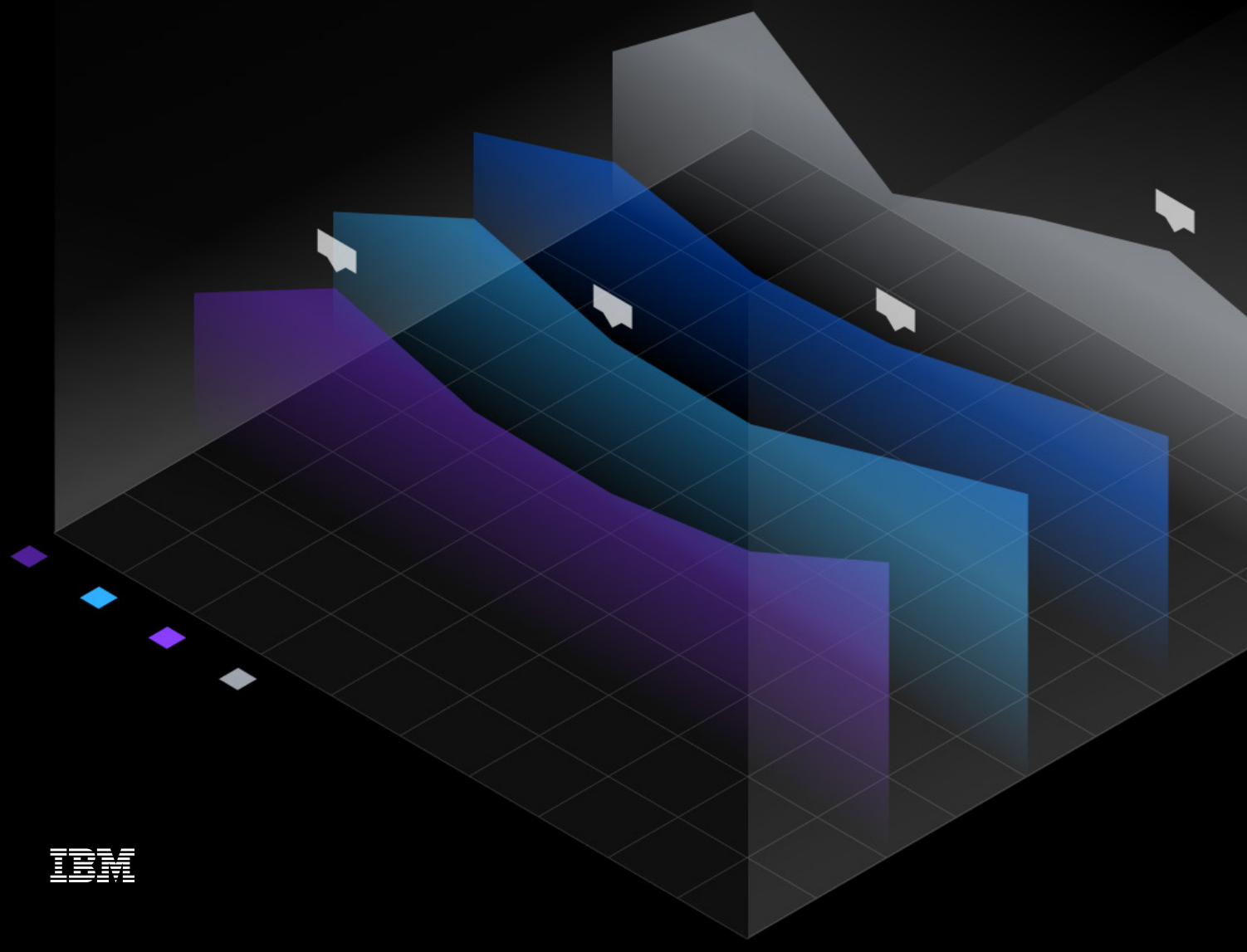
IBM Security

2020 年数据泄露成本报告



IBM

目录

执行摘要

这是 Ponemon Institute 连续第 15 年开展研究*发布年度《数据泄露成本报告》*，其中五年的报告由 IBM Security 赞助和发布。我们希望企业可以利用此研究加快创新，同时也希望当不同类型和规模的组织在面临数据泄露和网络安全事件风险时，也能留住客户信任。

该报告已成为网络安全行业的主要基准工具之一，让 IT、风险管理和安全领导者实时了解能够规避或加剧数据泄露成本的因素。此报告还会展示我们分析过的成本中的一致性和波动性，帮助我们洞悉数据泄露趋势。

在 2020 年 *的数据泄露成本报告*[*] *中*，Ponemon Institute 招募了 524 家在 2019 年 8 月至 2020 年 4 月期间经历过数据泄露的企业。为确保研究尽可能涉及更多行业的公司，本研究甄选了来自 17 个国家/地区、涵盖 17 个行业且规模各异的公司。我们的研究人员采访了 3,200 多位知情人士，他们所在的企业都发生过数据泄露事件。

数据泄露成本报告数据

524
发生泄露的组织

3,200
位接受访问的个人

17
个国家和地区

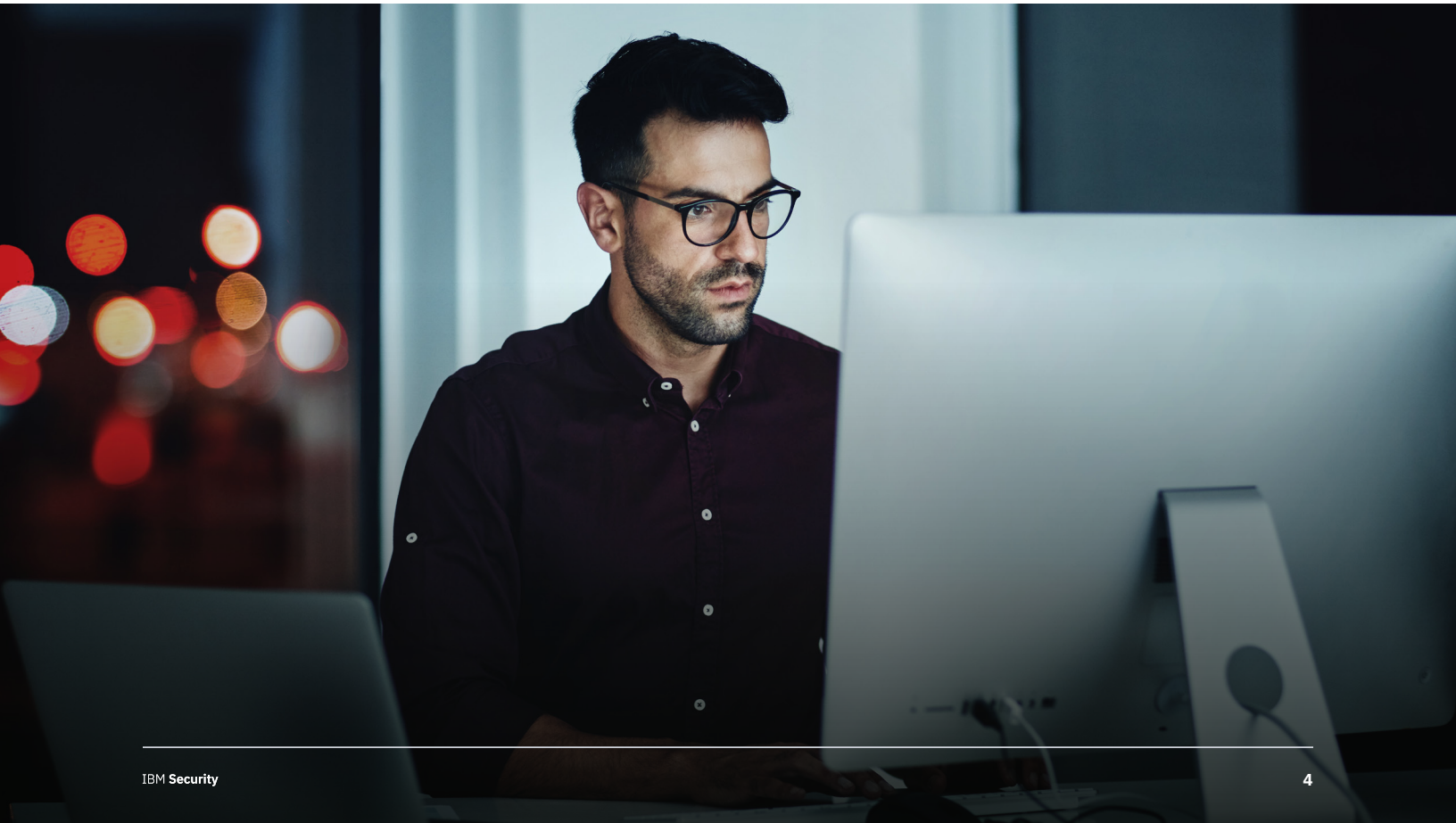
17
行业

[*]本报告中的年份是指发布年份，而不一定是发生泄露的年份。2020 年报告中分析的是 2019 年 8 月至 2020 年 4 月期间发生的数据泄露。

在访问的过程中，我们还提出了一些问题，以判断企业在发现泄露和立即响应数据泄露等活动上的支出。还有一些问题也会影响成本，例如数据泄露的根本原因；组织用于发现和控制事件的时间以及因为泄露导致业务中断并失去客户造成的预计损失。我们还考察了其他一些成本因素，例如泄露之前实施的安全措施，组织及其 IT 环境的特征等。

因此我们的报告可提供庞大的数据集、广泛的分析和趋势洞察。在后面的执行摘要中，我们简要介绍了如何计算数据泄露成本以及本次研究的一些重要发现。为深入了解数据，完整的结果部分列举了 49 张分析图和人口统计图。

基于研究得出的对组织而言最行之有效的措施，我们为 IT 领导者、网络安全战略家和风险管理员提供安全措施建议，降低数据泄露可能带来的财务损失和品牌损害。报告的最后详细阐释了我们的研究方法。



2020 年报告新增内容

我们希望每年更新报告，以提供既立足于往年报告又能找到突破点，紧跟日新月异的技术和趋势，以便企业更全面地了解风险和确保数据安全的标准。

2020 年注定是不平凡的一年。除了技术和威胁方面周而复始的变化之外，一场席卷全球的疫情让世界各地的企业和消费者的生活有了翻天覆地的变化。

尽管本次研究在新冠疫情迅速蔓延之前数月便已启动，但在研究的大多数泄露事件发生之后，我们仍然要求参与者回答一些补充性问题，这些问题都与新冠疫情之下开展远程工作所带来的潜在影响有关。我们发现，大多数组织 (76%) 都预计远程工作会让响应潜在的数据泄露面临更严峻的考验。

今年的报告中加入了新的研究，可更加深入地了解我们长期使用的数据类型 — 其中包括数据泄露每条记录的成本以及数据泄露的根本原因。我们首次在研究中细分了被盗的每条记录的成本，以便基于泄露的记录类型来分析成本，这些记录类型包括客户个人身份信息 (PII)、员工 PII 以及知识产权 (IP)。在分析数据泄露根本原因时，我们更加深入地探索了更具体的恶意泄露类型，其中包括凭据被盗和内部人员威胁等。

本次研究首次要求参与者识别被推定为对泄露负责的威胁主体类型，其中包括国家和受经济利益驱动的攻击者，我们的成本分析显示，最常见的恶意泄露类型，即受经济利益驱动的网络犯罪分子攻击导致的泄露，并非成本最高的类型。

随着勒索软件和破坏性恶意软件的攻击日益普遍，我们在今年的报告中新增了成本分析，结果发现，这些致命攻击的平均泄露成本要高于数据泄露的整体平均水平。

数据泄露统计信息

$3.86 百万
平均总成本

美国
成本最高的国家

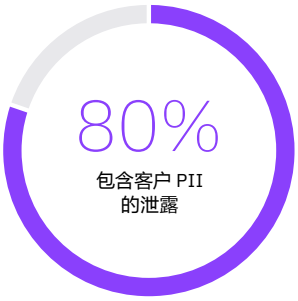
医疗保健
成本最高的行业

280 天
发现和控制所需的平均时间

今年的研究中还新增了几项成本因素，例如漏洞和红队测试的影响（使用一种对抗方法进行渗透测试）以及远程工作和安全技能短缺对这些成本的影响。毫不意外，在研究分析的 25 项可增加数据泄露平均成本的因素中，技能短缺排名前三，而红队测试则是可降低数据泄露平均成本排名前五的成本因素。

报告还审查了一些新的问题，例如深入探讨了首席信息安全官所发挥的作用以及网络安全保险涵盖的成本类型。

值得注意的是，在今年的报告中，数据泄露的平均总成本略有下降，从去年的 392 万美元下降至今年的 386 万美元，这一现象让一些人认为数据泄露成本已趋于饱和。



另一方面，我们的研究似乎显示，拥有更先进的安全流程（如自动化和正式的事件响应团队）的组织，与那些在这些领域的安全态势不那么先进的组织之间的数据泄露成本差距越来越大。

这是一份全球性报告，研究所涉及的范围之广，意味着我们不能在此次研究中强调所有国家/地区和行业的数据泄露成本的细微差别。正因为如此，我们开发了在线计算器和数据探索工具 (ibm.com/databreach)，方便您进行定制并发现自己需要的内容。

我们希望您能从中得到对您的组织富有意义的洞察，并得出有用的结论，更好地保护您的企业取得成功所依赖的数据。

我们如何计算数据泄露的成本

为计算数据泄露的平均成本，本研究排除了极小和极大规模的泄露。2020 年研究考察的数据泄露中被破坏的记录在 3,400 至 99,730 条不等。我们单独分析了 “大规模泄露” 的成本，在报告的 “完整的结果” 部分会对此加以详细说明。

本次研究使用了一种名为作业成本法 (ABC) 的会计方法，这种方法可识别活动并根据实际的使用分配成本。四项流程相关的活动造成了一系列与组织的数据泄露相关的支出：检测和升级、通知、数据泄露后响应以及失去业务。

下文详细介绍了这四个成本中心。

要更加深入地了解此报告使用的方法，请参阅 研究方法部分。

检测和升级

使公司能够合理发现泄露的活动。

- 取证和调查活动
- 评估与审计服务
- 危机管理
- 与管理层和董事会沟通

业务损失

可最大程度减少客户流失、业务中断和收入损失的活动。

- 因为系统停机造成的业务中断和收入损失
- 客户流失和获取新客户的成本
- 名誉受损和商誉降低

通知

让公司能够通知数据主体、数据保护监管机构及其他第三方的活动。

- 发送给数据主体的电子邮件、信函、通话或一般通知
- 确定法规要求
- 与监管机构沟通
- 联系外部专家

事后分析响应

帮助数据泄露受害者与公司沟通以及赔偿受害者和缴纳监管机构罚款的活动。

- 帮助台和入站通信
- 信用监控和身份保护服务
- 开设新帐户或新信用卡
- 法律支出
- 产品折扣
- 监管机构罚款

重要发现

本文的重要发现以 IBM Security 对 Ponemon Institute 编纂的研究数据所作的分析为基础。

-1.5%

平均总成本净变化
(2019-2020 年)

尽管数据泄露平均总成本同比略有下降，但许多公司的成本却不降反增。

表面来看，尽管成本从 2019 年研究中的 392 万美元下降至 2020 年研究中的 386 万美元，但最成熟的公司和行业的成本仍然较低，而那些在安全自动化和事件响应流程中落后一步的组织，其成本则要高出很多。更深入地分析单个丢失或被盗记录的平均成本（每条记录的成本）之后发现也普遍存在差异，具体视泄露中丢失或被盗的数据类型而异。

$150

每条记录的客户 PII 平均成本

在我们研究的数据泄露中，客户的个人可识别信息 (PII) 是最常受到破坏的记录类型，其成本也最高。

在遭到攻击的组织中，有 8% 的组织表示，数据泄露中被盗的客户 PII 远远高于任何其它记录类型。在所有数据泄露中，丢失或被盗记录的平均成本为 146 美元，而那些包含客户 PII 的被盗记录的平均成本为 150 美元。

恶意攻击引发的数据泄露中，客户 PII 每条记录的成本会增加至 175 美元。研究中有 24% 的数据泄露涉及到匿名客户数据，每条记录的平均成本为 143 美元，它将恶意攻击引起的数据泄露中的每条记录的成本增加至 171 美元。

+$137,000

远程工作对平均总成本的影响

新冠疫情期间的远程工作会增加数据泄露成本和事件响应时间。

在表示因为新冠疫情需要开展远程工作的组织中，70% 的组织认为此举会增加数据泄露的成本，76%的组织认为会增加发现和控制潜在数据泄露的时间。远程工作会使 386 万美元的数据泄露平均总成本增加近 137,000 美元，增加后的平均总成本为 400 万美元。

凭据被盗或泄露是导致恶意攻击数据泄露的最昂贵的原因。

每五家遭受恶意数据泄露的公司中就有一家 (19%) 是由于凭证被盗或泄露而被渗透，使这些公司的泄露平均总成本增加了近 100 万美元，达到 477 万美元。整体而言，恶意攻击是最常见的根本原因（占研究中的泄露的52%），其次是人为失误 (23%) 或系统故障 (25%)，平均总成本为 427 万美元。

+14%

云错误配置对平均总成本的影响

云端的错误配置是泄露的主要原因。

除了被盗或被破坏的凭据之外，错误配置的云服务器也是恶意攻击引起的数据泄露中最常见的初始威胁向量，占 19%。云错误配置导致的泄露平均成本增加了 50 多万美元，达到 441 万美元。

$1.52 百万

失去业务平均总成本

失去业务仍然是最主要的成本因素。

失去业务的成本约占数据泄露平均总成本的 40%，从 2019 年的 142 万美元增加至 2020 年的 152 万美元。失去业务的成本中包括更高的客户流失率，因为系统停机时间损失的收入以及因为声誉受损而增加获取新业务的成本。

358 万美元

与未部署安全自动化的组织相比，全面部署了安全自动化的组织平均节省的成本

安全自动化对数据泄露成本的影响在过去三年间也有所增长。

全面部署了安全自动化（使用了人工智能平台和自动化泄露编排）的企业，从 2018 年的 15% 增加到 2020 年的 21%。

同时，安全自动化在降低数据泄露平均成本方面的效力也在不断增强。尚未部署安全自动化的企业的平均总成本为 603 万美元，是全面部署安全自动化的企业的两倍以上，后者的数据泄露平均成本为 245 万美元。相比那些未部署安全自动化的公司，全面部署了安全自动化的公司节省的成本从 2018 年的 155 万美元增长到了 358 万美元。

100x

超过 5000 万条记录的泄露与普通泄露的成本倍数

大规模泄露成本飙升了数百万美元。

在超大数据泄露的样本中，泄露记录数量超过 100 万条的公司承担的成本是整体平均成本的很多倍。涉及 100 万条至 1000 万条记录的泄露的平均成本为 5000 万美元，是记录少于 100,000 条的泄露平均成本（386 万美元）的 25 倍以上。在记录超过 5000 万条的泄露中，平均成本为 3.92 亿美元，是平均值的 100 多倍。

国家主体导致的泄露成本最为高昂。

尽管大多数恶意泄露都由受经济利益驱动的网络攻击者发起，但国家主体发动的攻击往往成本最为高昂。2020 年的研究中，大多数恶意泄露 (53%) 都由受经济利益驱动的攻击者发起，相比之下，国家威胁主体参与了 13% 的恶意泄露，黑客分子占 13%，还有 21% 的数据泄露由动机不明的攻击者发起。但与受经济利益驱动的泄露的 423 万美元相比，推定为国家赞助的泄露的平均成本为 443 万美元。

+$292,000

安全系统复杂性对平均总成本的影响

安全复杂性和云迁移给公司带来了最高的成本。

在 25 个成本因素中，安全系统复杂性的成本最为高昂，它让泄露的平均总成本增加了 292,000 美元，调整后的平均总成本为 415 万美元。泄露时发生的大规模云迁移让泄露的平均成本增加了 267,000 美元，调整后的平均成本为 413 万美元。

+96 天

医疗保健与金融行业泄露生命周期

发现和控制泄露的平均时间因行业、地域和安全成熟度而千差万别。

在 2020 年的研究中，发现泄露的平均时间为 207 天，控制泄露的平均时间为 73 天，平均 “生命周期” 为 280 天。

医疗保健行业的平均泄露生命周期为 329 天，金融行业的平均生命周期比它短 96 天 (233 天)。与未部署安全自动化的公司相比，全面部署安全自动化的公司的生命周期可缩短 74 天，从原来的 308 天缩短至 234 天。

$2 万美元

与未组建 IR 团队或开展测试的组织相比 组建了事件响应团队并开展 IR 测试的组织平均节省的成本

事件响应 (IR) 准备状态是企业最大的成本节省因素。

组建了事件响应团队并广泛测试其事件响应计划的组织，其数据泄露的平均成本为 329 万美元。相比之下，未采取任一项措施的组织的平均总成本为 529 万美元，二者相差 200 万美元。在 2019 年的研究中，两种类型的组织之间的成本差距为 123 万美元。

12 从 2019 年的

研究以来，16 个国家/地区中有 12 个平均总成本有所增加

从 2019 年开始，地区和行业差异出现了较大的波动。

美国以 864 万美元的数据泄露成本继续高居榜首，中东以 652 万美元紧随其后。在 2019 年和 2020 年的研究中，16 个国家中有 12 个国家的平均总成本都有所增加，其中斯堪的纳维亚的增幅最大，为 12.8%。

医疗保健行业以 713 万美元连续第十年高居平均泄露成本榜首，与 2019 年的研究相比增长了 10.5%。同样，能源行业也比 2019 年增长了 14.1%，在 2020 年的研究中平均成本为 639 万美元。整体来看，17 个行业中有 13 个行业的平均总成本在逐年下降，降幅最高的分别是媒体、教育、公共部门和酒店。

完整的结果

在本部分中，我们提供本次研究的详细结果。
按照如下顺序呈现主题：

1. 全球调查结果和重点
2. 数据泄露的根本原因
3. 影响数据泄露成本的因素
4. 安全自动化趋势和效力
5. 发现并控制数据泄露的时间
6. 数据泄露的长尾成本
7. 新冠肺炎带来的潜在影响
8. 大规模泄露的成本

全球调查结果和重点

*数据泄露成本报告*是一份全球性报告，它综合了17 个国家/地区和 17 个行业的 524 家组织的结果，得出了全球平均值。但在某些情况下，为进行比较，报告会按照国家/地区或行业对结果进行细分。尽管一些国家/地区和行业的样本量较小，但研究中会尽量选择一些有代表性的组织。

重要发现

$7.13 百万

与 2019 年的研究相比，医疗保健行业数据泄露的平均成本增长了 10%

80%

记录中含有客户 PII 的泄露的比例，每条记录的平均成本为 150 美元

$5.52 百万

与员工人数不足 500 人的组织的 264 万美元的成本相比，员工人数超过 25,000 人的企业的泄露平均总成本

图 1

全球研究概览

国家/地区	2020 年样本	样本百分比	货币	研究年数
美国	63	12%	美元	15
印度	47	9%	印度卢比	9
英国	44	8%	英镑	13
德国	37	7%	欧元	12
法国	36	7%	欧元	7
巴西	35	7%	巴西雷亚尔	9
日本	33	6%	日元	11
中东*	29	6%	里亚尔	7
加拿大	26	5%	加元	6
韩国	24	5%	韩元 (KRW)	3
东盟#	23	4%	新加坡元	2
澳大利亚	23	4%	澳元	11
斯堪的纳维亚+	23	4%	冰岛克朗	2
意大利	21	4%	欧元	9
拉丁美洲**	21	4%	比索	1
土耳其	20	4%	土耳其里拉	3
南非	19	4%	南非美元	5
总计	524			

今年的研究考察了 17 个国家或地区样本中的泄露情况。

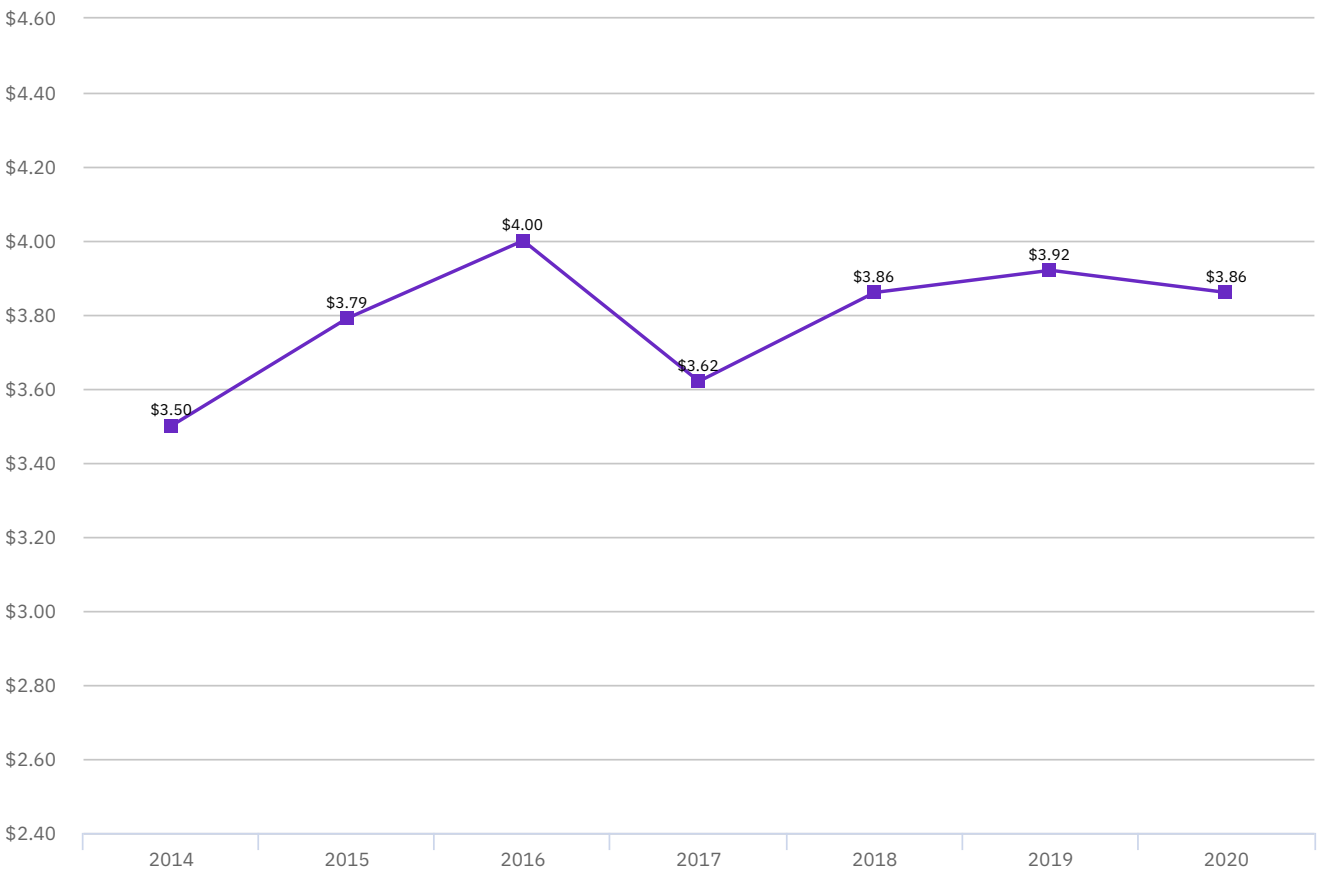
国家和地区包括美国、印度、英国、德国、巴西、日本、法国、中东、加拿大、意大利、韩国、澳大利亚、土耳其、东盟、南非、斯堪的纳维亚，还首次将拉丁美洲（墨西哥、阿根廷、智利和哥伦比亚）纳入研究范畴。**图 1** 显示了样本量、各国家/地区货币以及各国家/地区被纳入研究的年数。

