2016 年数据泄露成本研究：全球分析

基准研究 - IBM 赞助
Ponemon Institute LLC 独立执行
2016 年 6 月

2016[1] 年数据泄露成本研究：全球分析

Ponemon Institute，2016 年 6 月

第 1 部分.简介

IBM 与 Ponemon Institute 携手发布 *2016 年数据泄露成本研究：全球分析*。我们的研究发现，参与本项研究的 383 家企业的平均数据泄露总成本从 379 万美元增至 400 万美元[2]。至于包含敏感和机密信息的记录，每条丢失或被盗记录的平均成本则从 2015 年的 154 美元增至今年研究中得出的 158 美元。

除了成本计算数据，我们的全球研究还对未来 24 个月企业发生一次或多次数据泄露的概率进行了研究。我们预计，26%的重大数据泄露会导致 10,000 条记录丢失或被盗。

全球研究一览

- 383 家企业（遍布 12 个国家/地区）
- 平均数据泄露总成本为 400 万美元
- 自 2013 年以来，数据泄露总成本增加了 29%
- 每条丢失或被盗记录的平均成本为 158 美元
- 自 2013 年以来，每条记录平均成本增加 15%

今年的研究发现，巴西和南非企业发生重大数据泄露（包含 10,000 条或更多的记录）的概率最高。相比之下，德国和澳大利亚企业发生重大数据泄露的概率最低。

今年，共有 383 家企业参与研究，分别位于以下 12 个国家/地区：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（阿拉伯联合酋长国和沙特阿拉伯）、加拿大和南非（首次参与本研究）。所有参与企业均遭遇过数据泄露，受损记录[3] 从 3,000 条到略高于 101,500 条不等。我们将“受损记录”定义为在数据泄露过程中丢失或被盗了单条信息的记录。

数据泄露成本研究揭示了七大全球性趋势

经过对 2,013 家各行各业的企业数据泄露经历的多年研究，揭示出以下七大趋势。

1. 自首次开展本研究以来，数据泄露成本的波动并不太大。因此表明这是一项固定的成本，企业必需妥善做好应对准备并将其纳入数据保护战略。

2. 对于发生数据泄露的企业而言，丢失业务才是最严重的经济后果。经历数据泄露后，企业必需采取各种措施来维持客户的信任，从而减轻长期的财政影响。

3. 大部分数据泄露仍由犯罪性的和恶意性的攻击所导致。检测和控制这些数据泄露所需的时间也最长。因此，每条记录的成本也最高。

4. 企业发现，检测和控制数据泄露所需的时间越长，解决数据泄露问题的成本就越高。我们的研究发现，历年的检测和上报成本均有所增加。这意味着急需进行技术和内部技能投资，从而缩短检测和控制数据泄露所需的时间。

[1]本报告标注的日期为出版年份日期，而非实地调查完成日期。请注意，当前报告研究的绝大部分数据泄露事件均发生在 2015 日历年。

[2]当地货币已换算为美元。

[3]在本报告中，“受损记录平均成本”和“每条记录平均成本”两个术语的含义相同。

5. 鉴于罚款影响，受监管行业（如医疗保健和金融服务）的数据泄露成本最高，在业务丢失和客户流失方面也高于平均值。

6. 改进数据治理计划将有助于降低数据泄露成本。事故响应计划、CISO 任命、员工培训和意识计划以及业务持续性管理战略可进一步节约成本。

7. 投资开展某些数据丢失防护控制和活动（如加密和端点安全解决方案）对于防范数据泄露非常重要。今年的研究发现，鉴于企业参加了威胁共享体系并且部署了数据丢失防护技术，因此成本有所下降。

以下是一些最显著的企业发现和影响：

美国和德国的数据泄露成本最高，巴西和印度最低。美国的数据泄露每条记录平均成本为 221 美元，德国为 213 美元。巴西（100 美元）和印度（61 美元）的数据泄露成本最低。美国的企业平均总成本为 701 万美元，德国为 501 万美元。印度（160 万美元）和南非（187 万美元）的企业成本最低。

不同行业的数据泄露成本有所不同。每次丢失或被盗记录的全球平均数据泄露成本为 158 美元。但是，医疗机构的平均成本为 355 美元，教育业的平均成本为 246 美元。运输业（129 美元）、科研领域（112 美元）和公共部门（80 美元）的丢失或被盗记录平均成本最低。

黑客与内部犯罪分子是最主要的数据泄露制造者。今年的研究表明，48% 的泄露由恶意的或犯罪攻击所导致。缓解相关攻击的平均记录成本为 170 美元。相比之下，系统故障的平均记录成本为 138 美元，人为错误或疏忽的平均记录成本为 133 美元。美国和加拿大企业在缓解恶意或犯罪攻击方面花费的成本最高（分别为 236 美元/记录和 230 美元/记录）。印度的成本远低于此（76 美元/记录）。

不同国家/地区的恶意或犯罪攻击大不相同。60% 的阿拉伯地区数据泄露和 54% 的加拿大数据泄露均由黑客和内部犯罪分子所导致。而在南非地区，仅有 37% 的数据泄露是恶意攻击所导致的。与此相反，南非企业的人为错误数据泄露比例最高，印度企业的数据泄露则主要由系统故障或业务流程故障（分别占 37% 和 35%）所导致。

通过事故响应团队以及广泛使用加密来降低数据泄露成本。事故响应团队将每记录数据泄露成本降低了 16 美元，从 158 美元直降至 142 美元。然而，因第三方参与而导致的数据泄露却使每记录成本增加了 14 美元，从 158 美元增至 172 美元。

各种测量值揭示了数据泄露成本增加的原因。平均数据泄露总成本增加 5.4%，每条记录平均成本或记录成本增加 2.9%。数据泄露平均规模（丢失或被盗记录数）增加 3.2%。
非正常客户流失增加 2.9%，因而界定为大于正常业务运营中的预期客户流失。

客户流失增加了数据泄露成本。发生数据泄露后，某些国家/地区在保留客户方面会面临更多问题，因而成本会有所增长。法国、日本和意大利均在此列。巴西、南非和印度等国的客户流失率最低。流失率最高的行业包括金融业、医疗业和服务业。

某些国家/地区和行业更容易流失客户。法国的流失率依然最高，日本紧随其后。公共行业和零售业的非正常流失或流动率最高。尽管样本数较少对于推断各行业的客户流失率影响具有一定的阻碍作用，但金融、医疗和服务机构的非正常流失相对较高，而公共部门和教育机构的非正常流失则相对较低。

丢失的记录越多，数据泄露的成本越高。今年对 383 家企业的研究发现，数据泄露成本介于 210 万美元（丢失记录在 10,000 条以下）至 670 万美元（丢失或被盗记录在 50,000 条以上）之间。

加拿大的检测和上报成本最高，印度成本最低。与检测和上报相关的数据泄露成本主要用于取证和调查活动、评估和审计服务、危机团队管理及高管和董事会沟通。加拿大的平均检测和上报成本为 1.60 美元。相比之下，平均成本仅为 0.53 美元。

美国的告知成本最高。业务丢失成本是指非正常的客户流动，不仅会抬高客户获取活动的成本、损害信誉，还会有损商誉。美国成本为 0.59 美元，印度成本为 0.02 美元。

美国和德国的数据泄露后期响应成本最高。美国的数据泄露后期响应和检测相关成本为 1.72 美元，德国则为 1.54 美元。事后成本包括技术支持活动、入站通信、专项调查活动、补救措施、法律开支、产品折扣、身份保护服务以及监管干预。

美国企业数据泄露后的客户损失成本最高。美国企业的业务丢失成本非常高 （3.97 美元）。其成本构成包括非正常的客户流动、客户获取活动成本上升、信誉损害及商誉降低。

阿拉伯地区的直接成本最高，美国的间接成本最高。直接成本是指为完成给定活动（如聘请取证专家、雇用律师事务所或提供受害者身份保护服务）所需的直接开支。间接成本则是解决数据泄露问题期间耗费的时间、精力和其他组织资源。其中包括员工在数据泄露通知工作或事故调查过程中提供的协助。间接成本还包括商誉损害和客户流失。阿拉伯地区的直接成本最高 (57%)，美国的间接成本最高 (66%)。

某些国家/地区更容易发生数据泄露。在过去的三年中，这项研究一直对企业发生一次或多次数据泄露的概率进行调查。据估计，巴西和南非发生数据泄露的概率似乎最高。德国和澳大利亚发生数据泄露的概率最低。

识别并控制数据泄露所需的时间会对成本造成影响。第二年我们的研究展示了企业识别并控制数据泄露事故的速度与经济后果之间的关系。识别和控制恶意以及犯罪攻击所需的时间均最高（分别为 229 天和 82 天），识别和控制人为错误导致的数据泄露则要低得多（分别为 162 天和 59 天）。

数据泄露成本常见问题解答

本项研究的目的是什么？我们的目标是量化数据泄露的经济影响，并观察成本的变化趋势。我们认为，更好地了解成本以及影响成本的根源和因素有助于企业确定在防范或消除攻击后果时所需的合适投资和资源。

什么是数据泄露？数据泄露是指可能导致个人姓名以及病历和/或财务记录或借记卡信息面临风险的事件—这些记录可以是电子的或纸质格式的。在我们的研究中，我们共发现了导致数据泄露的三个主要原因：恶意或犯罪攻击、系统故障或人为错误。根据原因以及发生数据泄露后采取的保护措施，数据泄露成本可能有所不同。

什么是受损记录？我们将“记录”定义为在数据泄露过程中信息丢失或被盗的自然人（个人）的信息。例如零售企业的数据库，其中包括个人姓名及相关借记卡信息和其他个人身份信息。或者，也可能是医疗保险公司的投保人记录（包含医师和付款信息）。今年的研究发现，若发生某条记录丢失或被盗，为企业带来的平均成本为 158 美元

如何收集数据？Ponemon Institute 研究员在 10 个月内进行了 1,500 多次独立访谈，收集了深入的定性数据。自 2015 年 1 月起开始招募 2016 年研究企业，最终于 2016 年 3 月完成了访谈工作。在这 383 家参与企业中，我们分别与精通企业数据泄露及缓解泄露相关成本的 IT、合规和信息安全从业人员进行了交流。为保护隐私，我们未收集任何企业特定的信息。

如何计算成本？为计算数据泄露平均成本，我们需要采集企业产生的直接和间接开支。直接开支包括聘请取证专家、外包热线支持，以及针对未来的产品和服务提供无条件信用监控订阅和折扣。间接成本包括内部调查和沟通，以及客户流动或客户获取率降低所导致的客户损失外推值。

基准研究与调查研究之间有何区别？*数据泄露成本*研究的分析单位是企业。本项调研的分析单位则是每条记录。我们招募了 383 家企业参与本项研究。数据泄露的受损记录从 3,000 条一直到略大于 101,500 条。

可不可以使用数据泄露平均成本计算大规模泄露（如包含数百万条丢失或被盗记录的泄露事件）的经济后果？在我们的研究中，数据泄露平均成本不适用于灾难性或大规模数据泄露（如 Sony），因为这些并非是大部分企业所经历的典型数据泄露行为。为了反映全球企业的总体特征，得出在受保护信息丢失或被盗后了解相关成本时所使用的研究结论，我们未在分析中包含 100,000 条以上受损记录的大规模数据泄露事件。

每年对一组相同的企业进行跟踪吗？每年研究所涵盖的企业样本各不相同。换句话说，我们不会一直跟踪同一组企业。为了保持一致，我们会招募并匹配具有类似特征的企业，如企业所处的行业、员工人数、地理区域及数据泄露规模。自 2015 年启动本项研究开始，我们对全球 2,013 家企业的数据泄露经历进行了研究。

全球一览

今年的研究面向以下 12 个国家/地区开展：美国、德国、加拿大、法国、英国、意大利、日本、澳大利亚、阿拉伯地区、巴西、印度和南非（首次参与研究）。共有 383 家企业参与了本次研究。通过 12 份独立报告展现国家/地区特定结果。

