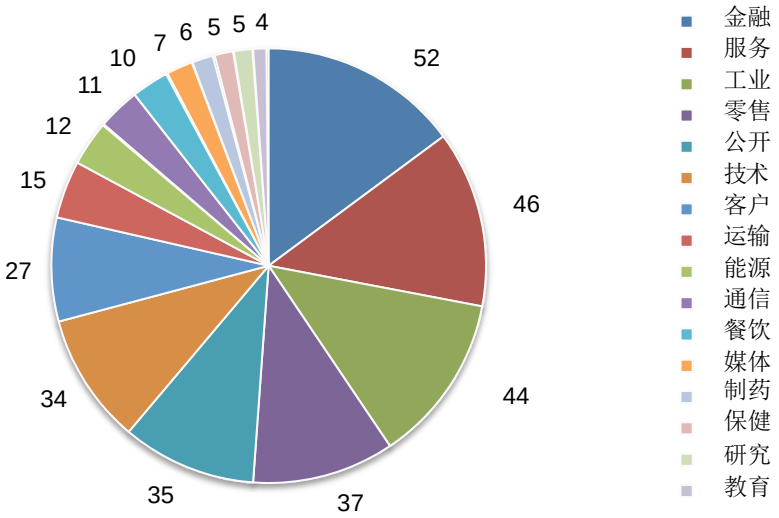
[5] 在某些情况下，营业收入是不完全的，数据泄露受害者仍然可能继续与数据泄露企业保持业务关系，但客户活动量实际上已经减少。这种局部下降在特定行业（例如金融服务或公共实体行业）中尤其突出，在这些行业中终止关系在成本上或经济上不可行

[6] 在此研究中，我们以公民、病人和学生信息为客户数据。

第四部分：机构特征和基准方法

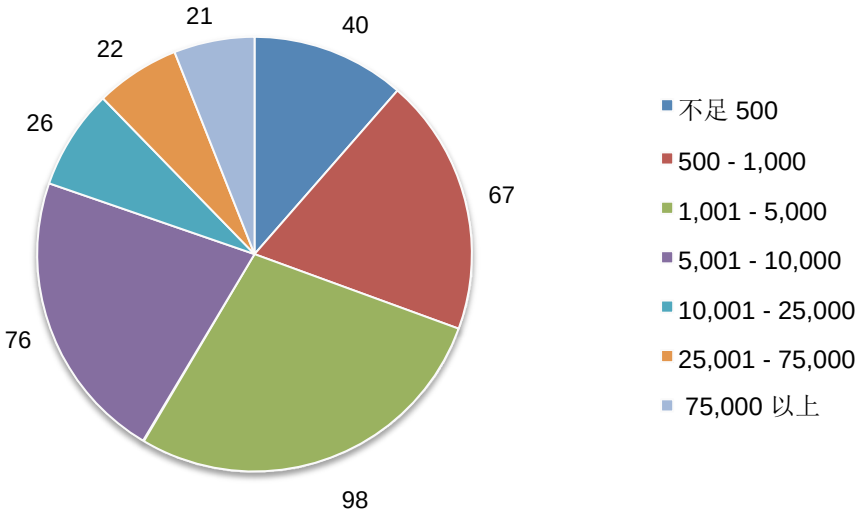
饼图 2 显示了按一级产业分类的基准机构分布情况。在今年的调研中，有 16 个行业参与。最大的领域是金融服务，包括银行、保险、投资管理付款处理程序。

饼图 2、按行业分类的基准采样分布情况
合并统计 (n = 350)



饼图 3 显示了按总人数统计的基准机构分布。占比最大的部分包括拥有 1000 多名员工的公司。

饼图 3、参与企业全球人数
合并统计 (n = 350)



数据收集方法不包括真实的会计信息，但依赖于根据每个参与者的认识和经历得出的数值计算。在每个类别中，成本估算都是一个两阶段程序。首先，基准工具要求个人对按照如下编号行格式中规定的范围变量标记的每个费用种类的直接成本进行估算。