*中东是位于沙特阿拉伯和阿拉伯联合酋长国的公司集群地
#东盟是位于新加坡，印度尼西亚，菲律宾，马来西亚，泰国和越南的公司集群地
+斯堪的纳维亚半岛是位于丹麦，瑞典，挪威和芬兰的公司集群地
** 拉丁美洲是位于墨西哥、阿根廷、智利和哥伦比亚的公司集群地

图 2

数据泄露的平均总成本

以百万美元为单位



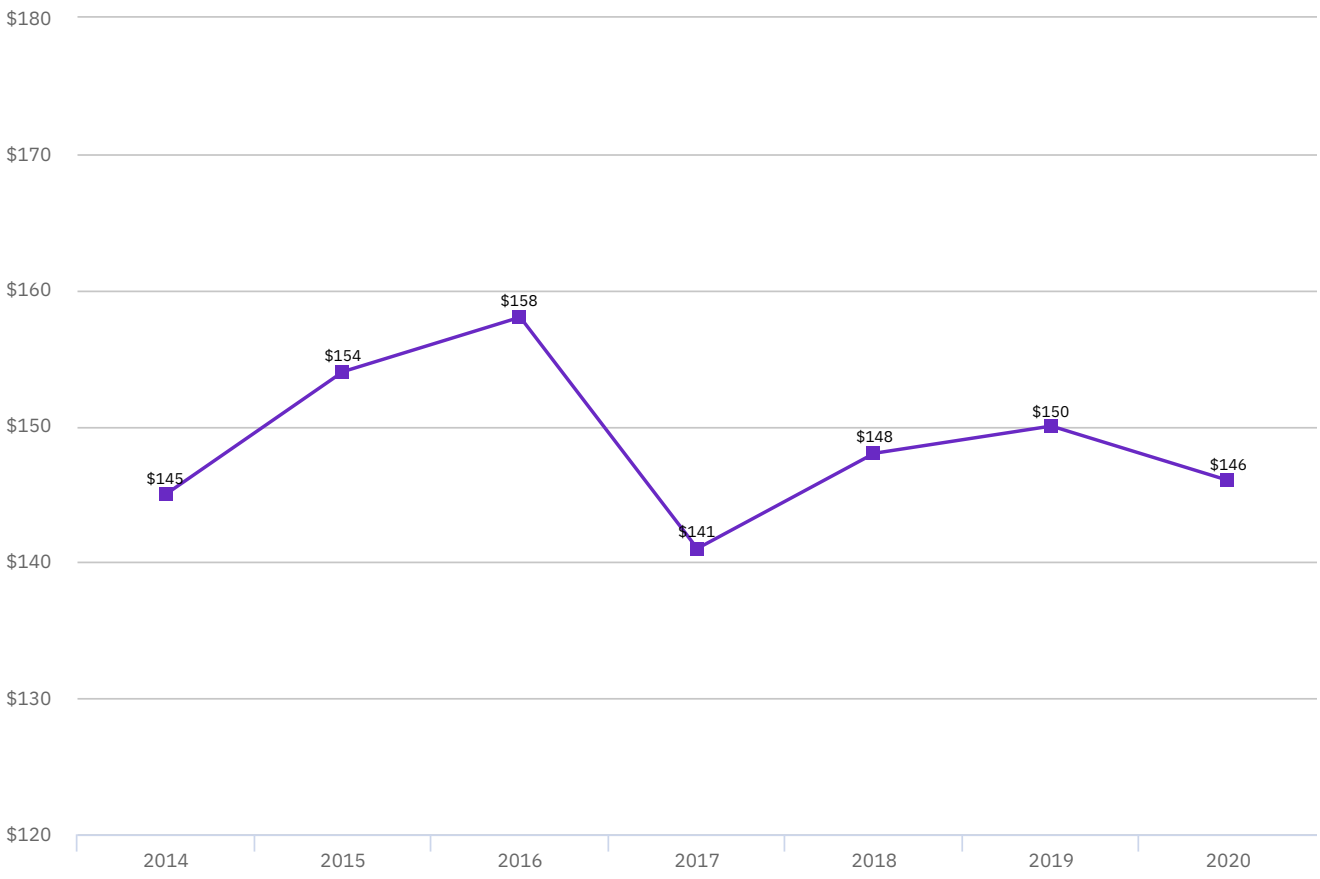
自 2014 年以来，数据泄露的平均总成本增长了 10%。

图 2 显示了七年来数据泄露的全球平均总成本。2020 年研究中的综合平均总成本为 386 万美元，与 2019 年的 392 万美元相比略有下降。过去七年的加权平均值为 379 万美元。

图 3

数据泄露的每条记录的平均成本

以美元为单位



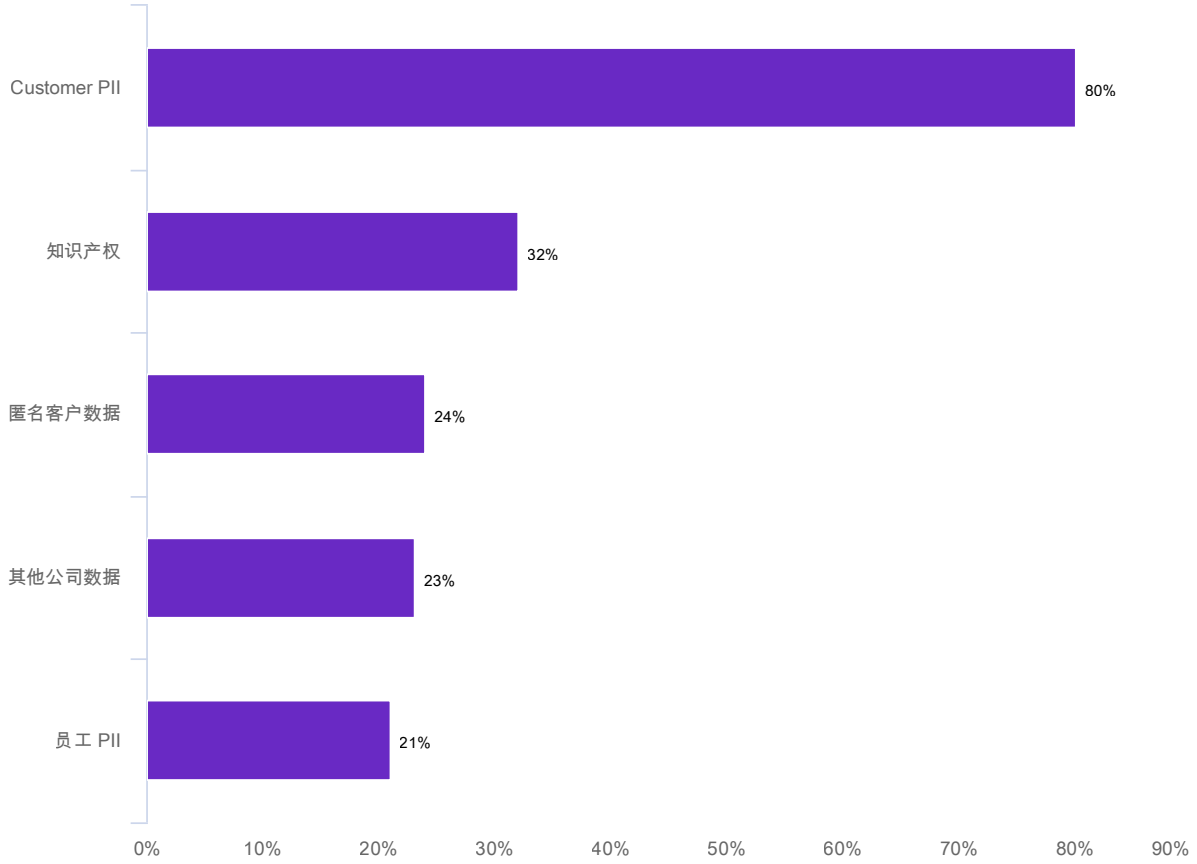
数据泄露的每条记录的成本小幅下降至 146 美元。

图 3 显示了过去七年来，每条被破坏记录的平均数据泄露成本。过去七年来，每条记录的加权平均成本为 149 美元。

图 4

被破坏的记录类型

涉及各类数据的泄露百分比



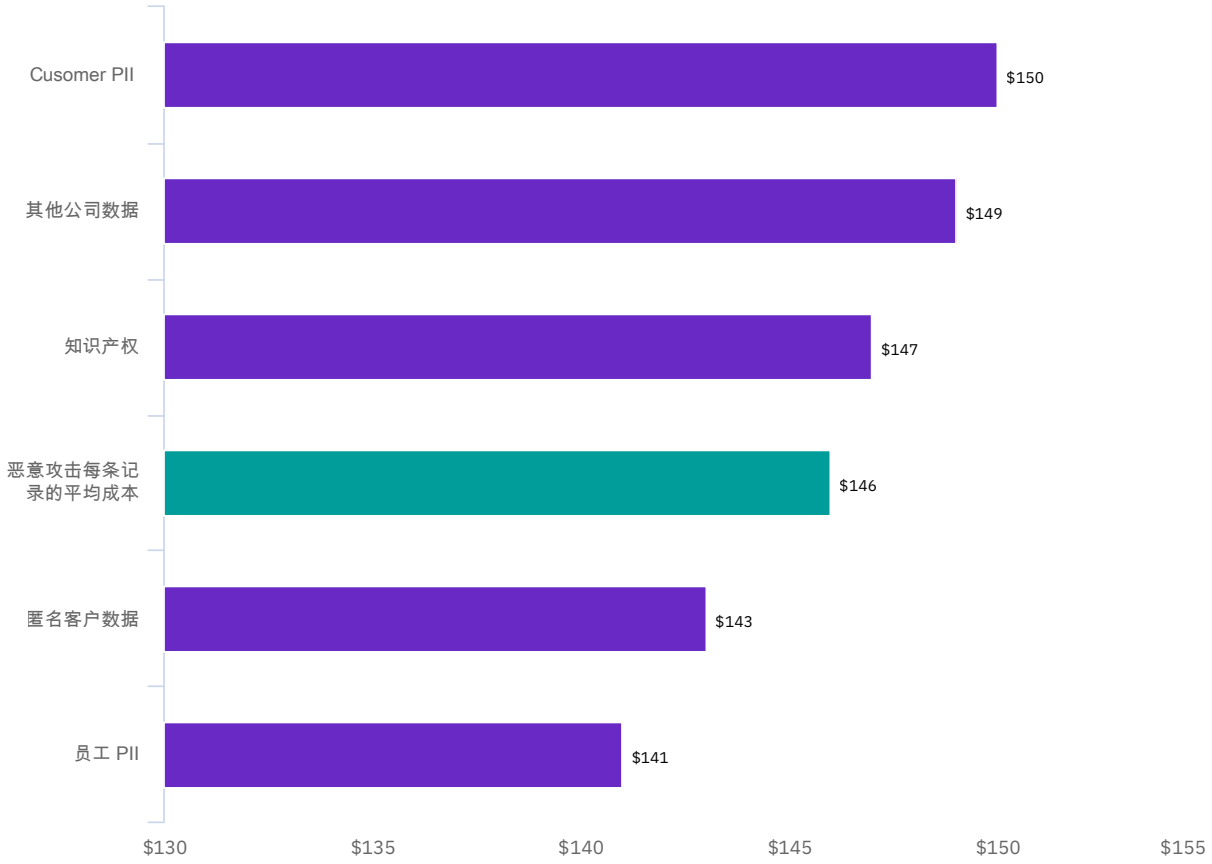
客户 PII 是发生泄露时最常丢失或被盗的数据类型。

图 4 显示出，80% 的数据泄露中都有客户 PII。32% 的数据泄露中都会发生知识产权被窃取，24% 的数据泄露中都会有匿名客户数据被盗的情况发生。

图 5

每条记录的平均成本（按被破坏的数据类型划分）

以美元为单位



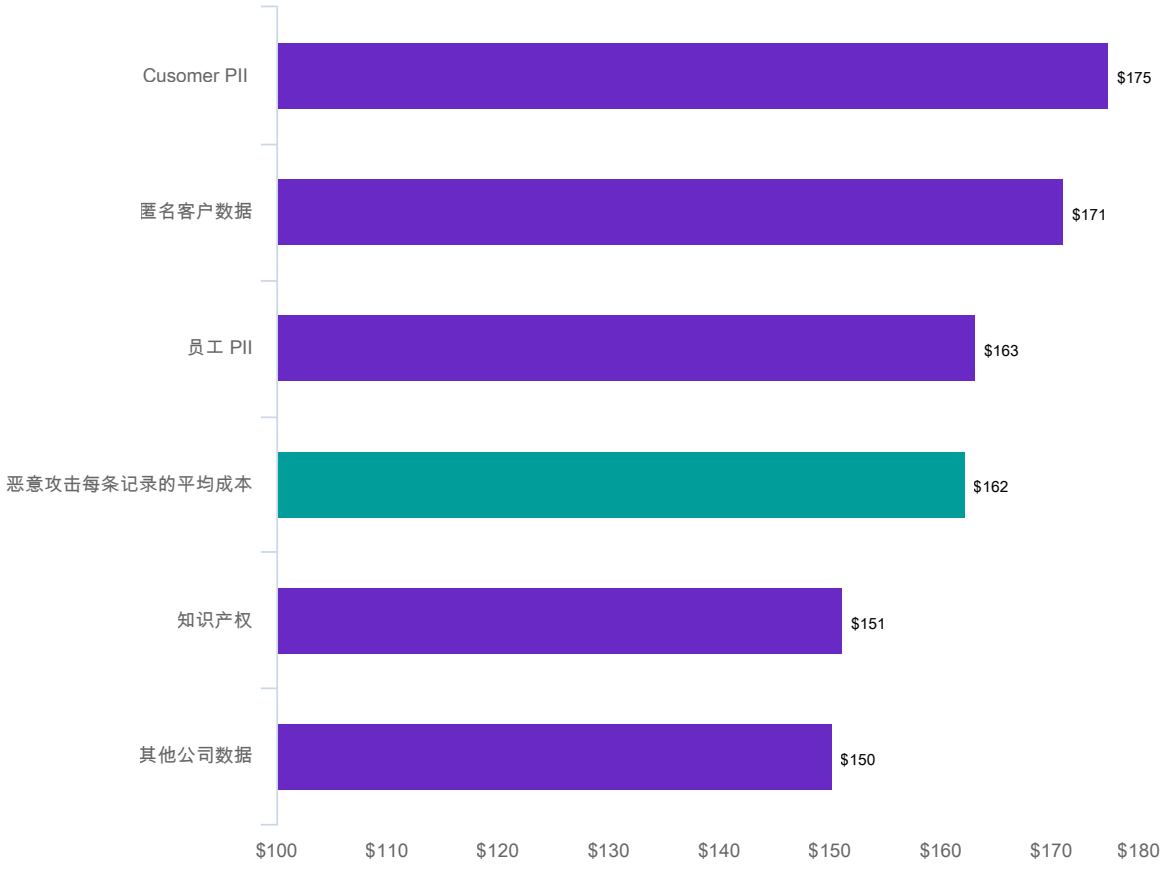
客户 PII 是数据泄露中成本最高的被盗数据类型。

如 **图 5** 所示，每条丢失或被盗记录的客户 PII 平均成本为 150 美元每条记录的知识产权成本为 147 美元，每条记录的匿名客户数据（非 PII）成本为 143 美元，每条记录的员工 PII 成本为 141 美元。

图 6

恶意攻击中每条记录的平均成本（按被盗数据类型划分）

以美元为单位



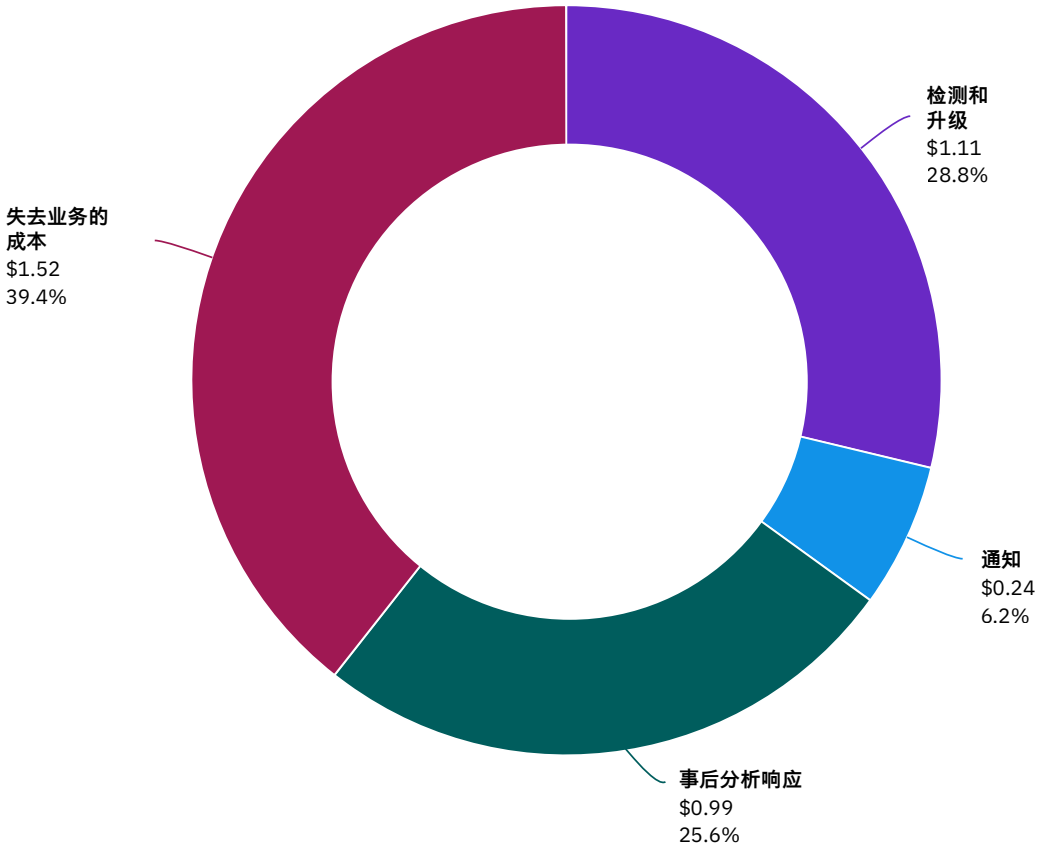
恶意攻击导致的数据泄露的每条记录的成本会更高。

如如**图 6** 所示，恶意攻击中客户 PII 的每条记录的成本为 175 美元，比其他任何类型的泄露中受损的客户 PII 的每条记录平均总成本（每条记录 150 美元）高出近 17%。

图 7

数据泄露平均总成本分为四类

以百万美元为单位



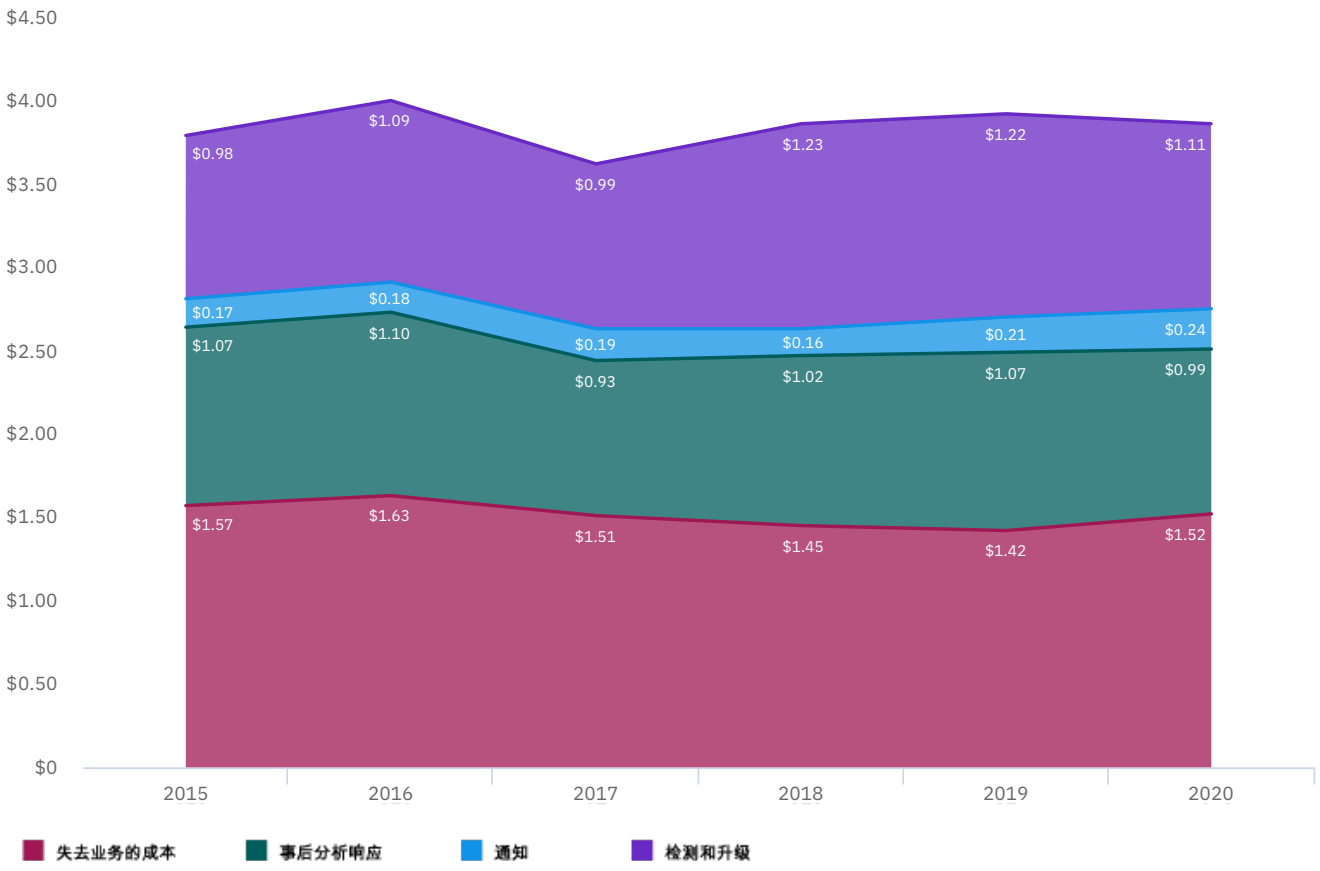
失去业务在数据泄露平均成本中占有最高比例。

图 7 以美元和数据泄露总成本的百分比表示了四个成本部分。失去业务的平均成本为 152 万美元或总成本的 39%。最低的成本部分是通知数据泄露，为 240,000 美元，或总成本的 6%。