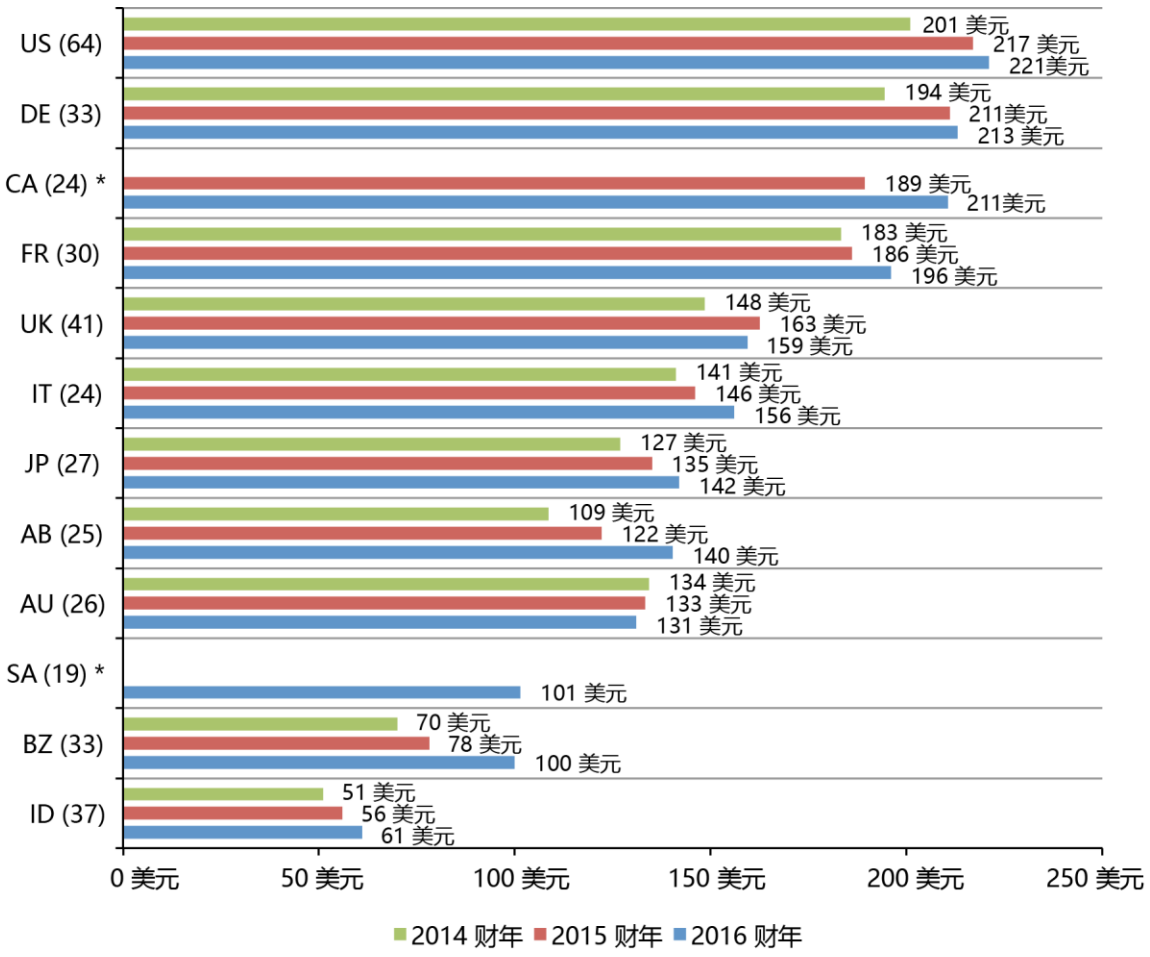
图 1 展示了三年来 12 个国家/地区数据泄露的平均每条记录成本（单位：美元）。如图所示，不同国家/地区样本之间的差异很显著。[4] 各个国家/地区的综合平均每条记录成本为 158 美元，而去年的平均成本则为 154 美元（不包括南非）。美国和德国的每条记录平均成本依然最高，分别为 221 美元和 213 美元。印度和巴西的成本最低，分别为 61 美元和 100 美元。

图 1.三年数据泄露的平均每条记录成本

总平均成本：2016 财年 = 158 美元，2015 财年 = 154 美元，2014 财年 = 145 美元

*并非所有年份均有历史数据（2016 财年 = 383，2015 财年 = 350，2014 财年 = 315）

单位：美元



[4] 每条记录平均成本是指数据泄露总成本除以数据泄露规模（即丢失或被盗的记录数）。

第 2 部分.主要发现

在本部分中，我们将介绍本次研究的详细发现。按如下顺序展示主题：

- 全球和行业数据泄露成本差别
- 引发数据泄露的根本原因
- 影响数据泄露成本的因素
- 受损记录出现频率和客户流动或流失趋势
- 数据泄露成本构成趋势
- 企业发生数据泄露的概率
- 识别并控制数据泄露所需的平均时间
- 业务持续性管理对数据泄露成本的影响

下表列出了本项全球研究使用的 12 个国家/地区、图例、样本大小和货币。另外，还显示了各个国家/地区年度报告涵盖的年限数，从 1 年（南非）到 11 年（美国）不等。

表 1.全球研究一览

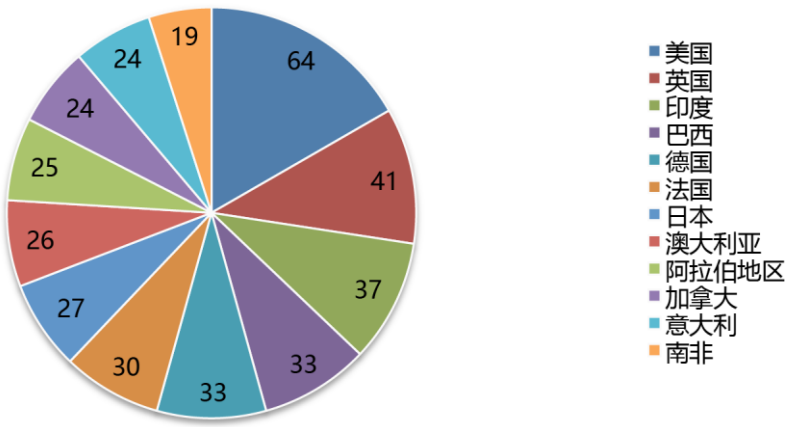
图例	国家/地区	样本	占比	货币	研究年限
AB	阿拉伯地区*	25	7%	阿联酋迪拉姆/沙特	3
AU	澳大利亚	26	7%	澳元	7
BZ	巴西	33	9%	雷亚尔	4
CA	加拿大	24	6%	加元	2
DE	德国	33	9%	欧元	8
FR	法国	30	8%	欧元	7
ID	印度	37	10%	卢比	5
IT	意大利	24	6%	欧元	5
JP	日本	27	7%	日元	5
SA	南非	19	5%	兰特	1
UK	英国	41	11%	英镑	9
US	美国	64	17%	美元	11
	总计	383	100%		

*阿拉伯地区 (AB) 是指沙特阿拉伯和阿拉伯联合酋长国的综合企业样本。

下图展示了 12 个国家/地区的 383 家参与企业的分布情况。从中可以看出，美国所占的比例最大（64 家企业），南非的样本数最少（19 家企业）。

饼图 1.基准样本出现频率（按国家/地区划分）

(n=383)



全球和行业数据泄露成本差别

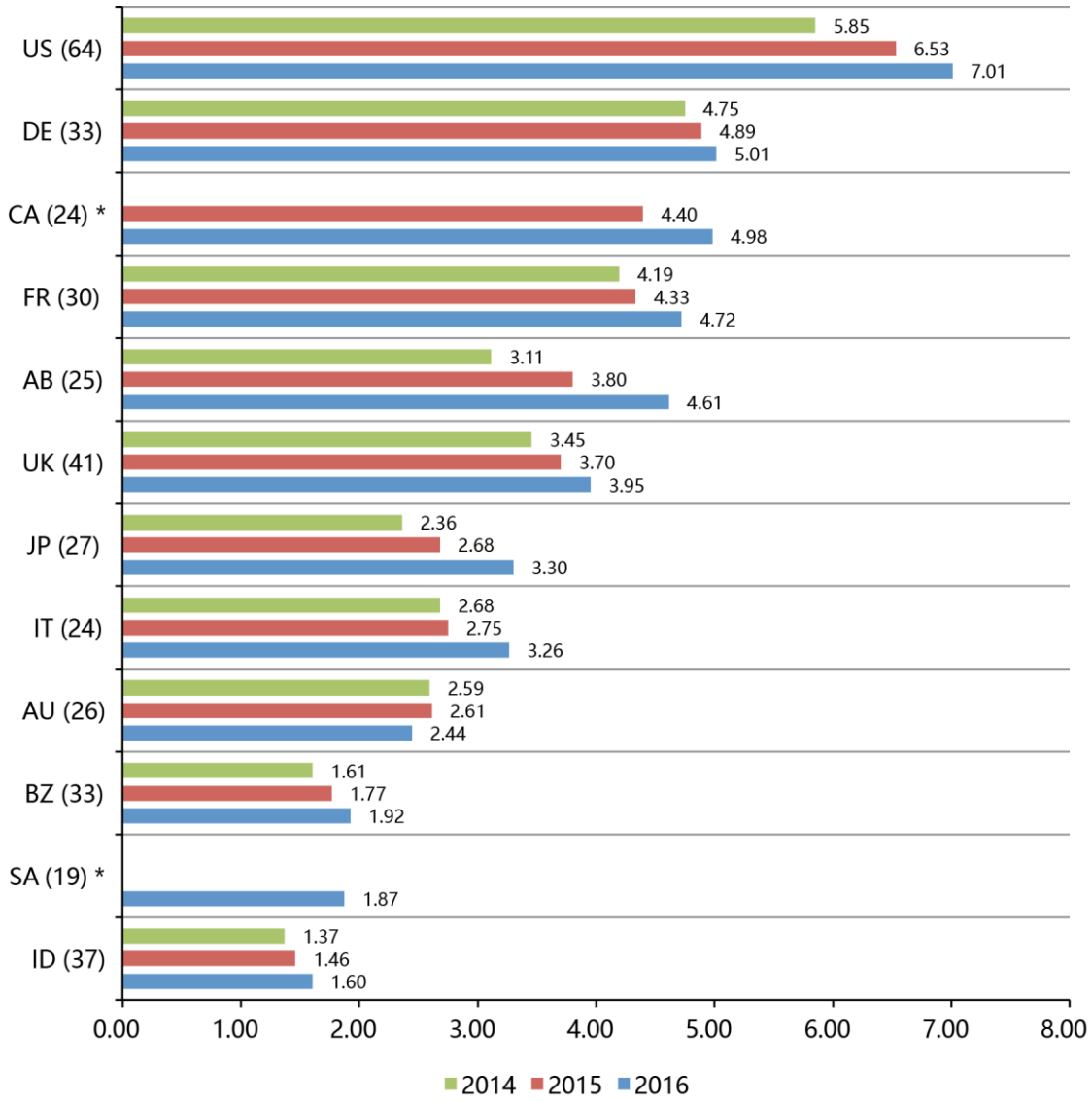
不同国家/地区的平均企业数据泄露成本有所不同。图 2 展示了今年研究的 12 个国家/地区的数据泄露总平均成本。除了澳大利亚和南非，与去年相比，所有国家/地区的总平均成本均有所增加。美国样本的总平均成本最高，价值超过 701 万美元；德国紧随其后，价值为 501 万美元。相比之下，印度和南非企业的总平均成本最低，分别为 160 万美元和 187 万美元。

图 2.三年数据泄露的企业总平均成本

总平均成本：2016 财年 = 4.0，2015 财年 = 3.8，2014 财年 = 3.50

*并非所有年份均有历史数据（2016 财年 = 383，2015 财年 = 350，2014 财年 = 315）

单位：美元（百万）

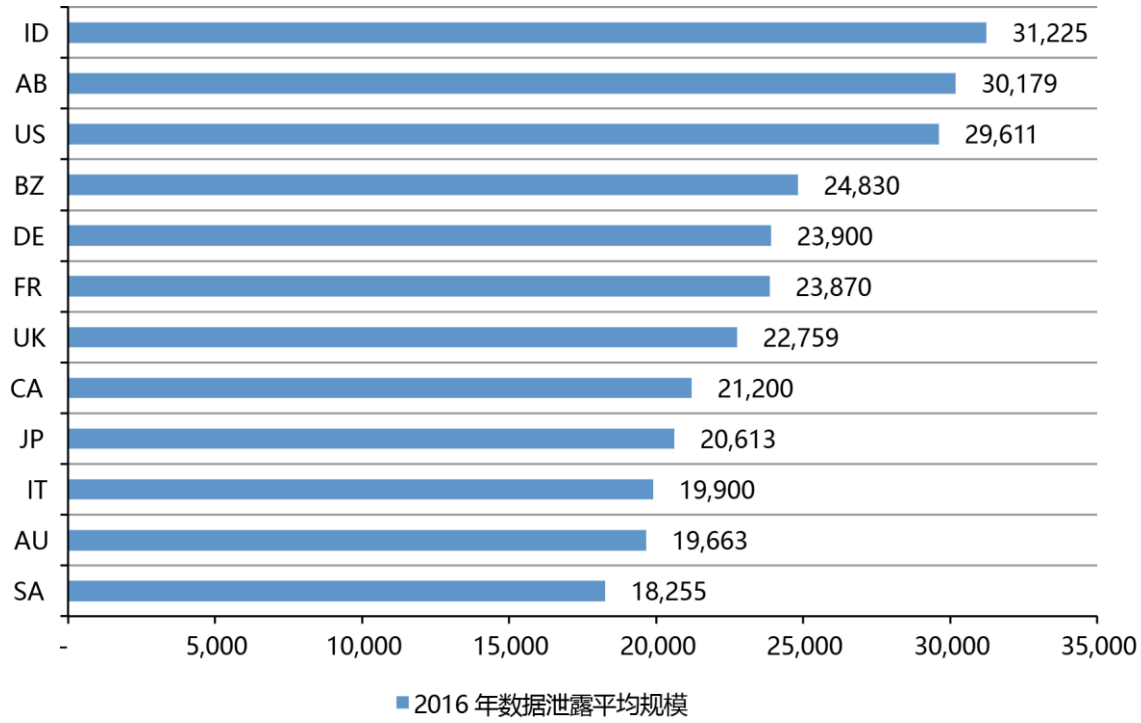


被泄露的或受损记录数。图 3 报告了本项研究展示的 12 个国家/地区的企业数据泄露平均规模。如图所示，印度、阿拉伯地区和美国企业的丢失或被盗记录平均数最高。南非的丢失或被盗记录平均数最低。在本报告中，我们还展现了丢失或被盗的记录数与数据泄露成本之间的关系。

