Ponemon INSTITUTE

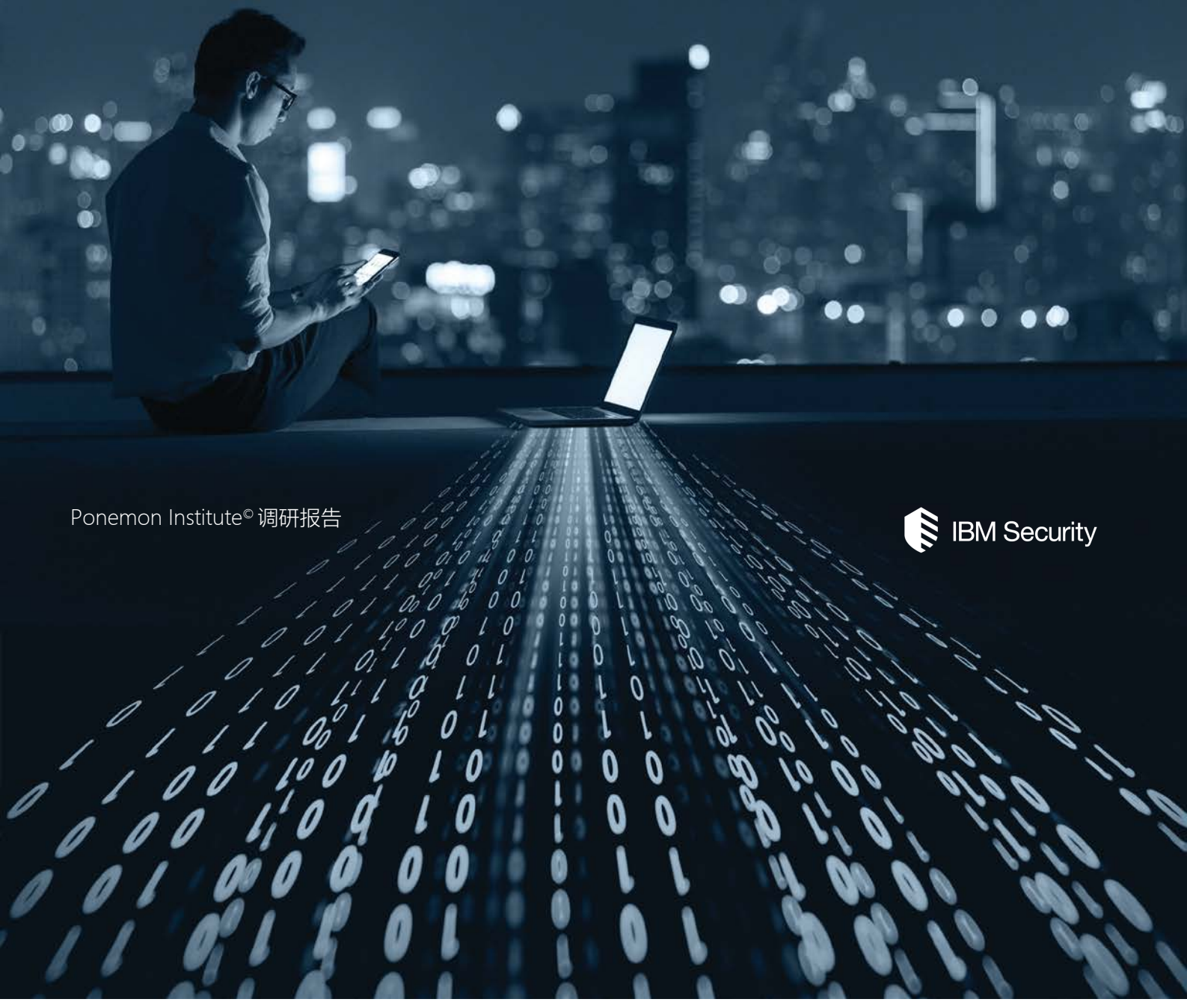
2017 年数据泄露成本调研

全球概述

IBM Security 事业部赞助的基准调研

由 Ponemon Institute LLC 独立开展

2017 年 6 月



Ponemon Institute© 调研报告

IBM Security

2017 年数据泄露成本调研：全球概述

Ponemon Institute，2017 年 6 月

第 1 部分：引言

IBM Security 和 Ponemon Institute 联合发布了"*2017 年数据泄露成本调研：全球概述*"[1] 报告。结果表明，参与本次调研的 419 家公司在数据泄露方面的平均总成本从 400 万美元降至 362 万美元[2]。本年度调研显示，对于含有敏感信息和机密信息的记录，*每条*丢失或被盗记录的平均成本已从 2016 年的 158 美元降至 141 美元。不过，尽管总体成本有所下降，但参与本年度调研的公司仍面临着更为严重的数据泄露问题。根据此次调研的结果，数据泄露事件的平均规模（丢失或被盗的记录条数）上升了 1.8%。

今年，美元走强对全球成本分析产生了重大影响，使得总体成本呈下滑趋势。因此，数据泄露成本下降了 17 美元，其中有近 8 美元（占比 48%）的成本下降可归因于汇率波动。[3] 为了与往年的做法保持一致，我们决定沿用之前的核算方法，而非在成本方面作出调整。要注意，这只会对全球分析产生影响，因为所有国家/地区级别的结果均以当地货币显示。

本年度的调研包含以下 11 个国家/地区及 2 个区域的样本：

- 美国
- 英国
- 德国
- 澳大利亚
- 法国
- 巴西
- 日本
- 意大利
- 印度
- 加拿大
- 南非
- 中东（包括阿拉伯联合酋长国和沙特阿拉伯）
- 东盟地区（包括新加坡、印度尼西亚、菲律宾和马来西亚）

全球调研情况一览

- 13 个国家/地区样本中涉及的 419 家公司
- 数据泄露的平均总成本为 362 万美元
- 平均总成本的年度降幅为 10%
- 每条丢失或被盗记录的平均成本 141 美元
- 单条成本的年度降幅为 11.4%
- 未来两年内再次发生资料数据泄露的可能性为 27.7%
- 再次发生资料数据泄露的可能性增幅为 2.1%

所有参与本次调研的组织均遭受过数据泄露，影响范围从 2,600 条记录到 100,000 条记录不等。受损记录是指用以识别在数据泄露事件中的信息丢失或被盗的自然人的记录；在本报告中，"每条受损记录的成本"与"单条成本"的含义相同。

除了呈现与数据泄露相关的各项成本因素之外，全球调研还明确了未来 24 个月中，组织面临一项或多项数据泄露的可能性。为了确定未来发生数据泄露事件的可能性，我们分析了两方面的因素：当前数据泄露事件的规模和组织所在位置。根据本年度调研的结果，我们估计平均有 27.7% 的组织会在未来 24 个月中面临资料数据泄露问题。去年，平均可能性为 25.6%。

[1] 本报告出具于发布产品的年限，而非完成现场调查的年限。请注意，本报告中所调研的大部分数据泄露事件发生于 2016 年。

[2] 当地货币单位均已转换为美元。

[3] 在当地货币与美元的换算过程中，单条成本与平均总成本均在预估的走低范围内，尤其是对于英国、德国、法国和意大利的公司（比如使用英镑 (£) 和欧元 (€) 的公司）。

南非、印度和巴西的组织很可能在未来 24 个月中面临资料数据泄露问题，与之相关的记录可能在 10,000 份以上。根据调研结果，南非出现数据泄露事件的可能性为 41%，是未来 24 个月内最有可能出现数据泄露事件的地区。未来，加拿大出现数据泄露事件的可能性为 14.5%，处于最低水平。

资料数据泄露事件是指至少涉及 1,000 条损失或被盗记录的事件，这些记录中包含有与消费者或客户相关的个人信息。本调研的涉猎范围不包括有关高价信息资产的数据泄露，比如知识产权、商业秘密、商业保密信息等。

为何数据泄露成本会在各个国家/地区之间有所波动

就中东、美国和日本的组织而言，我们如何解释今年数据泄露成本明显增高的情况？另一方面，为何德国、法国、澳大利亚和英国的组织能够在成功降低数据泄露成本的同时，采取有效的响应和补救措施？我们可以通过了解数据泄露成本的核算方法，阐明本调研中所涉国家/地区之间的差异。

对于"*2017 年数据泄露成本调研：全球概述*"，我们面向 11 个国家/地区及 2 个区域，邀请了 419 个组织参与本年度的调研。在这 419 个组织中，有 1,900 多名了解数据泄露事件的人员接受了采访。我们通过这些组织收集的首批数据点包括：(1) 数据泄露事件中丢失的客户记录有多少（即泄露规模），以及 (2) 发生数据泄露事件之后，组织损失的客户群占多大比例（即客户流失率）。这些信息有助于解释为何去年会出现数据泄露成本上升/下降的情况。

访谈期间，我们提出了一些问题，旨在了解组织投入了多少资源来开展数据泄露侦查及即刻响应方面的活动（如取证、调查等），以及他们在侦查到数据泄露事件之后，开展了哪些活动（如通知受害者、支付法律费用等）。具体的活动列表将在本报告的第 3 部分给出。其他会影响到成本的问题包括数据泄露的根本原因（即恶意攻击或犯罪攻击、内部疏忽或系统故障），以及侦查和遏制泄露事件所需的时间。

要注意，只有与本调研所涉 419 个组织经历数据泄露直接相关的事件才会用于核算对应的成本。举例来说，《通用数据保护条例 (GDPR)》等新规定、Shamoon 等恶意软件攻击和网络攻击会促使组织加大对数据治理实践方案及安全相关技术的投资力度，但不会直接影响到本调研所述及的数据泄露成本。

核算影响总体成本的数据泄露成本构成

以下信息将体现用于核算成本的数据，以及可能使得这些成本上升或下降的因素。我们认为，这些信息有助于组织优化资源分配决策，以便在遭遇不可避免的数据泄露事件时，最大程度地减少这些事件造成的财务影响。

- **数据泄露事件带来的意外客户损失及计划外客户损失（客户流失率）**

如果组织能够在遭遇数据泄露事件之前，设计有助于确保客户信任度和忠诚度的一系列项目，他们将能够减少数据泄露事件造成的业务/客户损失。根据本年度调研的结果，全球因数据泄露而损失客户的组织数量有所增加。但结果显示，如果首席隐私官、首席信息安全官等高层领导能够通过采取直接、主动的举措，提升客户对组织能够确保其个人信息安全的信任度，这将有助于组织降低客户流失率及数据泄露成本。此外，如果组织能够在发生数据泄露事件之后，为受害者提供泄露身份保护，他们将能够在降低客户流失率方面取得更大的成效。

■ **数据泄露事件的规模（丢失或被盗的记录条数）**

一般来说，丢失的记录条数越多，数据泄露的成本越高。因此，实施数据分类和审计数据保留项目非常重要，这不仅能够使得易受数据泄露事件影响的敏感信息和机密信息在可见性方面有所提升，还能够减少此类信息泄露的数量。

■ **识别和遏制数据泄露所需的时间**

识别和遏制数据泄露的速度越快，所需投入的成本就越低。在本年度的调研中，受访组织能够将识别数据泄露所需的时间从 2016 年的平均 201 天左右缩短至 191 天，同时将遏制数据泄露所需的时间从平均 70 天缩短至 66 天。我们认为，这些成效得益于组织投资了一些有助于提升安全水平的技术，比如安全分析、SIEM、企业级加密、威胁情报共享平台等。

从另一方面来看，安全问题的复杂性及颠覆性技术的部署可能会影响侦查和遏制数据泄露所需的时间。尽管采用一些相对复杂的 IT 安全架构有助于组织应对诸多的安全威胁，但太过复杂却反而不利于组织及时响应数据泄露事件。颠覆性技术、访问基于云的应用和数据，以及使用移动设备（包括 BYOD、移动应用等）会让应对 IT 安全风险及数据泄露事件变得更加复杂。此次调研的结果表明，在发生数据泄露时迁移至云平台和移动平台会使成本上升。

■ **数据泄露事件的侦查与升级**

侦查与升级成本一般涉及取证和调查活动、评估和审计服务、危机团队管理、与主管人员和董事会成员的沟通等。投资开展治理、风险管理与合规（GRC）项目有助于建立合适的内部框架，以便满足治理要求、评估企业各个部门的风险并追踪在治理要求下的合规情况，进而提升组织在侦查和升级数据泄露事件方面的能力。

■ **数据泄露产生的成本，包括通知受害者所需的成本等**

此类成本一般涉及服务台活动、入站通信、特殊调查活动、补救措施、法律开支、产品折扣、身份保护服务、监管干预等。调研结果表明，美国在通知方面投入的成本最高。

购买网络及数据泄露保险有助于管控数据泄露事件产生的财务影响。如本年度调研所示，保险保护和业务连续性管理能够在发生数据泄露事件之后，降低由此产生的成本。相比之下，急于通知受害者而不了解数据泄露范围、合规缺陷、聘请顾问等因素均会增加发生数据泄露事件之后的成本投入。此外，解决诉讼方面的开支也会增加发生数据泄露事件之后的成本投入。

■ **相比系统故障和人员疏忽（人为因素），恶意的内部攻击或犯罪攻击引起的成本投入更高**

在本次调研中，有近一半的受访组织（47%）能够确定发生数据泄露事件的根本原因是恶意攻击或犯罪攻击，由此引起的平均成本投入约 156 美元。相比之下，系统故障和人为失误或疏忽引起的平均成本投入则分别为 128 美元和 126 美元。可降低成本的因素包括：参与威胁共享、使用安全分析工具，以及招聘和挽留相关知识丰富的人员。

总体来看，澳大利亚、德国、法国和英国的组织能够提升其保留客户的能力，进而降低数据泄露成本。此外，澳大利亚、英国、德国的组织还能够控制客户记录丢失或被盗的数量，进而实现更大程度的成本降低。然而，中东各地和美国的组织则不同，他们面临着较高的客户流失率，而因此投入的成本也较高。就巴西、印度、中东、南非的组织来说，他们经历的数据泄露事件多为记录丢失或被盗，这使得他们投入的成本也有所增高。有关各个国家/地区的报告会更详细地阐述影响总体成本的数据泄露成本构成及相关因素。

以下所列是就组织而言最关键的调研结果和暗含事项：

全球数据泄露成本有所增加。平均数据泄露成本下降了 10%，而单条成本则下降了 2.9%。不过，数据泄露事件的平均规模（丢失或被盗的记录条数）却上升了 1.8%。去年，异常客户流失率没有变化，可界定为高于预期客户流失率。去年，平均总成本增加了 5.4%，而数据泄露事件的平均规模则上升了 3.2%。异常客户流失率和单条成本均上升了 2.9%。