图 8

四类数据泄露平均成本的趋势

以百万美元为单位



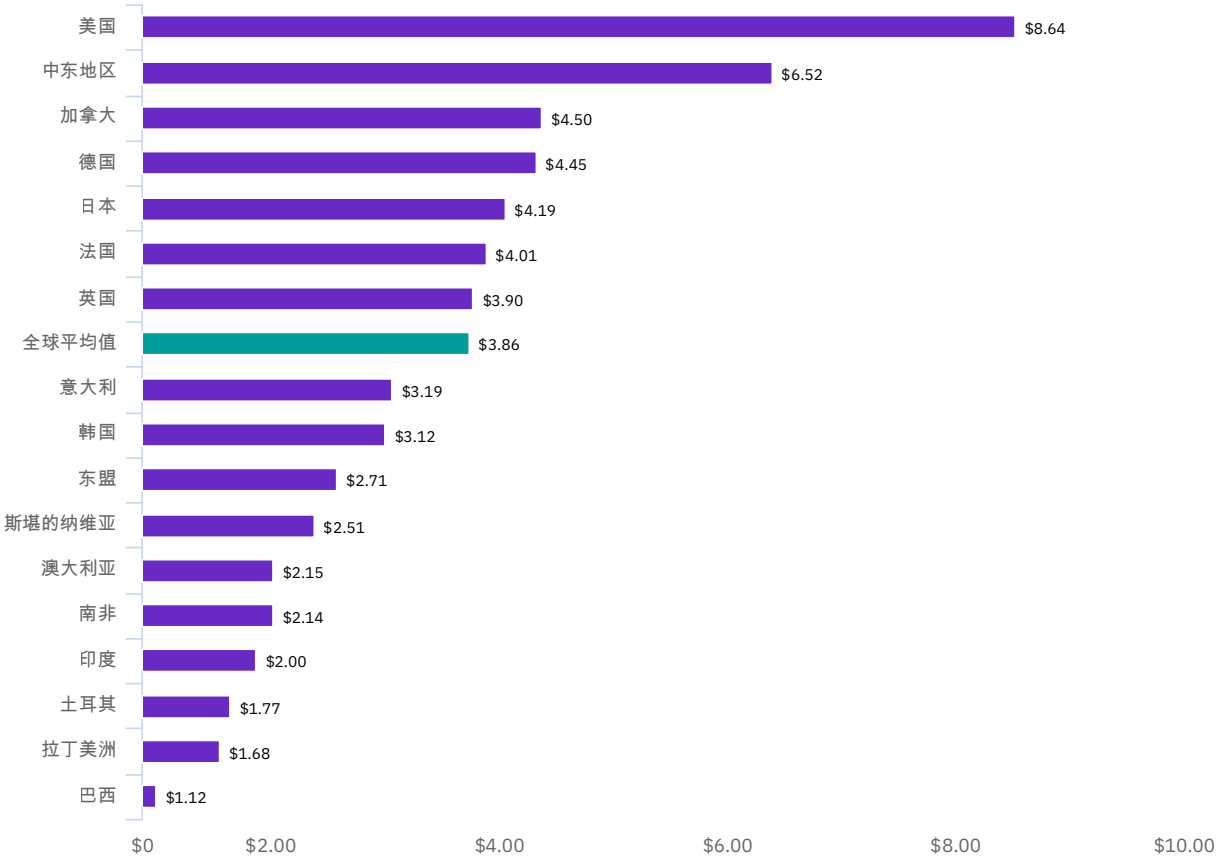
失去业务的成本同比略有增加。

图 8 显示了过去六年间失去业务、泄露后响应、通知和检测和升级的成本趋势。该模式显示了这些成本的一致性。通知仍是最低的成本部分，而失去业务则是最高的成本部分。

图 9

数据泄露的平均总成本（按国家或地区划分）

以百万美元为单位



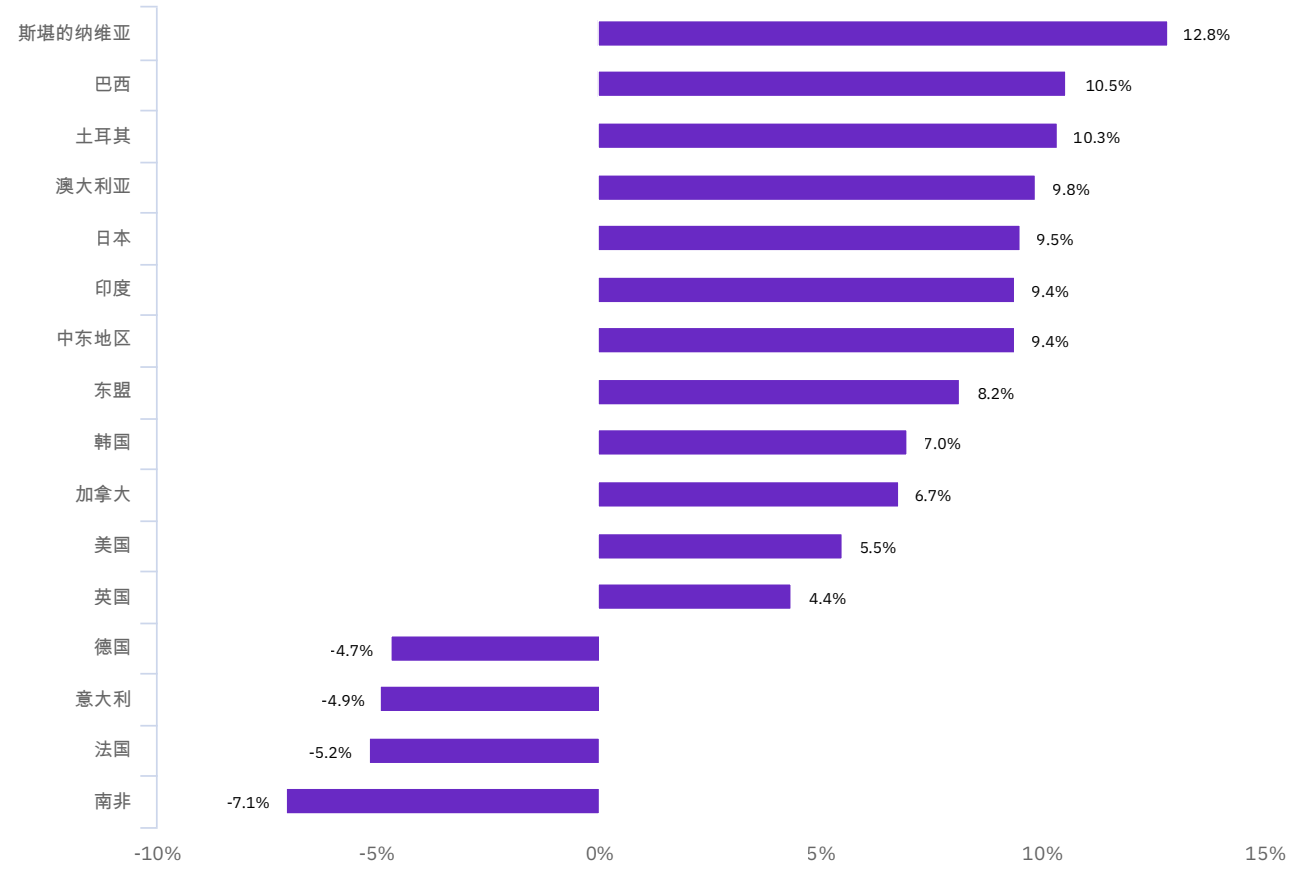
数据泄露的平均总成本因国家/地区而异。

图 9 显示了按国家/地区划分的数据泄露平均总成本。美国的组织以 864 万美元的总平均成本高居榜首，中东以 652 万美元紧随其后。相比之下，拉丁美洲和巴西的组织的平均总成本最低，分别为 168 万美元和 112 万美元。

图 10

2019-2020 年间各国家或地区的平均总成本百分比变化

以本国货币计算



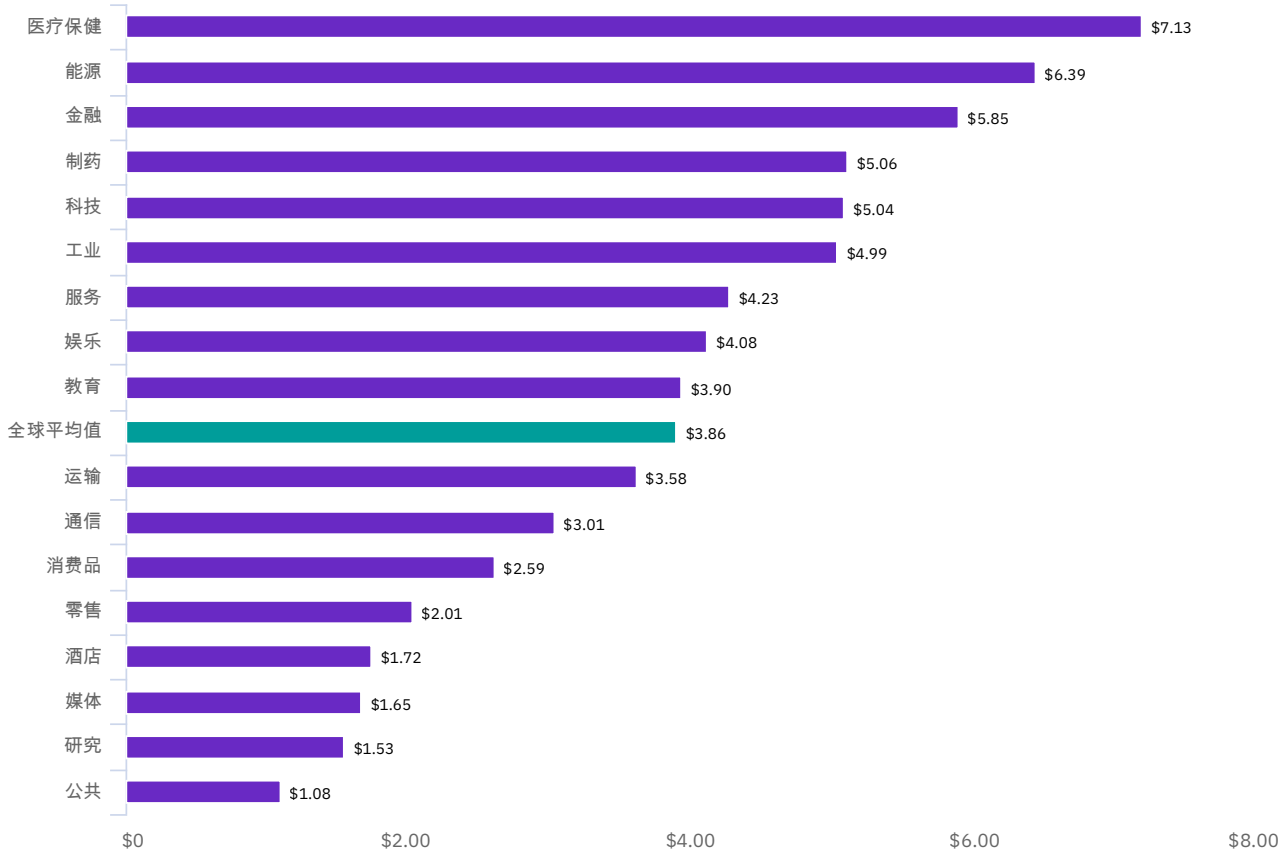
16 个国家中，有 12 个国家的数据泄露平均总成本有所增加。

如**图 10** 所示，在 2019 年至 2020 年的研究中，Scandinavia的数据泄露总成本增幅最大，法国和南非降幅最大。

图 11

数据泄露的平均总成本（按行业划分）

以百万美元为单位

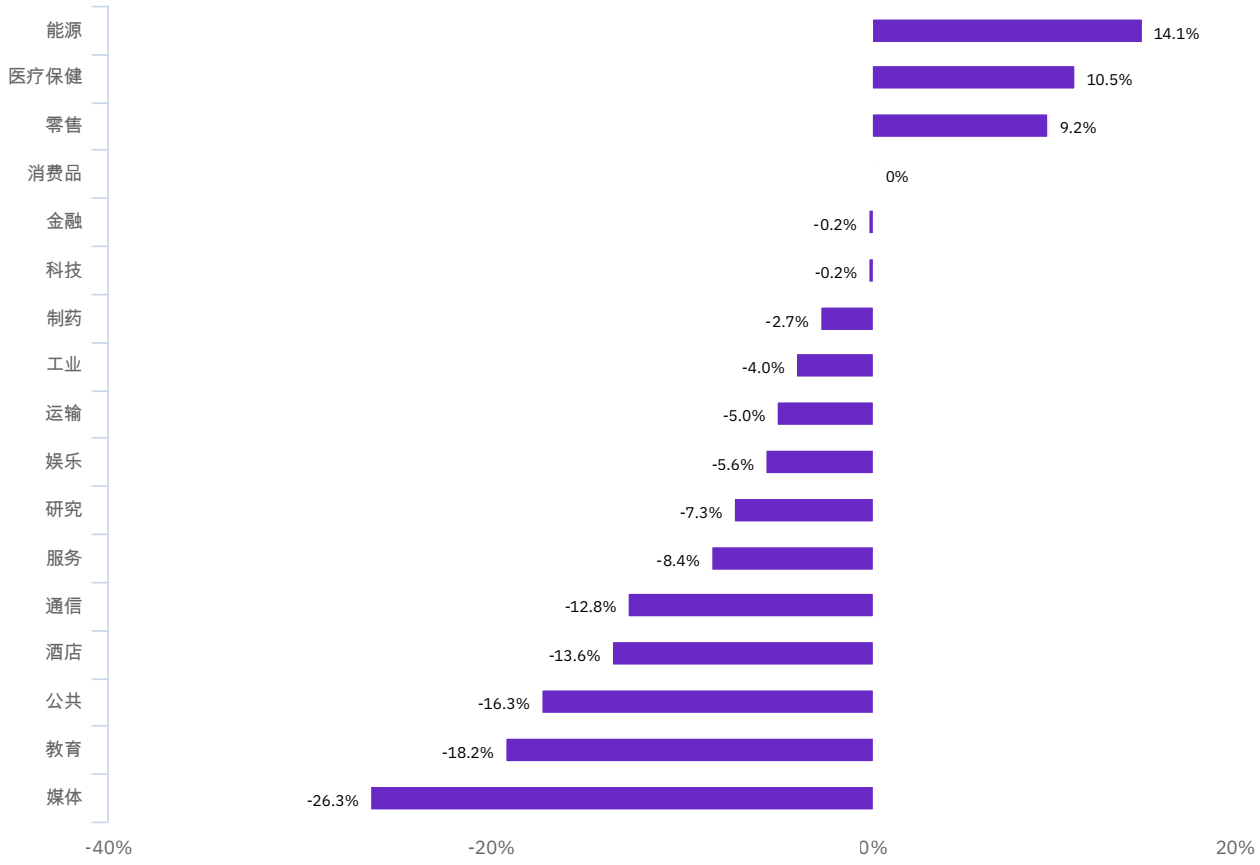


面临更严格法规要求的组织承担的数据泄露成本会更高。

如**图 11** 所示，医疗保健、能源、金融服务和制药行业发生的数据泄露平均总成本明显高于监管力度较小的行业，例如酒店、媒体和研究组织。在此研究中，公共部门组织的数据泄露成本一直处于末位，因为他们不太可能因为数据泄露而失去大量客户。

图 12

2019-2020 年间各行业平均总成本百分比变化



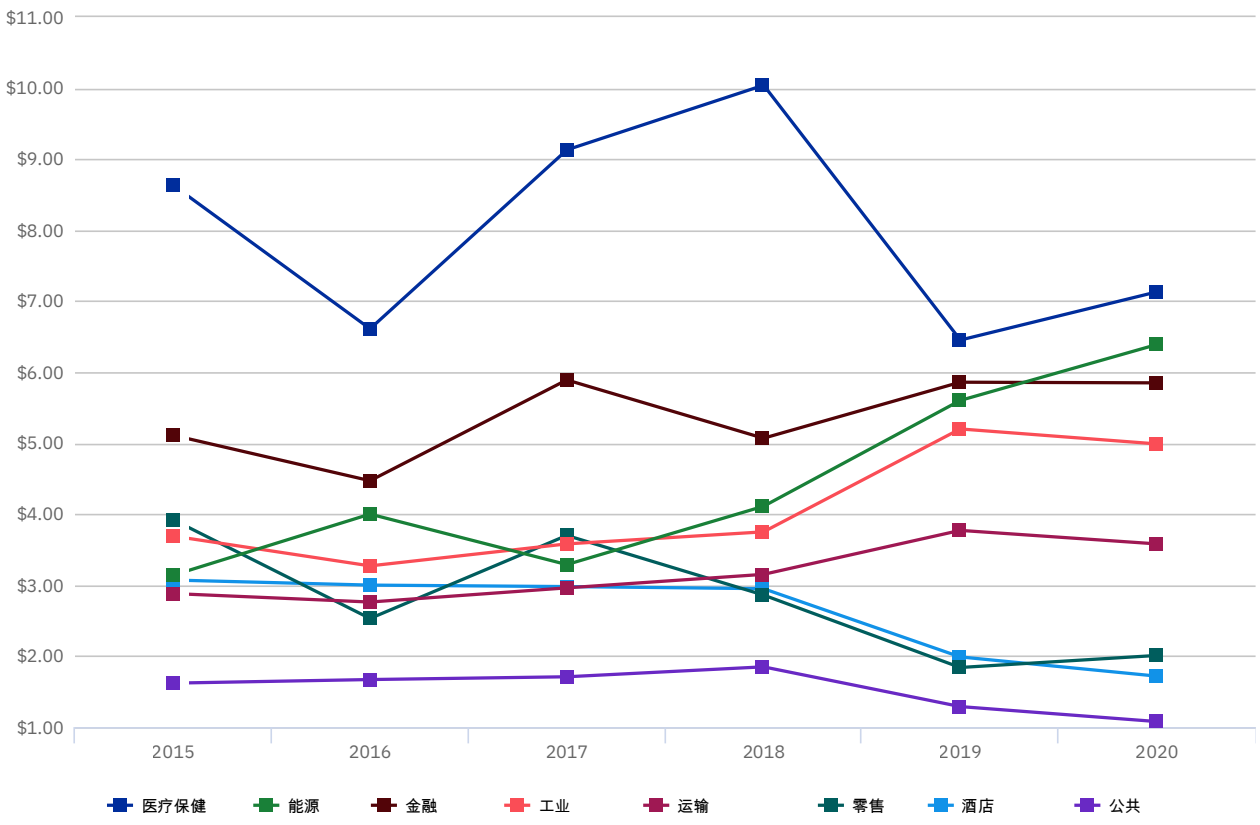
能源、医疗保健和零售行业数据泄露成本的增幅最高。

从**图 12** 可以看出，在 2019 年和 2020 年研究中涵盖的 17 个行业中，只有 3 个行业的数据泄露成本有所增加。能源、医疗保健和零售行业的平均总成本增幅最大，而公共部门、教育和媒体行业则出现了最大跌幅。

图 13

八个国家/地区的数据泄露平均总成本趋势

以百万美元为单位



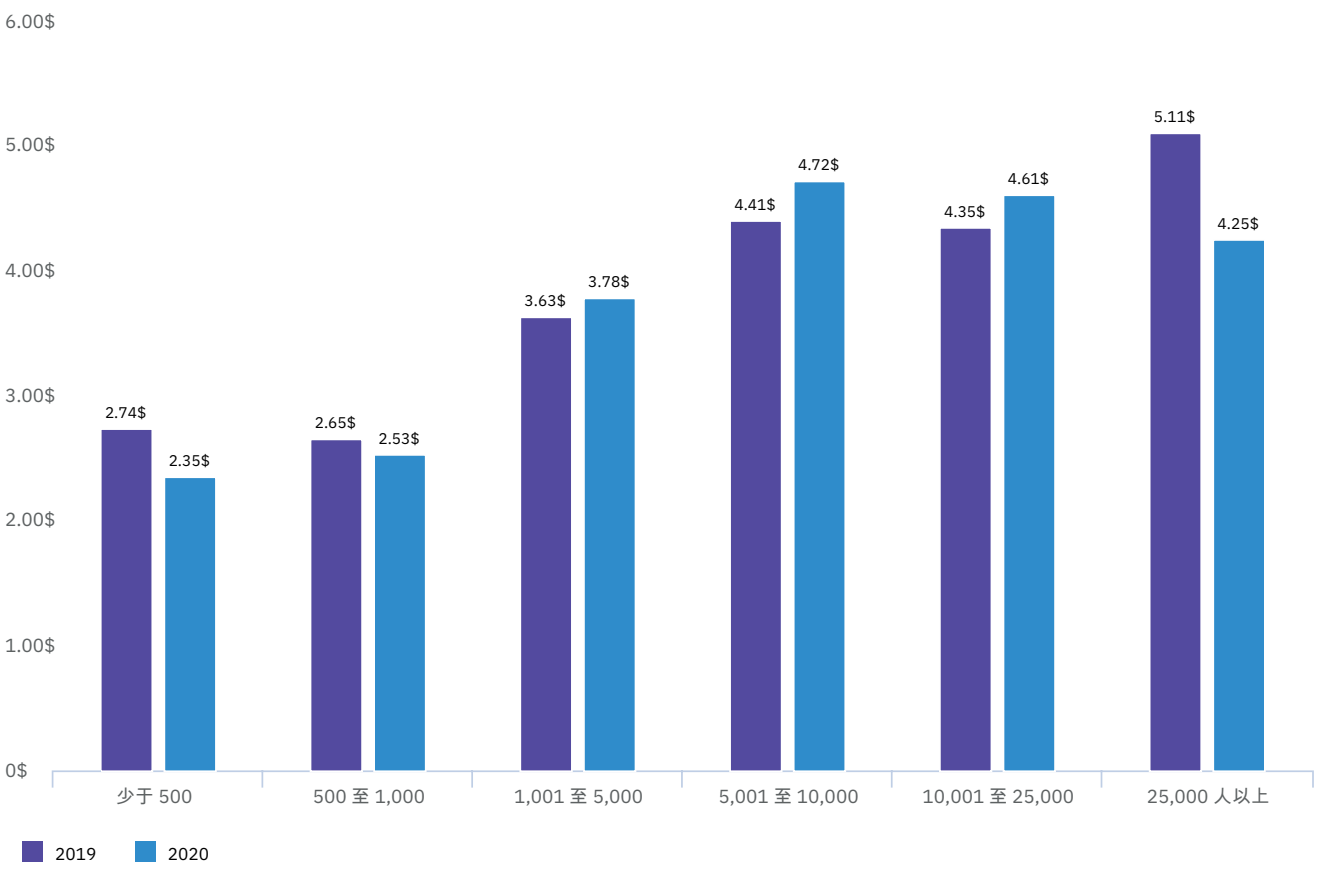
医疗保健和金融行业一直都是数据泄露成本最高的行业。

图 13 显示了过去六年间八个行业部门的线图。医疗保健一直是成本最高的行业，而公共部门一直是成本最低的行业。

图 14

按组织规模划分的数据泄露平均总成本

以百万美元为单位



中等规模组织的数据泄露平均成本有所增加。

从**图 14** 可以看出，在 2019 和 2020 年的研究中，规模最小的组织（1,000 名员工或更少）和规模最大的组织（员工人数超过 25,000 人）的数据泄露平均总成本有所下滑。员工人数超过 25,000 人的组织，平均总成本从 2019 年的 511 万美元下降到 2020 年的 425 万美元，下降幅度为 16.8%。但对于中等规模的组织而言，泄露总成本平均起来却有所增加。人数在 5,001 至 10,000 人的组织，泄露平均成本从 2019 年的 441 万美元增加至 2020 年的 472 万美元，增幅为 7%。从比例上看，越小的组织每位员工的平均成本反而更高。

数据泄露的根本原因

多年来，研究一直在通过参与者了解引起数据泄露的原因。前几年的报告将这些根本原因分为三类：系统故障（IT 和业务流程故障）；人为失误（玩忽职守的员工或承包商无意中引起数据泄露）；以及恶意攻击（由黑客或犯罪的内部人士引起）。

今年的报告仍将这些泄露分为三类。但是在更加深入的分析中，我们要求参与者提供更详细的与恶意攻击原因有关的信息，其中包括初始威胁向量和攻击者类型。我们在本部分提供了这些分析的结果。