图 3.泄露记录平均数（按国家/地区划分）

全球平均数 = 23,834

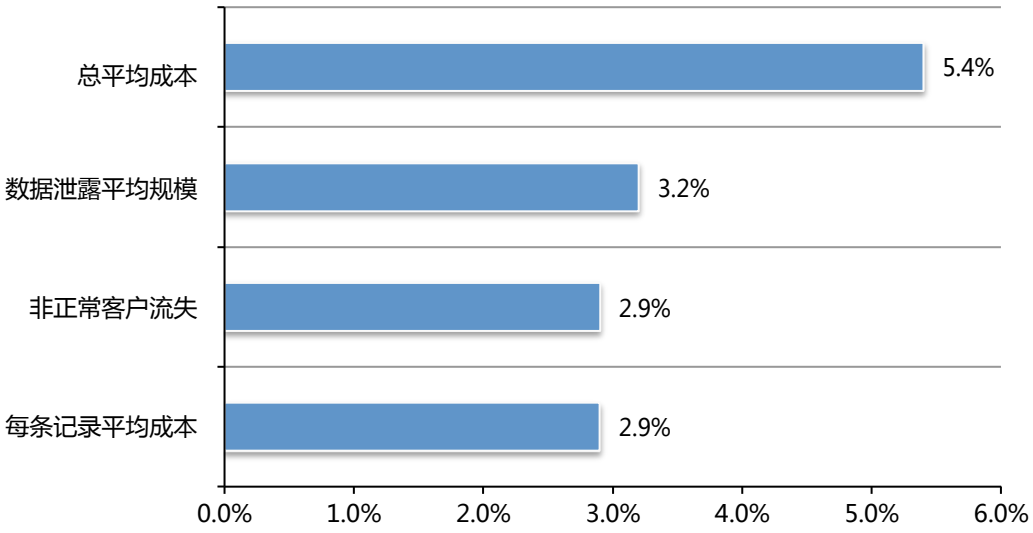
(n=383)



各种测量值揭示了数据泄露成本增加的原因。图 3 展示了四个指标，说明了数据泄露成本增加的原因。平均数据泄露总成本增加 5.4%，每条记录平均成本或记录成本增加 2.9%。数据泄露平均规模（丢失或被盗记录数）增加 3.2%。非正常客户流失增加 2.9%。非正常客户流失是指大于正常业务运营中的预期客户流失。

图 3.数据泄露成本度量

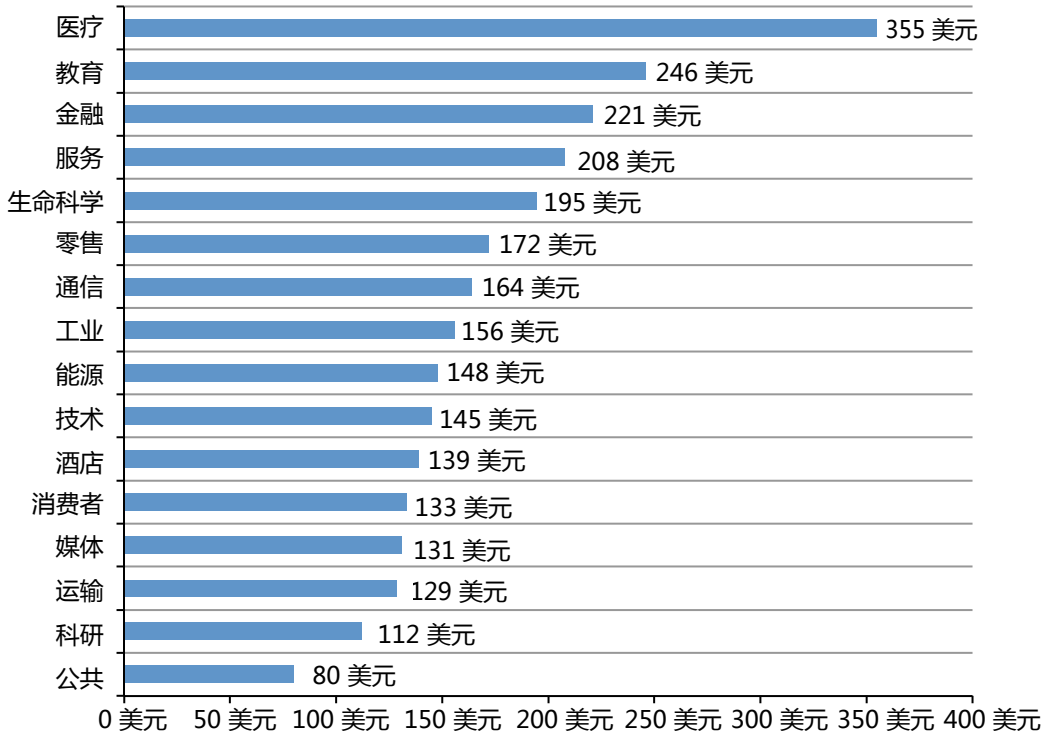
统一视图 (n=383)



某些行业的数据泄露成本较高。图 4 报告了统一样本的每条记录平均成本（按行业划分）。受到严格监管的行业（如医疗、教育和金融企业）的每条记录平均数据泄露成本远高于 158 美元的整体平均值。公共部门、科研和运输机构的每条记录平均成本则低于整体平均值。

图 4.每条记录平均成本（按行业划分）

统一视图 (n=383)；单位：美元

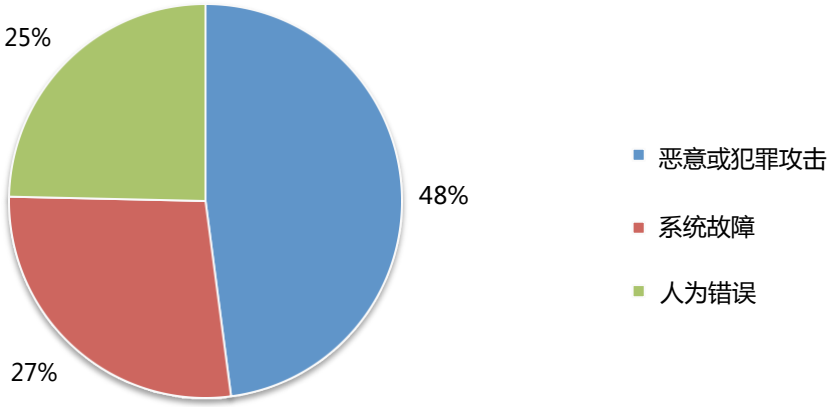


导致数据泄露的根本原因

绝大部分数据泄露由恶意或犯罪攻击导致。[5]饼图 2 从整体上对研究中展示的全部 12 个行业的数据泄露主要根源进行了概括说明。48% 的事故涉及恶意或犯罪攻击，25% 因员工或承包商疏忽（人为错误）导致，另有 27% 的事故涉及系统故障（包括 IT 和业务流程故障）。[6]

饼图 2.基准样本分布状况（按数据泄露根源划分）

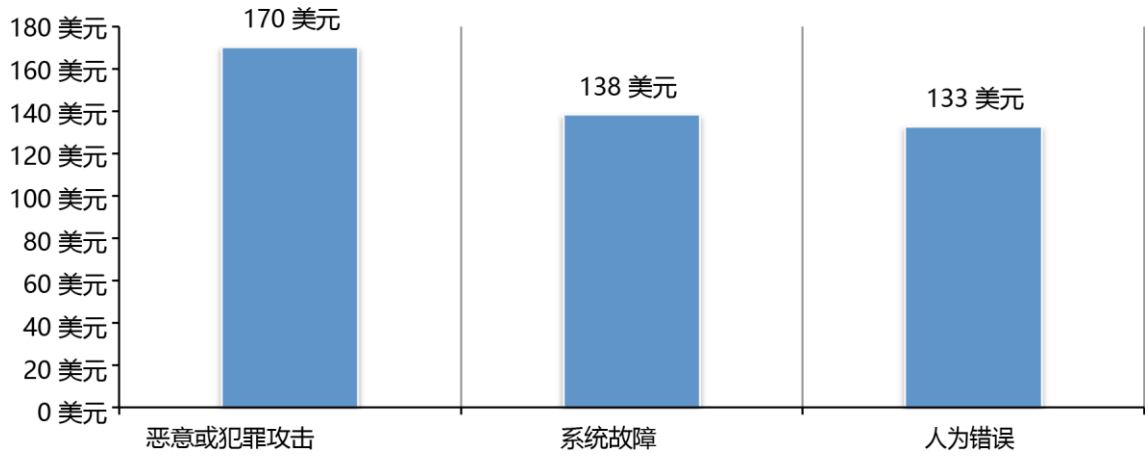
统一视图 (n=383)



恶意攻击在全球范围内带来的损失较高。图 5 报告了三大数据泄露事件根源的数据泄露每条记录平均成本。2016 年，恶意或犯罪攻击引发的数据泄露成本高达 170 美元，远高于系统故障和人为因素造成的数据泄露每条记录平均成本（分别为 138 美元和 133 美元）。

图 5.三大数据泄露根源的每条记录平均成本

统一视图 (n=383)；单位：美元



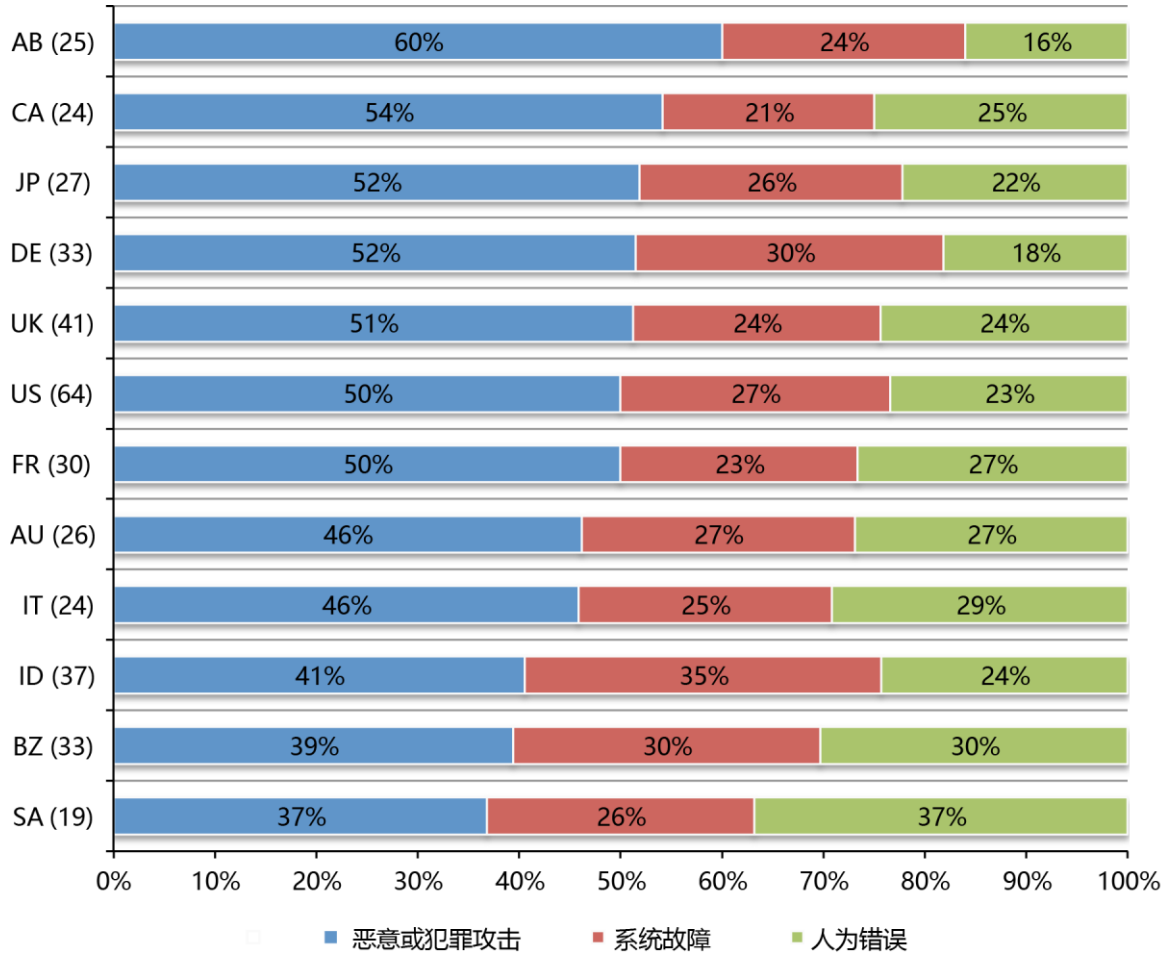
[5]疏忽的内部人员是指因个人粗心大意导致数据泄露的个人,如数据泄露事后调查中所定义的。恶意攻击可能由黑客或内部犯罪分子（员工、承包商或其他第三方）引发。