数据泄露事件在美国和加拿大产生的成本投入最高，在巴西和印度产生的成本投入最低。数据泄露事件在美国和加拿大地区产生的平均单条成本分别为 225 美元和 190 美元。数据泄露事件在巴西和印度产生的平均单条成本最低，分别为 79 美元和 64 美元。数据泄露事件在美国和中东产生的平均总组织成本分别为 735 万美元和 494 万美元。数据泄露事件在巴西和印度产生的平均总组织成本最低，分别为 152 万美元和 168 万美元。

数据泄露成本趋势在各个国家/地区之间有所差异。通过对比今年的数据泄露成本与过去四年的平均数据，我们发现 5 个国家/地区的数据泄露成本有所上升，而另外 7 个国家/地区的数据泄露成本则呈下降趋势。就平均总成本而言，德国的降幅最大 (-.91)，其次是法国 (-.68)、澳大利亚 (-.48) 和英国 (-.45)。平均总成本增幅最大的国家/地区依次是中东 (+.83)、美国 (+.66) 和日本 (+.52)。

某些行业因数据泄露事件而投入的成本更高。全球在每条丢失或被盗的记录方面投入的平均数据泄露成本为 141 美元。不过，医疗保健业和金融服务业的组织投入的成本更高，分别为 380 美元和 245 美元。媒体、研究及公共事业在每条丢失或被盗的记录方面投入的平均数据泄露成本最低，分别为 119 美元、101 美元和 71 美元。

某些国家/地区的组织更容易发生数据泄露事件。在过去四年中，本调研研究了组织在 24 个月内发生一次或多次数据泄露事件的可能性。南非和印度的预估发生率最高。德国和加拿大的预估发生率最低。

加拿大的侦查与升级成本最高，巴西的最低。在侦查与升级事件情况方面投入的数据泄露成本一般涉及取证和调查活动、评估和审计服务、危机团队管理、与主管人员和董事会成员的沟通等。加拿大的平均侦查与升级成本为 146 万美元。相比之下，巴西的平均侦查与升级成本则为 43 万美元。

美国的通知成本最高。此类成本一般涉及创建联系人数据库、明确各项监管要求、聘请外部专家、电子邮件退回、入站通信设置等。美国的组织在通知方面投入的成本最高，印度最低，分别为 69 万美元和 2 万美元。

美国和中东在数据泄露事件响应方面投入的成本最高。发生数据泄露事件之后的响应活动一般涉及服务台活动、入站通信、特殊调查活动、补救措施、法律开支、产品折扣、身份保护服务、监管干预等。美国和中东在这些方面投入的成本分别为 156 万美元和 143 万美元。

中东和加拿大的公司投入的直接单条成本最高，美国的公司投入的间接单条成本最高。中东和加拿大的公司投入的直接单条成本最高，均为 81 美元。这些成本是指开展特定活动所需的直接开支，比如聘请取证专家、聘请律师事务所、为受害者提供身份保护服务等。美国的组织投入的间接单条成本最高，为 146 美元。

间接成本包括以通知受害者和调查事件为目的的员工时间投入、付出及其他方面的组织资源投入，还包括组织的信誉损失、客户流失成本。

丢失的记录条数越多，数据泄露的成本越高。成本分析揭示了平均数据泄露总成本与事件规模之间的关系。在本年度的调研中，平均总成本的范围是 190 万美元到 630 万美元，对应的事件受损记录条数分别为 10,000 以下和 50,000 以上。去年，平均总成本的范围是 210 万美元到 670 万美元，对应的事件受损记录条数分别为 10,000 以下和 50,000 以上。

识别和遏制数据泄露的速度越快，所需投入的成本就越低。我们第三年的调研报告揭示了组织在识别和遏制数据泄露方面的速度与其财务影响之间的关系。通过整合基于 419 家公司的样本，我们得出的平均识别时间 (MTTI) 为 191 天，其范围在 24 天到 546 天不等。平均遏制时间 (MTTC) 为 66 天，其范围在 10 天到 164 天不等。恶意攻击和犯罪攻击所需投入的平均识别时间和遏制时间最多（分别为 214 天和 77 天），而人为失误所需投入的平均识别时间和遏制时间则相对较少（分别为 168 天和 54 天）。

大部分数据泄露事件因黑客及内部犯罪而起。根据本年度调研的结果，47% 的数据泄露事件因恶意攻击或犯罪攻击而起。从为解决此类攻击而创建的记录来看，每条记录的成本是 156 美元。相比之下，与每条记录相关的系统故障成本和人为失误或疏忽成本则分别为 128 美元和 126 美元。美国和加拿大的公司会将大部分成本投入到解决恶意攻击或犯罪攻击方面（每条记录投入的成本分别为 244 美元和 201 美元）。就此而言，印度投入的成本相对较少（每条记录投入的成本为 78 美元）

恶意攻击或犯罪攻击集中于中东和美国的组织。就中东和美国而言，分别有 59% 和 52% 的数据泄露事件是因黑客及内部犯罪而起。而在意大利和南非，仅有 40% 的数据泄露事件是因恶意攻击而起。意大利和东盟地区的组织因人为失误而造成的数据泄露事件的比例最高，分别为 36% 和 35%。德国和印度的组织则更有可能因系统故障或业务流程故障而引发的数据泄露事件，占比分别为 34% 和 33%。

建立事件响应团队、广泛采用加密技术有助于降低成本。根据本年度的调研结果，事件响应 (IR) 团队能够将每条受损记录产生的成本降低 19 美元之多。因此，具备强 IR 能力的公司可对每条记录实现高达 122 美元的成本调整（由 141 美元减 19 美元算得）。类似地，广泛采用加密技术也能够帮助组织将单条成本降低 16 美元，同时对每条记录实现高达 125 美元的成本调整（由 141 美元减 16 美元算得）。

涉及第三方的数据泄露事件及在发生泄露时广泛迁移至云端会使得由此产生的成本投入变得更高。如果数据泄露事件涉及第三方，则每条受损记录的数据泄露成本将增加 17 美元之多，而每条记录的平均调整成本则为 158 美元（由 141 美元加 17 美元算得）。发生数据泄露事件时，广泛迁移至云端会使得组织需承担的单条成本增加 14 美元，而每条记录的平均调整成本则为 155 美元（由 141 美元加 14 美元算得）。

本年度成本分析包含有 4 项新因素。以下因素会影响数据泄露成本：(1) 合规缺陷；(2) 广泛采用移动平台；(3) 委任 CPO；以及 (4) 使用安全分析工具。委任 CPO 能够将数据泄露成本降低 3 美元。部署安全分析工具能够将每条受损记录的成本降低 7 美元。不过，广泛采用移动平台及存在合规缺陷方面因素则会导致每条受损记录的成本分别增加 9 美元和 11 美元。

无法保留客户会产生严重的财务影响。保留客户与成本投入密切相关。损失 1% 以上的客户群会让组织面临高达 260 万美元的平均总成本投入。如果损失 4% 及以上的客户群，则组织平均投入的成本将为 510 万美元。对于日本、意大利和法国的组织，他们的客户流失率最高。而南非、巴西及东盟地区的组织则更善于保留客户。客户流失率最高的行业包括金融业、医疗保健业及服务业。美国的组织因损失客户而投入的成本最高，为 413 万美元。

数据泄露成本常见问答

什么是数据泄露？数据泄露是指以电子或纸质格式存储的个人姓名及其医疗记录和/或财务记录或借记卡等信息可能被置于风险之下的事件。在我们的调研中，我们明确了造成数据泄露的三大原因：恶意攻击或犯罪攻击、系统故障、人为失误。数据泄露的成本会因发生数据泄露的原因及当时所采取的防范措施的不同而有所不同。

什么是受损记录？受损记录是指用以识别在数据泄露事件中信息丢失或被盗的自然人（个人）的信息；例如零售公司的数据库，其中包含有个人的姓名及其信用卡信息和其他个人识别信息；或者是健康保险商的投保人记录以及医师和支付信息。根据本年度的调研结果，组织为每条受损记录投入的成本是 141 美元。

如何收集数据？我们的调研人员通过在 10 个月内面向 419 家公司开展 1,900 多次独立采访，收集了深入详尽的定性数据。受访组织的征集工作从 2016 年 2 月开始；所有采访工作于 2017 年 3 月结束。在 419 个受访组织中，我们分别对各个组织内了解其数据泄露事件及相关成本的 IT、合规性及信息安全从业者进行了访谈。为保护隐私，我们并未收集任何组织特定信息。

如何计算成本？为了计算数据泄露的平均成本，我们同时收集了组织所招致的直接开支与间接开支。直接开支包括聘请取证专家、获取热线支持，以及针对未来的产品和服务提供免费信用监控订阅及折扣而招致的开支。间接开支包括内部调查与通信而招致的开支，以及根据客户获得率的下降或客户流失而外推得出的成本。

基准调研与调查研究有何差异？*数据泄露成本调研*以组织为单位进行分析，而调查研究则以个人为单位进行分析。我们共征集了 419 个组织参与此次调研。数据泄露的规模从最低的 2,600 条受损记录到略高于 100,000 条受损记录。

数据泄露的平均成本是否可用于计算涉及数百万条记录丢失或被盗的特大型泄露事件？我们调查结果中给出的数据泄露的平均成本并不适用于灾难性或特大数据泄露事件（例如索尼数据泄露事件），这是因为这些事件不属于大多数组织的典型事件。为了确保调研结果在全球组织中具有代表性，同时也确保调研结果可用于了解受保护信息丢失或被盗后所产生的成本情况，我们在此次分析中并未将受损记录条数约超过 100,000 条的特大型数据泄露事件包含在内。

每年是否都会跟踪相同的组织？每个年度调研所征集的参与公司都不同。换句话说，我们并不会在每年都跟踪相同的组织。为了保证一致性，我们会征集并匹配具有类似特性的公司，诸如所属行业、员工数量、地域分布及数据泄露的规模等等。自启动此次调研以来，我们已经调查了 2,432 个组织的数据泄露情况。

全球调研情况一览

本年度的调研面向 11 个国家/地区及 2 个区域进行，包括美国、德国、加拿大、法国、英国、意大利、日本、澳大利亚、中东、巴西、印度、南非，以及首次开展调研的东盟（ASEAN）地区。共计 419 个组织参与了本次调研。国家/地区特定的结果以 13 份独立报告的形式提供。

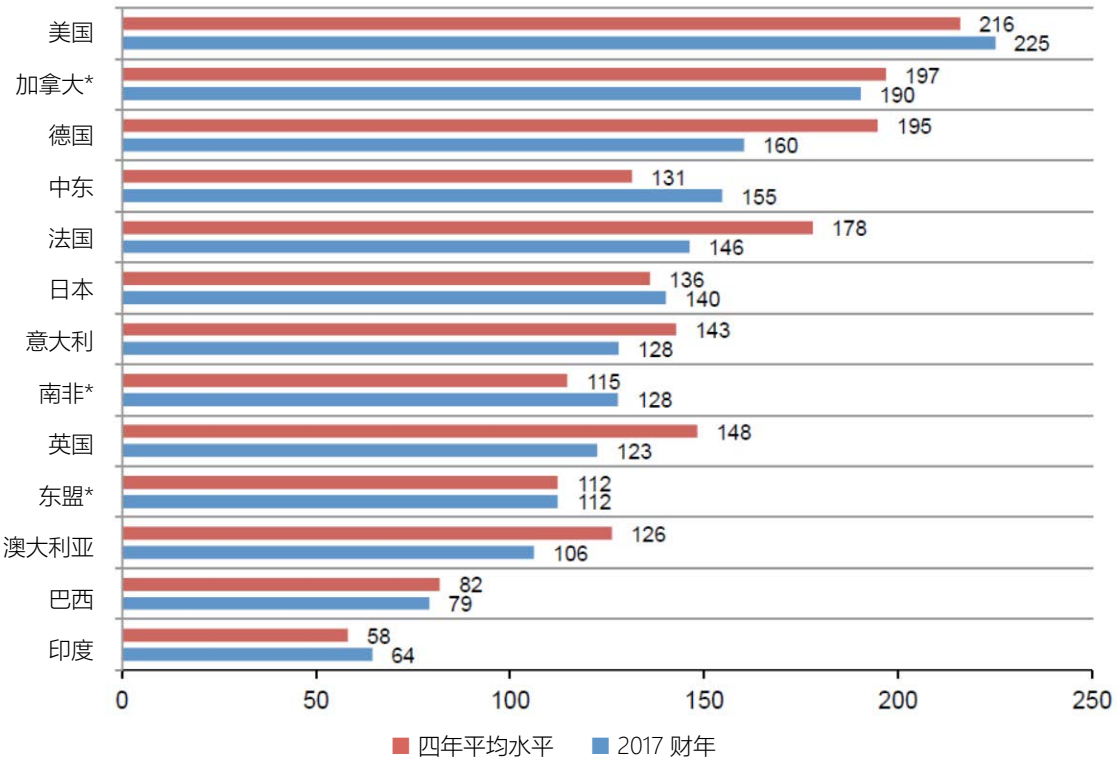
图 1 显示了国家/地区或区域调研期间，数据泄露在四年内的平均单条成本（以美元为单位）。如图所示，国家/地区之间存在较大的单条成本差异。[4] 所有国家/地区的合计单条成本为 141 美元，而去年的合计单条成本则为 158 美元（东盟样本除外）。美国、加拿大和德国仍然是单条成本最高的三个国家，对应的数额分别为 225 美元、190 美元和 160 美元。相比之下，印度、巴西和澳大利亚的单条成本则要低很多，分别为 64 美元、79 美元和 106 美元。

图 1. 与四年平均水平相比，2017 年的数据泄露单条成本

2017 财年的总平均值 = 141 美元；2016 财年的总平均值 = 158 美元；2015 财年的总平均值 = 154 美元；2014 财年的总平均值 = 145 美元

* 所有年限均无可用的历史数据

单位为美元 ($)



[4] 单条成本是指数据泄露的总体成本除以受损记录的条数（即数据泄露事件的规模）。

第 2 部分：重要调研结果

在本节中，我们将介绍此次调研的详细结果。我们将按照下列顺序呈现各个主题：

- 全球及各个行业在数据泄露成本方面的差异
- 数据泄露的根本原因
- 数据泄露成本的影响因素
- 受损记录及客户流失频率方面的趋势
- 数据泄露成本组成部分方面的趋势
- 组织出现数据泄露事件的可能性
- 识别和遏制数据泄露所需的平均时间

下表所列为本次全球调研中涉及的国家/地区、图例、样本量及货币种类。此外，表中也显示有为各个国家/地区出具年度报告的年数，范围从东盟的 1 年到美国的 12 年不等。