如何采用编号行：每个数据泄露成本类别下提供的编号行是为了获得您对发生的现金支出、劳务和管理费之和的最佳估计。请在以上下限集和上限集之间某处的点上做标记。访问程序过程中的任何时候，您都可以重新设定编号行的下限和上限。

直接成本估算后（提供成本类别）

从编号行而非各成本类别点概算获得的数值视为机密，确保更高的响应速度。基准工具也要求专业人员分别提供对间接成本和机会成本的第二次估算。

为了保持基准程序规模易于管理，我们小心地把项目限制在数据泄露成本测量过程中认为至关紧要的中心活动成本方面。根据与博学专家的讨论，最终的项目集合包括作业成本不变集。一旦收集到基准信息，重新对每个工具的一致性和完整性进行仔细检查。

为了实现机密性，基准工具不收集任何具体的公司信息。主题材料不包含任何可能联系到参加公司响应的任何跟踪记号或其他方法。

基准工具中包含数据泄露成本项目的范围仅限于适用于处理个人信息企业经营主要集合的已知成本类别。我们认为，以业务程序为中心的研究而不专门考虑数据保护或隐私合规活动，将得出更好的结果质量。

第五部分：限制

我们的调研应用了机密和专利基准方法，已在初期调研中成功采用。但是，这项基准调研存在固有限制，在利用调研结果得出结论之前，需要认真考虑这些限制。

- 非统计结果：我们的调研总结的是在过去的 12 个月中经历了数据泄露事件涉及客户或客户记录丢失或失窃的全球机构的代表性非统计样本。如果我们的取样方法不科学，统计推论、误差幅度和置信区间将不适用于这些数据。

- 非响应：当前的调研结果是根据小规模的基准典型样品得出的。在此项全球分析中，350 家公司完成了基准程序。未进行非响应偏差检测，因此总是可能存在一种情况，那就是未参与调研的公司实质上潜在数据泄露成本不一致。

- 采样框架偏差：因为我们的采样框架是根据判断得出的，结果的质量受框架所代表的被调研公司的数量的影响。我们认为，当前的采样框架偏向于那些隐私或信息保密计划更成熟的公司。

- 具体的公司信息：基准信息是敏感的、机密的。因此，当前的工具不会收集公司识别信息。允许个人采用范畴响应变量披露有关公司和行业类别的人口统计信息。

- 不可测量因素：为了保持访问脚本简洁、集中，我们决定在分析中忽略其他一些重要的变量，例如主导趋势和机构特征。被忽略的变量对基准结果的影响程度无法确定。

- 推断得出的成本结果：基准调研的质量是根据参加公司中应答者提供的机密信息响应诚信程度得出的。基准程序中可纳入特定制衡，但应答者有可能不提供准确信息或真实响应。除此以外，采用成本推断方法而非实际成本数据可能意外地产生偏差和误差。

如有任何关于此调研报告的问题或意见，或希望获得文件附加拷贝（包括引用或重复采用此报告的批准），请通过信函、电话或电子邮件与我们取得联系：

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

请访问 **www.ibm.com/security/data-breach** 获得所有报告的完整副本。

波耐蒙研究所

推进信息责任管理

波耐蒙研究所致力于从事独立研究和发展教育事业，在企业和政府机构中推进信息责任和隐私管理实践。我们的使命是从事影响人与组织的敏感信息管理和安全性问题的高级实证研究。

作为**美国调查研究组织委员会 (CASRO)** 的成员，我们拥护严格的数据机密性、隐私和道德研究标准。我们不会从个人那里收集任何可以确认个人身份的信息（或在我们的业务研究中收集任何可以确认公司情况的信息）。此外，我们拥有严格的质量标准，确保不向调研对象询问任何无关的、不相关的或不适当的问题。

如想了解更多 IBM 业务连续性信息，请访问业务连续性主页。或拨打热线：400-810-1818 转 5169