[6]最常见的恶意或犯罪攻击类型包括恶意软件感染、内部犯罪分子、网络钓鱼/社交工程和 SQL 注入。

国家/地区数据泄露根源的差别。图 6 显示了 12 个国家/地区样本的主要数据泄露根源。60% 的阿拉伯地区企业最可能遭受恶意或犯罪攻击。相比之下，南非和巴西企业遭受此类数据泄露的概率最低。与此相反，南非企业的人为错误数据泄露比例最高，印度企业的数据泄露则主要由系统故障或业务流程故障所导致。

图 6.基准样本分布状况（按数据泄露根源划分）

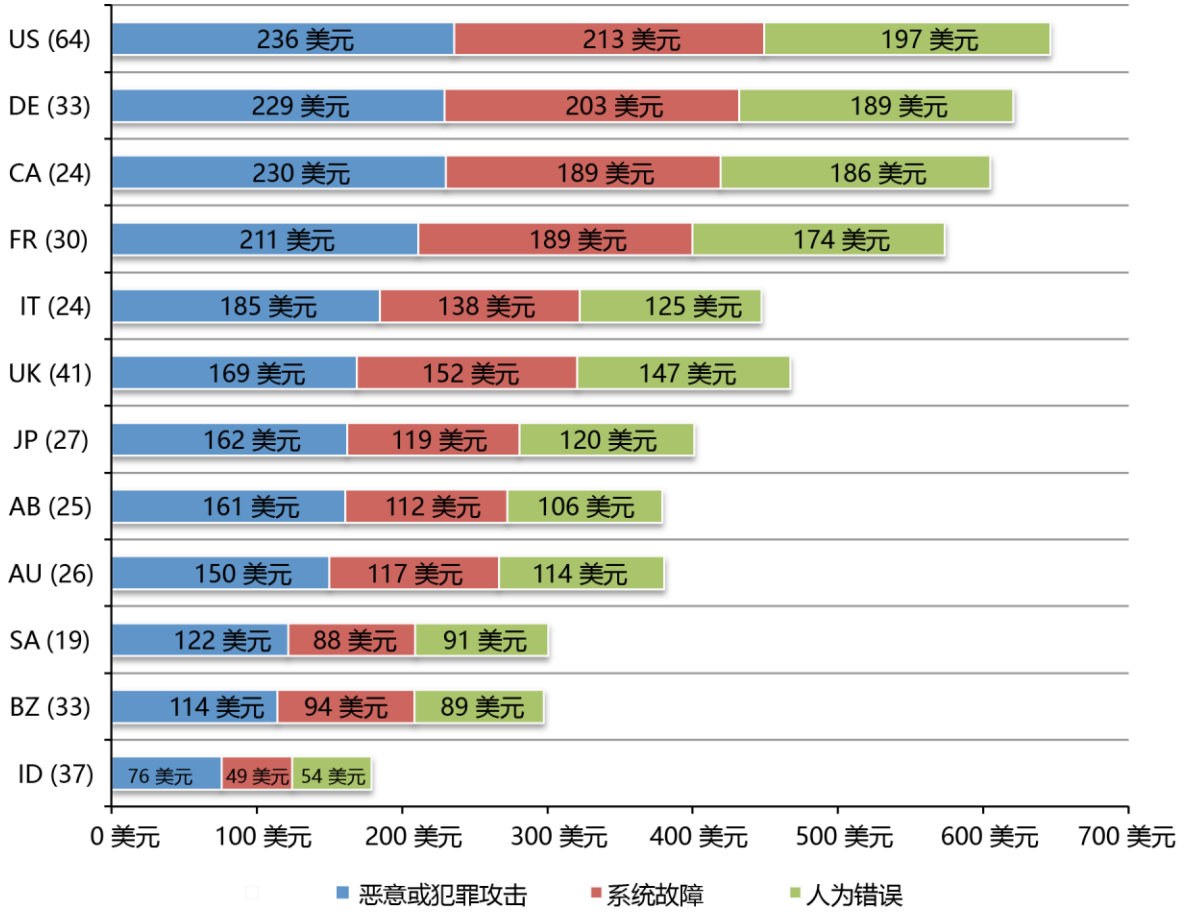
(n=383)



不同国家/地区三大根源的每条记录平均成本有所不同。图 7 按照国家样本报告了三大数据泄露根源的每条记录平均成本。相关结果清晰地表明，恶意或犯罪攻击导致的数据泄露成本始终高于系统故障或人为错误导致的成本。另外，本图表明不同国家/地区的样本差异很大。更确切地说，在美国，每条受损记录的恶意或犯罪数据泄露事故成本为 236 美元。而印度的每条记录平均成本仅为 76 美元。

图 7.三大根源的每条记录平均成本

(n=383)



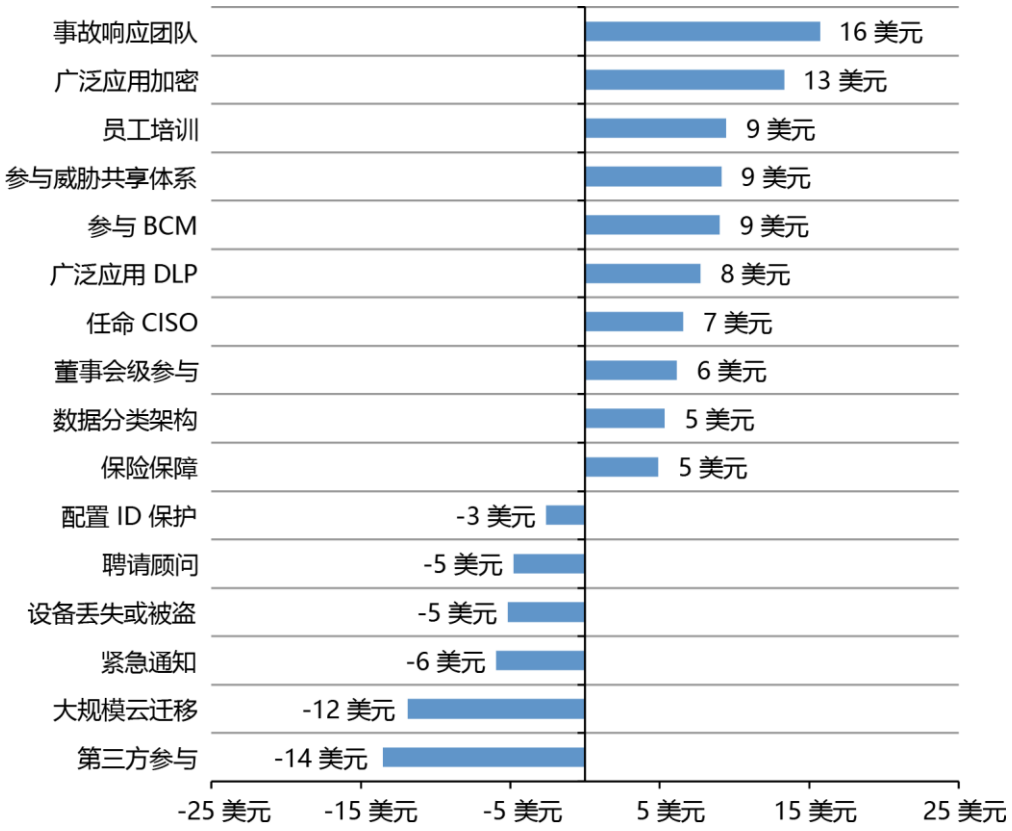
影响数据泄露成本的因素

某些因素会降低数据泄露的成本。图 8 提供了会增加或降低数据泄露时每条记录平均成本的 16 项因素。如图所示，事故响应团队、广泛应用加密、员工培训、参与威胁共享体系或业务持续性管理均有助于降低数据泄露时每条记录平均成本。

第三方参与事故、大规模云迁移、紧急通知或设备丢失或被盗所引发的数据泄露则会增加泄露的每条记录平均成本（显示为负数）。例如，事故响应团队将数据泄露成本降低了 16 美元，从 158 美元直降至 142 美元。然而，第三方参与导致数据泄露的成本增加 14 美元，从 158 美元增至 172 美元。

图 8.16 项因素对于数据泄露时每条记录平均成本的影响

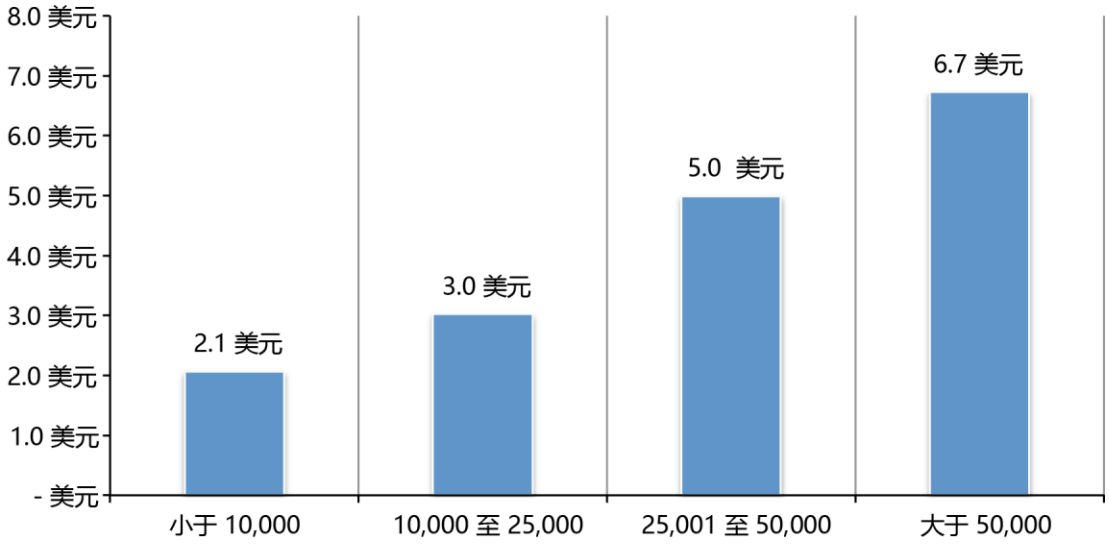
统一视图 (n=383)；单位：美元



受损记录的出现频率和客户流动趋势

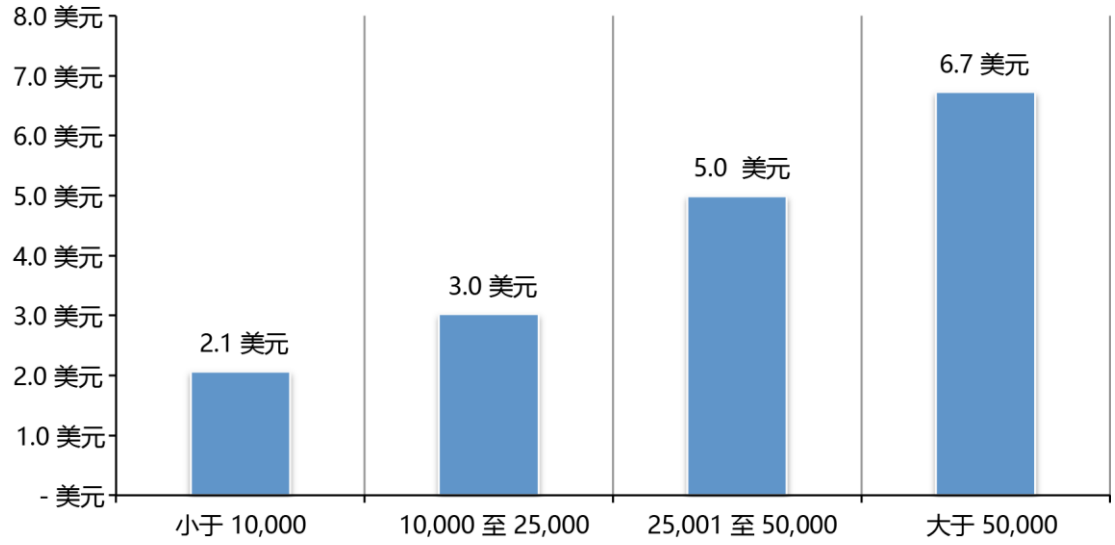
丢失的记录越多，数据泄露的成本越高。图 9 显示了 383 家企业数据泄露总成本与事故规模之间的关系（按泄露事故的规模升序排列）。今年的研究显示，成本介于 210 万美元至 670 万美元之间。