重要发现

52%

恶意攻击引起的泄露的比例，平均成本为 427 万美元

19%

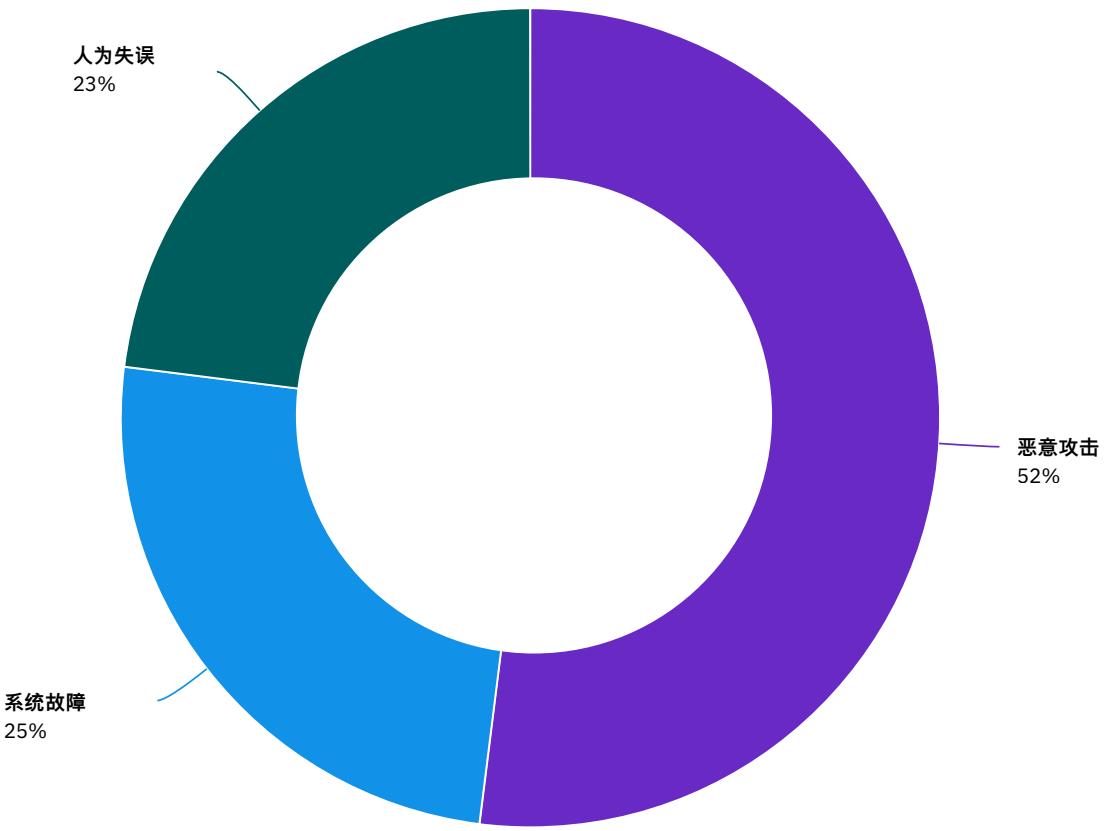
凭据被盗 (19%) 和云错误配置 (19%) 引起的恶意泄露的比例

$4.43 百万

国家攻击者引起的数据泄露的平均成本，13% 的恶意攻击由国家主体发起

图 15

数据泄露根本原因细分为三类



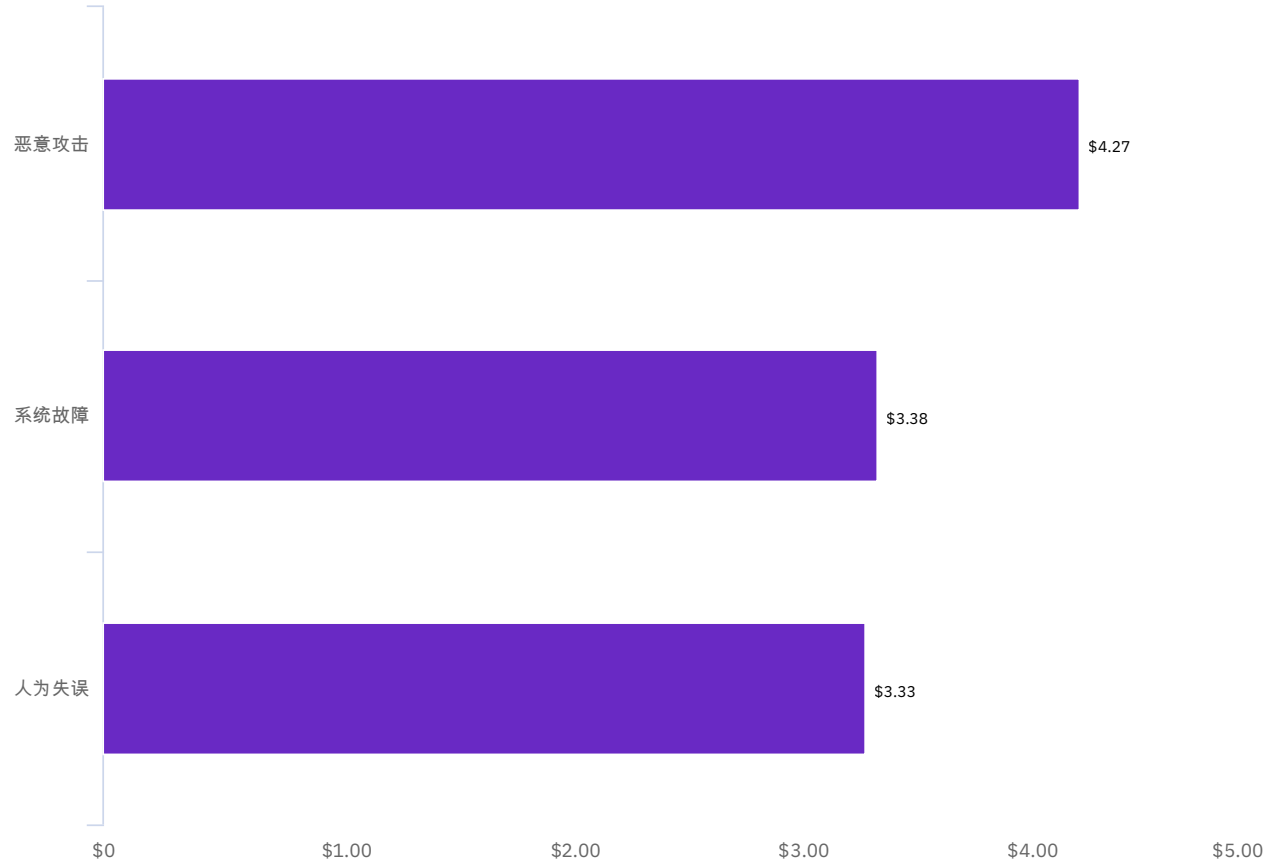
恶意攻击是大部分数据泄露的罪魁祸首。

图 15 汇总了三大类别的数据泄露根本原因。52% 的事件中涉及到恶意攻击，系统故障和人为失误的比例分别为 25% 和 23%。

图 16

三种数据泄露根本原因的平均总成本

以百万美元为单位



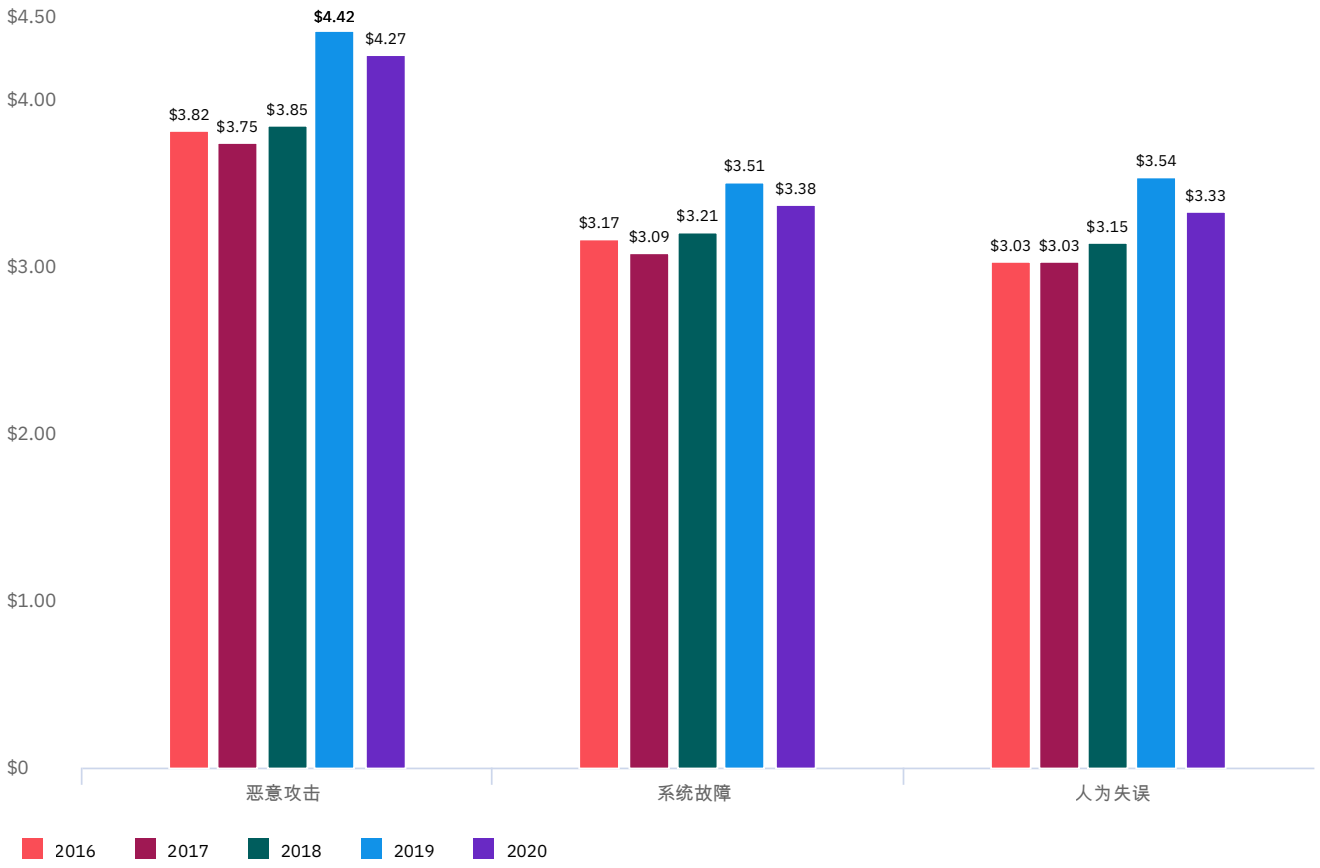
恶意攻击是成本最为高昂的根本原因。

如 **图 16** 所示，在 2020 年的研究中，恶意攻击导致的数据泄露的平均成本为 427 万美元，比系统故障或人为失误引发的数据泄露的成本高出近 100 万美元。

图 17

平均总成本的趋势（按数据泄露的根本原因划分）

以百万美元为单位

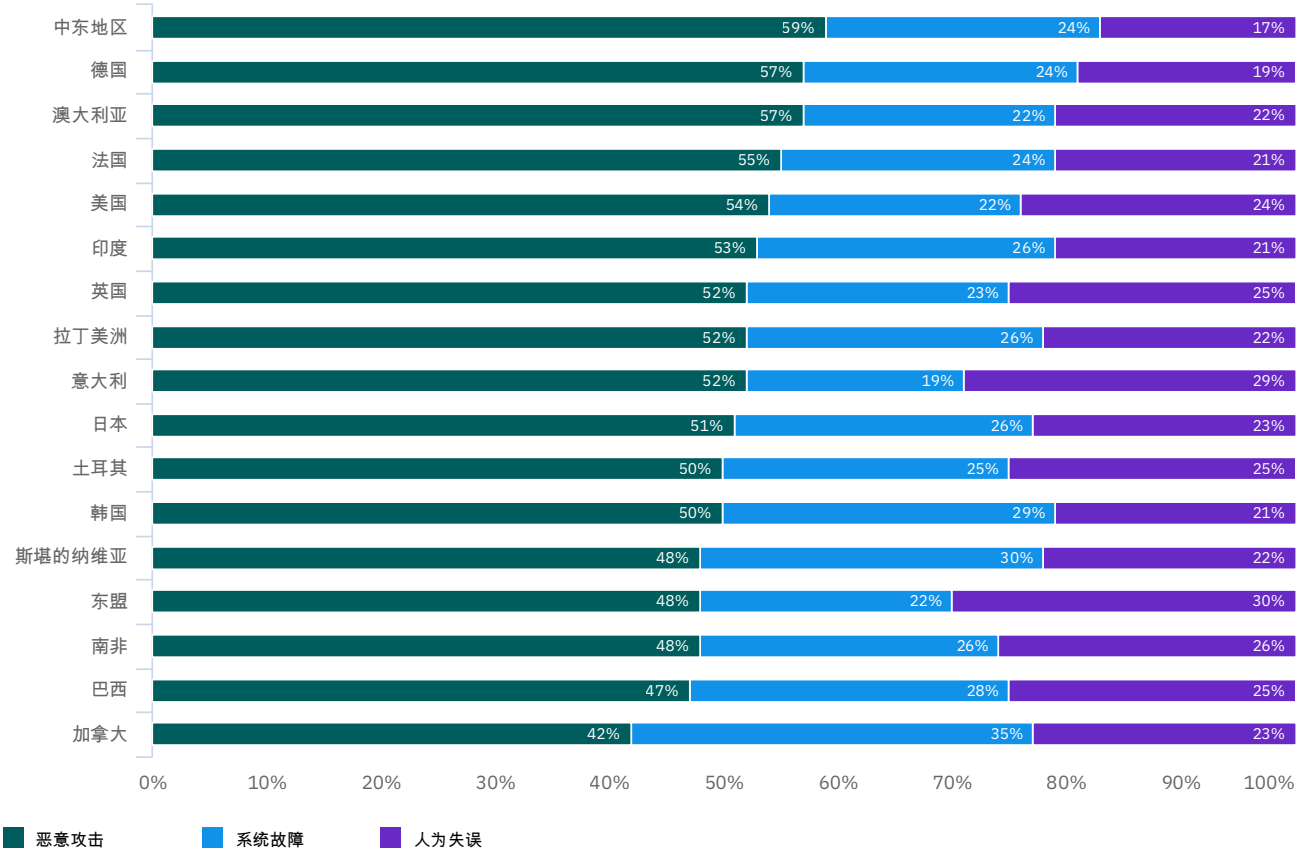


过去五年来，成本最为高昂的仍是恶意攻击泄露。

图 17 显示了过去五年间三种数据泄露根本原因的平均总成本。从研究中可以得知，自 2016 年以来，根本原因的模式一直非常平稳，与 2019 年相比，2020 年的成本略有下降。自 2016 年以来，恶意泄露的平均总成本增长了近 12%。

图 18

数据泄露根本原因细分（按国家或地区划分）

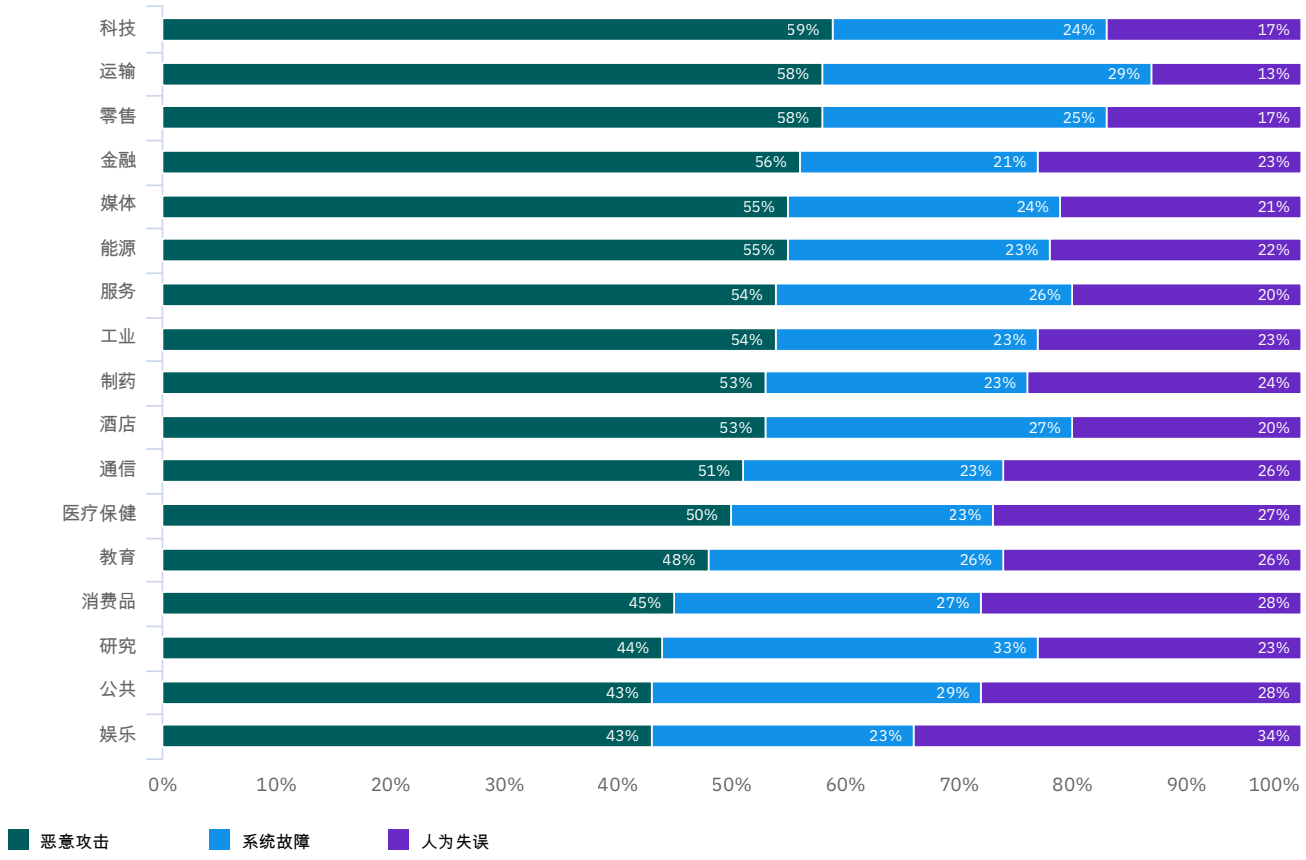


泄露的根本原因会因地域而异。

从 **图 18** 可以看出，中东、德国和澳大利亚因为恶意攻击引起数据泄露的比例最高，而南非、巴西和加拿大因为恶意攻击引起数据泄露的比例最低。加拿大因为系统故障引起数据泄露的比例最高。东盟和意大利因为人为错误导致数据泄露的比例最高。

图 19

各行业数据泄露根本原因细分



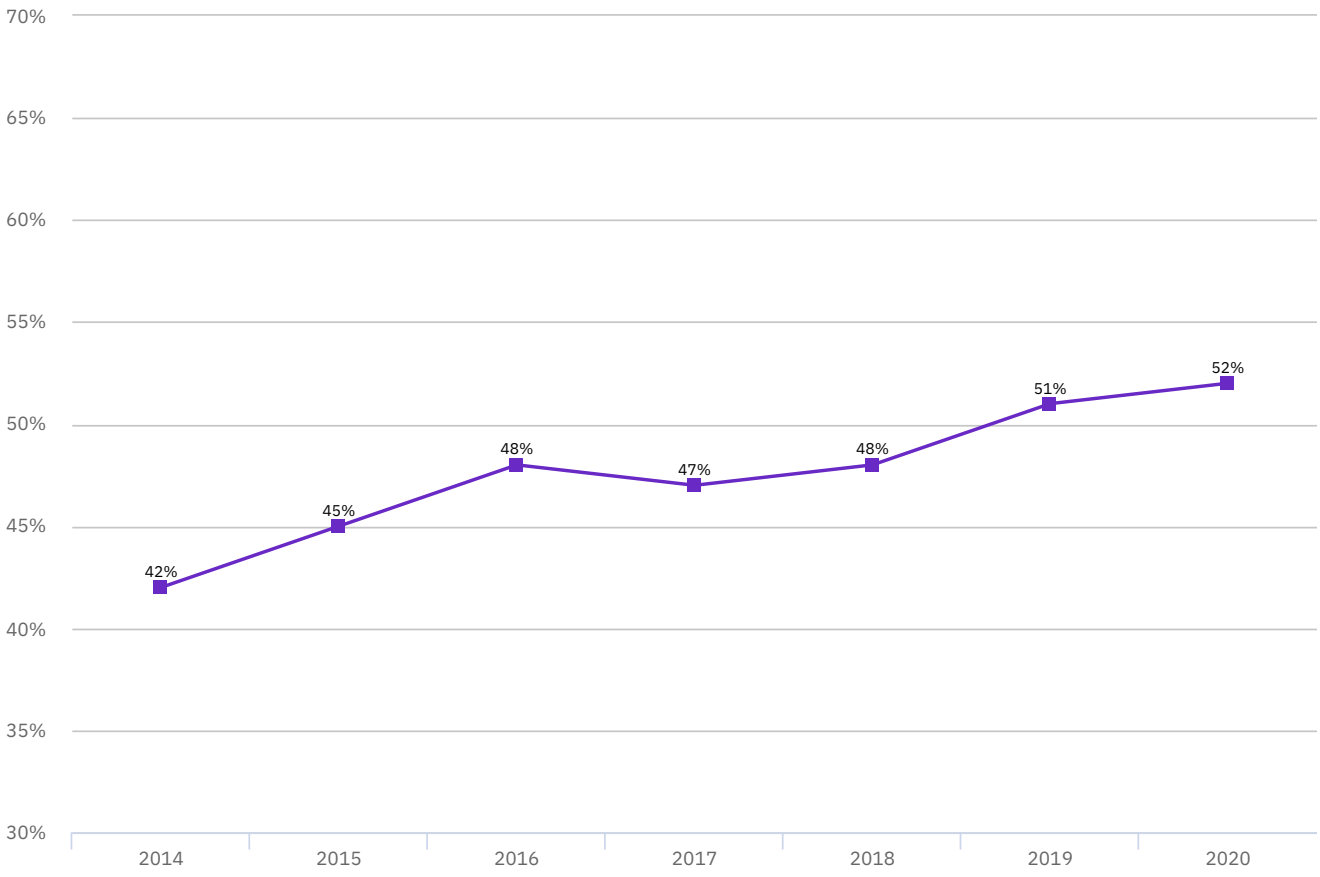
不同行业数据泄露根本原因的细分也各不相同。

如**图 19** 所示，科技、运输、零售和金融行业受到恶意攻击的比例最高。娱乐、公共部门和消费品行业因人为失误导致数据泄露的比例最高。系统故障是在研究、公共部门和运输行业更为常见的数据泄露根本原因。

图 20

恶意攻击导致的数据泄露的趋势

所有泄露的百分比



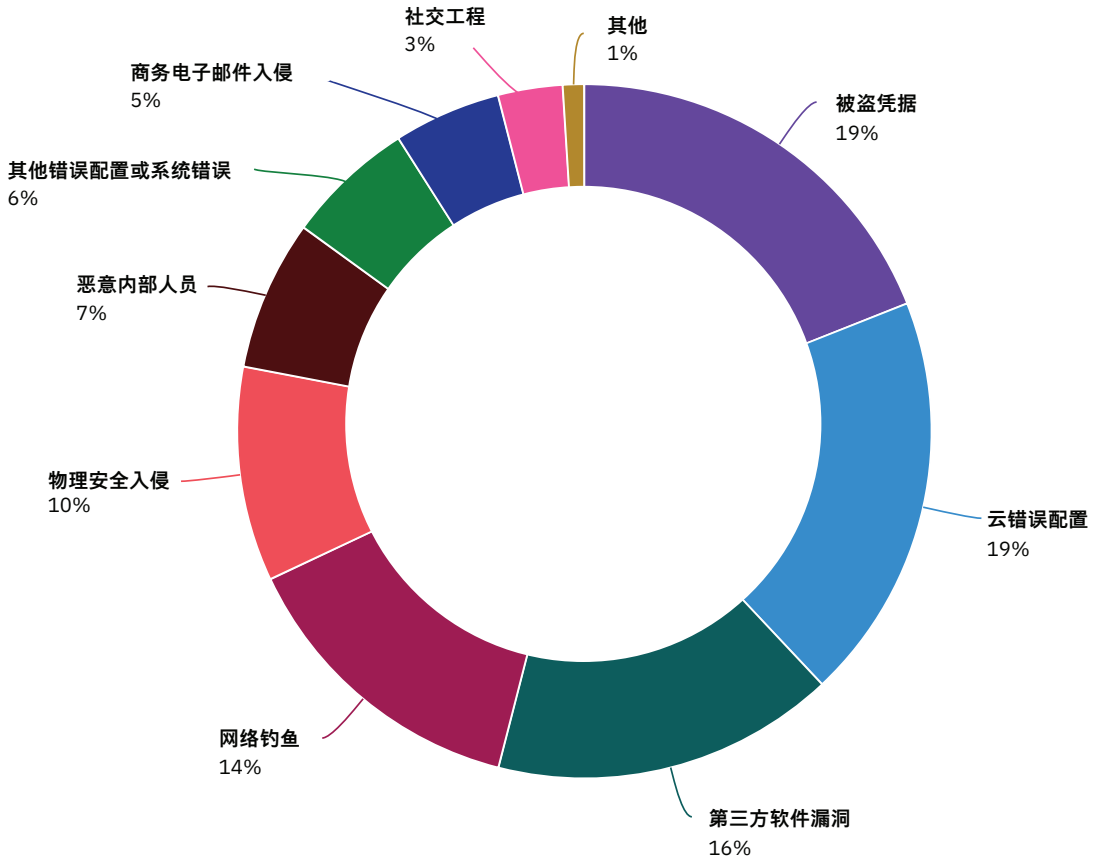
恶意攻击引起的泄露比例一直在稳步上升。

从**图 20** 可以看出，报告中的恶意攻击数据泄露的比例从 2014 年的 42% 上升至 2020 年的 52%。增加的 10 个百分点表示恶意攻击引发泄露的比例增长了近 24%（增长率）。

图 21

恶意攻击数据泄露根本原因细分（按威胁向量划分）

恶意攻击引起的泄露的百分比

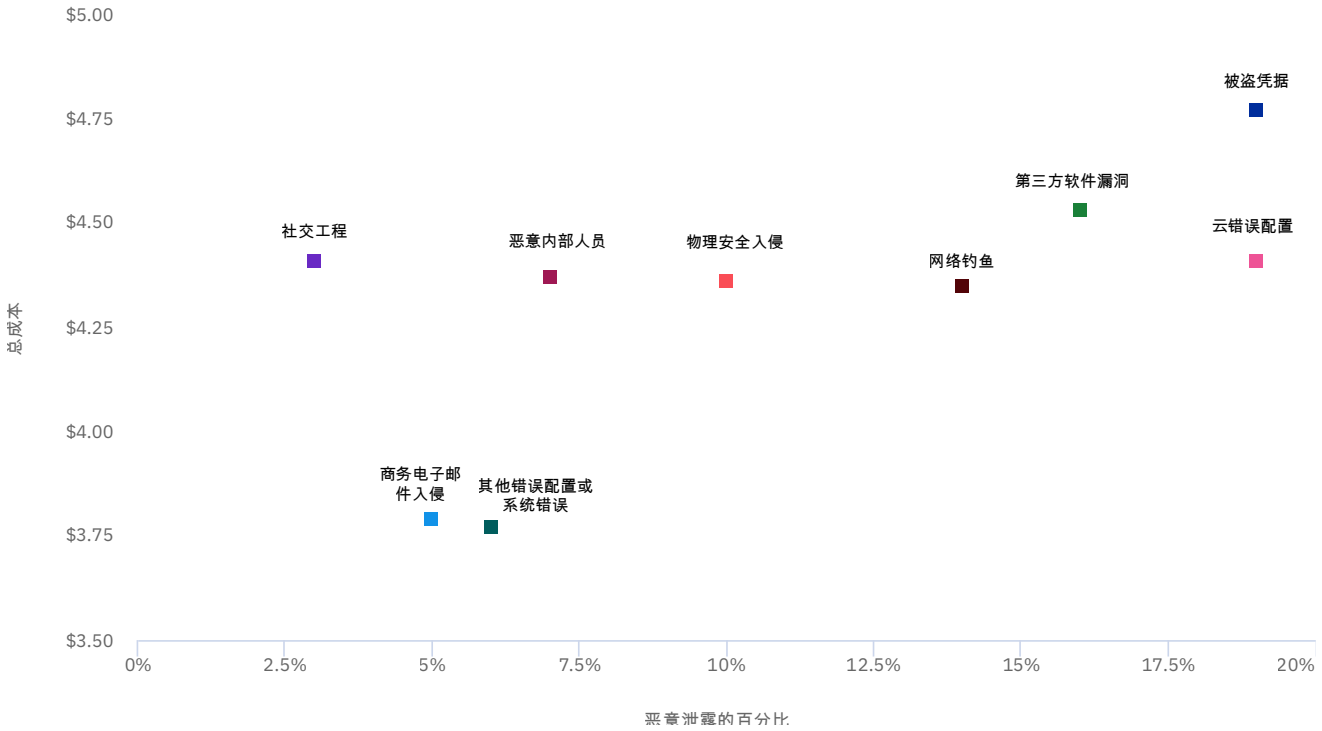


凭据被盗、云错误配置或第三方软件漏洞，是引起大部分恶意泄露的三大原因。

被盗用/泄露的凭据和云配置错误是主要的初始威胁向量，分别占到恶意泄露的 19%。如 **图 21** 所示，第三方软件漏洞也是主要的初始威胁向量，在恶意泄露中占 16%。