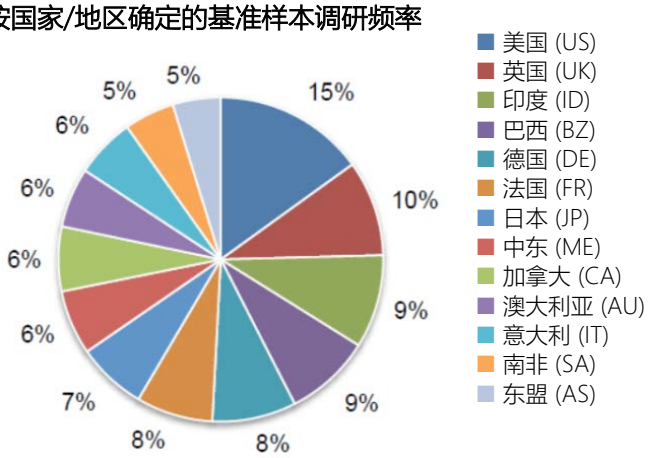
表 1. 全球调研情况一览

图例	国家/地区	样本	%	货币	调研年数
US	美国	63	15%	美元	12
UK	英国	40	10%	英镑	10
ID	印度	39	9%	卢比	6
BZ	巴西	36	9%	雷亚尔	5
DE	德国	35	8%	欧元	9
FR	法国	32	8%	欧元	8
JP	日本	29	7%	日元	6
ME	中东*	27	6%	迪拉姆/沙特里亚尔	4
CA	加拿大	27	6%	加元	3
AU	澳大利亚	25	6%	澳元	8
IT	意大利	25	6%	欧元	6
SA	南非	21	5%	兰特	2
AS	东盟#	20	5%	新加坡元	1
	总计	419	100%		

* ME 表示沙特阿拉伯和阿拉伯联合酋长国的公司集群样本

ASEAN 表示新加坡、印度尼西亚、菲律宾和马来西亚的公司集群样本

饼分图 1. 按国家/地区确定的基准样本调研频率



全球及各个行业在数据泄露成本方面的差异

按国家/地区确定的组织平均数据泄露成本。图 2 对比了今年的数据泄露平均总成本与四年的平均水平。平均总成本降幅最大的国家/地区依次是德国 (-.91)、法国 (-.68)、澳大利亚 (-.48) 和英国 (-.45)。相比之下，平均总成本增幅最大的国家/地区依次是中东 (+.83)、美国 (+.66) 和日本 (+.52)。

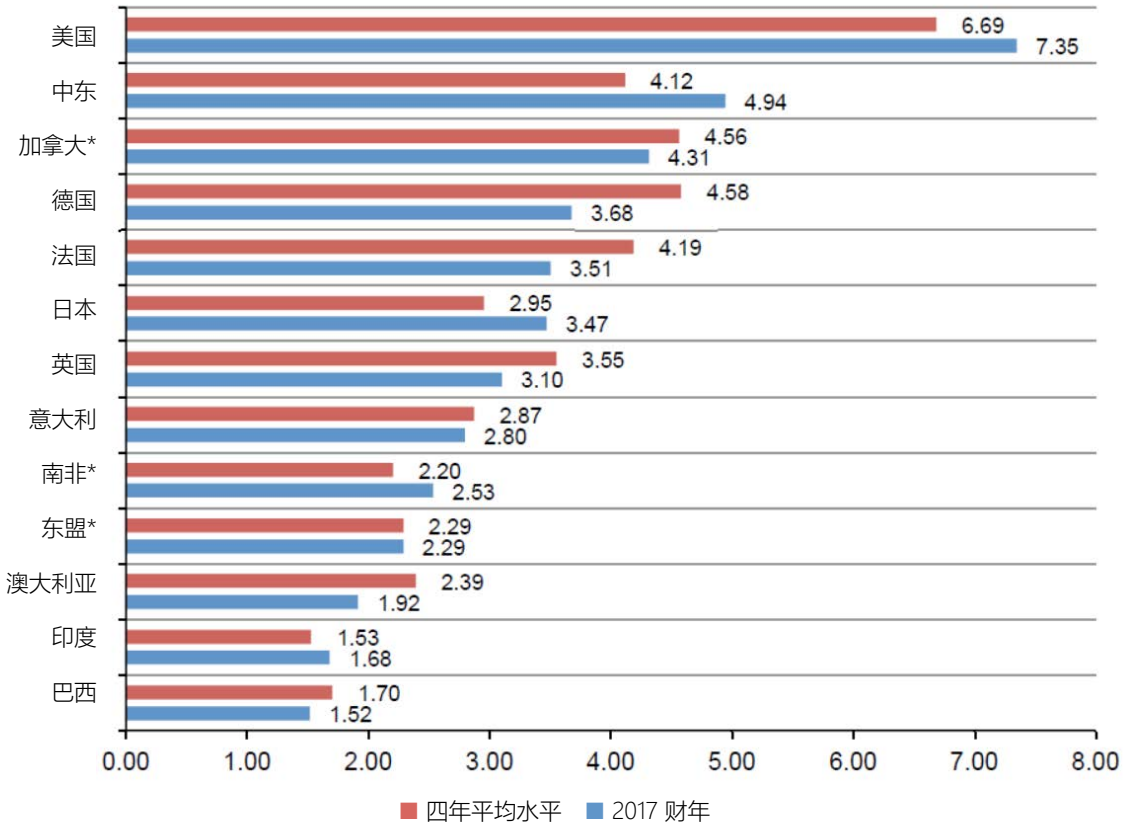
根据 2017 财年的调研结果，美国组织的平均总成本最高（735 万美元），其次是中东（494 万美元）。相比之下，巴西组织和印度组织的平均总成本最低，分别是 152 万美元和 168 万美元。

图 2. 与四年平均水平相比，今年的数据泄露平均总成本

2017 财年的总平均值 = 362 万美元；2016 财年的总平均值 = 400 万美元；2015 财年的总平均值 = 379 万美元；2014 财年的总平均值 = 350 万美元

* 所有年限均无可用的历史数据

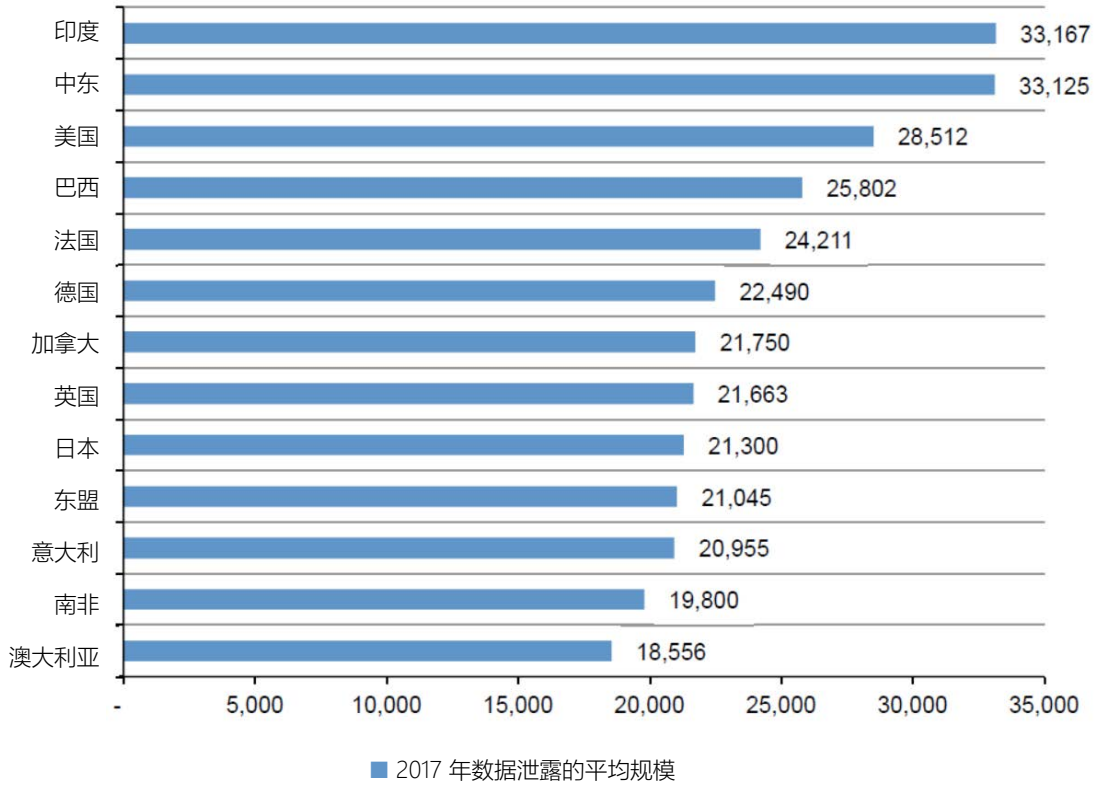
单位为美元（以百万计）



按国家/地区或区域确定的暴露记录条数或受损记录条数。图 3 显示了在参与本次调研的各个国家/地区及区域的组织中，出现数据泄露事件的平均规模。大体上，印度、中东和美国的组织平均泄露的记录条数最多。相比之下，澳大利亚、南非和意大利的组织平均泄露的记录条数最少。在本报告的后半部分，我们会阐明丢失或被盗的记录条数与数据泄露成本之间的关系。

图 3. 按国家/地区或区域确定的记录平均泄露条数

全球平均值 = 24,089



数据泄露衡量标准的净变动比例在各个国家/地区之间的差异[5]。图 4 显示了 4 项指标，旨在表明过去一年中数据泄露衡量标准的变动比例。[6] 这些指标包括：(1) 异常客户流失率（自发生数据泄露事件以来，高于预期的客户流失情况）；(2) 数据泄露事件的规模（丢失或被盗的记录条数）；(3) 数据泄露的平均总成本；以及 (4) 单条成本。以下为所述指标在各个国家/地区的增减情况。

一年内的净变动比例上浮

- 异常客户流失率：巴西、印度、意大利、日本、中东、南非和美国
- 数据泄露事件的规模：巴西、加拿大、法国、印度、意大利、日本、中东和南非
- 平均总成本：巴西、印度、意大利、日本、中东、南非和美国
- 单条成本：巴西、印度、意大利、日本、中东和美国

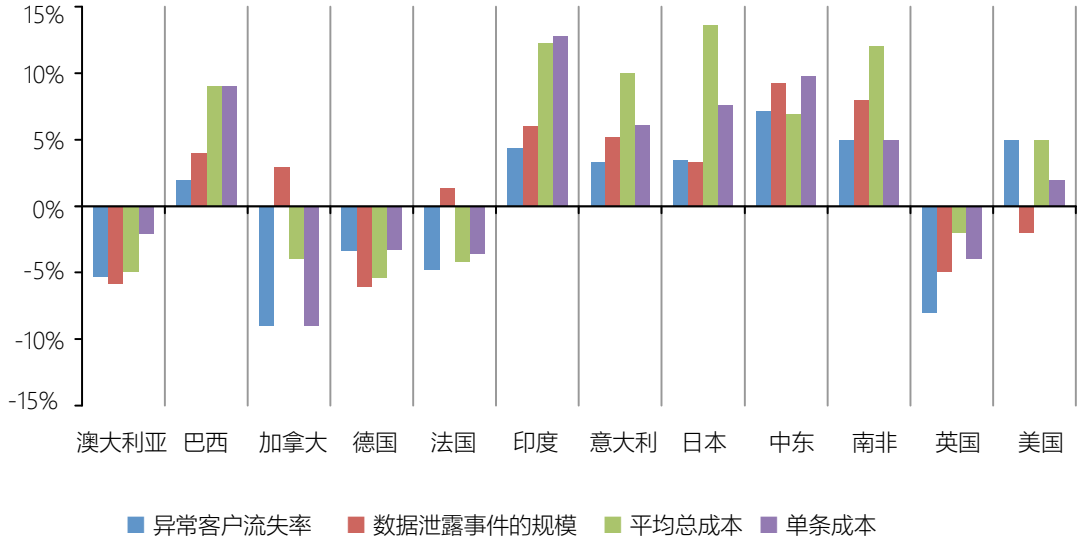
一年内的净变动比例下调

- 异常客户流失率：澳大利亚、加拿大、德国、法国和英国
- 数据泄露事件的规模：澳大利亚、德国、英国和美国
- 平均总成本：澳大利亚、加拿大、德国、法国和英国
- 单条成本：澳大利亚、加拿大、德国、法国和英国

如图 4 所示，有更多国家/地区（巴西、印度、意大利、日本、中东和南非）在所有 4 项成本衡量标准方面呈现出净变动比例上浮趋势。仅有 3 个国家/地区（澳大利亚、德国和英国）能够在所有 4 项成本衡量标准方面实现改善，因而呈现出净变动比例下调趋势。