图 9.总成本（按数据泄露的规模划分）
统一视图 (n=383)；单位：百万美元



客户流失越大,数据泄露时每条记录平均成本越高。图 10 报告了 383 家企业数据泄露时每条记录平均成本分布状况（按非正常客户流失率升序排列）。现有客户流失低于 1% 的企业其平均数据泄露成本为 270 万美元；倘若现有客户流失率超过 4%，则平均成本将跃升至 550 万美元。

图 10.数据泄露总成本（按非正常客户流失率划分）
统一视图 (n=383)；单位：百万美元

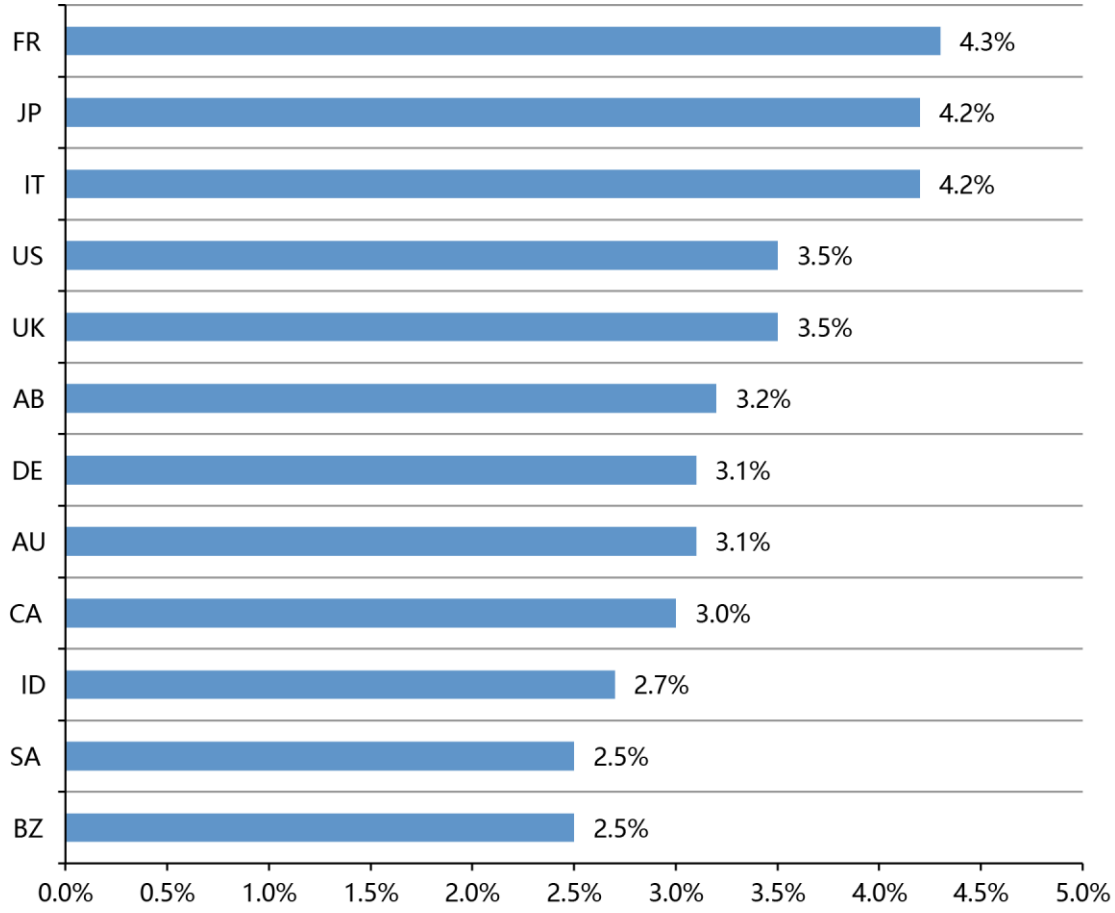


某些国家/地区更容易流失客户。图 11 报告了本项研究展示的 12 个国家/地区的平均非正常客户流失率。结果表明，不同国家/地区之间存在显著的差异。法国的流失率依然最高，日本紧随其后。公共行业和零售业的非正常流失或流动率最高。

这一发现表明，流失率较高的国家/地区企业可重点开展客户保留活动，维护声誉和品牌价值，从而大幅降低数据泄露成本。

图 11.三年非正常流失率（按国家/地区样本划分）

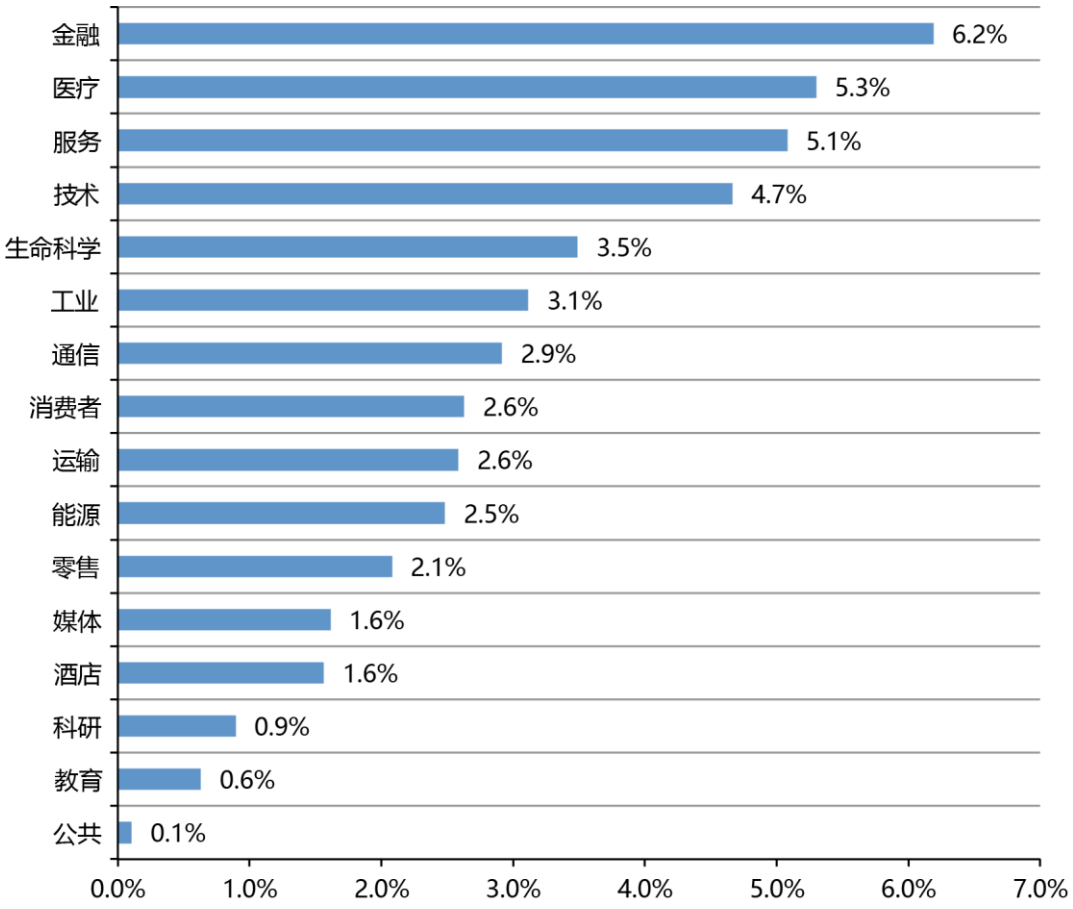
(n = 383)



某些行业更容易流失客户。图 12 报告了 2016 年度基准企业的非正常流失率。尽管样本数较少对于推断各行业的客户流失率影响具有一定的阻碍作用，但金融、医疗和服务机构的非正常流失相对较高，而公共部门和教育机构的非正常流失则相对较低。[7]

图 12.非正常流失率（按基准企业的行业分类划分）

(n = 383)



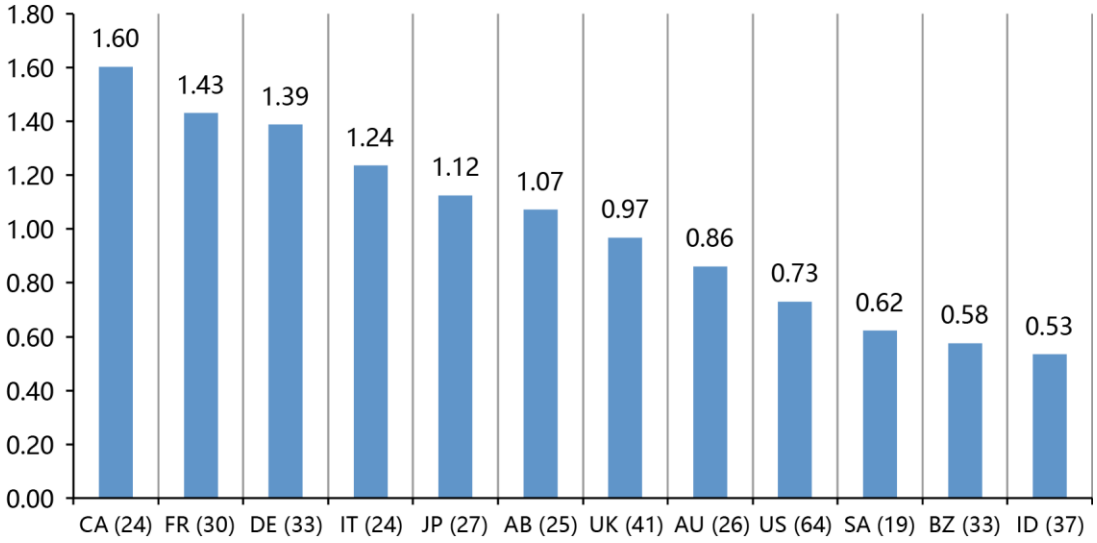
[7]鉴于政府机构客户通常别无选择，因此公共机构采用另外一种流失框架。

数据泄露成本构成趋势

加拿大的检测和上报成本最高，印度成本最低。与检测和上报相关的数据泄露成本主要用于取证和调查活动、评估和审计服务、危机团队管理及高管和董事会沟通。如图 13 所示，加拿大的平均检测和上报成本为 1.60 美元。相比之下，印度平均成本仅为 0.53 美元。

图 13.检测和上报成本

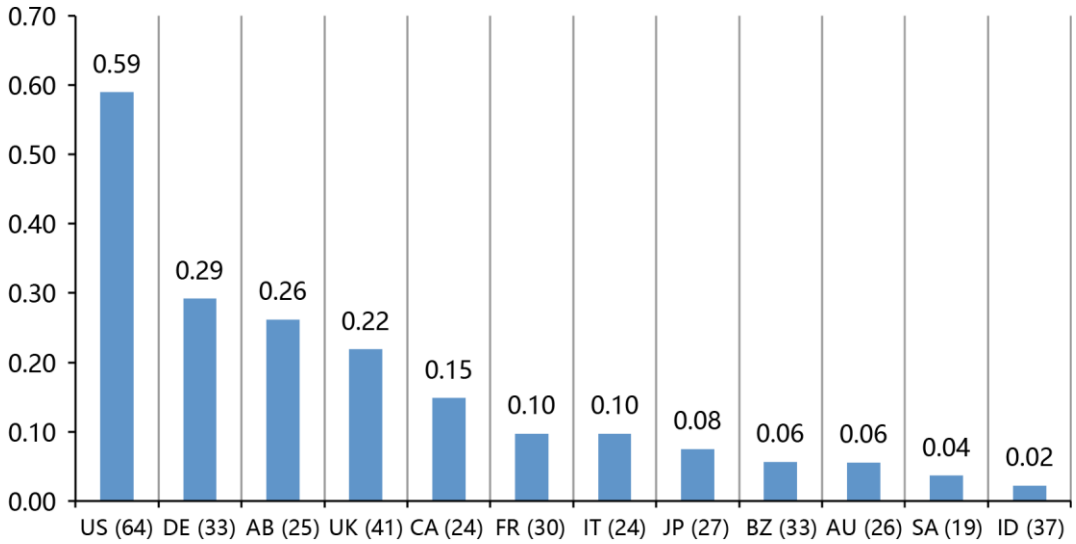
(n = 383)；单位：美元（百万）



美国的告知成本最高。通知相关活动包括与创建联系人数据库、确定各类监管要求、聘请外部专家、邮政开支、电子邮件反弹及入站通信建立有关的 IT 活动。目前美国企业的通知成本最高（0.59 美元），如图 14 所示。