图 22

恶意攻击数据泄露的平均成本和频率（按根本原因向量划分）

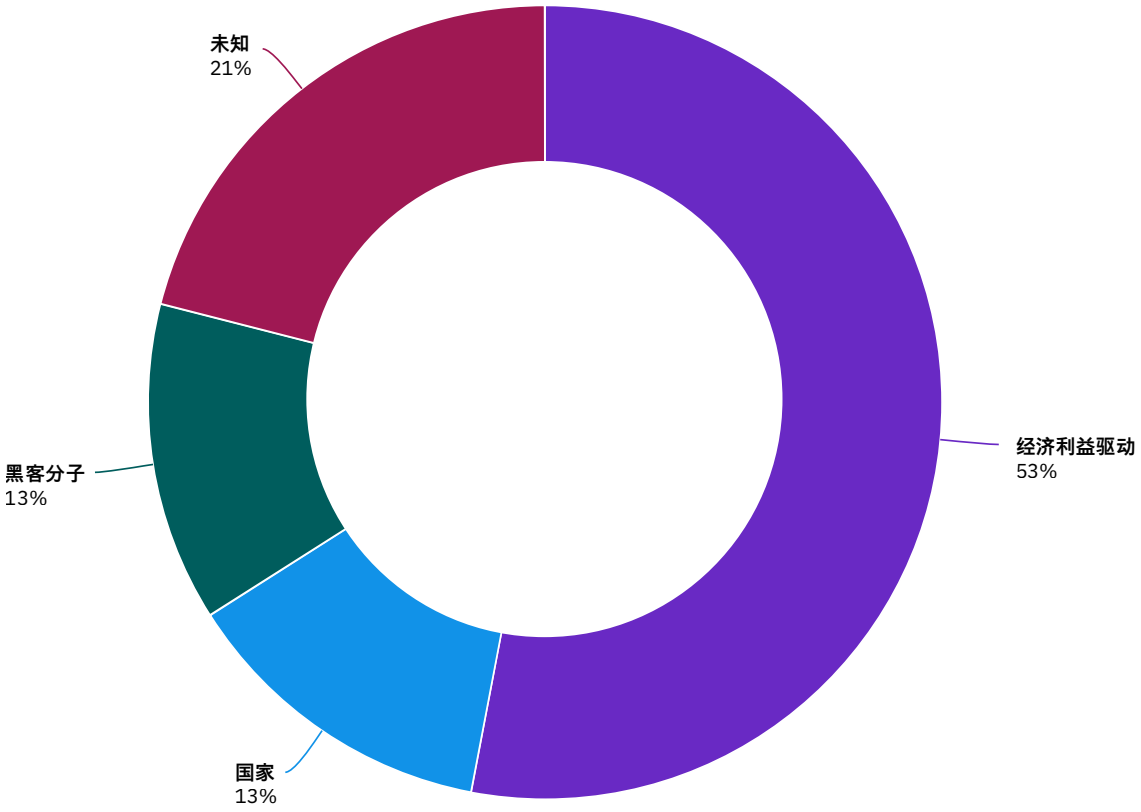


凭据被盗是成本最高也是最常见的威胁向量。

图 22 利用散点图显示了恶意泄露中的九个初始威胁向量，X 轴上显示了泄露的百分比，Y 轴上显示了平均总成本。凭据被盗是图中右上方最远的威胁向量，这表示它的频率和成本在恶意数据泄露中都占有很高的比例。

图 23

按威胁向量类型归纳的恶意攻击数据泄露



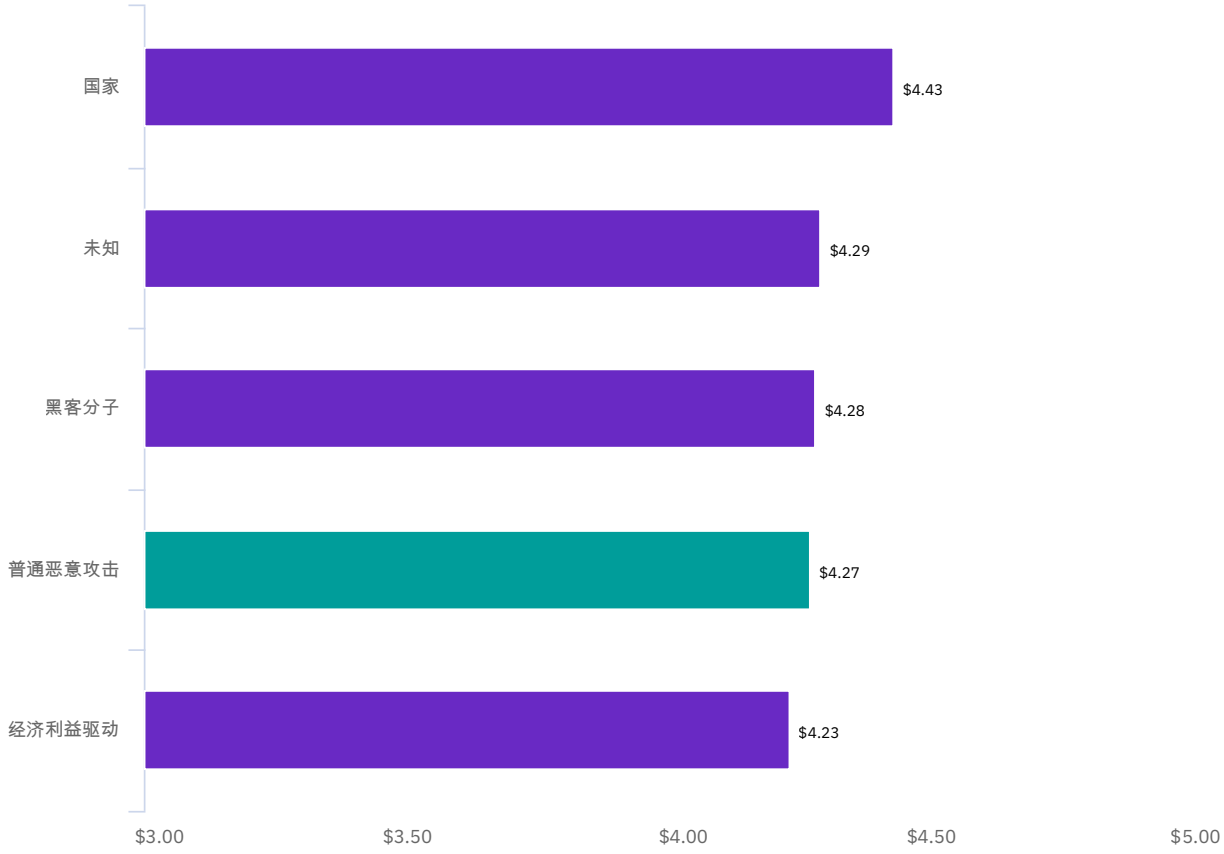
受经济利益驱动的攻击者是大多数恶意数据泄露的始作俑者。

如 **图 23** 所示，大多数恶意泄露 (53%) 都由经济利益驱动的攻击者发起。国家威胁主体参与了 13% 的恶意泄露，黑客分子占 13%，还有 21% 的此类数据泄露由动机不明的攻击者发起。

图 24

恶意攻击数据泄露的平均成本（按威胁主体类型划分）

以百万美元为单位



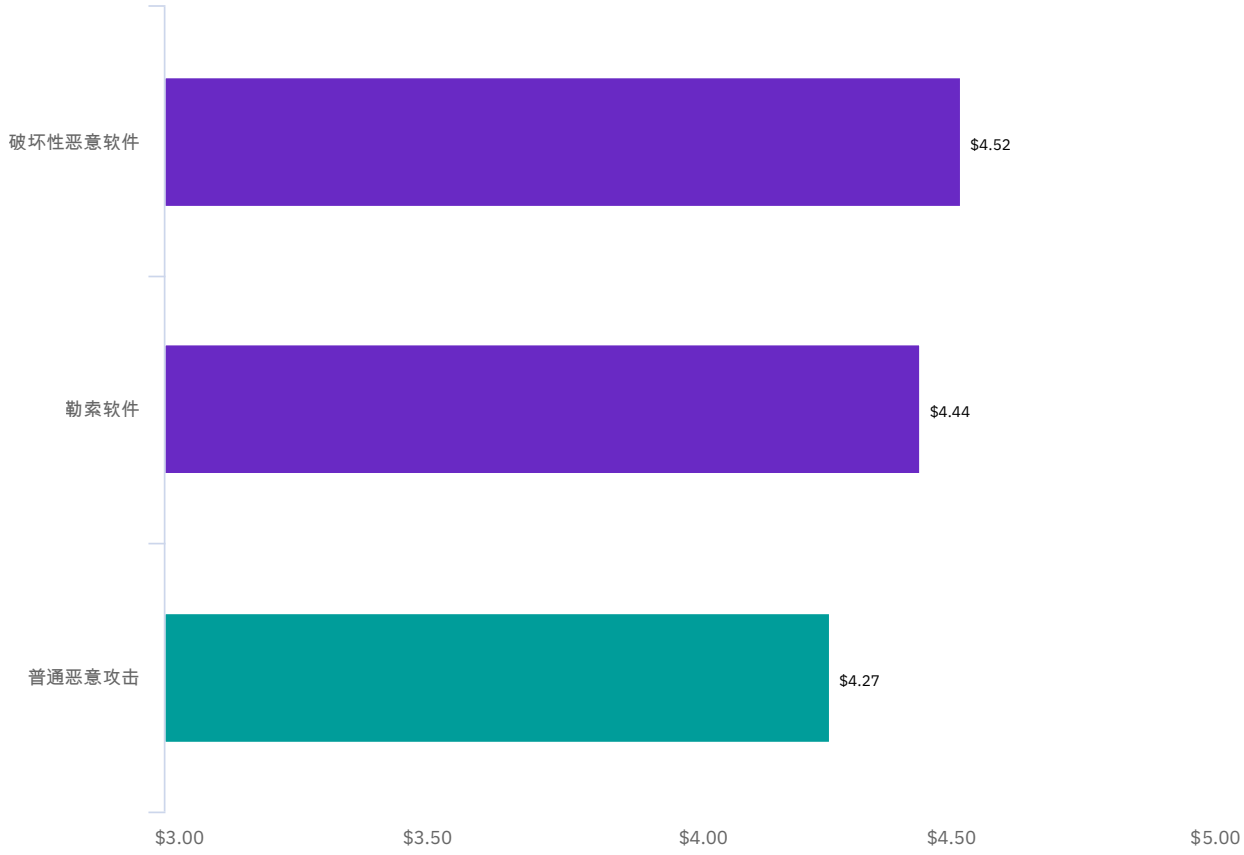
国家攻击者发起的恶意泄露造成的成本最为高昂。

图 24 按威胁主体类型显示了数据泄露的成本。成本最高的恶意泄露由国家主体发起，平均成本为 443 万美元。黑客分子发起的恶意泄露的平均成本为 428 万美元，受经济利益驱动的网络犯罪分子发起的恶意泄露的平均成本为 423 万美元。

图 25

勒索软件或破坏性恶意软件漏洞的平均成本

以百万美元为单位



勒索软件和破坏性的恶意软件漏洞比普通的恶意攻击成本更高。

如 **图 25** 所示，以破坏性/雨刷式攻击破坏数据的恶意攻击（平均成本为 452 万美元）和勒索软件攻击（444 万美元），其成本比普通的恶意泄露（427 万美元）或普通的数据泄露（386 万美元）成本更高。

影响数据泄露成本的因素

本部分更加深入地探讨了影响数据泄露的多个因素，其中包括不同类型的安全技术和实践、IT 环境以及第三方介入。今年的研究分析了 25 个独特的成本因素，它们可以缓解影响（降低泄露的平均总成本）或放大影响（增加泄露的平均总成本）。

今年的报告中新增了多个因素：红队测试、漏洞测试以及安全托管服务（缓解成本的因素）和安全技能短缺以及远程工作（放大成本的因素）。

本部分还深度解析了三个可缓解数据泄露成本影响的领域：CISO 的角色、网络保险和事件响应团队。

重要发现

$291,870

增加与复杂安全系统相关的数据泄露的平均总成本

51%

利用网络保险索赔支付咨询和法律服务成本的组织的比例

46%

表示 CISO 最应该对数据泄露负责的受访者的比例

图 26

25 个重要因素对数据泄露平均总成本的影响

美国 386 万美元平均总成本的变化

安全系统复杂性和事件响应计划测试，对数据泄露的总成本影响最大。

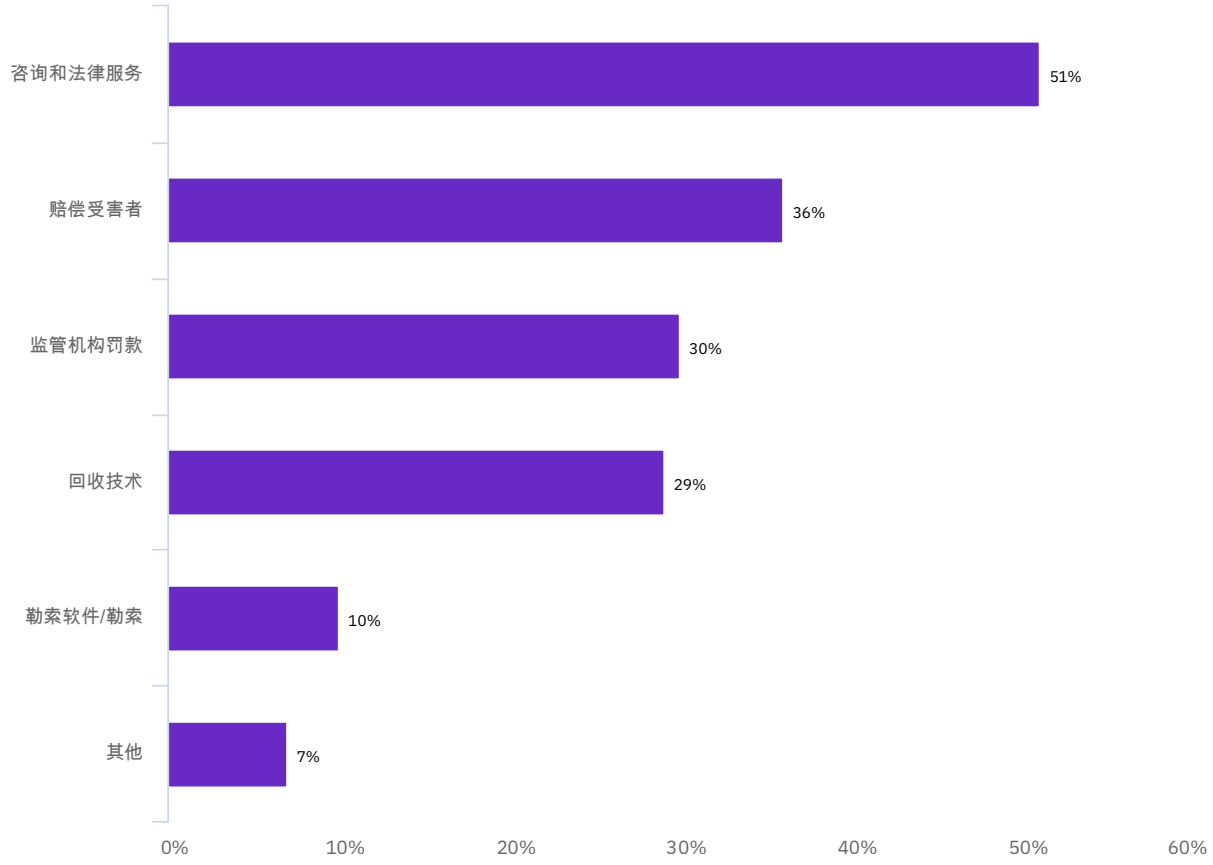
从**图 26** 可以看出 25 个因素对 386 万美元的数据泄露平均总成本的平均成本影响。各种使能技术和内部专业知识不足导致的安全系统复杂性，使数据泄露的平均总成本平均增加了 291,870 美元。向云端迁移产生了更高的数据泄露平均成本，平均成本增加了 267,469 美元。

可降低数据泄露平均总成本的因素包括广泛测试事件响应计划和业务连续性管理，这两项因素分别将平均成本降低了 295,267 美元和 278,697 美元。

图 27

使用网络安全保险索赔支付的成本类型

响应的百分比，允许多个响应



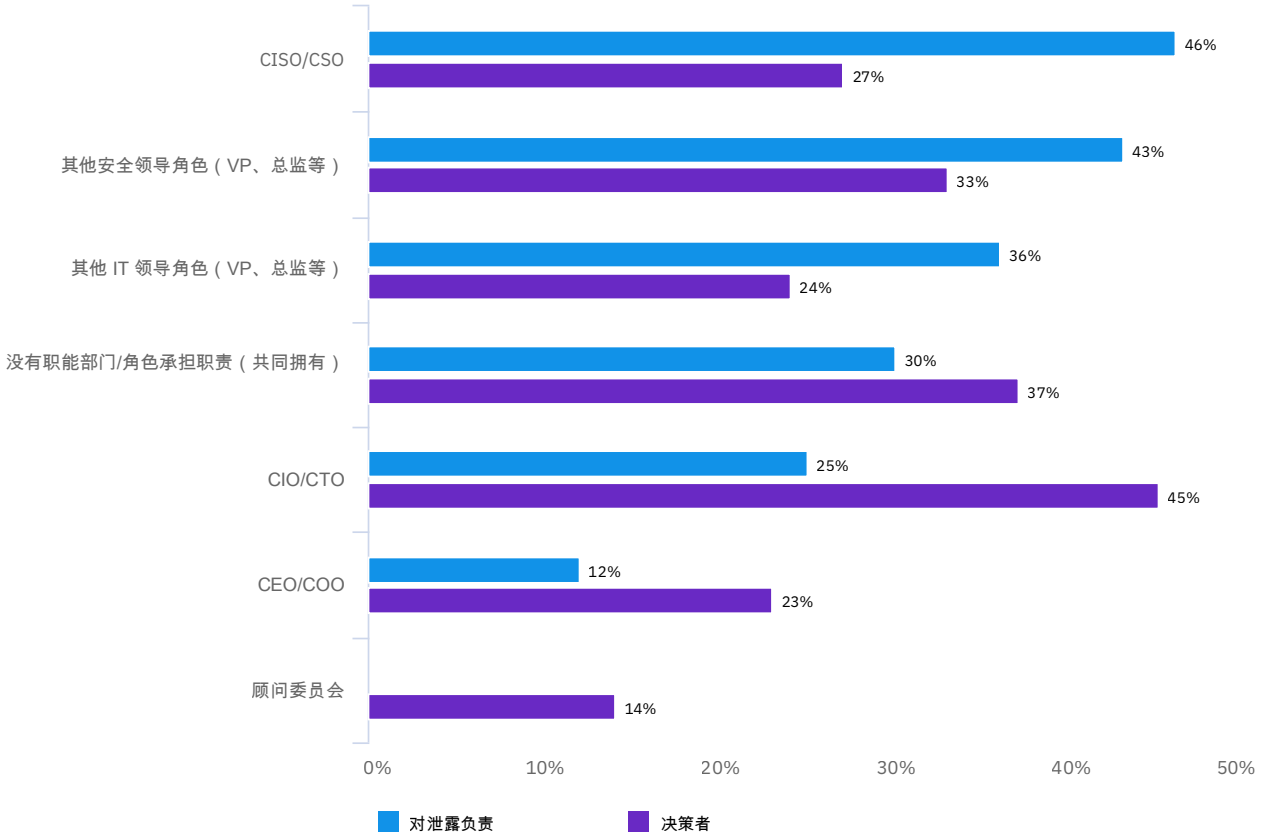
网络保险通常可涵盖第三方服务和受害者赔偿的费用。

从**图 27** 可以看出，51% 的组织会利用网络保险索赔来支付第三方咨询和法律服务的费用。36% 的组织利用网络保险向受害者支付赔偿费用。只有 10% 的组织利用网络保险索赔支付勒索软件或勒索的费用。

图 28

谁对数据泄露、网络安全政策和技术决策负有最大责任？

响应的百分比，允许多个响应



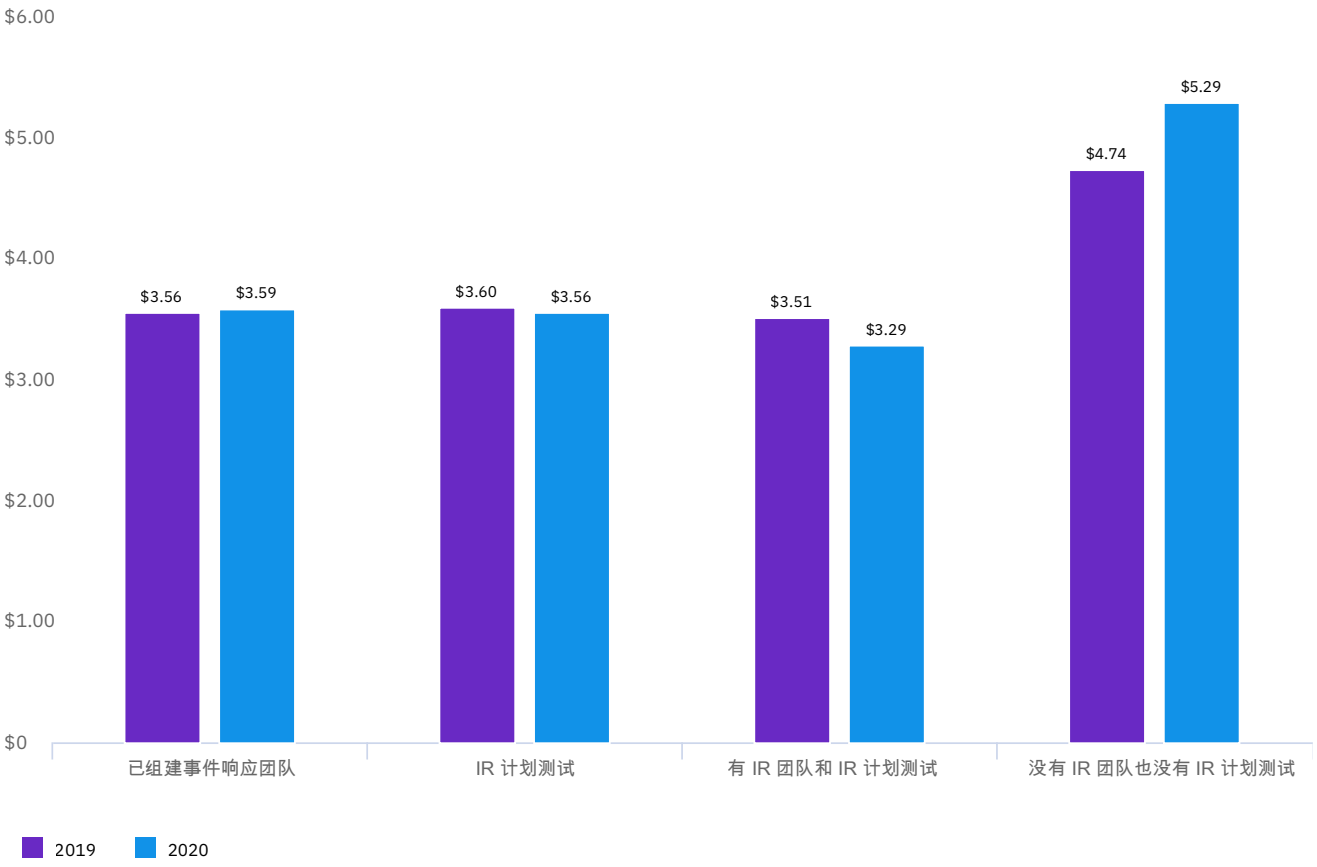
CISO 最有可能对数据泄露承担最终责任。

如**图 28** 所示，46% 的受访者表示，CISO/CSO 应该对数据泄露负责，但只有 27% 的受访者表示 CISO/CSO 最应该对网络安全政策和技术决策负责。CEO 和 COO 对数据泄露负责的可能性最小，而 CIO/CTO 通常被认为是网络安全政策和技术的最终决策者。