图 4. 过去一年中数据泄露衡量标准的变动比例

净变动是指 2017 年与 2016 年所获结果之间的差异



[5] ASEAN 未包含在本分析中，因为与之相关的国家/地区是第一年被纳入本调研的范畴。

[6] 图 4 所示的比例变动为基于成本数据的核算结果，对应的成本单位为当地货币而非美元。因此，本分析结果不会因货币汇率波动而受到影响。

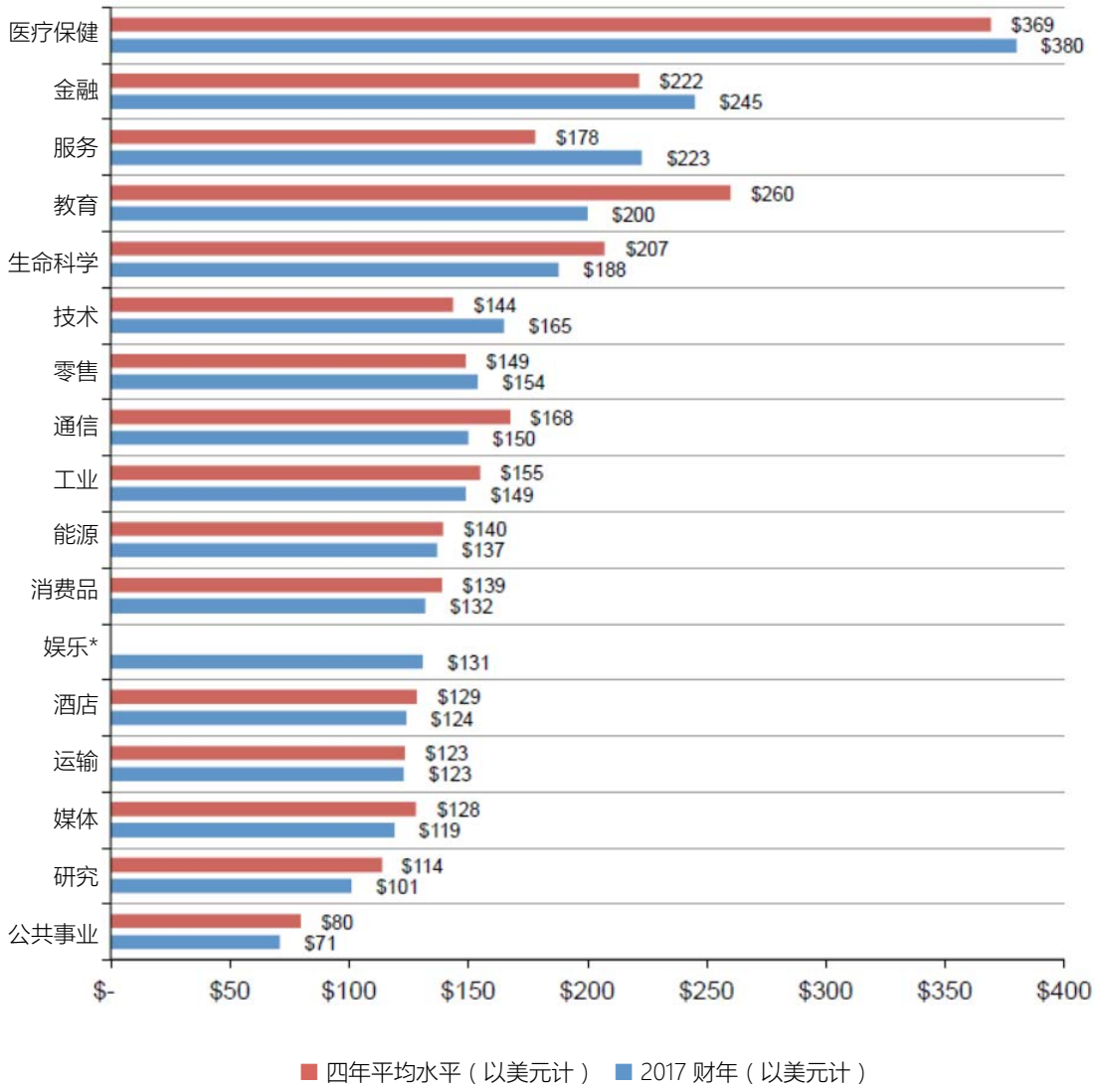
某些行业的数据泄露成本要高于其他行业。图 5 对比了按行业分类的汇总样本在本年度的单条成本情况与四年的平均水平。对于医疗保健、教育、金融等受严格监管的行业，组织在数据泄露方面的单条成本远远高于总平均值，即 141 美元。公共事业、研究、媒体和运输行业的组织在数据泄露方面的单条成本则远远低于总平均值。

与四年平均水平相比，单条成本增幅最显著的行业依次为服务（+45 美元）、金融（+23 美元）、技术（+21 美元），以及医疗保健（+11 美元）。降幅最显著的行业依次为教育（-60 美元）、生命科学（-19 美元）和通信（-18 美元）。

图 5. 按行业分类确定的单条成本

* 所有年限均无可用的历史数据

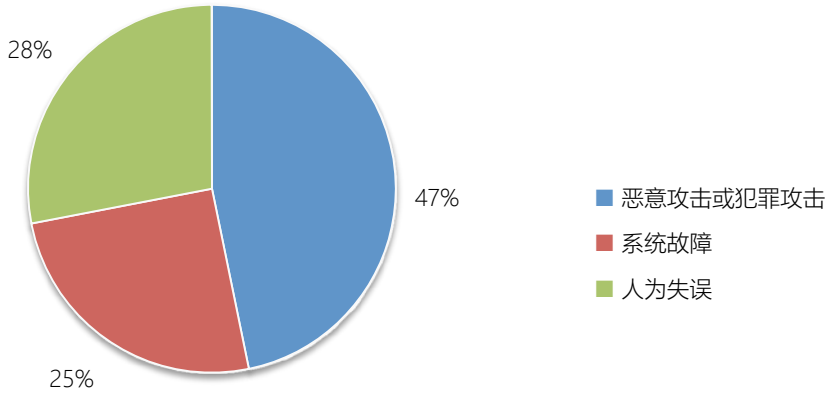
单位为美元 ($)



数据泄露的根本原因

大部分数据泄露事件因恶意攻击或犯罪攻击而起。[7] 饼分图 2 根据各个国家/地区组织的总体情况，汇总了出现数据泄露事件的几大根本原因。在这些事件中，有 47% 涉及恶意攻击或犯罪攻击，25% 因员工或承包商疏忽所致（人为因素），28% 与系统故障相关，包括 IT 故障、业务流程故障等等。[8]

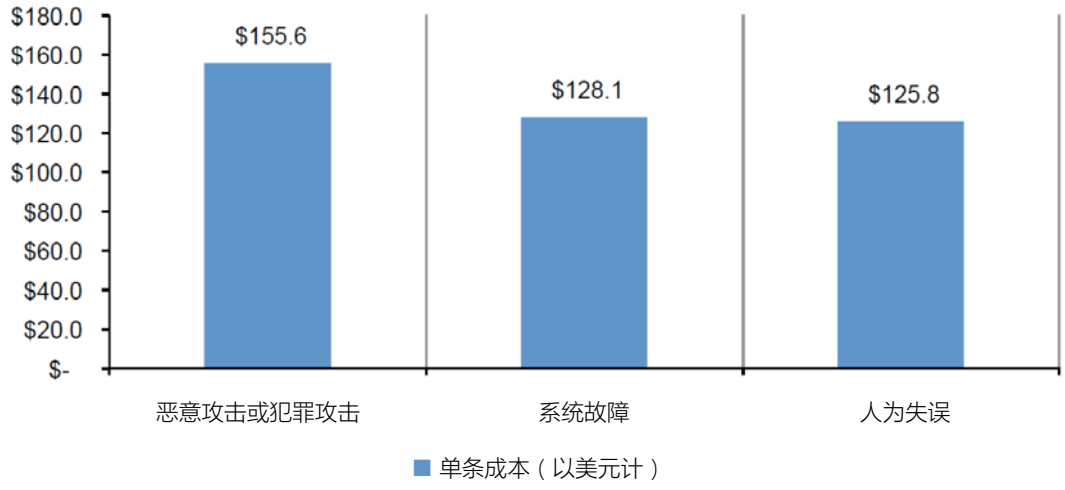
饼分图 2. 基准样本的分布（按数据泄露的根本原因）



恶意攻击对应的成本投入较高。图 6 所示为引发数据泄露事件的三大根本原因对应的单条成本情况。2017 年，因恶意攻击或犯罪攻击而产生的数据泄露成本为 156 美元。此结果明显高于因系统故障和人为因素而产生的数据泄露单条成本，对应的数据分别为 128 美元和 126 美元。

图 6. 数据泄露根本原因的单条成本

以美元为单位

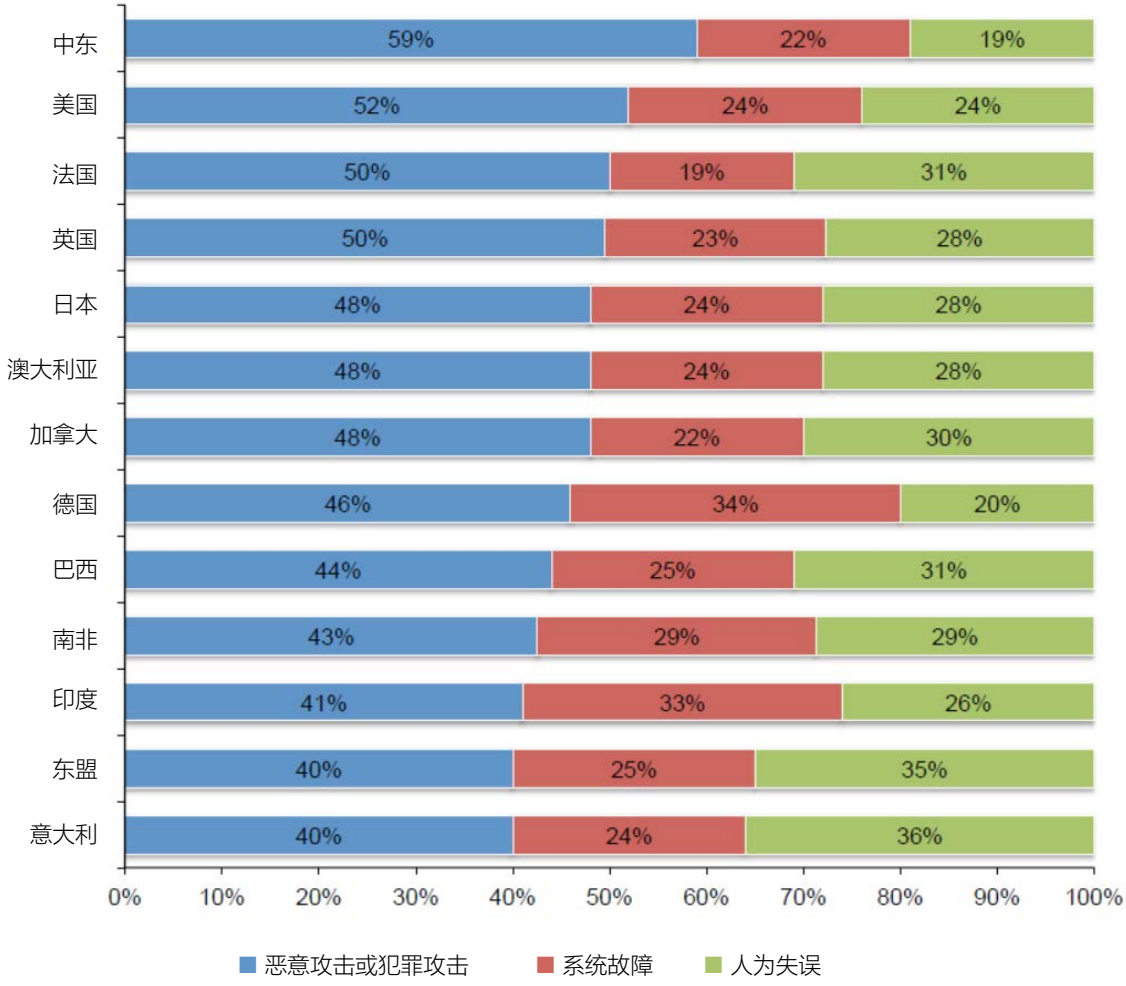


[7] 渎职的内部人员是指因其疏忽而导致数据泄露的个人，一般通过数据泄露后的调查而确定。恶意攻击的发起方可能是黑客或内部人员（比如员工、承包商或其他第三方）。

[8] 最常见的恶意攻击或犯罪攻击形式包括恶意软件感染、内部犯罪、钓鱼攻击、社交工程攻击，以及 SQL 注入。

按国家/地区和区域确定的数据泄露根本原因之间的比例差异。图 7 显示了 11 个国家/地区及 2 个区域中，发生数据泄露事件的几大根本原因。就中东地区的组织而言，他们更容易受到恶意攻击或犯罪攻击（占比 59%）。相比之下，意大利、东盟和印度的组织则较少经历因犯罪攻击而引发的数据泄露事件。印度和东盟的公司因人为失误（非犯罪）而发生数据泄露事件的比例最高，而德国和印度的组织则更容易经历因系统故障或业务流程故障而引发的数据泄露事件。

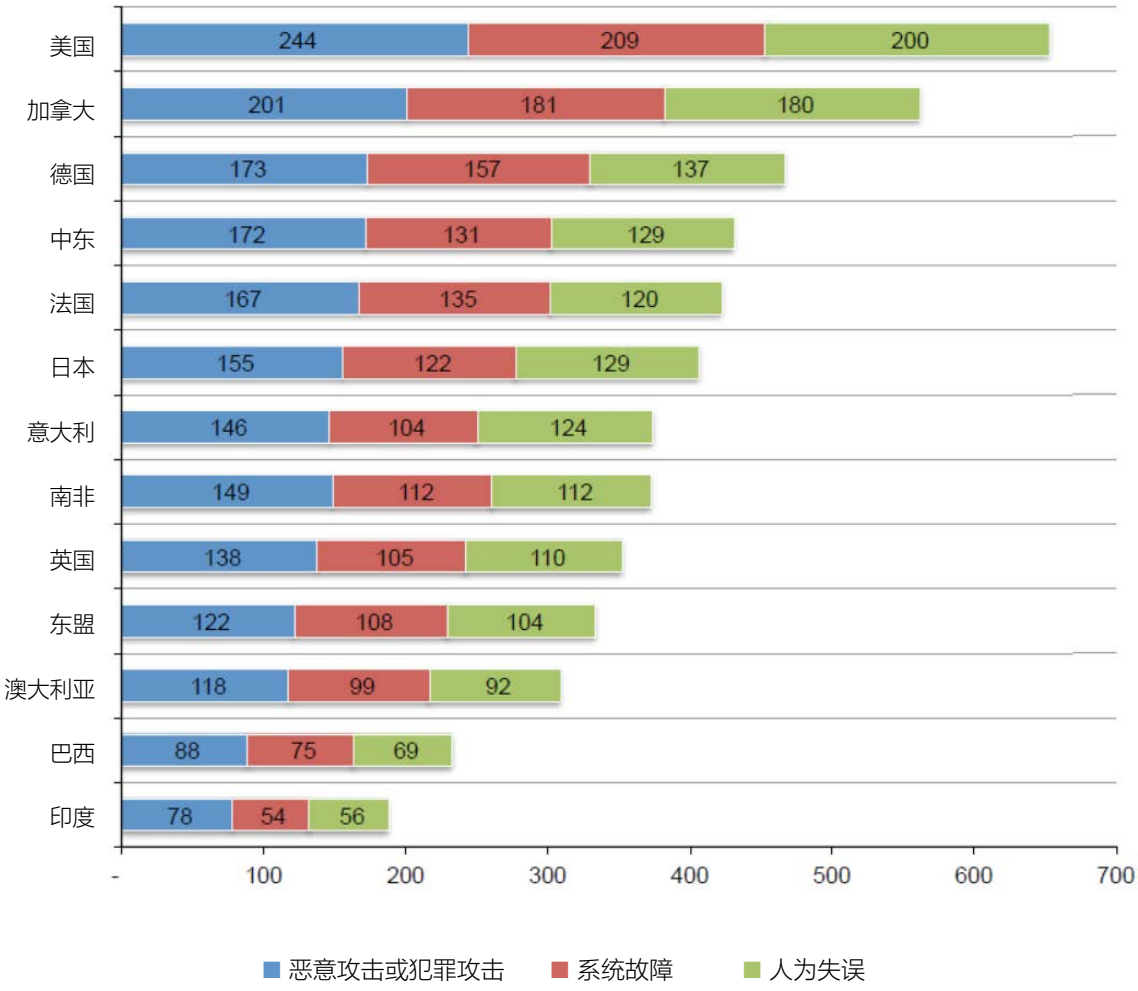
图 7. 按国家/地区和区域确定的数据泄露根本原因占比



根本原因对应的单条成本。图 8 所示为引发数据泄露事件的三大根本原因对应的单条成本情况。结果很明显，因恶意攻击或犯罪攻击而产生的数据泄露成本基本高于因系统故障或人为失误而产生的数据泄露成本。而且，国家/地区之间也存在广泛的差异。对于美国的组织来说，他们在因恶意攻击或犯罪攻击而引发的数据泄露事件方面承担的单条受损记录成本为 244 美元，而从印度的组织来看，他们在因犯罪攻击而引发的数据泄露事件方面承担的单条成本则仅为 78 美元。