图 14.告知成本

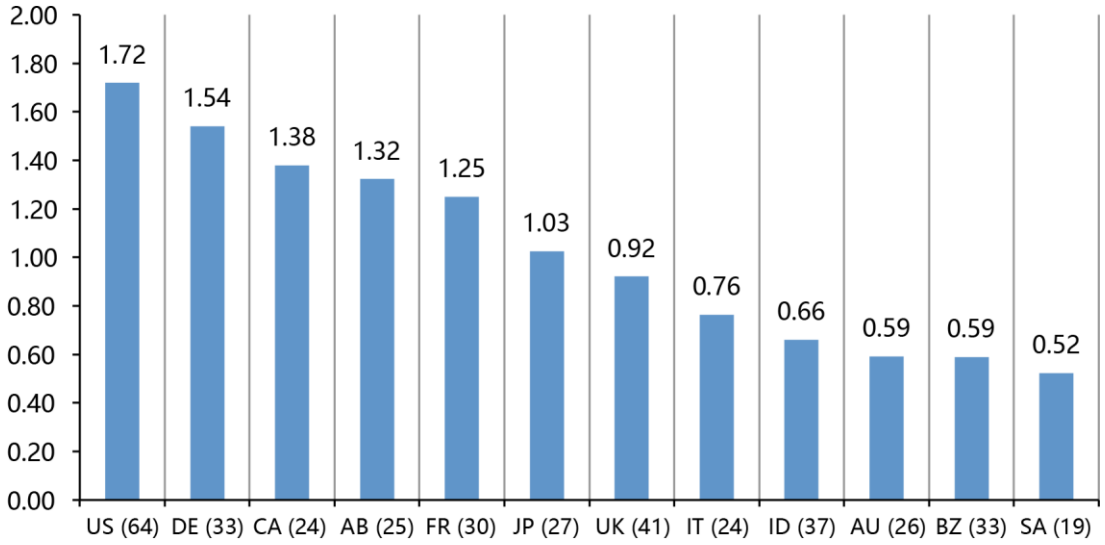
(n = 383)；单位：美元（百万）



美国和德国的数据泄露后期响应成本最高。美国的事后响应和检测相关成本为 1.72 美元，德国则为 1.54 美元,如图 15 所示。事后成本包括技术支持活动、入站通信、专项调查活动、补救措施、法律开支、产品折扣、身份保护服务及监管干预。

图 15.事后响应成本

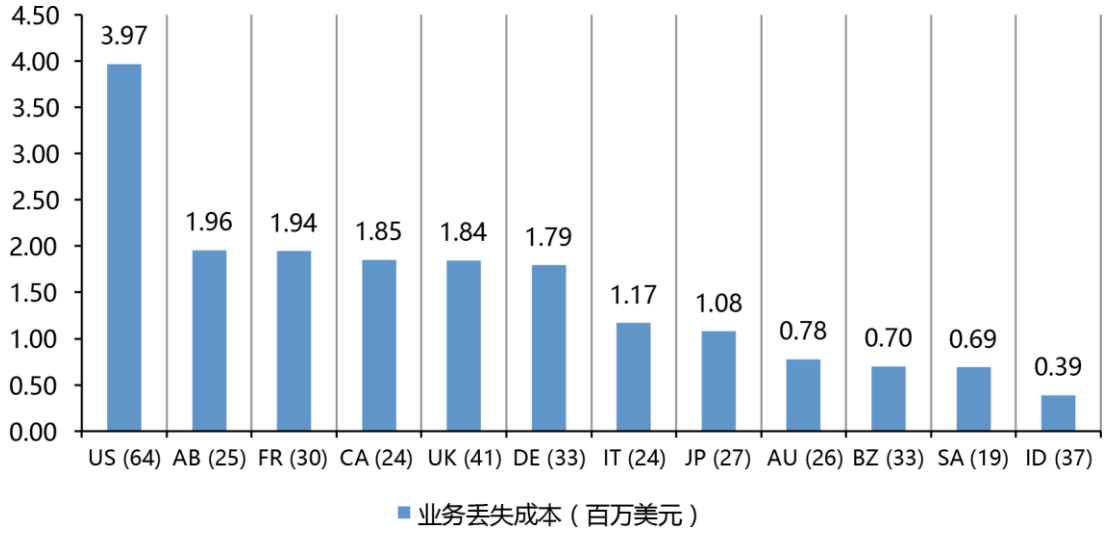
(n = 383)；单位：美元（百万）



美国企业数据泄露后的客户损失成本最高。图 16 表明,美国企业的业务丢失成本尤其高（3.97）。其成本构成包括非正常的客户流动、客户获取活动成本上升、信誉损害及商誉降低。

图 16.业务丢失成本

(n = 383)；单位：美元（百万）



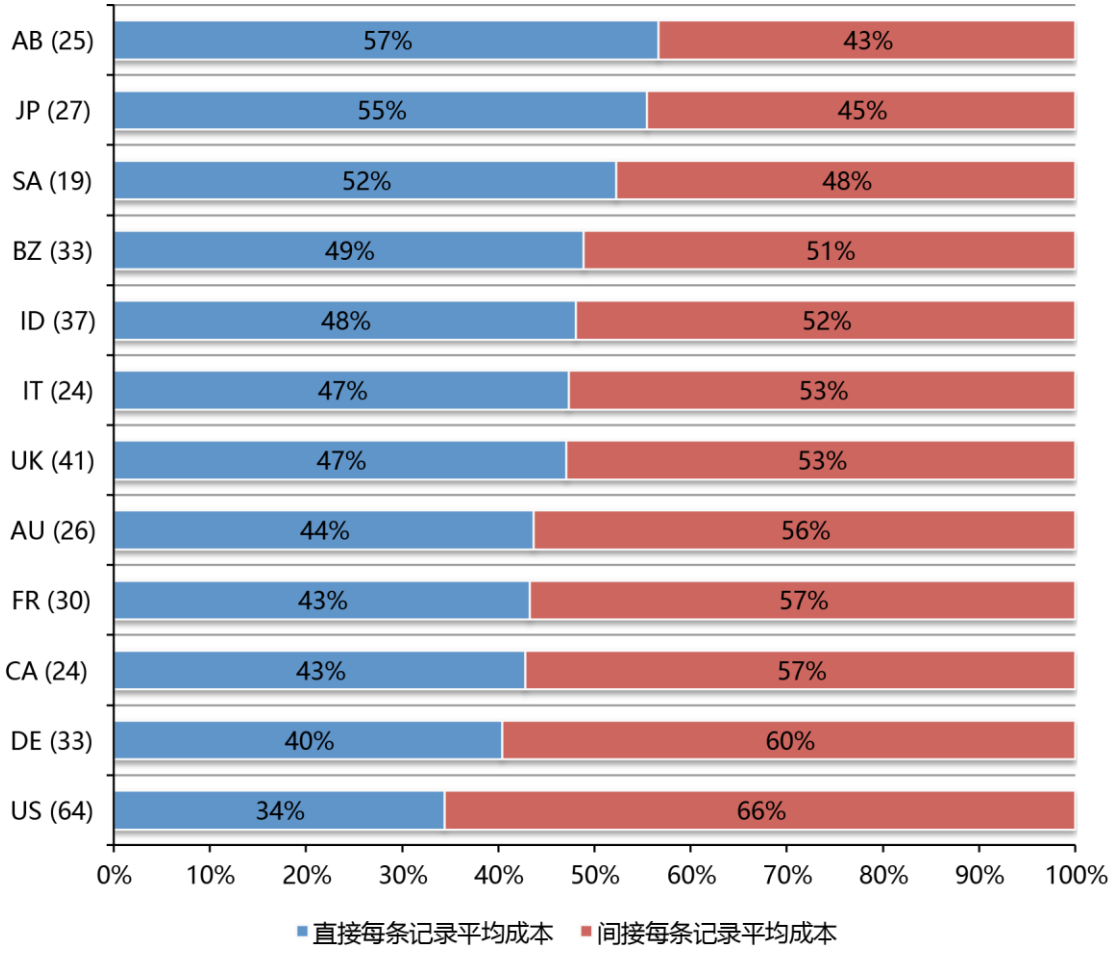
不同国家/地区的直接和间接数据泄露成本比例有所不同。

阿拉伯地区的直接成本最高，美国的间接成本最高。直接成本是指为完成给定活动（如聘请取证专家、雇用律师事务所或提供受害者身份保护服务）所需的直接开支。间接成本则是解决数据泄露问题期间耗费的时间、精力和其他组织资源。其中包括利用现有员工帮助开展数据泄露通知工作或事故调查。间接成本还包括商誉损害和客户流失。

图 17 报告了全部 12 个国家/地区的直接和间接数据泄露的每条记录平均成本比例。阿拉伯地区的直接成本最高 (57%)，美国的间接成本最高 (66%)。

图 17.直接和间接数据泄露的每条记录平均成本比例

统一视图 (n=383)



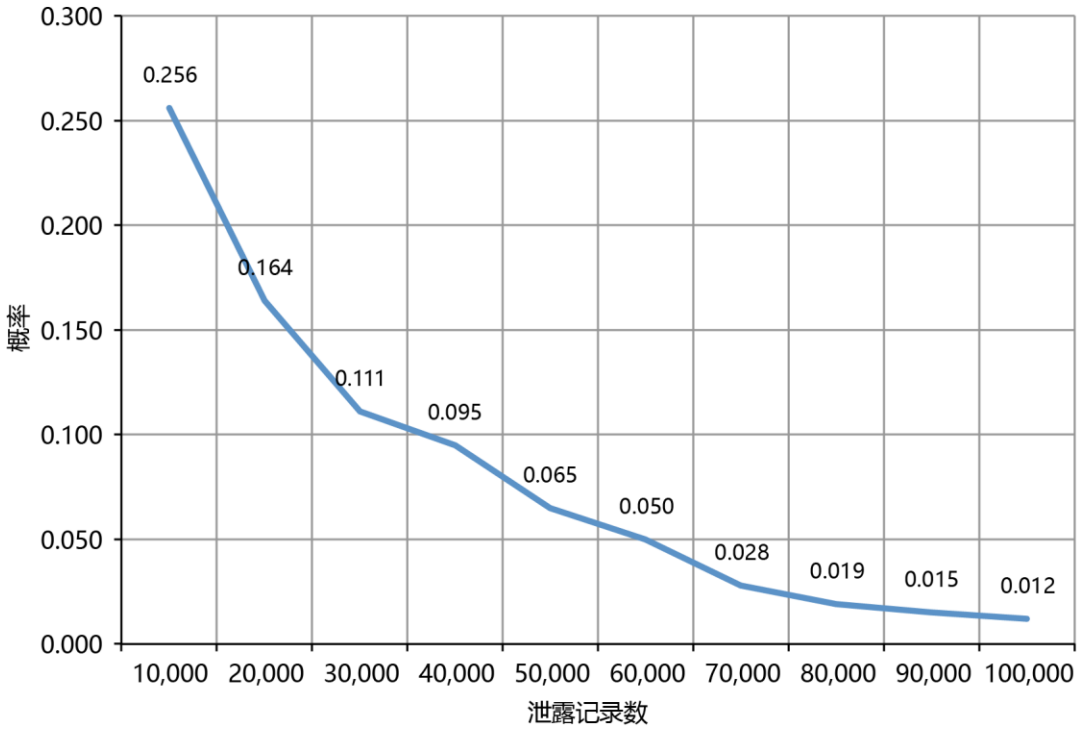
企业发生数据泄露的概率

我们的研究对未来 24 个月发生一项或多项数据泄露的概率进行了分析。根据研究中掌握的企业经验，我们相信我们可以根据以下两项因素预测数据泄露概率：丢失或被盗的记录数和企业所属行业。

图 18 显示了发生 10,000 至 100,000 条受损记录的数据泄露事故的主观概率。[8] 从中可以看出，随着规模的增加，数据泄露的发生概率稳步降低。预计未来 24 个月发生包含 10,000 条记录（最低规模）的数据泄露的概率约为 26%，发生包含 100,000 条记录的数据泄露的概率不足 1%。

图 18.发生包含 10,000 至 100,000 条记录的数据泄露的概率

统一视图 (n=383)



[8]估算的概率是采用点估计技术通过受访者样本中采集得到。主要人员（如参与成本评估访谈的 CISO 或 CPO）对 10 级数据泄露事故（10,000 到 100,000 条丢失或被盗记录）的数据泄露概率进行了估计。此估算任务中使用的时间范围是未来 24 个月。我们对 383 家参与企业的总概率分布状况分别进行了推断。