图 29

有事件响应团队和 IR 规划测试的数据泄露平均总成本

以百万美元为单位



事件响应团队和事件响应计划测试双剑合璧，可显著降低数据泄露的成本。

如**图 29** 所示，组建了事件响应团队并广泛测试其事件响应计划的组织，其数据泄露的平均成本为 329 万美元。相比之下，未采取任一项措施的组织的平均总成本为 529 万美元，二者相差 200 万美元。

安全自动化趋势和效力

这是我们第三年审视数据泄露成本与安全自动化之间的关系。在本报告中，安全自动化是指在发现和控制网络漏洞利用或漏洞时加大或替代人为干预的安全技术。此类技术依赖人工智能、机器学习、分析和自动编排。

重要发现

21%

2020 年全面部署安全自动化的组织比 2018 年的 15% 有所上升

$3.58百万

没有部署安全自动化的组织与全面部署自动化的组织在数据泄露平均总成本方面的差异

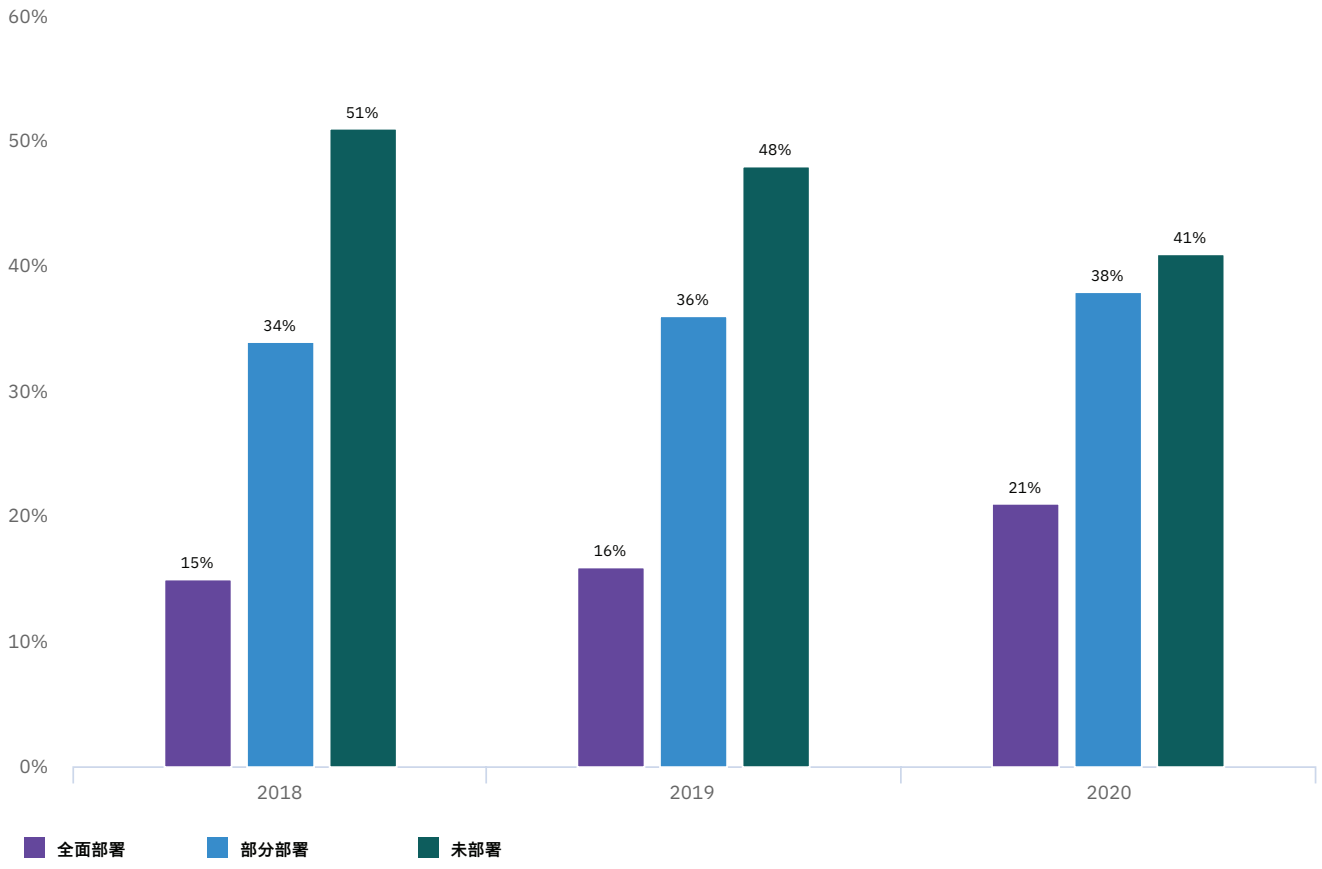
30%

德国全面部署安全自动化的组织的比例在所有国家中排名最高

图 30

比较三个部署水平的安全自动化状态

每种自动化水平的组织所占的百分比



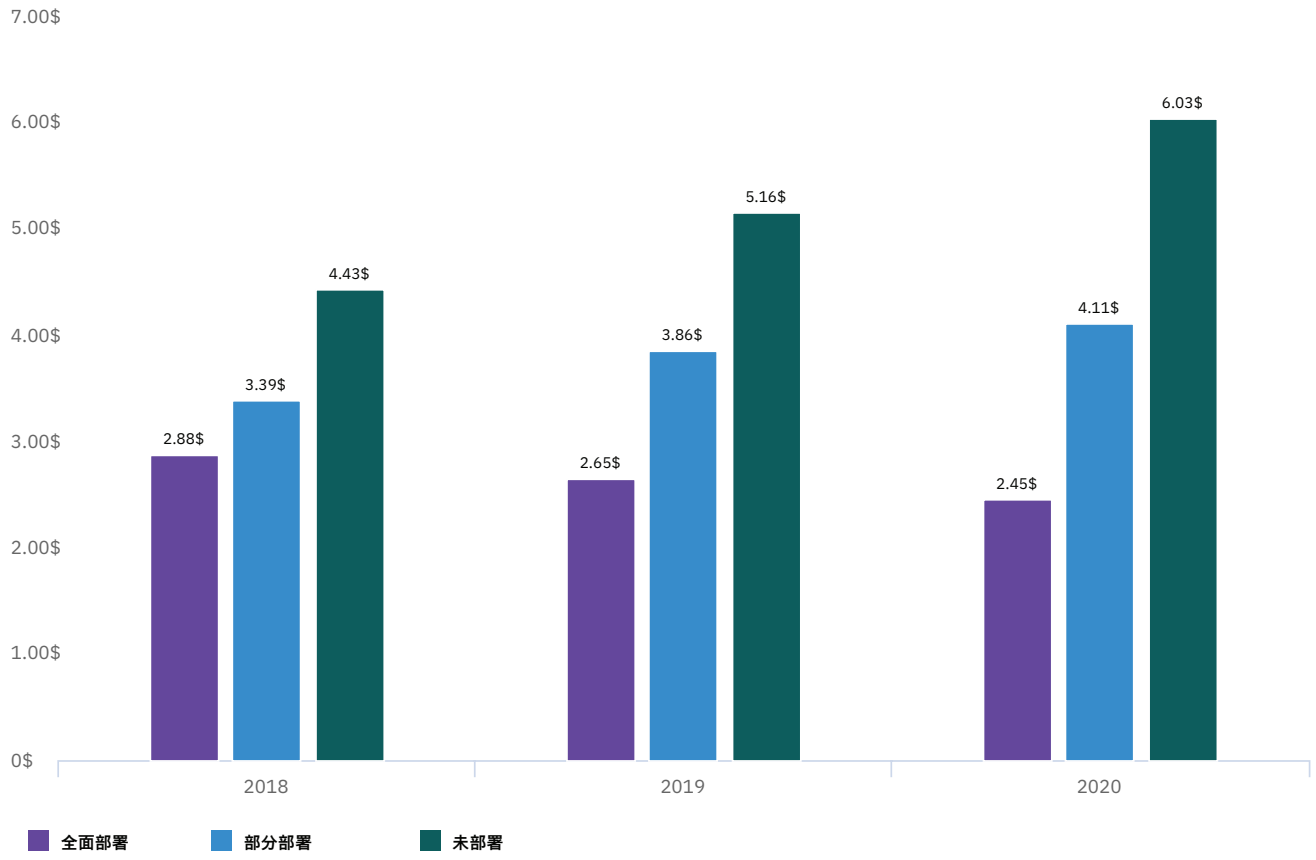
全面部署自动化的比例在过去三年间有所增加。

如**图 30** 所示，在 2020 年的研究中，只有 21% 的公司全面部署了安全自动化，2018 年这一比例为 15%，2019 年为 16%。在 2020 年的研究中，还有 38% 的公司部分部署了自动化，41% 的公司尚未部署自动化。

图 31

各安全自动化部署水平的数据泄露平均总成本

以百万美元为单位



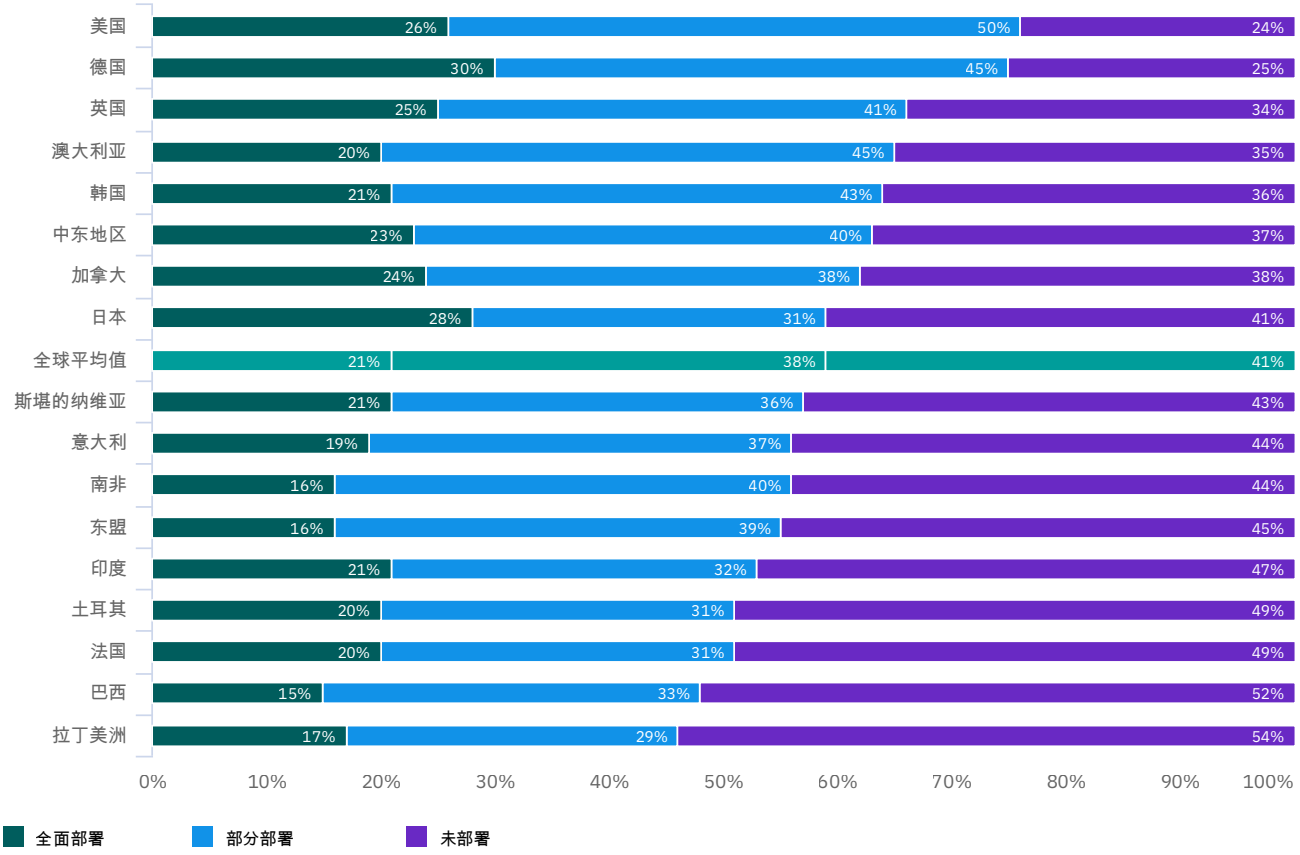
安全自动化对数据泄露成本的影响在过去三年间有所增加。

如**图 31** 所示，在 2020 年的研究中，全面部署了安全自动化的组织的数据泄露平均总成本为 245 万美元，比尚未部署安全自动化的组织的平均成本少 358 万美元。在 2018 年的研究中，全面部署了自动化的组织与未部署自动化的组织，二者的数据泄露平均成本差距为 155 万美元，2019 年这一差距为 251 万美元。

图 32

各国家/地区的安全自动化部署平均水平

三种自动化水平的组织所占的百分比



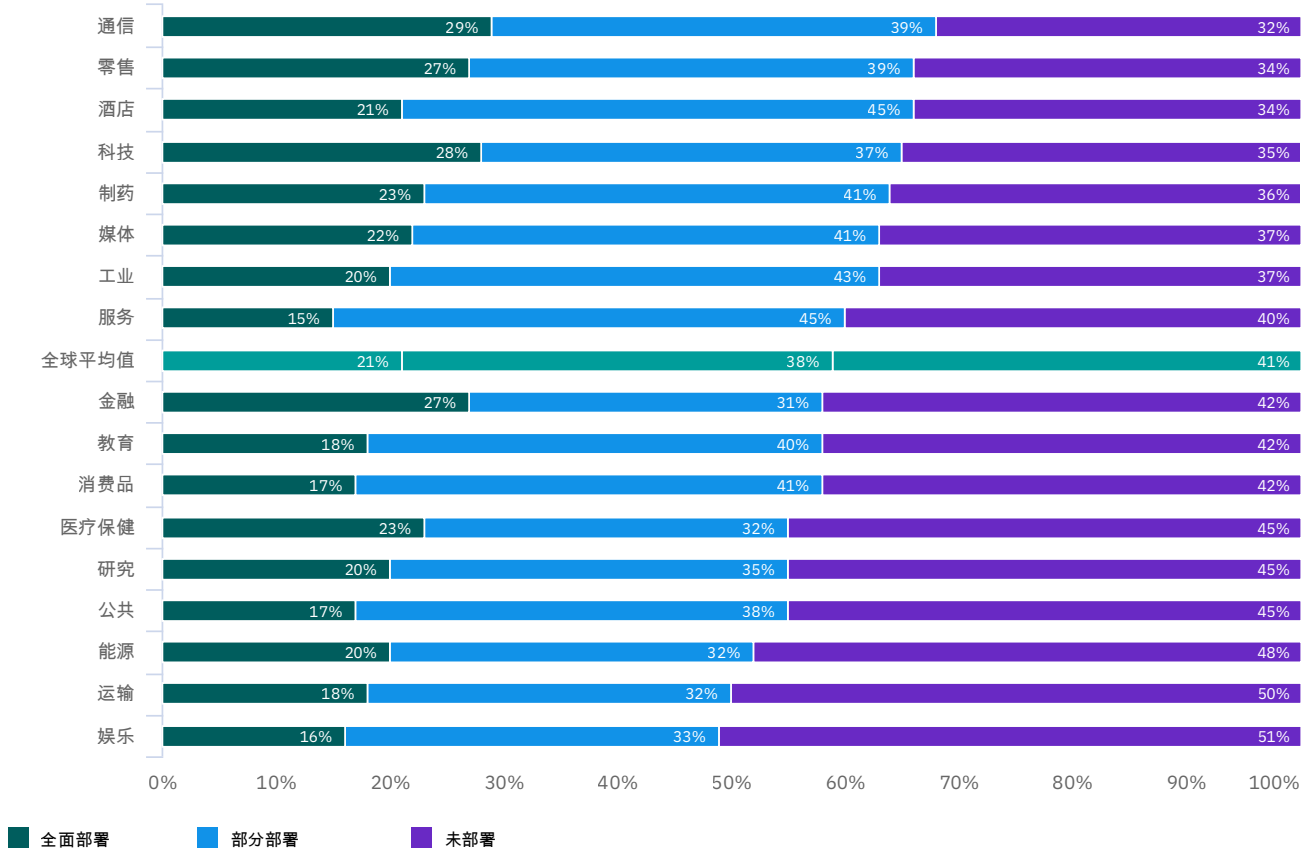
安全自动化的状态因国家和地区而异。

从**图 32** 可以看出，美国和德国全面部署或部分部署自动化的组织比例更高（美国为 76%，德国为 75%）。美国全面部署安全自动化的比例为 26%，德国为 30%。在未部署自动化的国家中，拉丁美洲和巴西所占的比例最高，分别为 54% 和 52%。

图 33

各行业的安全自动化部署平均水平

三种自动化水平的组织所占的百分比



部署的安全自动化水平因行业而异。

从**图 33** 可以看出，通信、科技和零售行业的组织全面或部分部署自动化的比例最高。金融行业的组织全面部署安全自动化的比例 (27%) 高于组织的平均比例。但是在金融行业里，部分部署自动化的组织所占比例相对较低 (31%)，这意味着金融行业里全面和部分部署自动化的综合比例低于全球平均水平 (58%，全球平均水平为 59%)。娱乐和运输行业没有部署自动化的组织比例最高。

发现并控制数据泄露的时间

前几年的研究结果发现，发现和控制数据泄露的速度越快，成本就越低。发现的平均时间是检测到已发生事件所需的时间。控制时间是指组织在检测到事件并最终恢复服务所需的时间。

从初次检测出泄露到控制泄露之间经历的时间，我们称之为数据泄露生命周期。这些指标可用于判断组织事件响应和控制流程的效力。本次研究首次考察了安全自动化对数据泄露生命周期方向的影响。

重要发现

280 天

发现并控制数据泄露的平均时间

315 天

发现和控制恶意攻击引起的数据泄露的平均时间

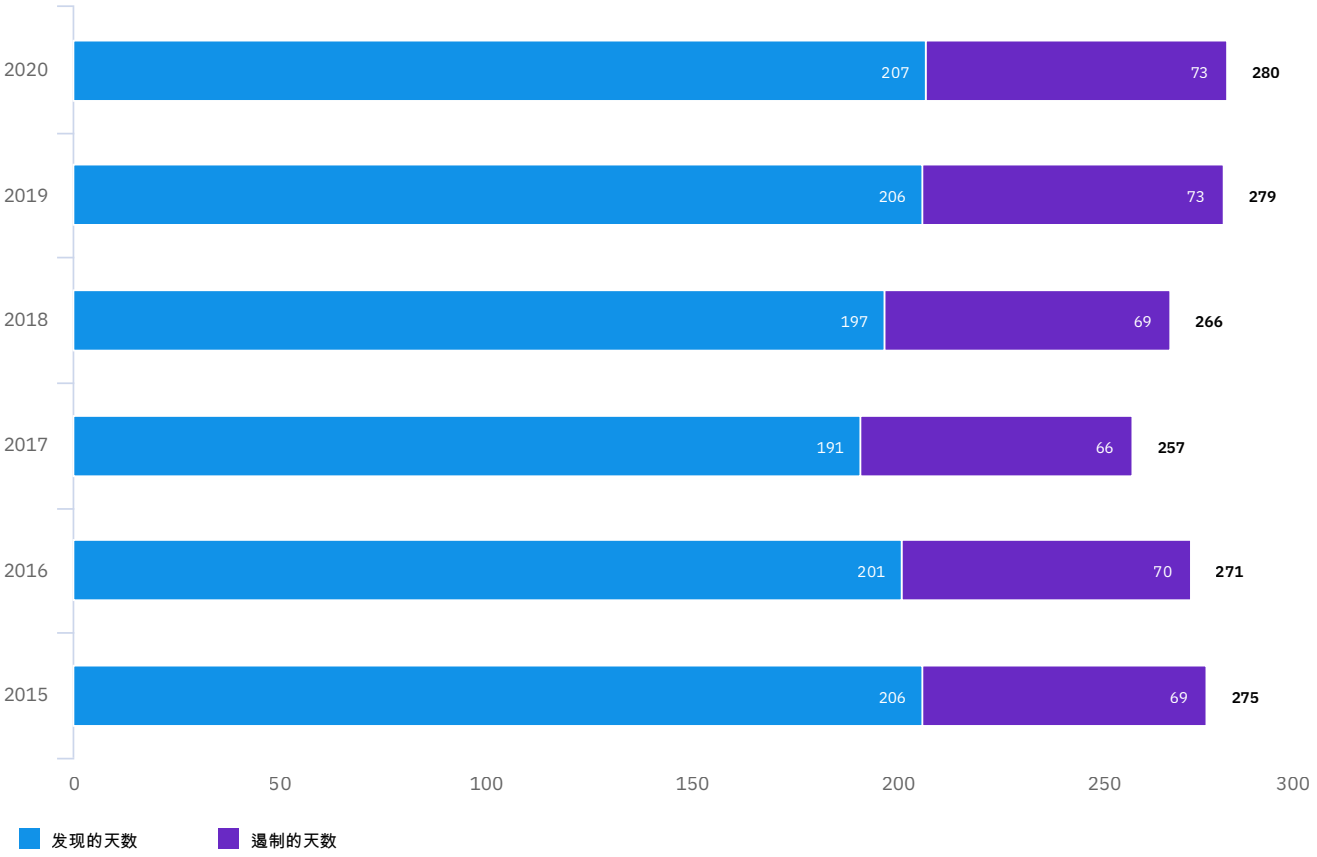
$1.12 百万

与 200 天以上相比，在 200 天以内控制数据泄露所节省的平均成本

图 34

发现并控制数据泄露的平均时间

以天为单位



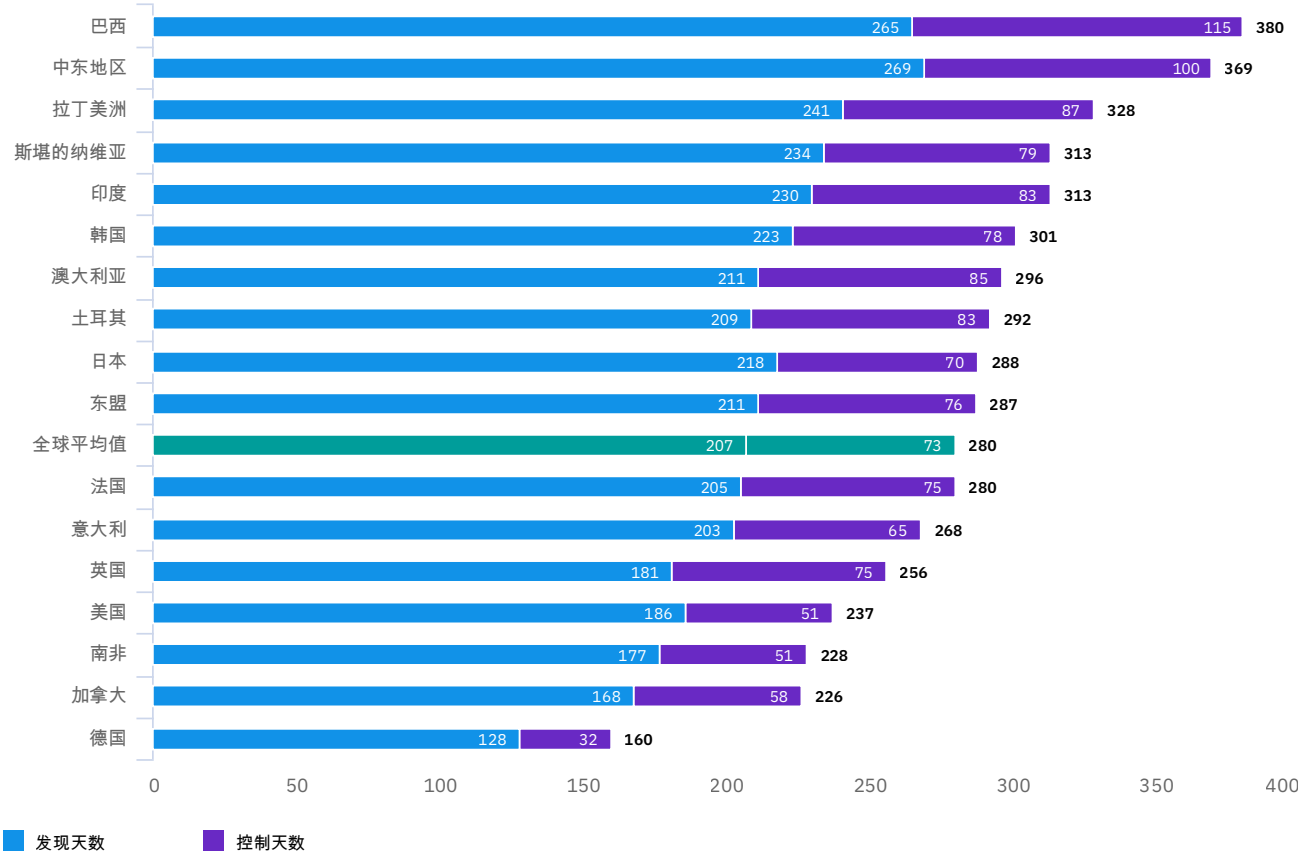
发现和控制泄露的平均时间一直较为平稳。

如**图 34** 所示，在过去的几份报告中，发现和控制数据泄露的时间变化不大。在 2020 年的研究中，发现泄露的平均时间为 207 天，控制泄露的平均时间为 73 天，共计 280 天。2019 年，数据泄露生命周期为 279 天。