图 8. 按国家/地区和区域确定的三大数据泄露根本原因对应的单条成本

以美元为单位



数据泄露成本的影响因素

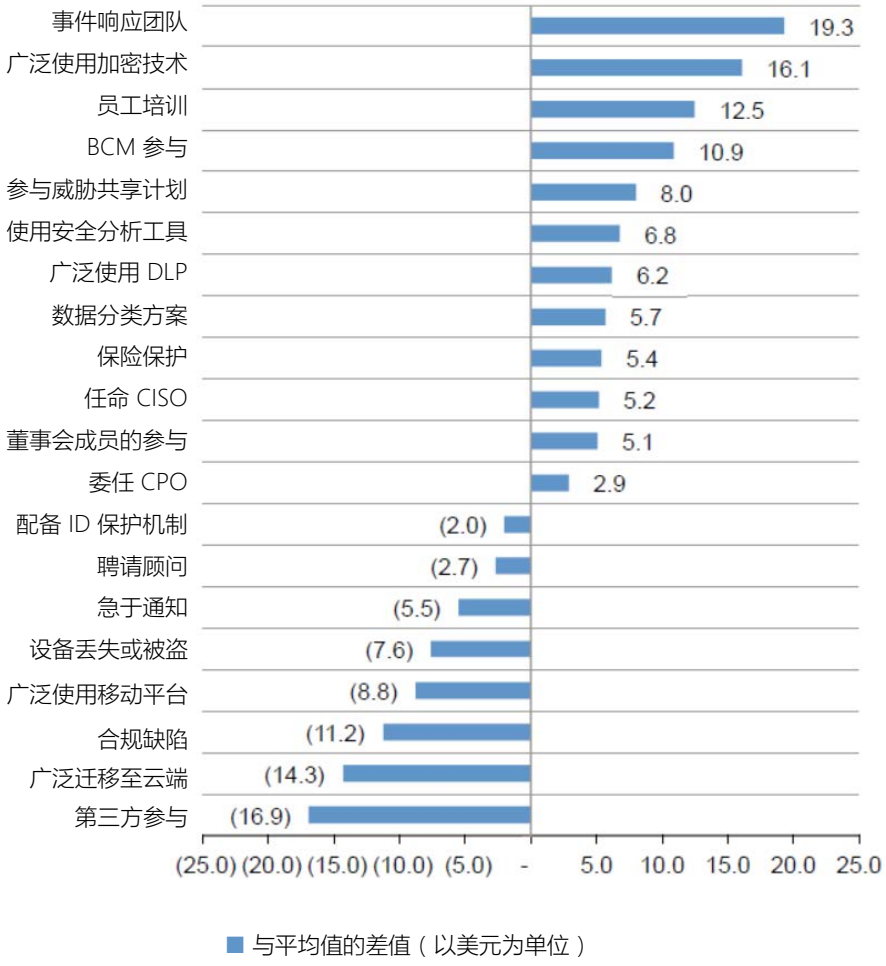
某些因素会使数据泄露成本上升或下降。图 9 列出了 20 项会使数据泄露成本上升或下降的因素。如图所示，事件响应团队、广泛使用加密技术、员工培训、BCM 参与、参与威胁共享计划及使用安全分析工具等因素使得单条受损记录产生的数据泄露单条成本下降了 7 美元或以上。

第三方参与、广泛迁移至云端、合规缺陷、广泛使用移动平台、设备丢失或被盗、急于通知等因素使得数据泄露的单条成本（以负数显示）上升了 5 美元或以上。

为了说明这些因素对数据泄露成本有何影响，我们全面分析了事件响应团队产生的影响，此因素使得数据泄露成本在 141 美元（平均值）的基础上下降了 19 美元，即降至 122 美元。相比之下，第三方参与则使得数据泄露成本上升了 17 美元，即从 141 美元增至 158 美元。

图 9. 20 个因素对数据泄露单条成本的影响

以美元为单位

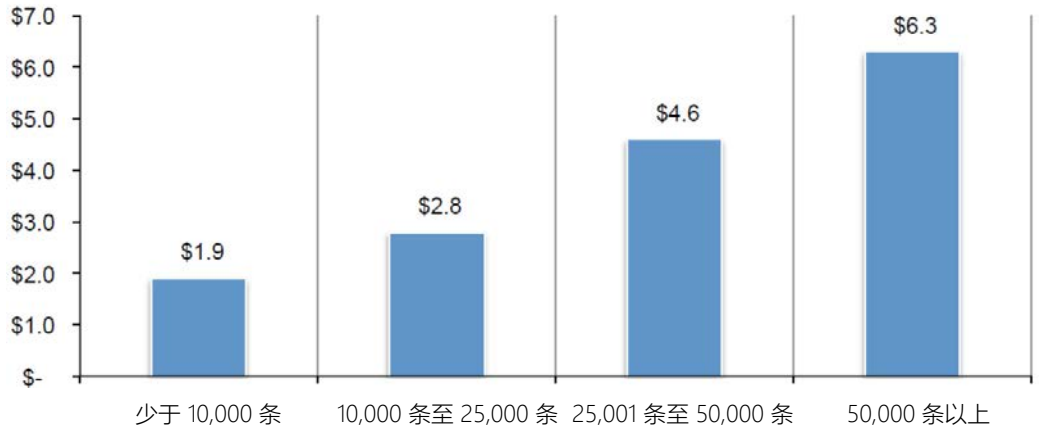


受损记录及客户流失频率方面的趋势

丢失的记录条数越多，数据泄露的成本越高。图 10 显示了数据泄露平均总成本与事件规模之间的关系，其中，与 419 个组织的数据泄露事件规模相关的成本以升序排列。在本年度的调研中，平均总成本的范围是 190 万美元到 630 万美元，对应的事件受损记录条数分别为 10,000 以下和 50,000 以上。

图 10. 按数据泄露事件规模确定的平均总成本

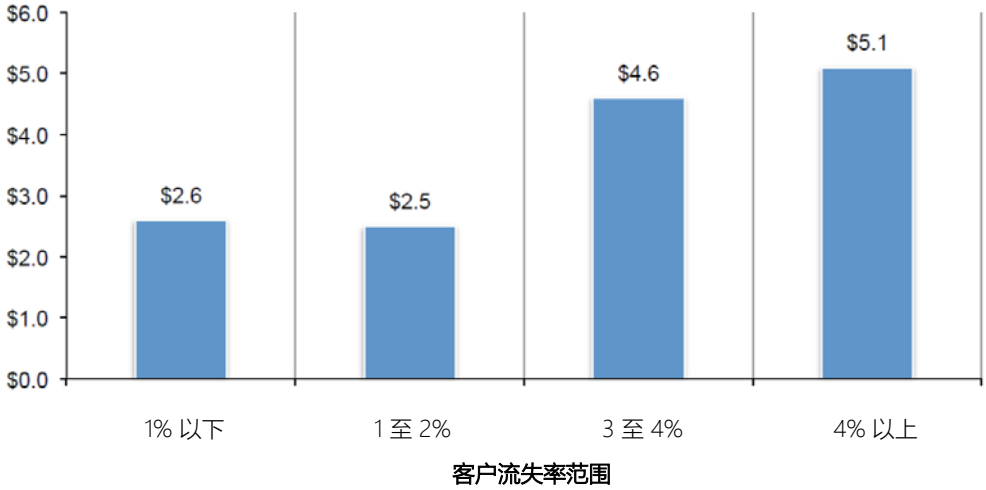
以美元为单位（以百万计）



客户流失得越多，数据泄露的成本越高。图 11 显示了 419 个组织出现 4 种异常客户流失率对应的数据泄露平均总成本，此 4 种流失率的范围从 1% 以下到 4% 以上不等。客户流失率在 1% 以下的公司要承担的平均总成本为 260 万美元。据我们估计，客户流失率在 4% 以上的公司要承担的平均总成本为 510 万美元。

图 11. 按异常客户流失率确定的平均总成本

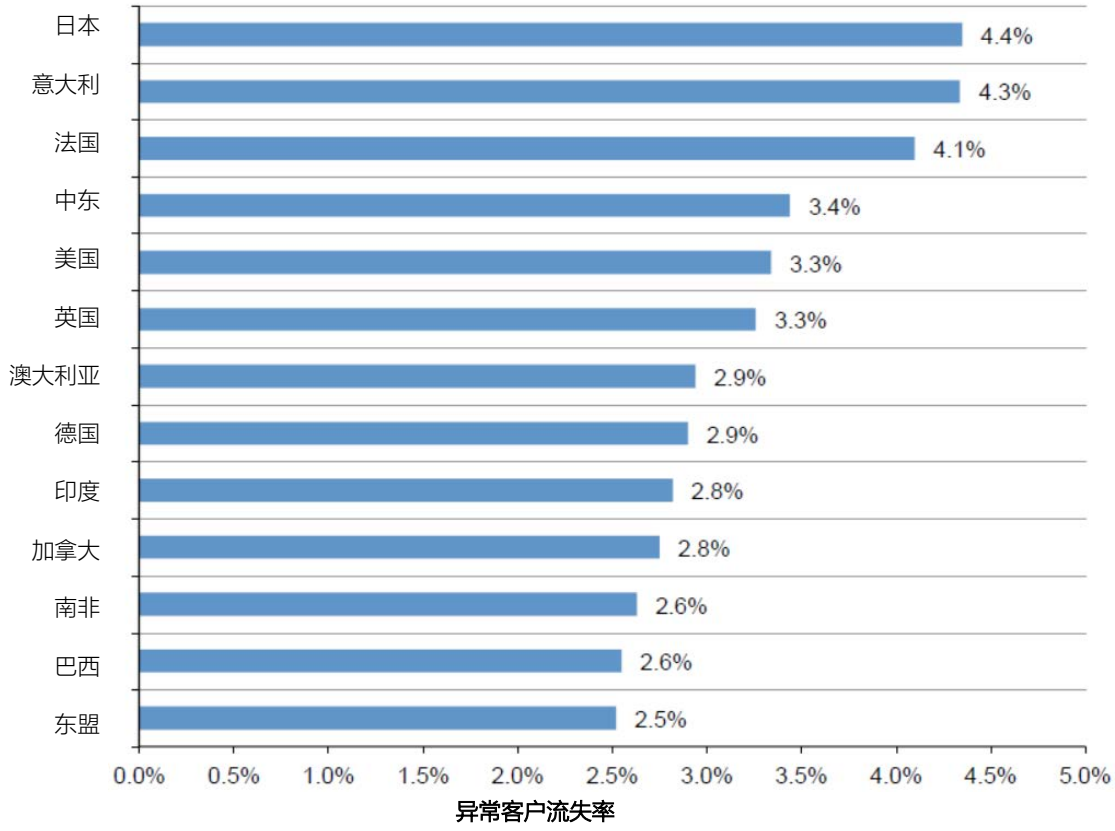
以美元为单位（以百万计）



某些国家/地区更容易出现客户流失的情况。图 12 显示了本次调研中各个国家/地区或区域样本对应的平均异常客户流失率。结果表明，各个国家/地区之间存在明显差异。日本、意大利和法国的异常客户流失率最高，而东盟、巴西和南非的异常客户流失率则最低。我们通过汇总 419 家公司所得的客户流失率总平均值为 3.24%。去年，平均客户流失率为 2.90%。因此，对于各个国家/地区中客户流失率较高的组织，他们可以通过重点开展客户保留活动来确保组织声誉及品牌价值，进而显著降低数据泄露成本。

图 12. 按国家/地区样本确定的异常客户流失率

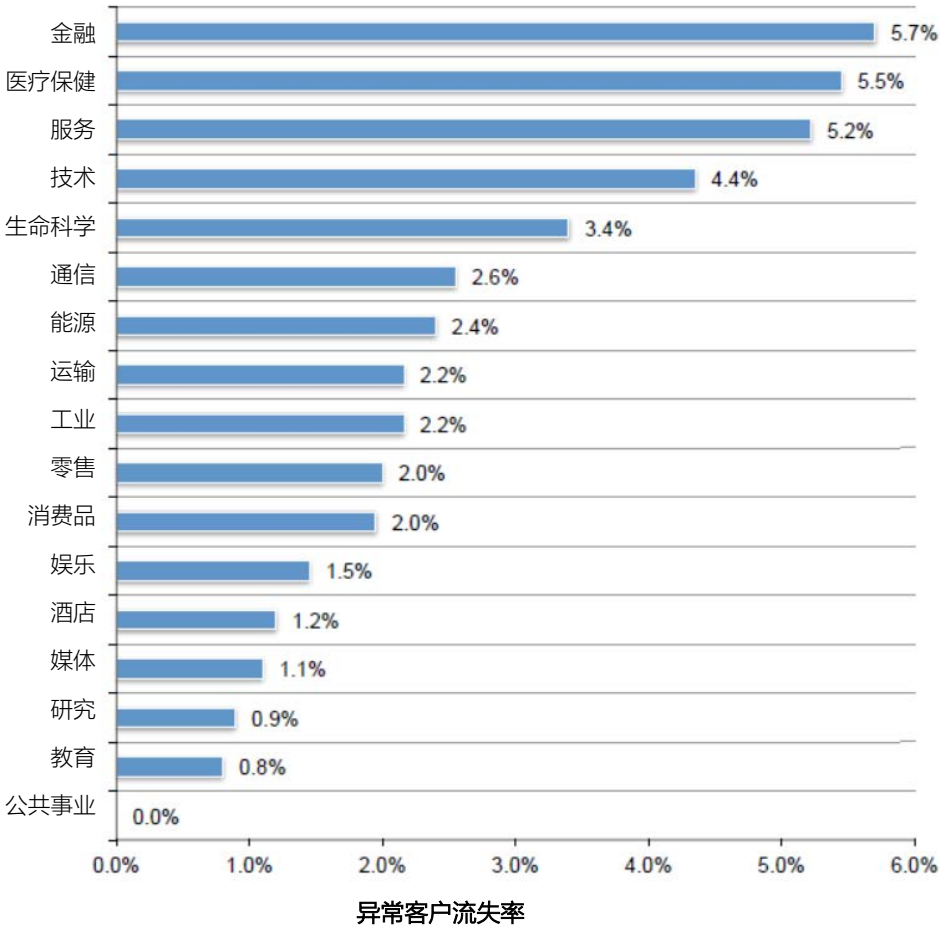
2017 财年的总平均值 = 3.24%



某些行业更容易出现客户流失的情况。图 13 显示了基于 17 个行业的异常客户流失率。由于本调研的样本量较小，我们无法从大体来分析行业对客户流失率的影响。不过，金融、医疗保健及服务业的组织出现的异常客户流失率较高，而公共事业及教育业的组织出现的异常客户流失率则相对较低。[9]