某些国家/地区的企业更容易发生数据泄露。图 19 对参与本项研究的 12 个国家/地区发生数据泄露（最低包含 10,000 条记录）的概率进行了汇总。尽管样本数较少对我们推断国家/地区差异具有一定的阻碍作用，但不同国家/地区估算得出的重大数据泄露概率差异很大。

据估计，巴西和南非发生数据泄露的概率似乎最高。德国和澳大利亚发生数据泄露的概率最低。

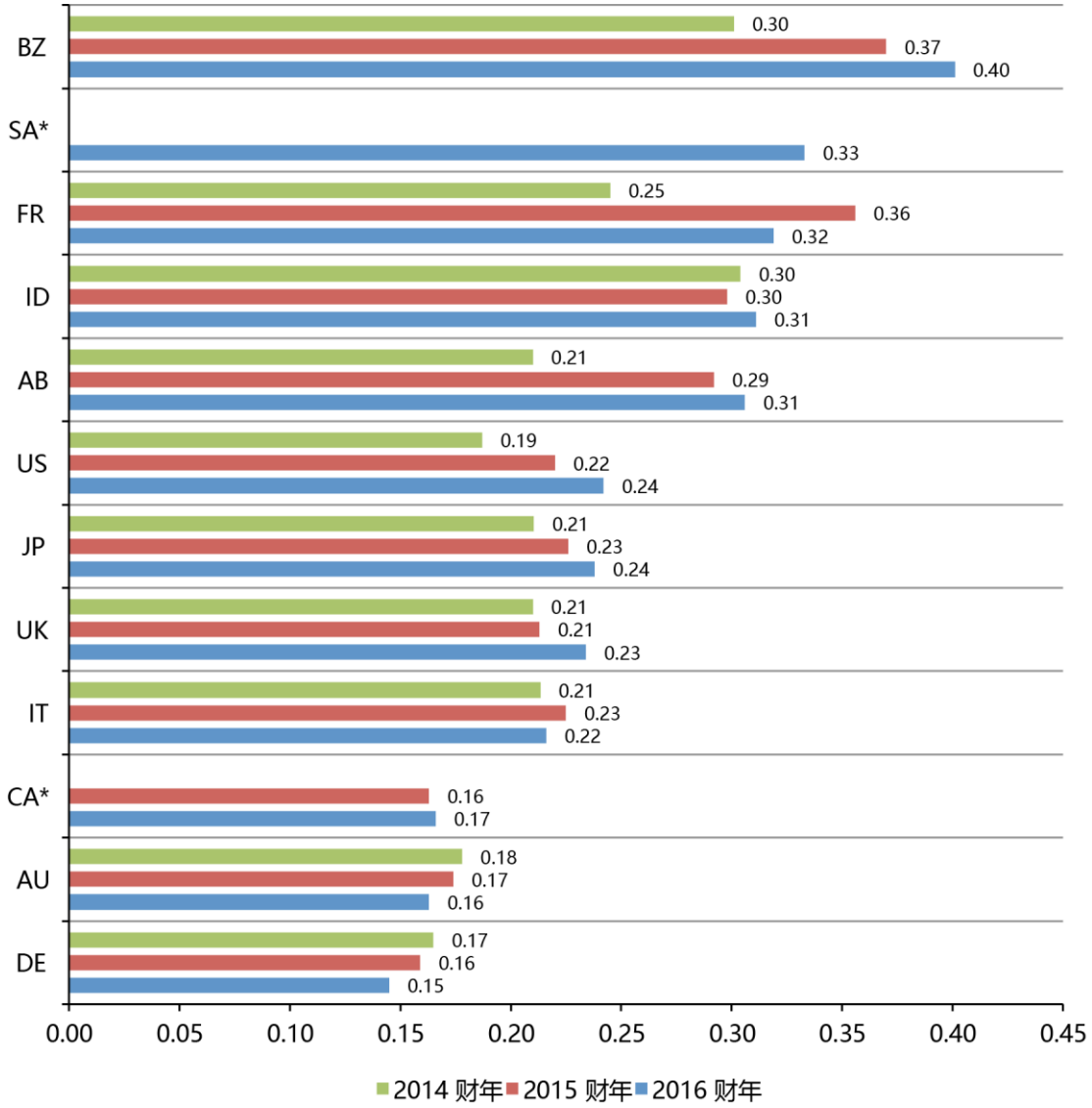
图 19.发生包含 10,000 条记录的数据泄露的概率（按国家/地区划分）

总平均概率 = 25.6%

最低 10,000 条受损记录

*并非所有年份都有历史数据

统一视图（2016 财年 = 383，2015 财年 = 350，2014 财年 = 315）



识别并控制数据泄露所需的时间会对成本造成影响

平均识别时间 (MTTI) 和平均控制时间 (MTTC) 指标用于确定企业实施事故响应及控制流程的有效性。MTTI 指标旨在帮助企业了解需多长时间才能检测到已发生的事故，而 MTTC 指标则用于测量响应小组解决问题并最终恢复服务正常运行所需的时间。

图 20 提供了数据泄露的平均识别时间 (MTTI) 和平均控制时间 (MTTC) 数据。根据 383 家企业的综合样本，估算出的平均识别时间为 201 天，时间范围介于 20 至 569 天。平均控制时间 70 天，时间范围介于 11 至 126 天。

图 20.数据泄露事故的平均识别时间和平均控制时间（单位：天）

统一视图 (n = 383)

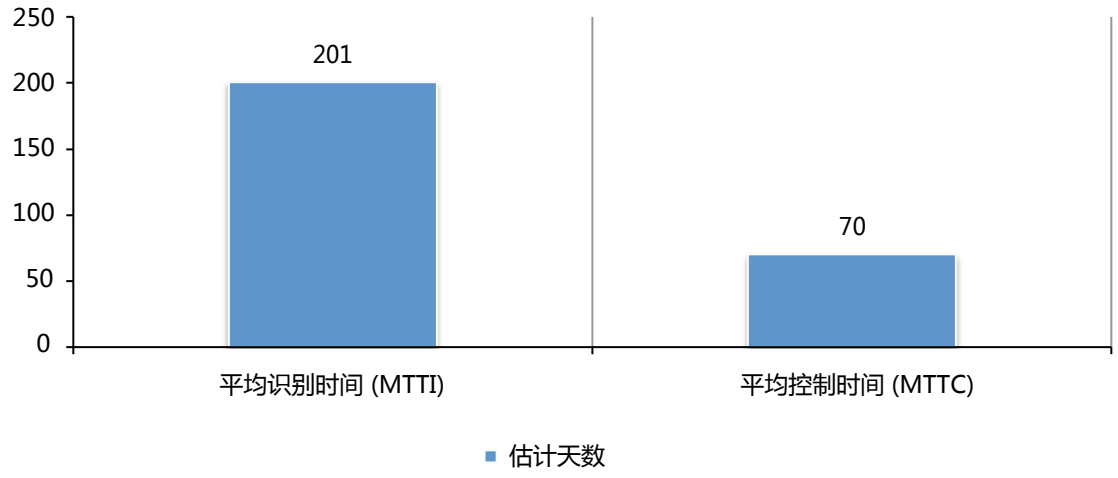


图 21 提供了三大数据泄露事故根源的 MTTI 和 MTTC。如图所示，恶意犯罪攻击的识别时间和控制时间均最高（分别为 229 天和 82 天），人为错误导致的数据泄露成本则低得多（分别为 162 天和 59 天）。

图 21.数据泄露事故的平均识别时间和平均控制时间（按根源划分；单位：天）

统一视图 (n = 383)

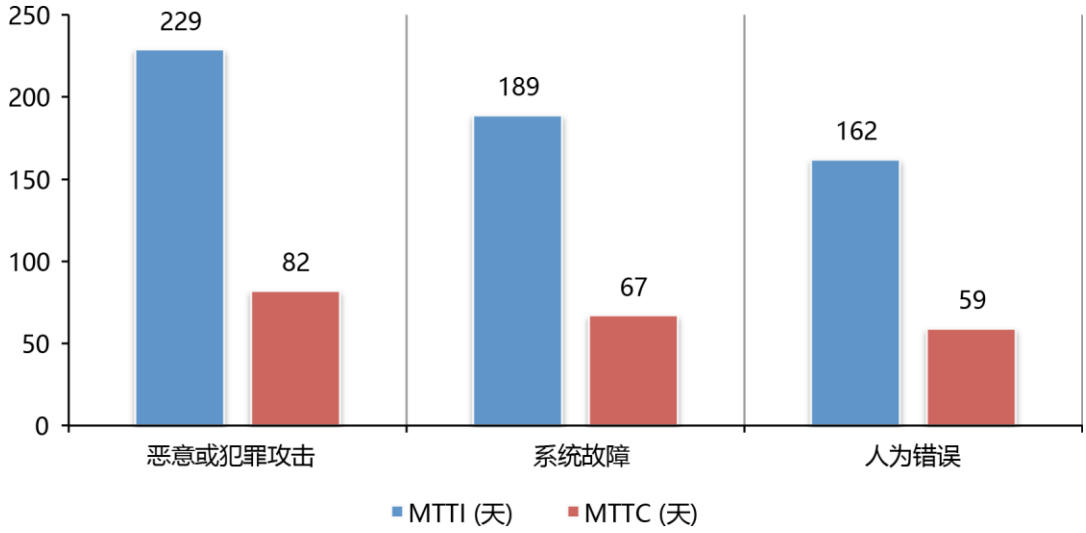


图 22 显示了 12 个国家/地区的 383 家企业的数据泄露总成本与平均时间之间的线性关系。这种重大关系表明了无法快速识别数据泄露将会导致成本更高，以及制定好事故响应计划的重要性。如果 MTTI 不足 100 天，识别数据泄露的平均成本为 323 万美元。如果超过 100 天，则成本为 438 万美元。

图 22.平均识别时间与总平均成本之间的关系

统一视图 (n=383)；单位：百万美元

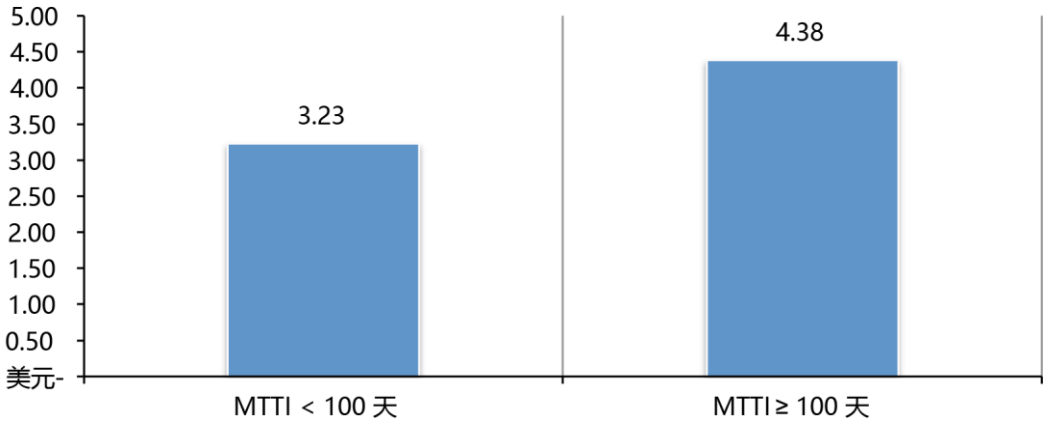
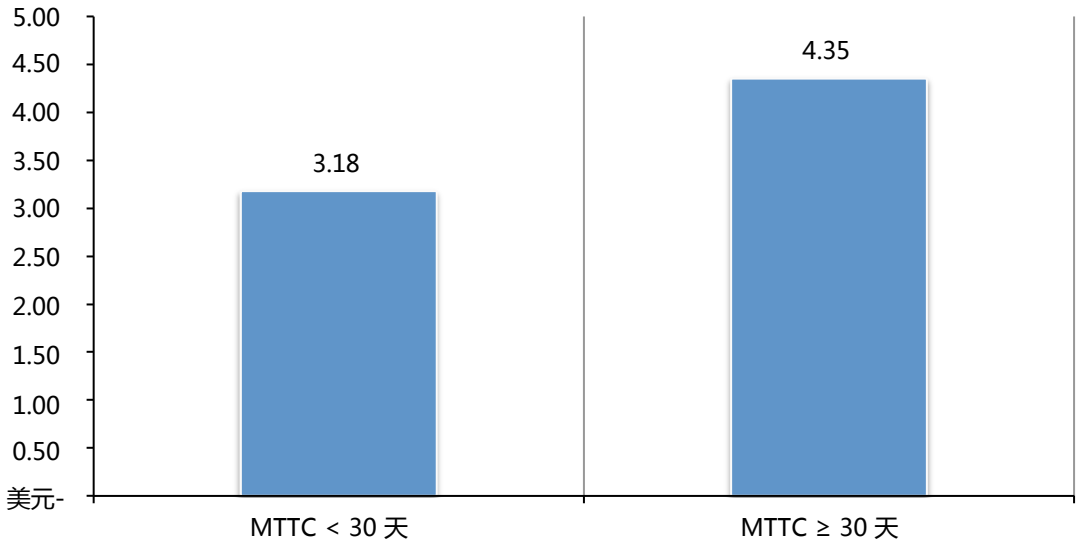