图 35

发现和控制数据泄露的平均时间（按国家或地区划分）

以天为单位



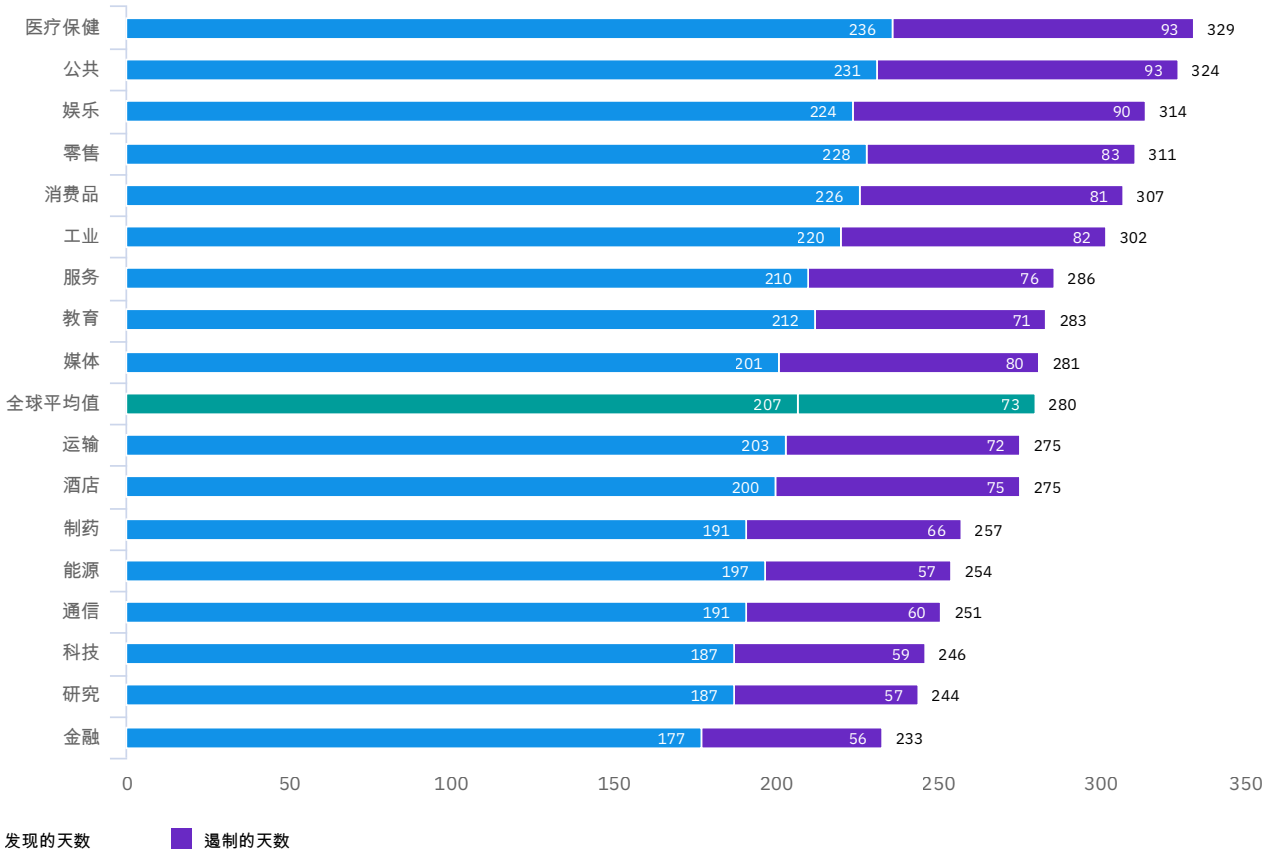
各国家/地区在平均泄露生命周期方面存在显著差距。

如**图 35** 所示，巴西和中东发现和控制数据泄露所需的平均时间远远高于平均值，分别为 380 天和 369 天。南非、加拿大和德国的数据泄露生命周期较短，德国的组织平均只需 160 天即可控制泄露。

图 36

各行业发现并控制数据泄露的平均时间

以天为单位



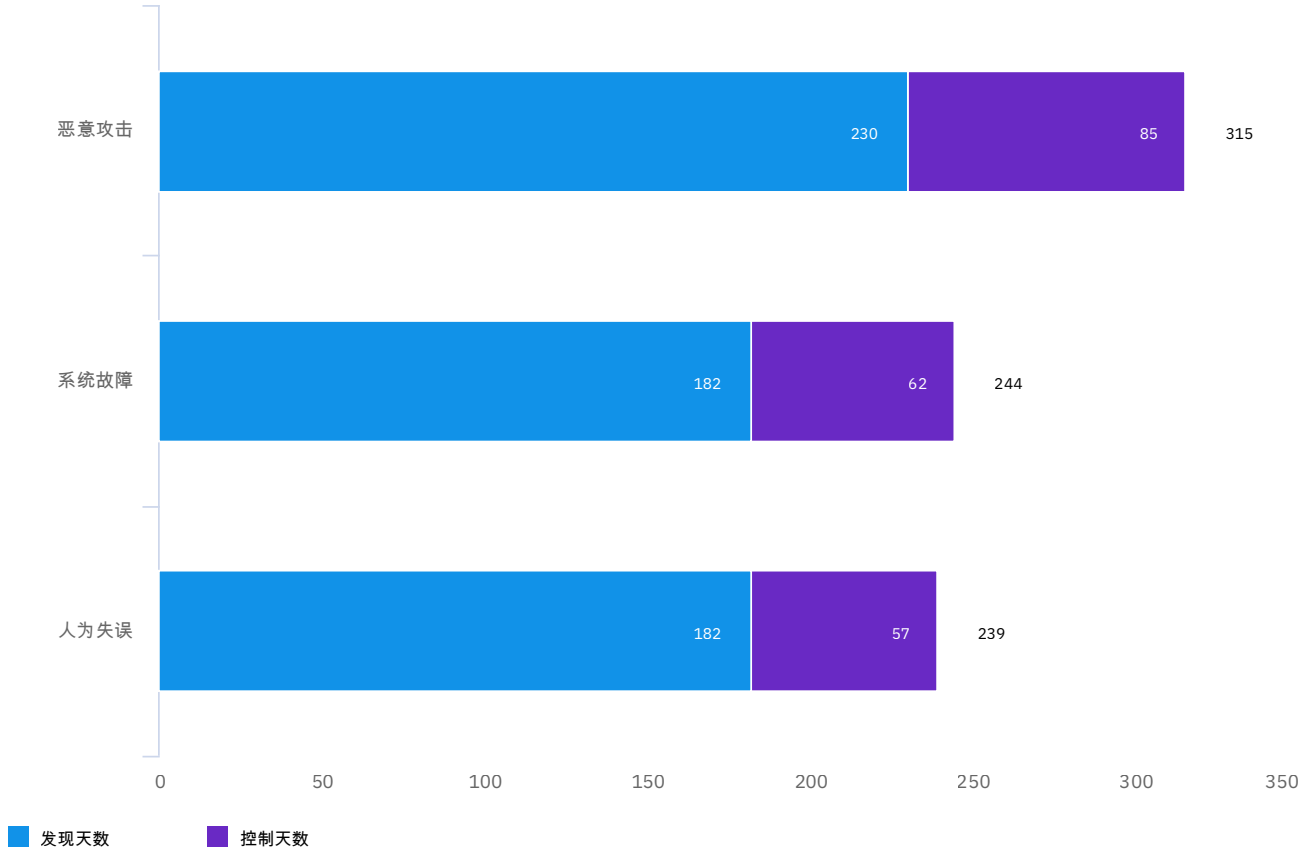
金融行业与医疗保健行业在控制泄露方面的时间相距甚远。

如**图 36** 所示，医疗保健行业发现和控制泄露的平均时间最长，达 329 天。金融行业发现和控制泄露的平均时间最短，为 233 天。九个行业高于 280 天的全球平均泄露生命周期，另八个行业低于此水平。

图 37

发现并控制数据泄露的平均时间（按根本原因划分）

以天为单位



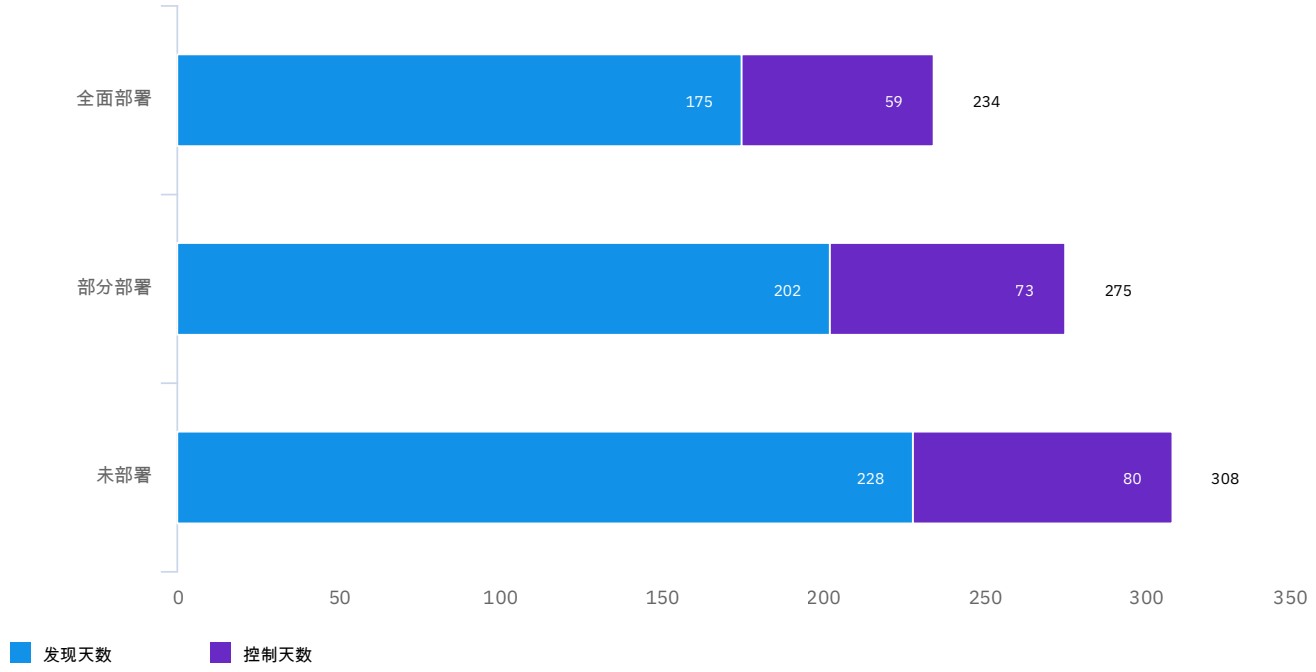
恶意攻击导致的数据泄露所需的发现和控制时间最长。

如 **图 37** 所示，在 2020 年的研究中，与其他根本原因导致的泄露相比，发现和控制恶意泄露的平均时间为 315 天。发现和控制系统故障引发的泄露平均需要 244 天，发现和控制人为失误引发的泄露平均需要 239 天。与普通的数据泄露相比，发现恶意泄露的时间要长 23 天。发现恶意泄露的平均时间为 230 天，而总体平均需要 207 天。

图 38

发现并控制数据泄露的平均时间（按安全自动化水平划分）

以天为单位



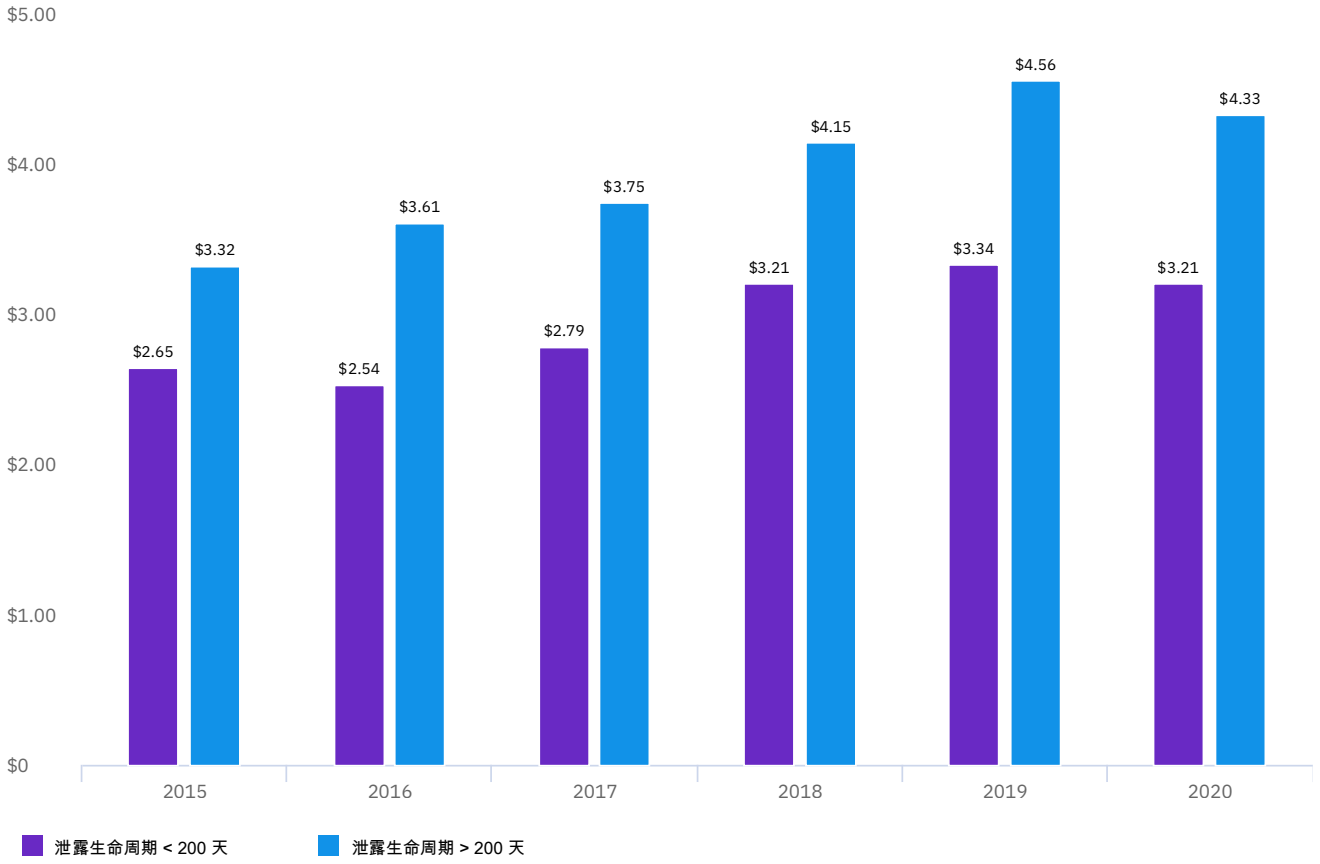
安全自动化缩短了发现和控制数据泄露的时间。

本次研究首次考察了自动化对数据泄露生命周期的影响。从**图 38** 可以看出，全面部署自动化之后，发现泄露的平均时间为 175 天，控制泄露的平均时间为 59 天。若未部署自动化，发现泄露的平均时间会大幅增加至 228 天，控制泄露的时间会增加至 80 天，总计 308 天。

图 39

基于数据泄露平均生命周期的数据泄露平均总成本

以百万美元为单位



数据泄露生命周期影响了泄露的平均成本。

过去六年的研究得出了一致的结果，即生命周期（发现泄露的时间与控制泄露的时间之和）在 200 天以上的数据泄露成本远远高于生命周期不到 200 天的数据泄露。如**图 39** 所示，在 2020 年的研究中，生命周期超过 200 天的泄露的平均成本比不到 200 天的泄露平均要高出 112 万美元（200 天以上为 433 万美元，不到 200 天为 321 万美元）。

数据泄露的长尾成本

数据泄露的成本影响在事件发生之后持续多年。在去年的研究中，我们首次考察了数据泄露在两年或两年多之后对组织的影响。研究结果显示，泄露发生后的第一年成本最高，但在两年多之后又会卷土重来。

我们还考察了受到高度监管的行业的组织与数据保护法规较为宽松的行业在“长尾成本”方面的差异。我们定义的接受高度监管的行业包括：能源、医疗保健、消费品、金融、科技、制药、通信、公共部门和教育。零售、工业、娱乐、媒体、研究服务和酒店行业的组织所在的监管环境较为宽松。在对监管严厉和监管宽松的行业所作的分析中，我们得出了如下结论：监管和法律成本可能是导致泄露发生多年之后成本上升的原因。

在 2020 年的研究中，我们以 101 家公司为样本，这些公司承担了两年或两年以上的数据泄露成本。

重要发现

61%

第一年发生的数据泄露成本的平均比例

44%

受到严厉监管的行业第一年发生的数据泄露成本的平均比例

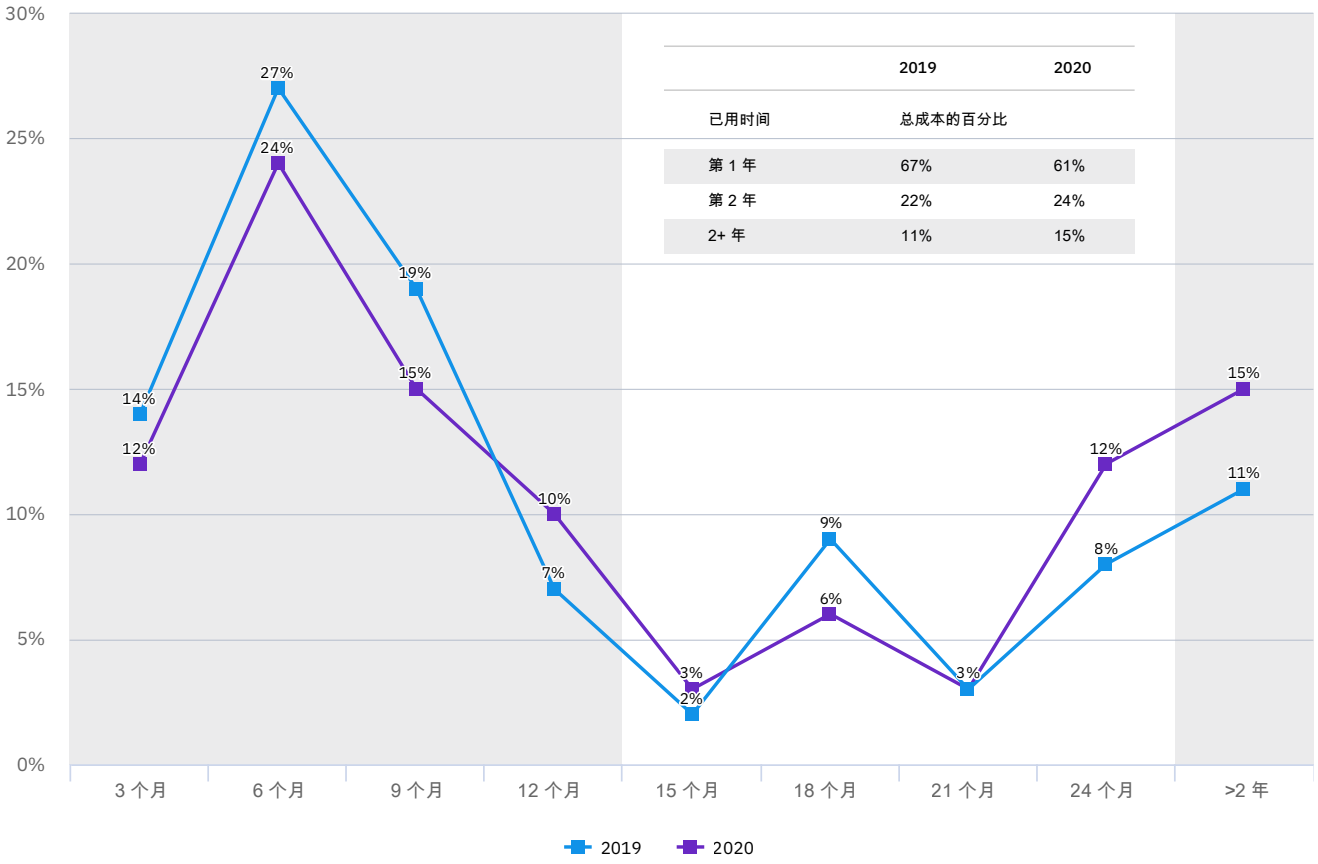
92%

监管宽松的行业前两年发生的数据泄露成本的平均比例

图 40

两年多之后数据泄露平均成本的分布情况

以三个月为间隔发生的成本百分比



已用时间	2019 总成本的百分比	2020
第 1 年	67%	61%
第 2 年	22%	24%
2+ 年	11%	15%

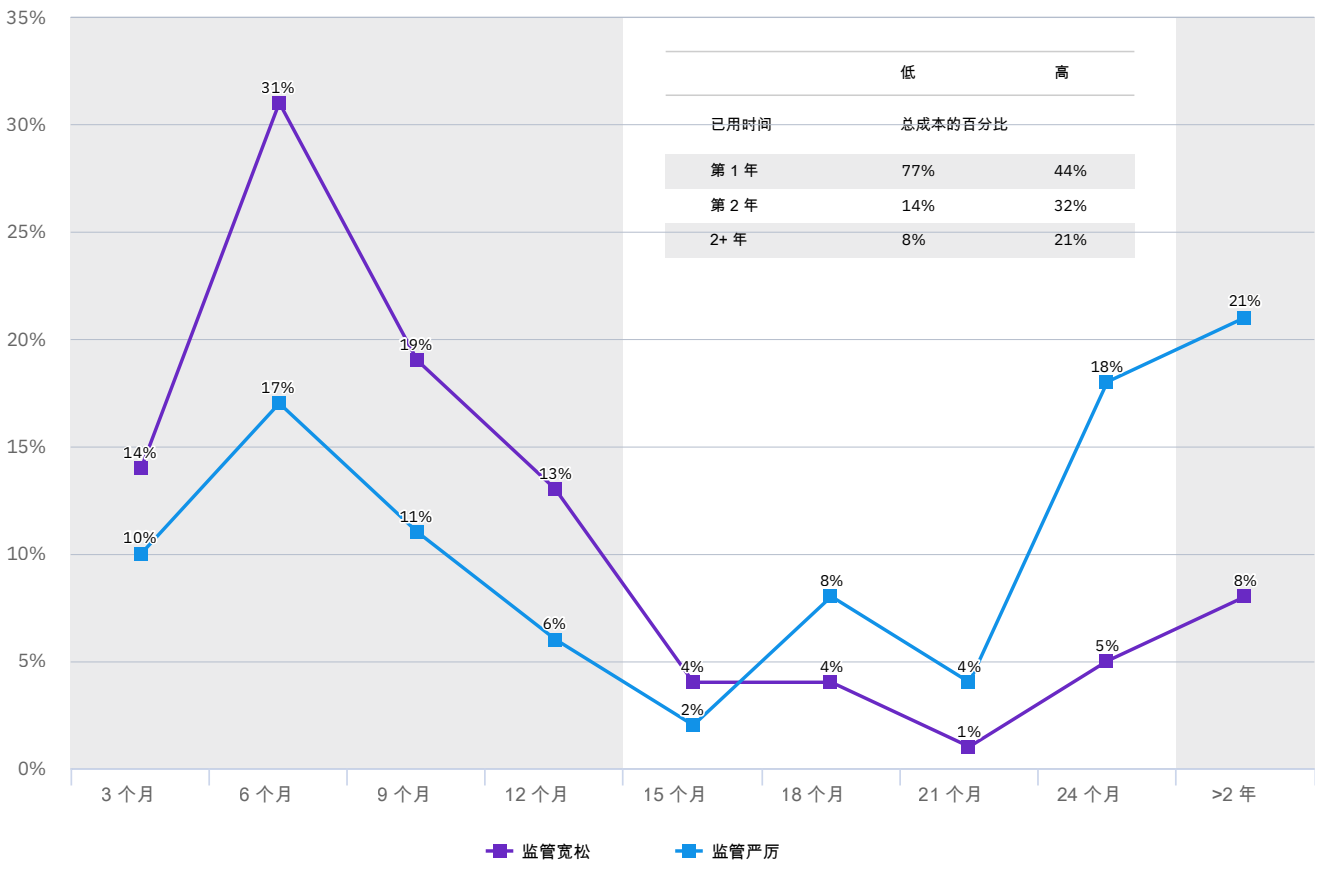
在 2020 年的研究中，两年后发生的泄露成本的比例有所增加。

如**图 40** 所示，长尾成本分析发现，数据泄露的成本平均有 61% 发生在第一年，24% 发生在第二年，还有 15% 发生在两年后。与 2019 年分析中的 11% 相比，泄露发生两年多之后的成本略有增加。