图 13. 按行业确定的异常客户流失率

2017 财年的总平均值 = 3.24%



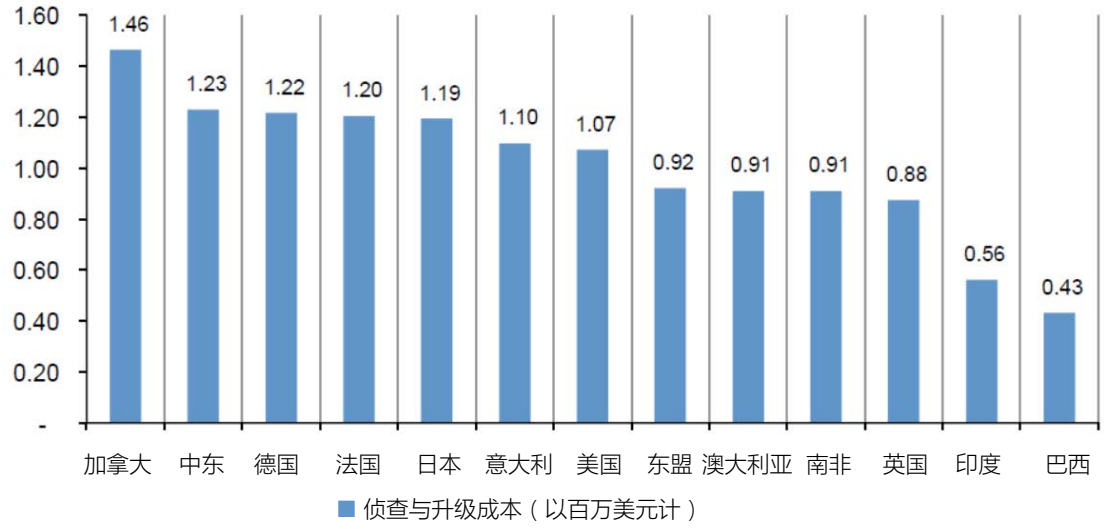
[9] 由于政府组织的客户一般没有备选项，因此公共事业组织会采用不同的客户流失率框架。

数据泄露成本组成部分方面的趋势

加拿大的侦查与升级成本最高，巴西的最低。侦查与升级成本一般涉及取证和调查活动、评估和审计服务、危机团队管理、与主管人员和董事会成员的沟通等。如图 14 所示，加拿大的平均侦查与升级成本为 146 万美元。相比之下，巴西的平均侦查与升级成本则仅为 43 万美元。

图 14. 侦查与升级成本

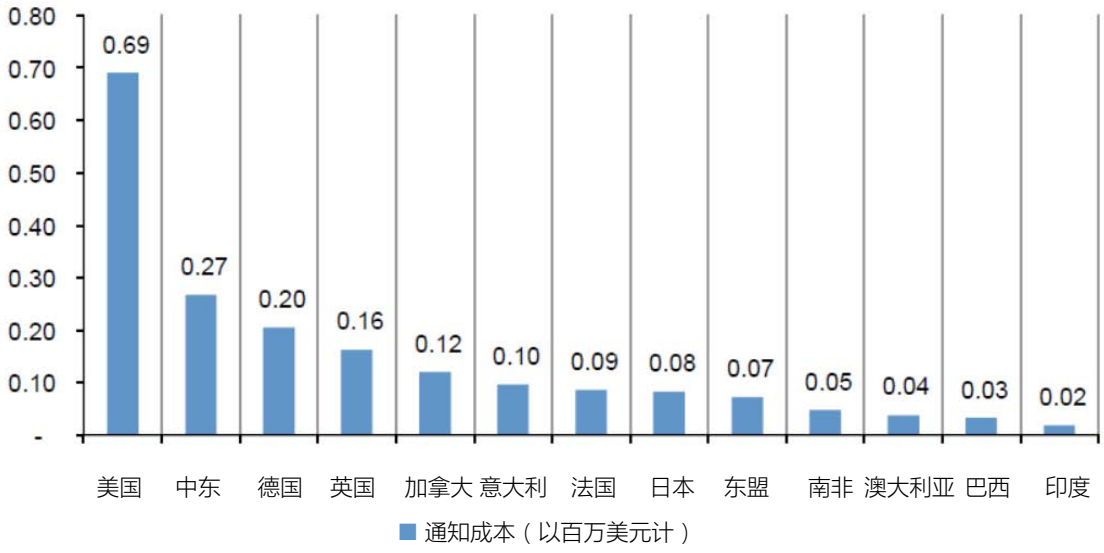
以美元为单位（以百万计）



美国组织要承担的通知成本最高。此类成本一般涉及创建联系人数据库、明确各项监管要求、聘请外部专家、电子邮件退回、入站通信设置等。到目前为止，美国组织要承担的通知成本最高（69 万美元），而印度组织要承担的通知成本则最低（2 万美元），具体如图 15 所示。

图 15. 通知成本

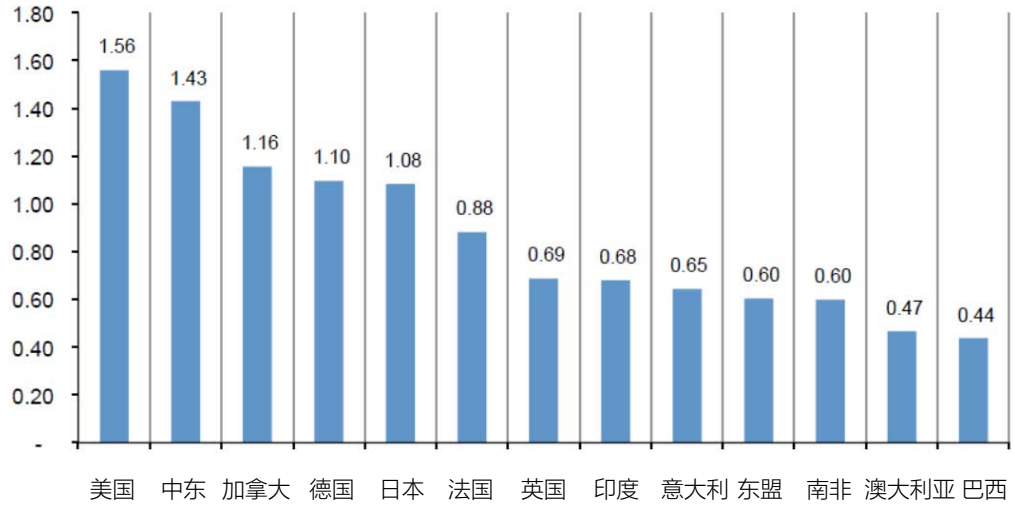
以美元为单位（以百万计）



美国和中东的组织在发生数据泄露事件后，要承担的响应成本最高。就美国的组织而言，与事后响应及侦查相关的成本为 156 万美元，而中东的组织在此方面要承担的成本则为 143 万美元，具体如图 16 所示。事后成本一般涉及服务台活动、入站通信、特殊调查活动、补救措施、法律开支、产品折扣、身份保护服务、监管干预等。

图 16. 事后响应成本

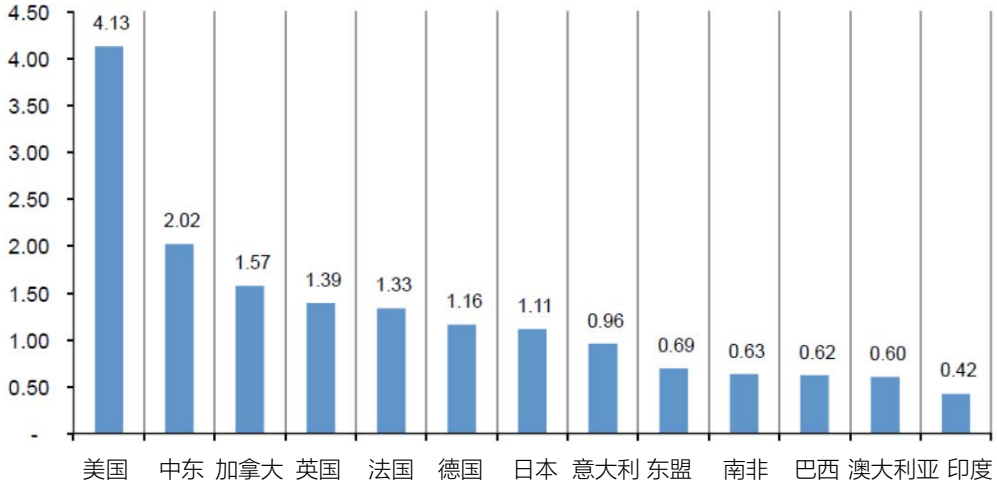
以美元为单位的事后响应成本（以百万计）



美国的组织在发生数据泄露事件之后，要承担的客户损失成本最高。如图 17 所示，美国的组织在损失业务方面要承担的成本明显较高，为 413 万美元。此类成本构成一般涉及异常客户流失率、客户争取活动增多、声誉损失、信誉丧失等。

图 17. 业务损失成本

以美元为单位的业务损失成本（以百万计）



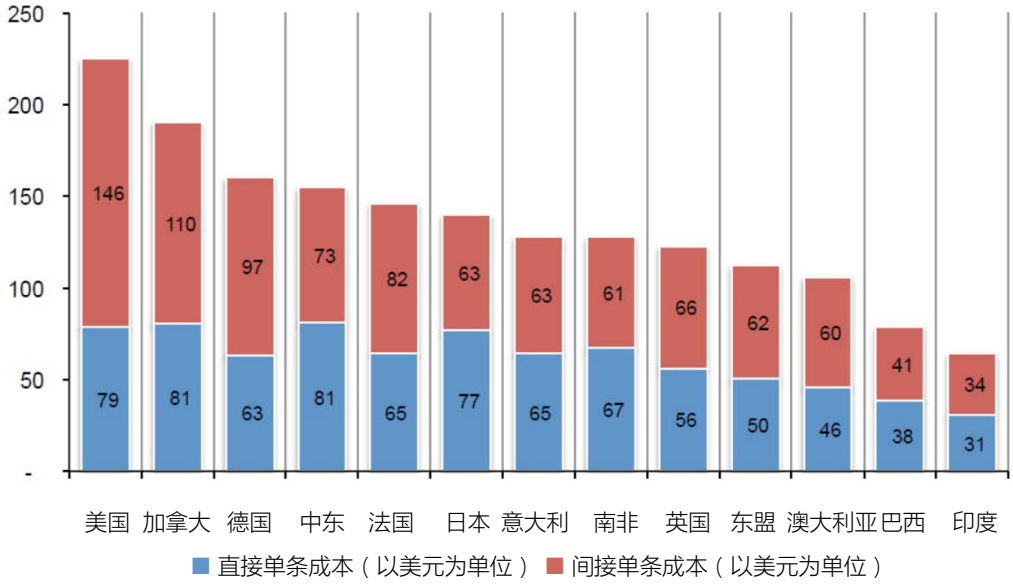
直接成本和间接成本的占比按国家/地区的不同而有所差异

中东和加拿大的组织投入的直接成本最高，美国的组织投入的间接成本最高。直接成本涉及开展特定活动所需的开支，比如聘请取证专家、聘请律师事务所、为受害者提供身份保护服务等。

间接成本与资源分配相关，比如通知受害者和调查泄露事件所需的员工时间及投入等。间接成本还包括信誉损失和客户流失。如图 18 所示，中东和加拿大的组织投入的直接单条成本最高，为 81 美元。美国的组织投入的间接单条成本最高，为 146 美元。

图 18. 数据泄露事件对应的直接单条成本和间接单条成本

以美元为单位

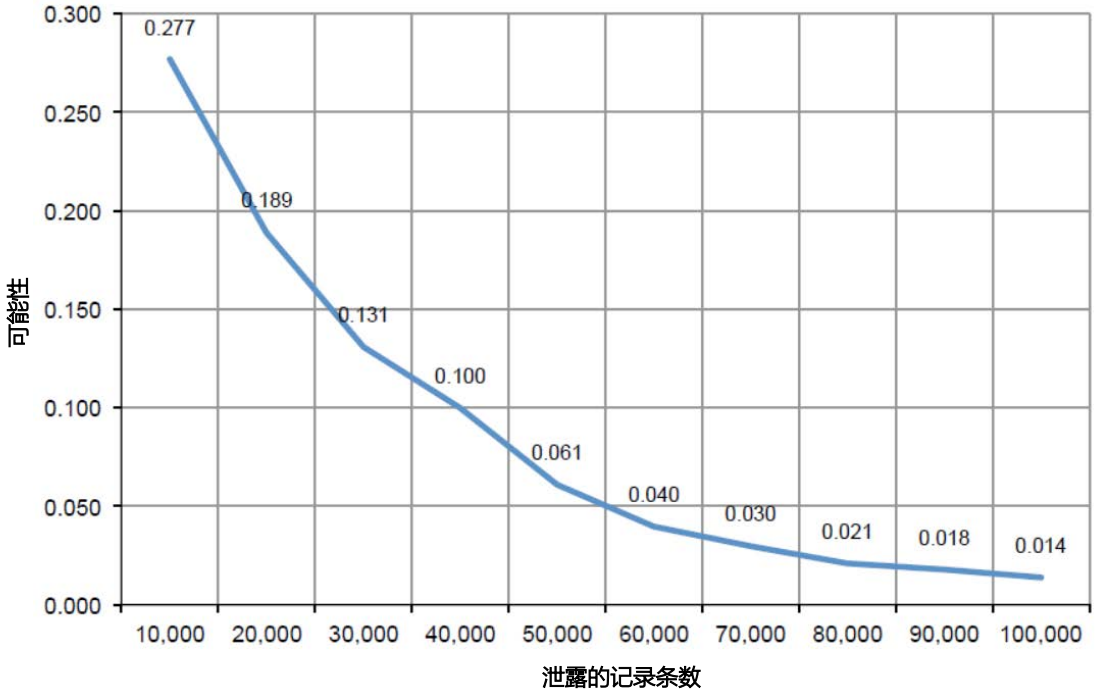


组织出现其他数据泄露事件的可能性

数据泄露事件的规模越大，组织越有可能在未来 24 个月内出现其他数据泄露事件。根据参与我们调研的组织在数据泄露事件方面的经历，出现数据泄露事件的可能性可基于两方面因素进行预测：丢失或被盗的记录条数，以及组织所在的位置。