图 23 还显示了数据泄露总成本与 MTTC 之间的线性回归分析线。与图 22 类似，这种重大关系表明未能快速控制数据泄露将会导致更高的成本。如果在 30 天内控制数据泄露，则控制成本为 318 万美元。如果超过 30 天，则成本为 435 万美元。

图 23.平均控制时间与总平均成本之间的关系

统一视图 (n=383)；单位：百万美元



第 3 部分.如何计算数据泄露成本

为了计算数据泄露成本,我们使用了名为作业成本法（Activity-Based Costing，ABC）的成本核算方法。这种方法不仅可以识别活动，而且还能根据实际使用情况来指定成本。
我们要求参与本项基准研究的企业估算为了解决数据泄露而从事的各项活动的成本。

发现并立即响应数据泄露的典型活动如下所示：

- 开展调查和取证，确定数据泄露根源
- 确定可能的数据泄露受害者
- 组织事故响应小组
- 进行沟通和公共关系宣传
- 准备声明文件及面向数据泄露受害者和监管机构的其他必要报告
- 实施呼叫中心程序和专项培训

以下是发现数据泄露后需要进行的一些典型活动：

- 审计和咨询活动
- 防御法律服务
- 合规法律服务
- 面向数据泄露受害者的免费或优惠服务
- 识别保护服务
- 通过计算客户流失或流动来确定客户业务损失
- 客户获取和忠诚度计划成本

一旦企业估算出这些活动的成本范围，我们即可根据以下定义将成本划分为直接成本、间接成本和机会成本：

- *直接成本* – 完成指定活动需支出的直接开支。
- *间接成本* – 以非直接现金形式支出的时间、精力以及其他组织资源。
- *机会成本* – 由于向受害者公布（及向媒体公开揭露）数据泄露而导致了负面声誉效应，从而丧失了业务机遇所产生的成本。

我们的研究还对核心流程相关活动进行了细致审查，此类活动可造成与企业的数据泄露检测、响应、控制和补救有关的一系列开支。“主要发现”部分（第 2 部分）显示的各项活动的成本。4 个成本中心如下：

- 检测或发现：支持企业合理检测面临风险（存储中的）或已在进行的个人数据泄露的活动。
- 上报：在指定时间段内向有关人员报告受保护信息被泄露所需的活动。
- 通知：支持企业通过信函、电话销售、电子邮件或一般公告通知数据主体其个人信息丢失或被盗。
- 数据泄露后期活动：帮助数据泄露受害者与企业沟通的活动，提出其他问题或咨询建议，以便尽量减轻潜在的危害。数据泄露后期活动还包括信用报告监控或补发新帐户（或信用卡）。

除了上述流程相关的活动，大部分企业还需投入与数据泄露事故相关的机会成本，这是现有及未来客户信任度或信心降低所导致的。因此，我们机构的研究显示，与数据泄露事故有关的负面宣传会带来声誉影响，很可能导致客户流动或流失率异常以及新客户获取率下降。

为了推断这些机会成本，我们使用了成本估算方法，依靠各参与企业定义的普通客户“终身价值”进行估算。

- 现有客户的流动：最有可能因数据泄露事故终止合作关系的客户的估算值。增量损耗是指因数据泄露事故引起的非正常流动。此数值为年度比例，根据基准访谈流程期间管理层提供的估计值计算而来[9]

- 客户获取率降低：因数据泄露的影响而不会与企业建立关系的目标客户估计值。这一数值将作为年度比例提供。

我们承认，非客户数据丢失（如员工记录）可能不会影响企业的客户流失或流动。[10] 在这些情况下，数据泄露不涉及客户或消费者数据（包括付款交易信息）时，我们预计企业成本类别所占的比重会更低。

[9]在某些情况下，客户流动是部分性流动，其中数据泄露受害者依然与数据泄露企业保持关系，但客户活动量其实有所下降。这种部分下降在某些行业（如金融服务或公共部门实体）表现尤为显著，因为终止双方合作关系要么费用昂贵，要么不具备经济可行性。

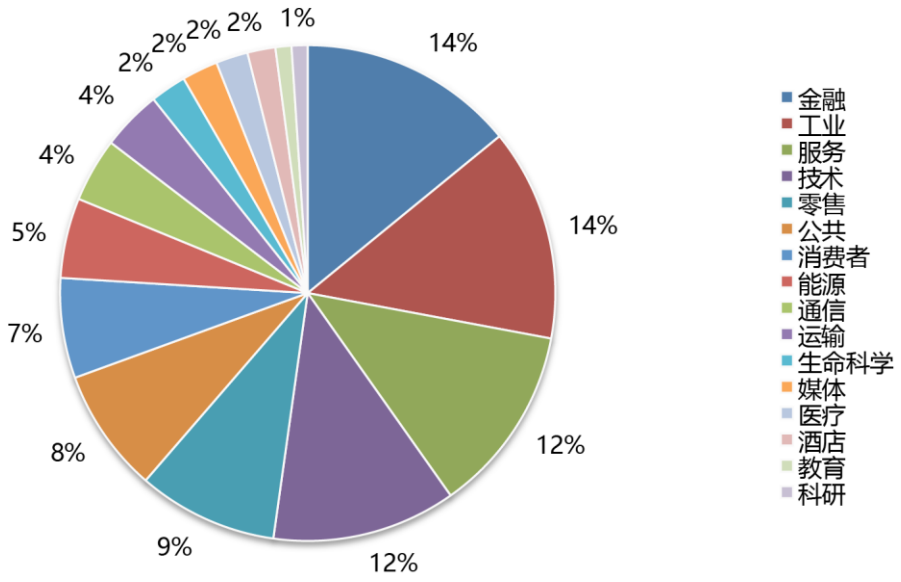
[10]在本项研究中，我们将公民、患者和学员信息视为客户数据。

第 4 部分.组织特征与基准方法

饼图 3 显示了基准企业的分布状况（按主导产业分类划分）。在今年的研究中，我们选择了 16 个行业。金融服务是规模最大的一个行业，其中包括银行、保险、投资管理和付款处理机构。

饼图 3.基准样本分布状况（按行业部门划分）

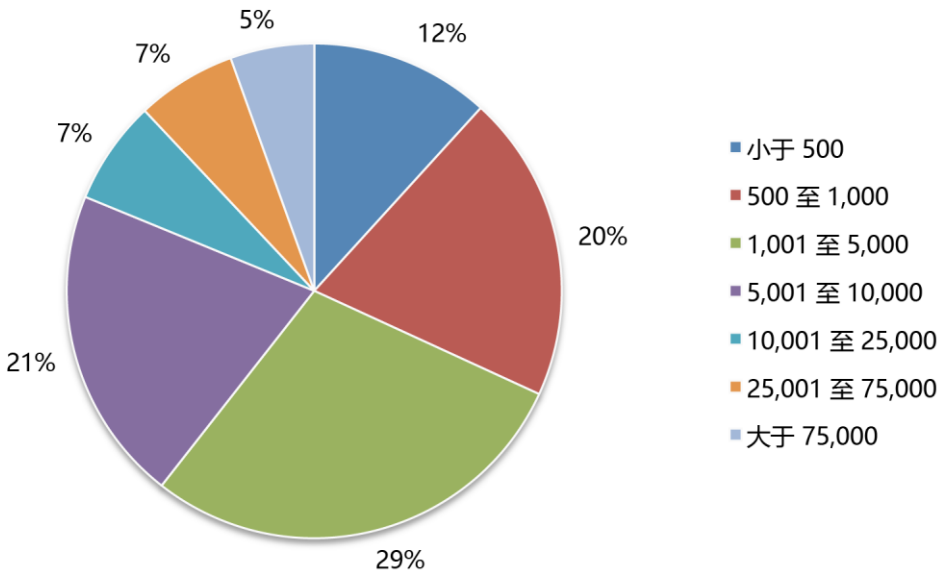
统一视图 (n=383)



饼图 4 显示了基准企业的分布状况（按总人数划分）。最大的行业包括员工人数超过 1,000 名的企业。

饼图 4.参与企业全球总人数

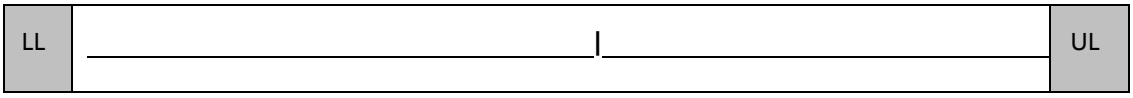
统一视图 (n=383)



数据收集方法不包括实际会计信息，而是根据各参与方的知识和经验实施数值估算。每类成本估算流程均包含两个阶段。首先，基准仪表要求个人按下列数轴格式标记既定的范围变量，评估各成本类别的直接成本估算价值。

如何使用数轴：数轴在每个数据泄露成本类别下提供了一种获取所产生的现金支出、劳动及开销总额的最佳估计值方法。请在上方设置的下限与上限之间的某个位置标记一点。您可以在访谈流程期间的某个时刻重置数轴下限和上限。

在这里公布 [显示的成本类别] 的直接成本估计值



数值从数轴获取，而非显示的各成本类别的点估计值，该数值要保持机密性并可确保实现更高的响应率。基准仪表还要求从业人员对间接成本和机会成本单独进行二次估算。

为了确保基准流程始终保持可管理的规模，我们对项目进行了谨慎的限制，仅考量我们认为对于测量数据泄露成本至关重要的一些成本活动中心。经过与顶级专家进行讨论，最终这组项目包括了一组固定成本活动。收集基准信息时，再三仔细检查每种仪表，从而实现一致性和完整性。

为了完全保密起见，基准仪表并不采集任何企业特定的信息。主题材料不含任何跟踪代码或者可能链接参与企业响应的其他方法。

基准方法覆盖的数据泄露成本项范围仅限于已知的成本类别，这些类别适于处理个人信息的一组广泛业务运营活动。我们认为，研究重点是业务流程而非数据保护或隐私合规性活动，这样才会得到更高质量的成果。

第 5 部分.限制

我们的研究采用了早期研究已成功部署的机密和专有基准方法。但是，这种基准研究方法存在一些固有的局限性，通过发现结果得出结论时必需仔细加以考量。

- 非统计结果：我们的研究对过去 12 个月中经历数据泄露（客户或消费者记录丢失或被盗）的一些全球实体进行了典型非统计样本分析。鉴于我们的抽样方法并不科学，因此不能对这些数据应用统计推断、误差范围和置信区间。

- 非响应：当前的发现是根据小规模代表性基准样本得出的。在这项全球研究中，共有 383 家企业完成了基准流程。非响应偏差未经测试，因此未参与企业的基本数据泄露成本很可能大为不同。

- 采样范围偏差：鉴于对采样范围存有偏见，因此采样范围对研究企业群体的代表程度会影响结果的质量。我们相信，当前采样范围偏重于隐私或信息安全计划较为成熟的企业。

- 企业特定信息：基准信息不仅敏感而且极为机密。
因此，当前方法无法采集企业识别信息。另外，人们还可以使用分类响应变量揭示有关企业和行业类别的人口统计学信息。

- 不可测量因素：为确保访谈脚本简明扼要，我们决定在分析中省略其他一些重要变量，如主导趋势和企业特征。变量的省略程度可能解释了一些无法确定的基准结果。

- 推断成本结果：基准研究的质量取决于参与企业的受访者提供的机密响应的完整性。尽管可在基准流程中纳入一定的制衡因素，但受访者很可能始终无法做出准确或真实的响应。此外，采用成本推断方法（而非实际成本数据）很可能无意中引入偏见和误差。

如对本研究报告存有疑问或意见，或者希望获取其他文件副本（包括引用或重用本报告的权限），请通过信函、电话或电子邮件联系：

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

请在以下网址获取所有国家/地区报告的完整副本：**www.ibm.com/security/data-breach**

Ponemon Institute LLC

出色可靠的信息管理

Ponemon Institute 致力于独立研究和教育，旨在推动企业和政府机构内部采用可靠的信息和隐私管理实践。我们的使命是，对影响个人和企业敏感信息的管理及安全的关键问题进行以经验为依据的高质量研究。

作为**美国调查研究组织委员会（CASRO）**的成员，我们坚持遵循严格的数据机密性、隐私和伦理道德研究标准。我们并不通过个人收集任何个人身份信息（也不会通过我们的企业调查收集公司可识别信息）。此外，我们还拥有严格的质量标准，可确保不会向调查对象询问无关的、离题的或不恰当的问题。