图 19 显示了未来 24 个月内出现数据泄露事件的主观概率分布，其中至少涉及 10,000 条受损记录，至多涉及 100,000 条受损记录。[10] 如图所示，随着受损记录条数的增加，出现数据泄露事件的可能性呈稳定下降趋势。在 24 个月内，出现至少涉及 10,000 条记录的数据泄露事件的可能性预计在 27.7% 左右。而出现至少涉及 100,000 条记录的数据泄露事件的可能性则在 1% 以下。

图 19. 出现数据泄露事件的可能性（至少涉及 10,000 条记录，至多涉及 100,000 条记录）



[10] 通过运用点预估技术，基于样本受访者捕获的预估概率。CISO、CPO 等接受成本评估采访的关键个人针对 10 个级别的数据泄露事件（涉及的丢失或被盗记录条数在 10,000 条到 100,000 条不等），提供了他们对数据泄露可能性的预估结果。用于执行此项预估任务的时间范围是未来 24 个月。在参与调研的 419 家公司中，每家公司均有给出经外推得出的聚合概览分布。

南非、印度和巴西的组织更有可能出现其他数据泄露事件。图 20 汇总了国家/地区或区域样本在 24 个月内出现至少涉及 10,000 条记录的数据泄露事件的概率。该图比较了本年度的结果与四年的平均水平。虽然我们因样本量较小而无法从大体上分析各个国家/地区之间的差异，但我们还是可以通过预估的资料数据泄露可能性看出，各个国家/地区之间存在较大的差异。

结果显示，南非、印度和巴西的预估数据泄露可能性最高，分别为 40.6%、40.1% 和 39.3%。加拿大和德国的预估数据泄露可能性最低，分别为 14.5% 和 15.3%。

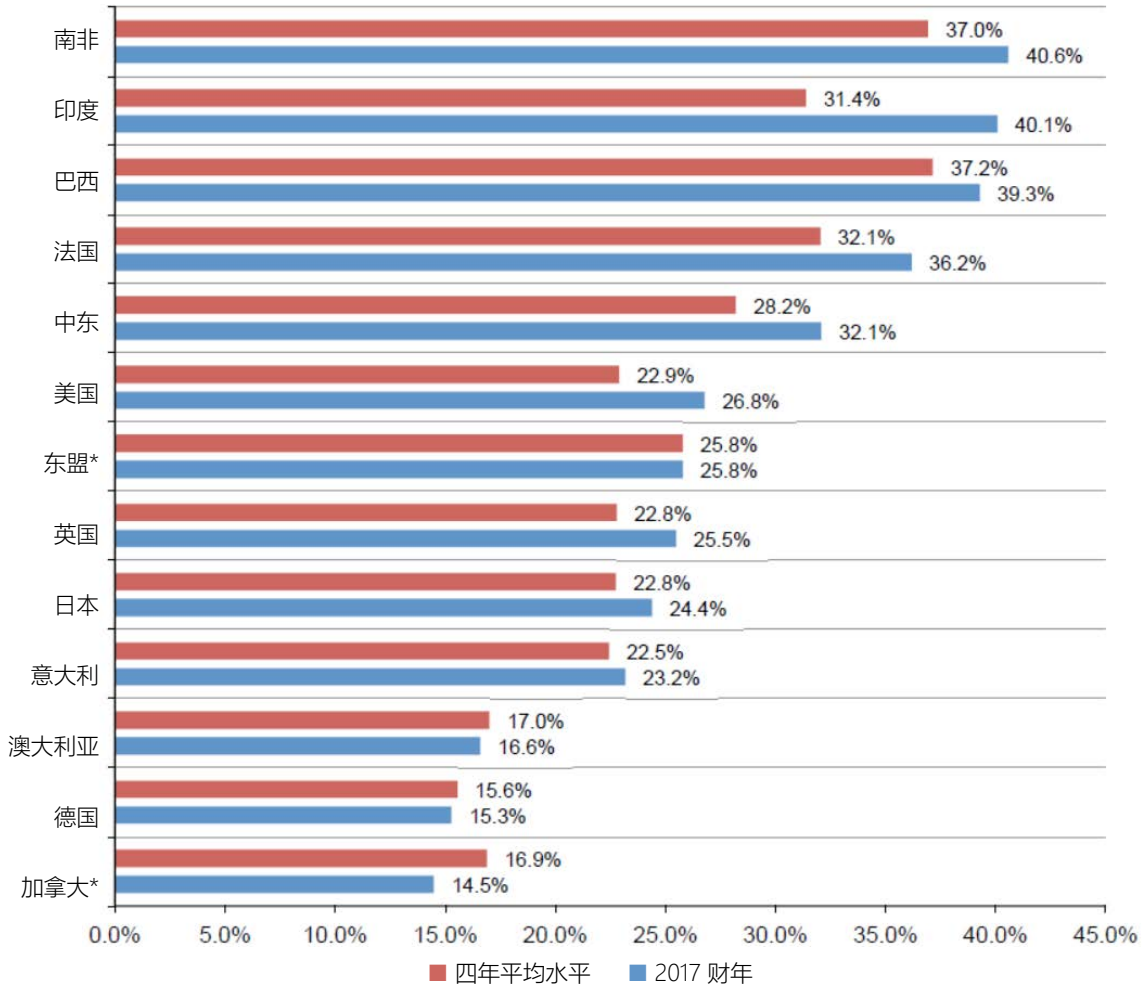
值得注意的是，13 个国家/地区中有 9 个在数据泄露可能性方面呈上升趋势。印度的增幅最大 (8.7%)，其次是法国 (4.2%)。相比之下，加拿大的降幅最大，为 2.4%。

图 20. 与四年平均水平相比，2017 年出现至少涉及 10,000 条记录的数据泄露事件的可能性

2017 财年的总平均值 = 27.7%；2016 财年的总平均值 = 25.6%；2015 财年的总平均值 = 24.5%；2014 财年的总平均值 = 22.2%

至少涉及 10,000 条受损记录

* 所有年限均无可用的历史数据

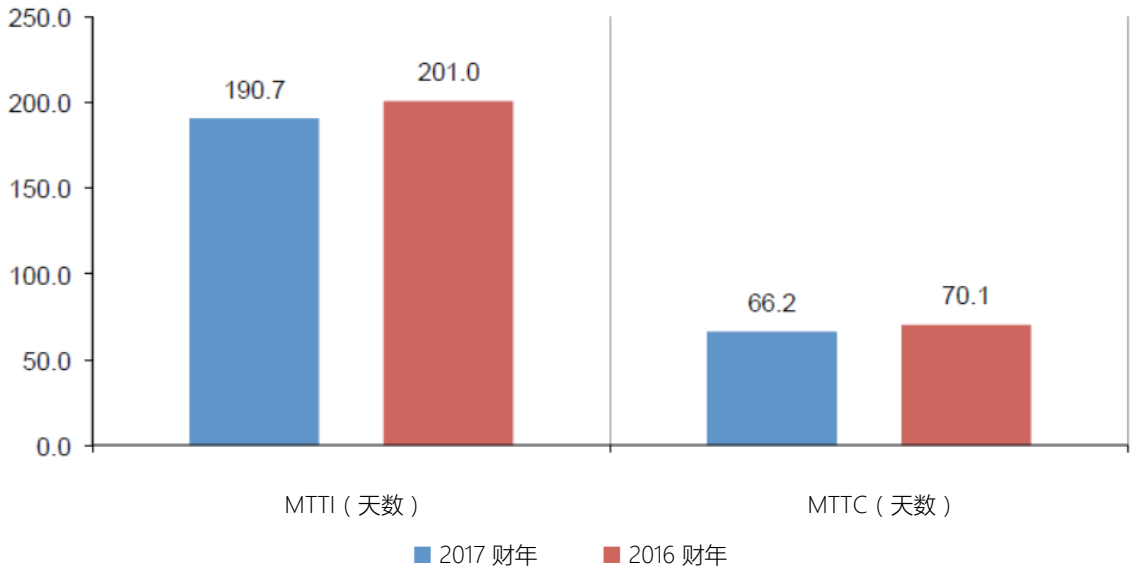


识别和遏制数据泄露所需的时间会影响成本

识别和遏制数据泄露的速度越快，所需投入的成本就越低。MTTI 和 MTTC 指标可用于确定组织在事件响应与遏制流程方面的效率。MTTI 指标有助于组织了解其侦查已发生数据泄露事件所需的时间，而 MTTC 指标则可用于衡量响应人员解决某种情况并最终恢复服务所需的时间。

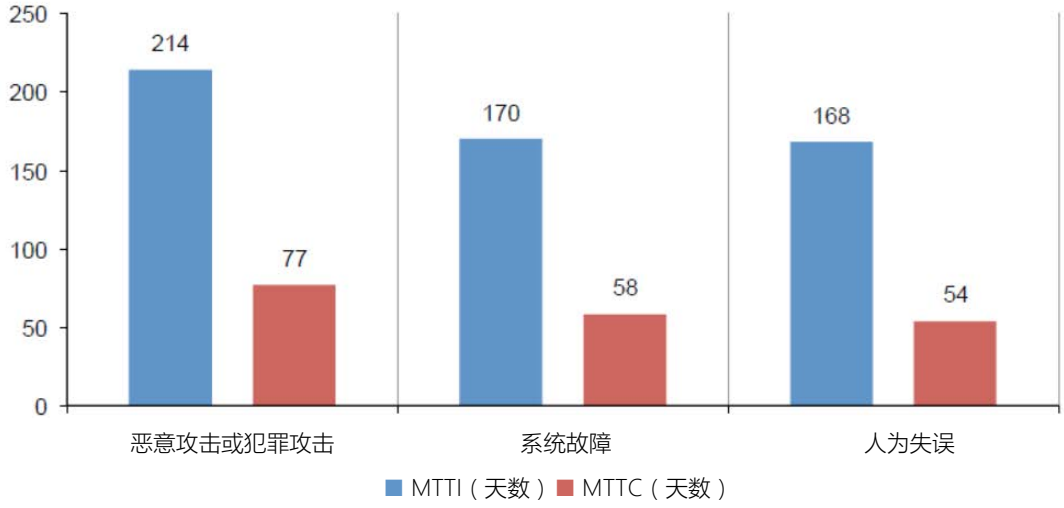
如图 21 所示，自去年以来，与数据泄露相关的 MTTI 和 MTTC 有所下降。在本年度调研中，我们通过整合有关 419 家公司的样本数据，确定 MTTI 为 191 天。MTTC 为 66 天，其范围在 10 天到 164 天不等。去年的 MTTI 和 MTTC 分别为 201 天和 70 天。

图 21. 去年，识别和遏制数据泄露所需的天数



识别和侦查恶意攻击或犯罪攻击所需的时间更长。图 22 显示了数据泄露事件之三大根本原因对应的 MTTI 和 MTTC。如图所示，恶意攻击和犯罪攻击对应的识别时间和遏制时间最长，分别是 214 天和 77 天。相比之下，人为失误导致数据泄露对应的识别时间和遏制时间则要短很多，分别是 168 天和 54 天。

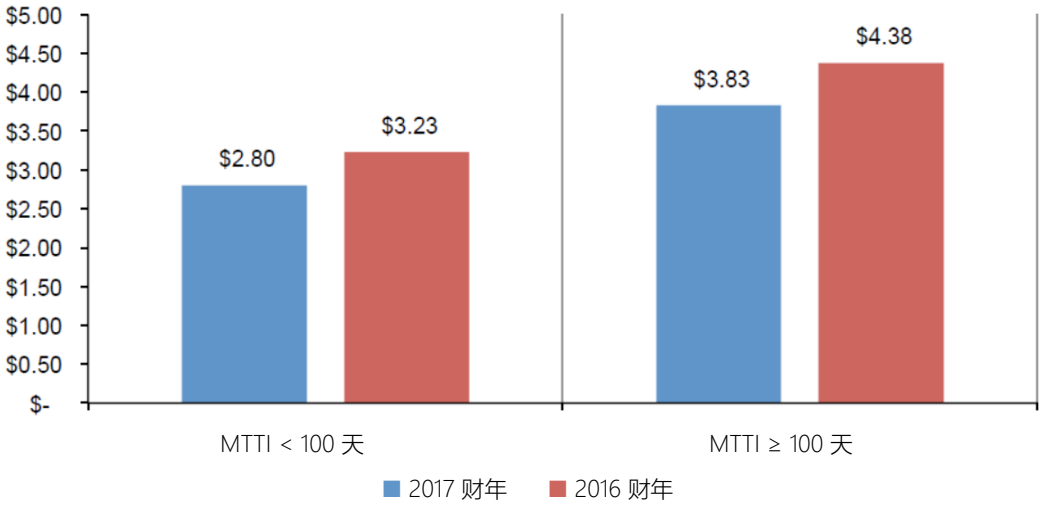
图 22. 按根本原因确定的识别和遏制数据泄露事件所需的天数



无法迅速识别数据泄露会导致成本上升。图 23 显示了针对 419 家公司确定的总数据泄露成本与泄露识别之间的关系。我们基于 MTTI 在 100 天以下的公司和 MTTI 在 100 天以上的公司，进行了样本交叉整合。如果 MTTI 在 100 天以下，则数据泄露的预估平均总成本为 280 万美元。如果 MTTI 在 100 天以上，则数据泄露的预估平均总成本为 383 万美元。此两类子样本之间的显著差异表明，无法迅速识别数据泄露会导致成本上升。通过使用有助于强化侦查或取证功能的工具，我们能够显著降低数据泄露成本。去年，与此两类子样本相关的平均总成本分别为 323 万美元（识别所需时间在 100 天以下）和 438 万美元（识别所需时间为 100 天或以上）。

图 23. 识别所需平均时间与平均总成本之间的关系

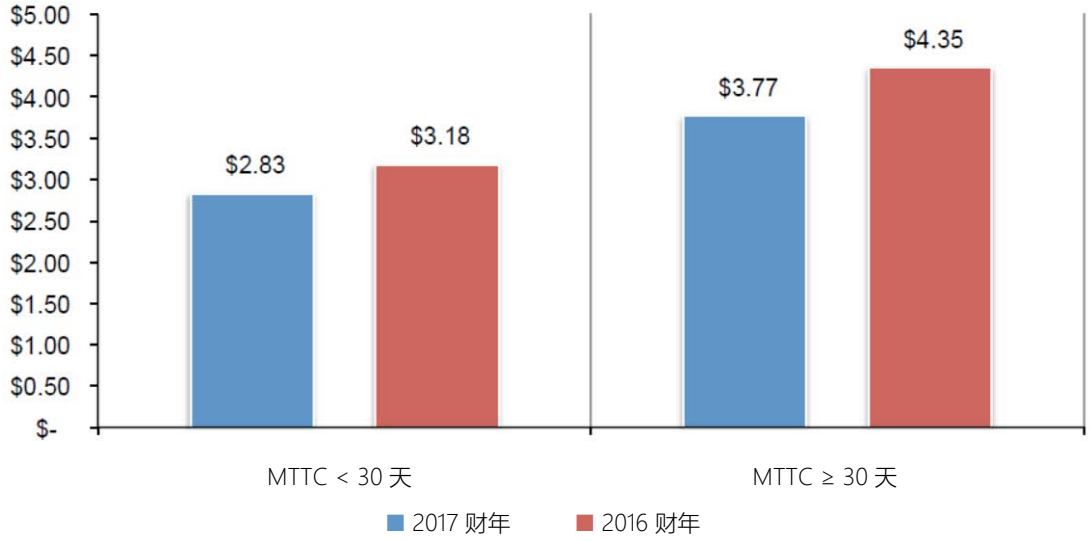
以美元为单位（以百万计）



遏制数据泄露所需的时间会影响成本。图 24 显示了针对 419 家公司确定的总数据泄露成本与泄露遏制之间的关系。我们基于 MTTC 在 30 天以下的公司和 MTTC 在 30 天以上的公司，进行了样本交叉整合。如果 MTTC 在 30 天以下，则数据泄露的预估平均总成本为 283 万美元。如果 MTTC 在 30 天以上，则数据泄露的预估平均总成本为 377 万美元。此两类子样本之间的显著差异表明，无法迅速遏制数据泄露会导致成本上升。通过使用全功能事件响应流程等有助于强化补救功能的工具和流程，我们能够显著降低数据泄露成本。去年，与此两类子样本相关的平均总成本分别为 318 万美元（遏制所需时间在 30 天以下）和 435 万美元（遏制所需时间为 30 天或以上）。

图 24. 遏制所需平均时间与平均总成本之间的关系

以美元为单位（以百万计）



第 3 部分：如何计算数据泄露成本

为了计算数据泄露的成本，我们使用了基于活动的成本计算 (ABC) 方法。该方法会识别各种活动，然后根据实际使用情况分配成本。我们要求参与此次基准调研的公司估算他们为解决数据泄露事件进行的所有活动对应的成本。

发现并立即响应数据泄露事件时常见的活动包括：

- 进行调查与取证，以确定数据泄露的根本原因
- 确定数据泄露的可能受害者
- 组织事件响应团队
- 进行沟通及公共关系宣传
- 准备将发送至数据泄露受害者及监管机构的通知文档及其他所需文档
- 实施呼叫中心程序及专业化培训

在发现数据泄露后组织通常会实施的活动包括：

- 审计与咨询服务
- 法律服务 - 辩护
- 法律服务 - 合规性
- 向数据泄露受害者提供的免费或折扣服务
- 身份保护服务
- 根据客户流失率或流动率计算客户业务损失
- 客户获取与忠诚度计划成本

公司估算出上述活动的成本范围后，我们会按照以下定义将此类成本归类为直接成本、间接成本和机会成本：

- *直接成本* – 完成给定活动所产生的直接开支。
- *间接成本* – 为解决数据泄露事件而分配的时间、投入及其他组织资源（直接成本开支除外）。
- *机会成本* – 由于在受害者获知发生了数据泄露之后（以及在向媒体公开披露之后）而对公司声誉造成的负面影响而导致的业务机会流失所对应的成本。

我们的调研也包括核心流程相关的活动，这些活动也会由于组织针对数据泄露所进行的检测、响应、遏制和补救而产生开支。有关每类活动的成本，请参见"第 2 部分：重要调研结果"章节。四个成本中心分别为：

- 检测或发现：公司合理检测处于风险之中（存储中）或传输中的个人数据泄露而进行的活动。
- 提交：在规定期限内向适当个人报告受保护信息泄露而必须进行的活动。
- 通知：公司通过信函、外部呼叫中心、电子邮件或常规通知的形式告知数据主体其个人信息已丢失或被盗而进行的活动。
- 数据泄露事后处理：通过与数据泄露事件的受害者交流，帮助他们最大程度降低潜在危害，同时提供其他方面的协助，比如监控信用报告、重建新账户或信用卡等等。

除了开展与上述流程相关的活动之外，大部分公司还分析了与数据泄露事件相关的机会成本。导致这些成本产生的原因在于，当前客户和未来客户对公司丧失信任或信心。因此，Ponemon Institute 的调研也考虑了由于数据泄露事件相关的公司声誉受损所导致的异常客户流动或流失率以及新客户获取方面的减少量。

为了外推这些机会成本，我们使用了一种成本估算方法，该方法主要基于针对每个参与调研公司所确定的平均客户"生命周期价值"。

- 现有客户的流失率：最有可能由于数据泄露事件而与公司终止关系的客户的预估数量。增量损失是指由于数据泄露事件而导致的异常流动。该数字以年度百分比进行计算，主要基于在基准访谈过程中管理层所提供的预估数据而得出。[11]
- 客户获取方面的减少量：由于发生了数据泄露将不会与公司建立合作关系的目标客户的预估数量。该数量以年度百分比的形式提供。

我们认为员工记录等非客户数据的丢失将不会影响组织的客户流失率或流动率。[12] 在这些情况下，我们预计，如果数据泄露未涉及到客户数据或消费者数据（包括客户/消费者的支付交易信息），将会产生较低的业务成本。

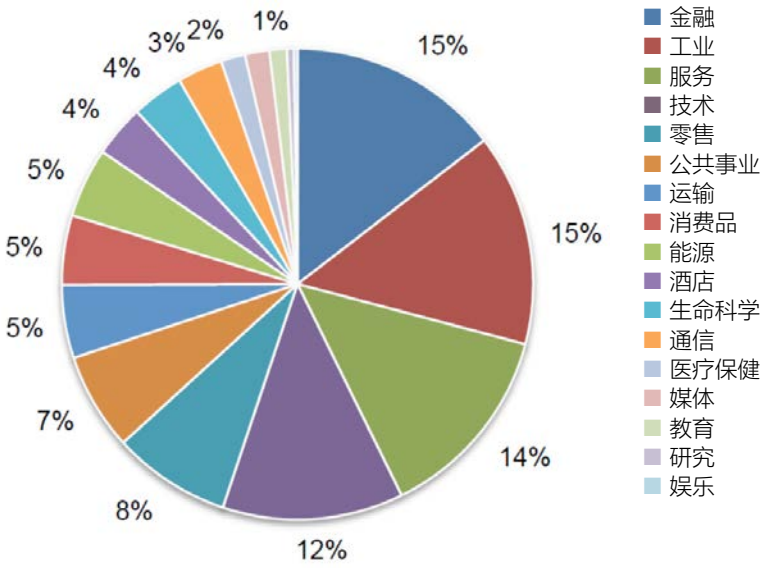
[11] 在多种示例中，客户流动都仅限于局部范围，在这些情况中，数据泄露的受害者仍旧会继续与组织进行合作，但客户的合作量实际上会有所下降。这种部分性的下降在特定行业中会尤为显著，例如金融服务、公共事业等等，因为这些行业的合作终止成本非常高昂或者从经济上来说并不可行。

[12] 在此次调研中，公民、病患和学生相关信息均归类为客户数据。

第 4 部分：组织特性及基准方法

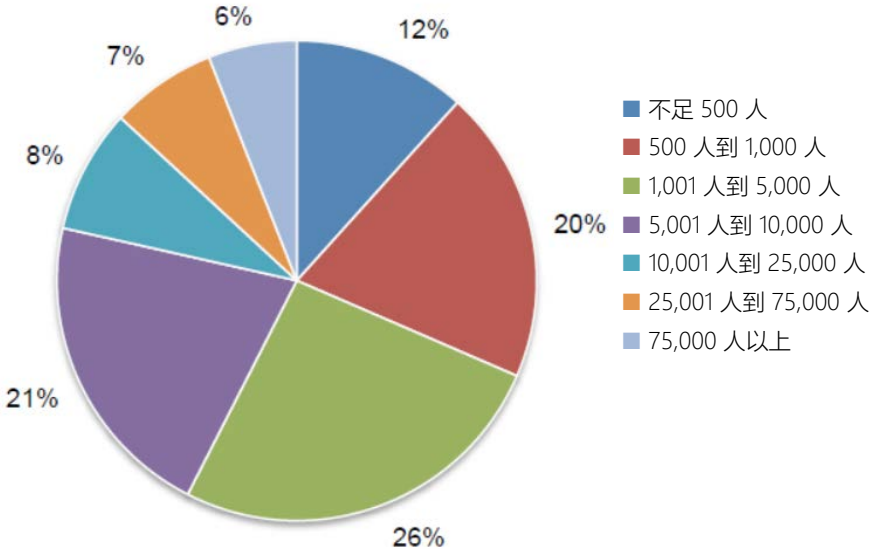
饼分图 3 显示了基准组织按主要行业分类的分布情况。本年度调研涉及十七 (17) 个行业。占比最大行业为金融服务公司和工业公司所在的行业。就金融服务公司而言，受访者包括银行、保险公司、投资管理公司，以及支付处理公司。

饼分图 3. 按行业细分确定的基准样本分布



饼分图 4 显示了按员工总数确定的基准组织分布。最大的细分类别包括员工总数在 1,001 人到 5,000 人范围内的公司。最小的细分类别包括员工总数在 75,000 人以上的公司。

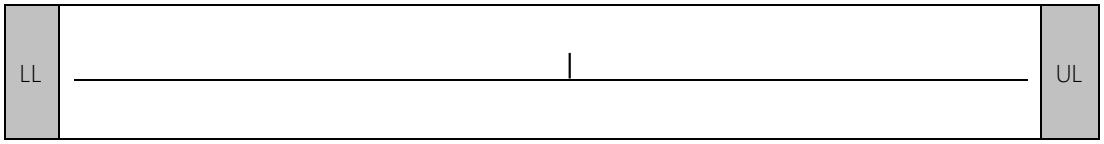
饼分图 4. 参与公司的全球员工总数



数据收集方法未包括实际会计信息，而主要依赖于以各参与者知识及经验背景为基础的数值估算。基准工具会要求个人针对各个成本类别划分直接成本预估的等级，具体通过标记以下列数轴形式定义的范围变量。

数轴的用法：各数据泄露成本类别中提供的数轴可用于获取最佳预估结果，以便我们了解现金支出总和、劳力资源投入及其他方面的开销。请在线上设定的上下限之间，标记一个数据点（有且仅有一个）。受访期间，您可以随时重设数轴的上下限。

请在此给出直接成本的预估结果 [依据现有成本类别]



通过数轴而非各现有成本类别估值点获取的数值不仅有助于确保机密性，还可以进一步提升响应率。基准工具也会要求相关领域的实践者分别提供有关间接成本及机会成本的二次预估结果。

为了保证基准调研流程在可管理规模范围内，我们对各调研项作出了缜密的限制，仅考虑对数据泄露成本评估有关键影响的成本活动中心。通过与经验丰富的专家进行探讨，最终的调研项仅包括一组固定的成本活动。在收集基准信息的基础上，我们仔细复查了各个基准工具，以便确保结果的一致性及完整性。

为了确保百分之百的机密性，基准工具不会捕获任何公司特定的信息。受访者资料中不含任何追踪代码，或其他能将受访者作答结果与受访公司之间建立联系的方法。

我们的基准工具中包含的数据泄露成本项范围仅限于已知的成本类别，适用于多种可对个人信息加以处理的业务运营操作。我们认为，以业务流程而非数据保护或隐私合规活动为核心的业务流程有助于产生质量更高的结果。

第 5 部分：限制事项

我们的调研采用高度机密的专有基准法，此方法已在早期调研中成功部署。不过，此基准调研中仍存在一些固有的限制事项，需在根据调研结果作出结论之前予以审慎考虑。

- 非统计性结果：调研过程中，我们利用了一系列具有代表性的非统计性样本，涉及在过去 12 个月内发生过客户或消费者记录丢失或窃取等数据泄露事件的全球实体。统计推断、误差幅度及置信区间不适用于这些数据，因为我们的取样方法不属于科学性方法。
- 非响应性：当前的调研结果基于具有代表性的小容量基准样本。在本次全球调研中，419 家公司完成了基准流程。由于整个流程中未检测无响应偏差，因此始终存在一种可能，即未参与调研的公司在潜在数据泄露成本方面会有实质性差异。
- 取样框架偏差：由于我们的取样框架属于判断式框架，所得结果的质量会因取样框架在所调研公司总人数方面所具备的代表性而受到不同程度的影响。我们认为，当前的取样框架会更多地偏向于具备更为成熟的隐私政策或信息安全项目的公司。
- 公司特定信息：基准信息属于较为敏感的机密信息。因此，当前采用的调研工具不会捕获可识别公司身份的信息。此外，该工具也允许个人使用类别响应变量，以披露与公司及行业类别相关的人口统计信息。
- 未衡量的因素：为确保访谈脚本的简洁凝练，我们在分析结果中省略一些其他的关键变量，比如领先趋势、组织特征等。这些变量的省略程度即可说明不可确定基准结果的原因。
- 外推的成本结果：基准调研的质量高低取决于在参与调研的公司中，受访者是否给出完整、可信的回答。尽管我们可在基准流程中加入特定的制衡原则，但始终存在一种可能，即受访者未给出准确、真实的回答。此外，采用成本外推法而非实际成本数据也会不可避免地产生一些偏差及不精确的结果。
- 货币换算损益：今年，美元走强对全球成本分析产生了显著影响。在当地货币与美元的换算过程中，单条成本与平均总成本均在预估的走低范围内，尤其是对于英国、德国、法国和意大利的公司（比如使用英镑 (£) 和欧元 (€) 的公司）。为了与往年的做法保持一致，我们决定沿用之前的核算方法，而非在成本方面作出调整。要注意，这只会对全球分析产生影响，因为所有国家/地区级别的结果均以当地货币显示。

如果您对本调研报告存有任何疑问或意见，或希望获取额外的文件副本（包括引用或重用本报告的权限），请通过信件、电话或电子邮件联系我们：

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

如欲获取所有国家或地区报告的完整副本，请登录：www.ibm.com/security/data-breach

Ponemon Institute LLC

致力于推动富于责任感的信息管理

Ponemon Institute 致力于进行独立调研和培训，旨在推动企业和政府中可靠的信息和隐私管理实践。我们的使命是对可能影响人员和组织敏感信息的管理和安全性的关键问题进行高质量的实证调研。

我们遵守严格的数据保密、隐私和道德调研标准。我们不会从个人收集任何个人识别信息（或在业务调研中出现的公司识别信息）。此外，我们还执行严格的质量标准，确保不会向当事人提出不相关或不适当的问题。