图 41

宽松和严厉监管环境下数据泄露平均成本的分布情况

以三个月为间隔发生的总成本百分比



已用时间	低	高
	总成本的百分比	
第 1 年	77%	44%
第 2 年	14%	32%
2+ 年	8%	21%

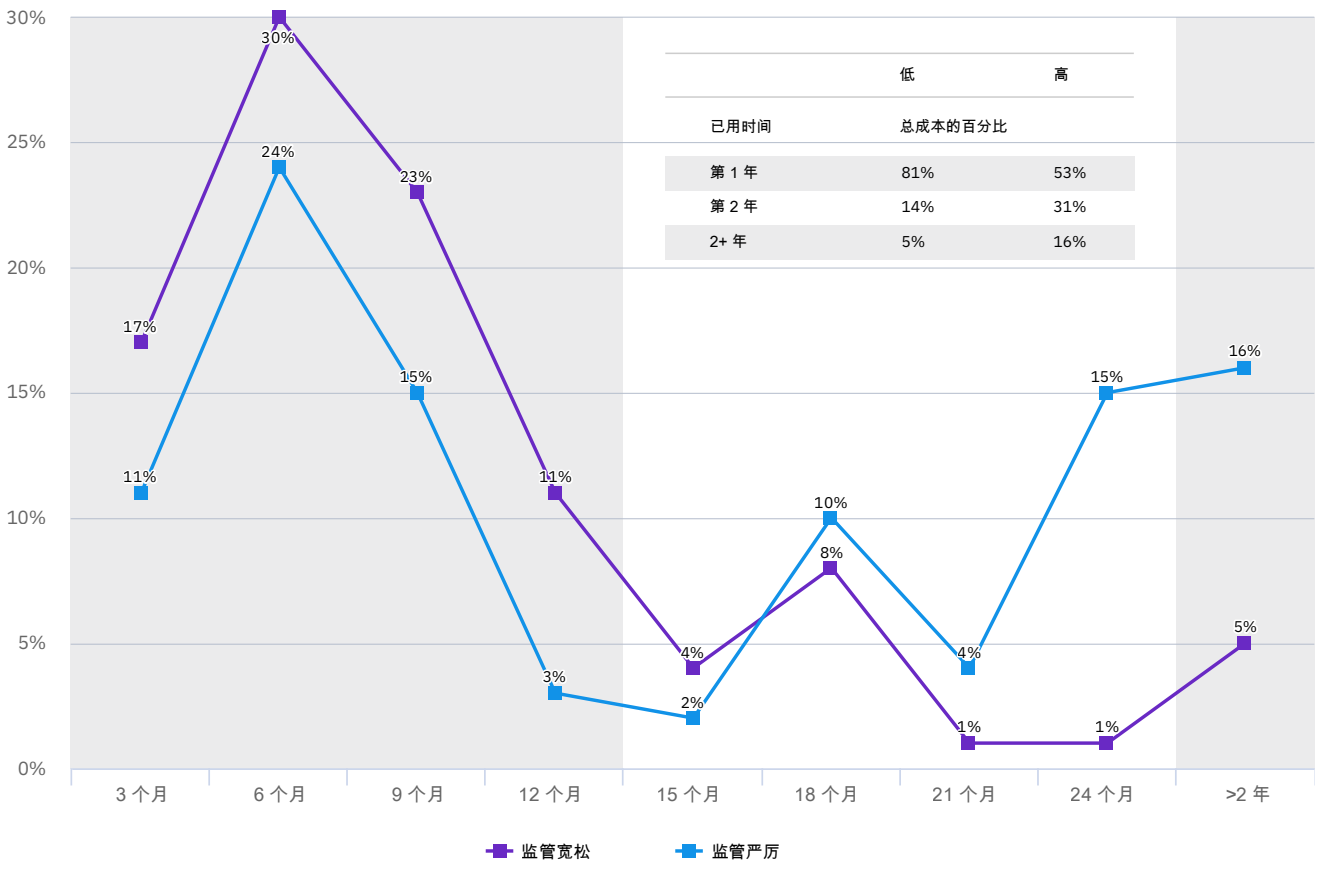
受到高度监管的行业，在泄露发生一年之后承担了大部分成本。

如**图 41** 所示，较为宽松的监管环境下的组织更有可能在第一年承担数据泄露的全部成本。在监管较为宽松的行业中，平均有 77% 的成本发生在第一年，而在监管较为严厉的组织内，平均有 44% 的泄露成本发生在第一年。

图 42

宽松和严厉监管环境下数据泄露平均成本的分布情况(2019 年报告)

以三个月为间隔发生的总成本百分比



	低	高
已用时间	总成本的百分比	
第 1 年	81%	53%
第 2 年	14%	31%
2+ 年	5%	16%

从 2019 年对严厉监管环境和宽松监管环境的分析看出，泄露发生两年多之后产生的成本比例有所下滑。

图 42 显示了 2019 年研究中，宽松的数据保护监管环境与严厉的数据保护监管环境下的长尾泄露成本。在 2019 年的研究中，受到高度监管的行业平均有 16% 的成本发生在两年之后。而在 2020 年的研究中，受到高度监管的行业平均有 21% 的成本发生在两年之后(参阅图 41)。

新冠肺炎带来的潜在影响

新冠肺炎疫情极大改变了组织的经营方式，大量员工在家办公，增加了对视频会议、云应用和网络资源的需求。为了解这一新的态势，我们在研究中增加了几个问题，以收集研究参与者对新冠疫情对数据泄露成本潜在影响的看法。

重要发现

54%

为应对新冠疫情需要远程工作的组织的百分比

76%

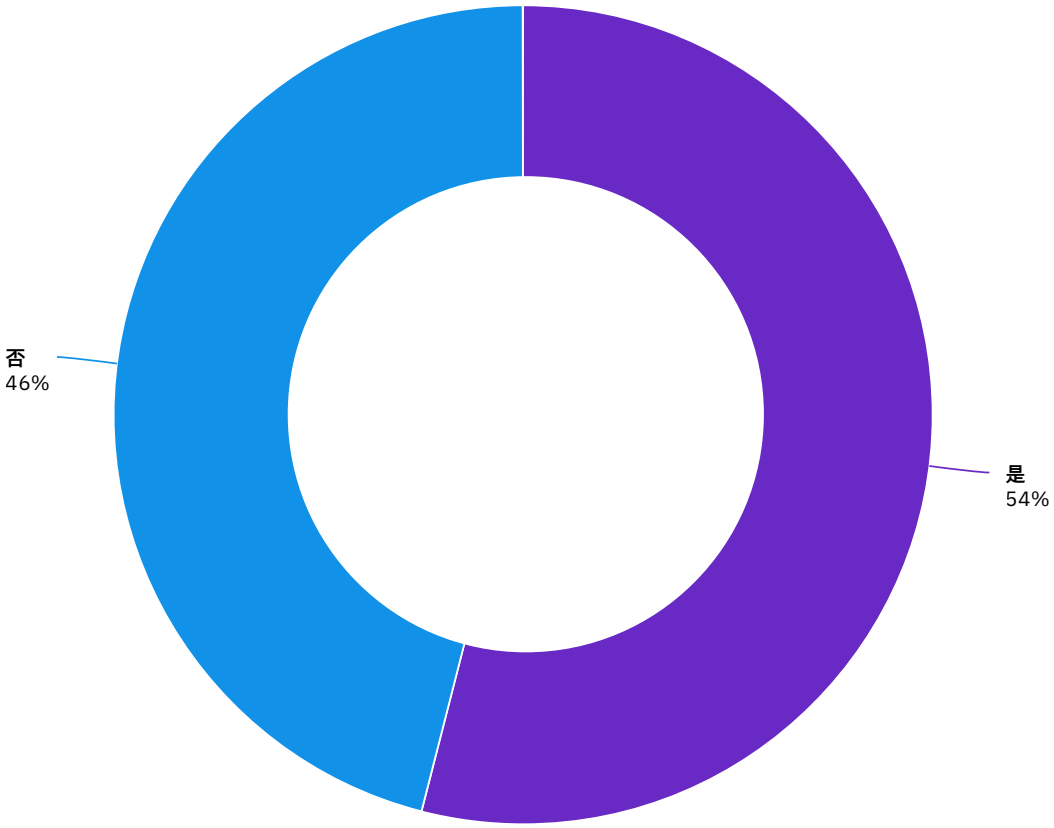
认为远程工作会增加发现和控制数据泄露时间的参与者比例

70%

认为远程工作会增加数据泄露成本的参与者比例

图 43

您的组织是否因为新冠疫情而要求员工远程工作？

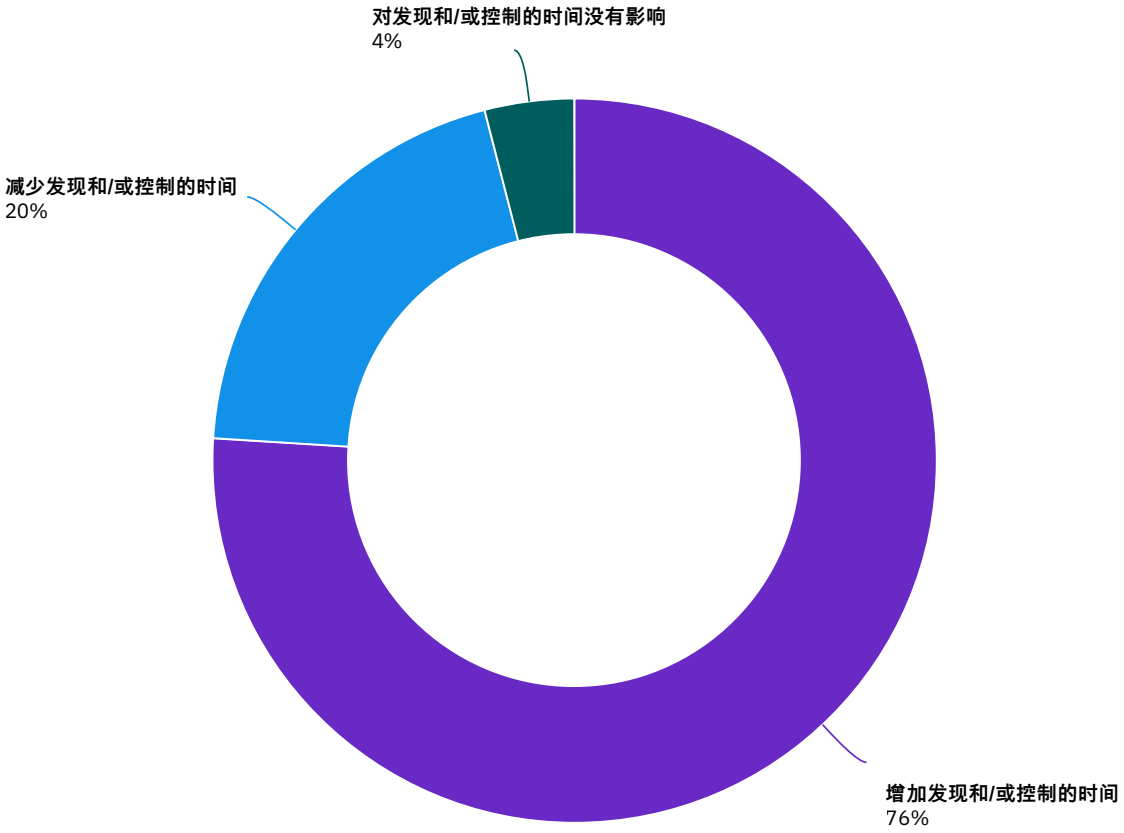


新冠疫情之下，大多数组织都需要远程工作。

如**图 43** 所示，为应对新冠疫情，研究中的大多数组织 (54%) 都需要远程工作。

图 44

远程工作对您响应数据泄露的能力有何影响？

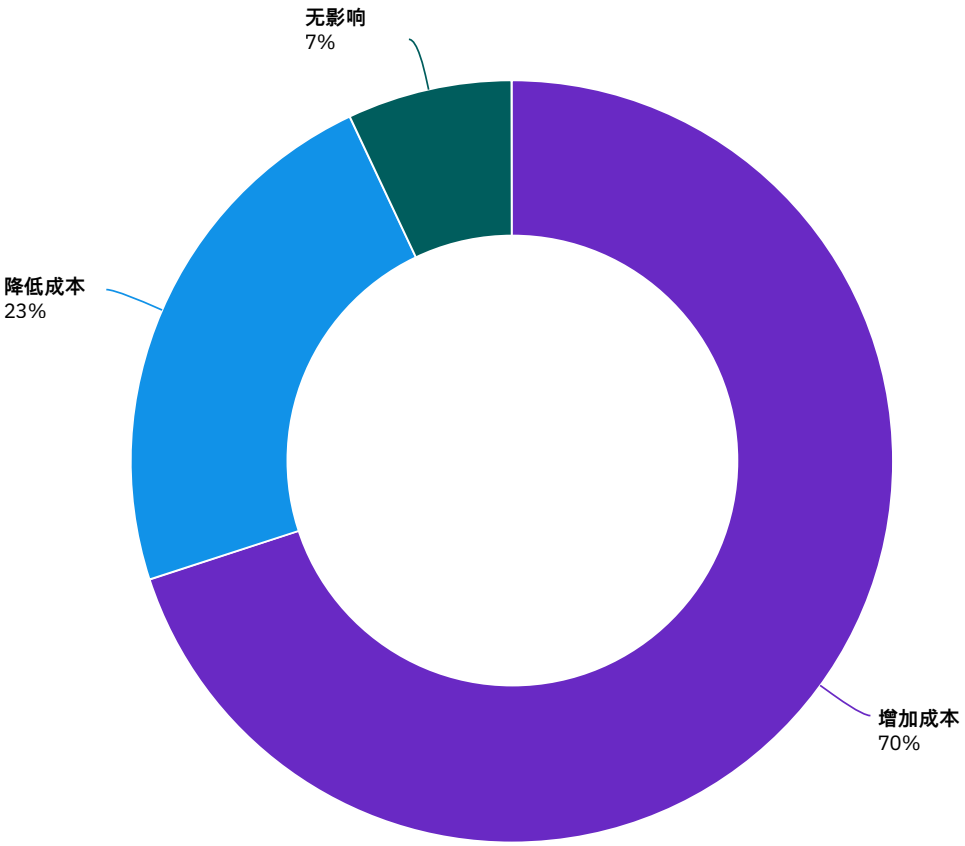


四分之三的受访者预计可能需要更长的时间才能发现和控制数据泄露。

从**图 44** 可以看出，在表示组织因为新冠疫情需要开展远程工作的受访者中，有超过四分之三 (76%) 的受访者认为此举会增加发现和控制数据泄露的时间，20% 的受访者认为会缩短发现和控制泄露的时间，还有 4% 表示不会有任何影响。

图 45

远程工作如何影响数据泄露的成本？



远程工作会增加潜在数据泄露的成本。

如**图 45** 所示，在表示组织因为新冠疫情需要开展远程工作的受访者中，70% 的受访者认为此举会增加潜在数据泄露的成本。还有 23% 的受访者表示会降低数据泄露的成本，另外 7% 的受访者则表示不会有任何影响。

大规模泄露的成本

今年是我们第三年评估破坏记录达 100 多万条的数据泄露的成本，也就是我们所说的大规模数据泄露。这种大规模泄露在大多数企业都并不常见，但一旦发生大规模泄露，就会对消费者和行业产生巨大的影响。自我们在 2018 年的研究中对它进行分析以来，大规模泄露的平均成本一直在增加。

今年的调查分析了 17 家公司，这些公司都遭遇了 100 万条甚至更多记录丢失或被盗的数据泄露。为全面阐释我们的方法，请参阅此报告末尾处的数据泄露成本常见问题。

重要发现

$392 百万

超过 5,000 万条记录的泄露的平均成本

100x

涉及 5,000 万条以上的记录与普通数据泄露在平均成本方面的差异

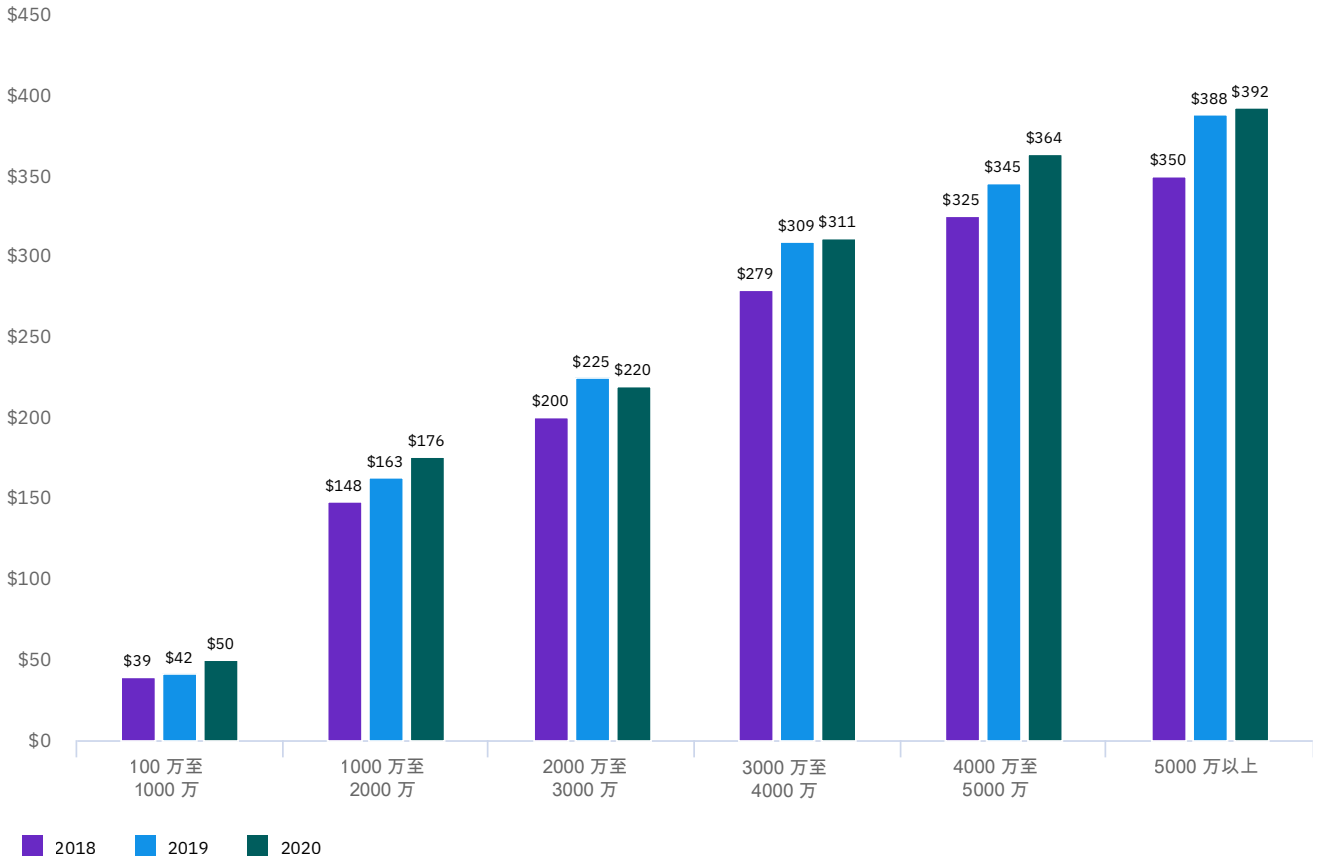
$19 百万

在 2019 年至 2020 年的研究中，涉及 4,000 万至 5,000 万条记录的泄露的平均成本有所增加

图 46

大型泄露的平均总成本（按丢失的记录数量计算）

以百万美元为单位



大规模泄露的成本屡创新高。

如**图 46** 所示，涉及 100 万条至 1,000 万条记录的泄露的平均成本为 5,000 万美元，是记录少于 100,000 条的泄露平均成本（386 万美元）的 25 倍以上。规模在 100 万至 1,000 万条记录的泄露增长速度最快，已从 2018 年的 3,900 万美元 (22%) 增长至 2020 年的 5,000 万美元。

记录超过 5,000 万条的泄露的平均成本为 3.92 亿美元，是数据泄露平均成本的 100 多倍。绝对成本增幅最大的是超过 5,000 万条记录的泄露，已从 2018 年的平均 3.5 亿美元增加到 2020 年的 3.92 亿美元。

可最大程度降低数据泄露带来的财务损失和品牌影响的措施

*在本部分中，IBM Security 概述了参与研究的组织为降低数据泄露带来的财务成本和名誉损失，所采取的措施。**

投资安全编排、自动化和响应 (SOAR) 以缩短发现和响应时间。

在数据泄露成本研究中，安全自动化可显著降低发现和响应泄露的平均时间以及平均成本。SOAR 软件和服务可帮助您的组织利用自动化、流程标准化以及与现有安全工具的集成加快事件响应。人工智能、分析和自动编排等自动化技术都可降低数据泄露平均成本。

采用零信任安全模型，以防止在未经授权的情况下访问敏感数据。

研究结果显示，丢失和被盗的凭据以及云错误配置是数据泄露最常见的三大根本原因。随着组织逐渐向远程工作和更少连接的混合多云环境转变，零信任策略让员工在适当的情境下对相关信息进行有限访问，从而保护数据和资源。

对响应计划开展压力测试以增强网络弹性。

与那些既未组建 IT 团队又未测试任何 IR 计划的组织相比，研究中既有事件响应 (IR) 团队又测试了事件响应计划的组织，其数据泄露平均总成本降低了 200 万美元。我们常说 “像实战一样训练，像训练一样实战”，就意味着要制定并测试事件响应方案，以优化企业高效迅速响应攻击的能力。

*安全实践建议仅供参考，并不能保证结果。

使用有助于保护和监控端点与远程员工的工具。

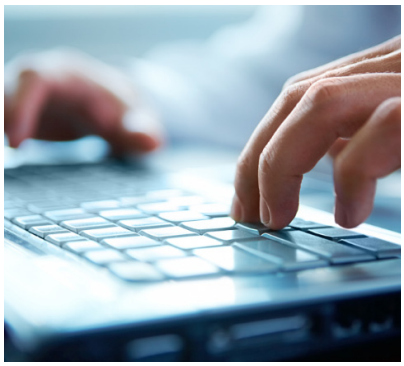
在因为新冠疫情需要开展远程工作的组织中，70% 的组织认为此举会增加数据泄露的成本。统一的端点管理 (UEM) 以及身份和访问管理 (IAM) 产品和服务，可让安全团队更加深入地了解公司以及自带 (BYO) 笔记本电脑、台式机、平板电脑、移动设备和 IoT（其中包括组织没有物理访问权限的端点）的可疑活动，从而缩短调查和响应时间以隔离并控制破坏。

投资治理、风险管理与合规计划。

检测和升级成本仅次于损失业务的成本，是研究中排名第二的泄露成本类别。可评估企业风险并跟踪政府要求遵从性的内部审计框架，有助于增强组织检测数据泄露并加大控制力度的能力。

最大程度降低 IT 和安全环境的复杂性。

在今年的研究中，在列举的 25 个因素中，安全系统的复杂性是导致数据泄露平均成本增加的头号因素。第三方引起的数据泄露，广泛的云迁移和 IoT/OT 环境也推高了数据泄露成本。能够在分散的系统之间共享数据的安全工具，可帮助安全团队检测复杂的混合多云环境中的事件。

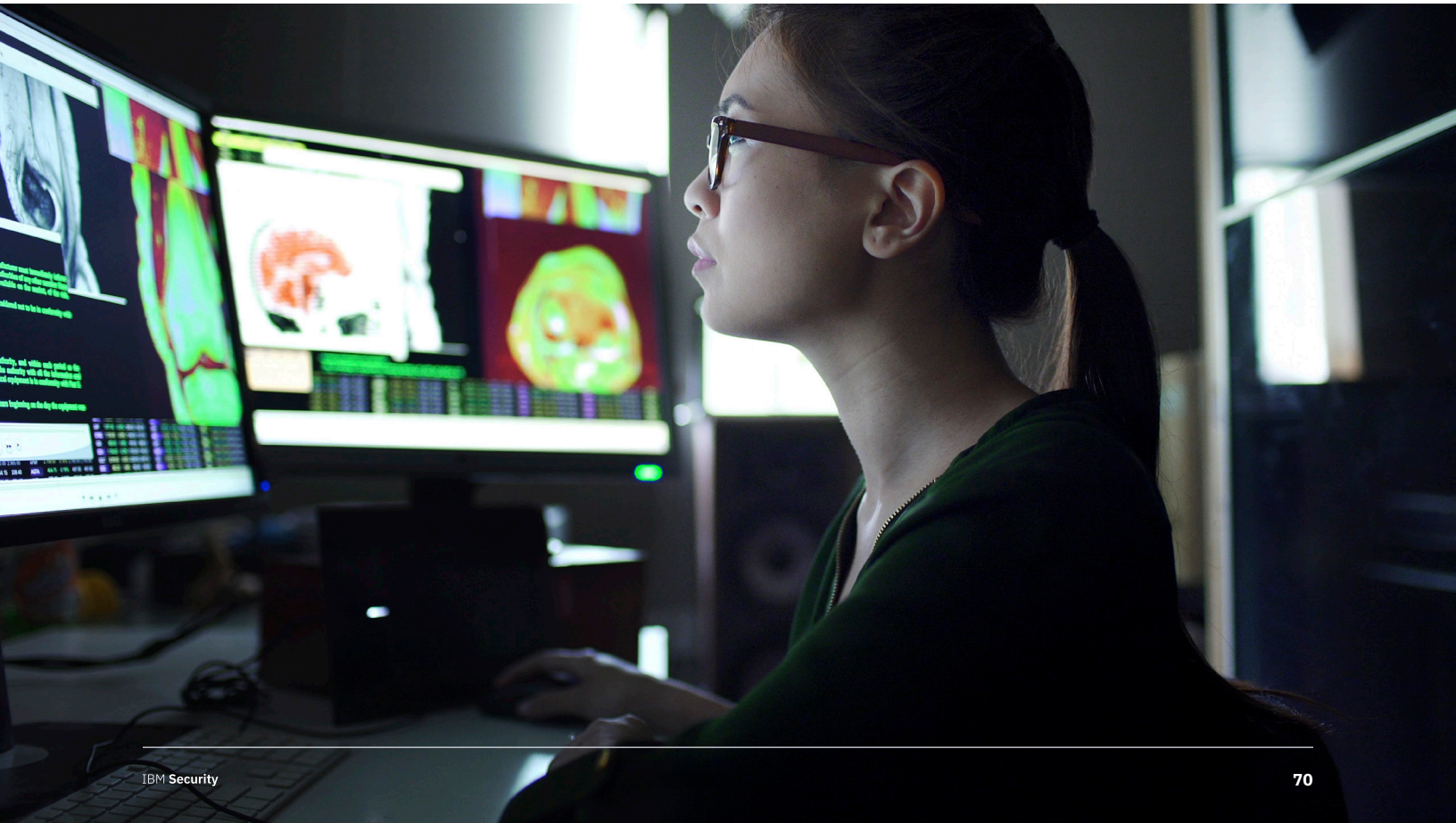


利用政策和技术保护云环境中的敏感数据。

随着云环境中托管的数据量和价值不断增加，组织应该采取措施保护云托管的数据库。数据分类方案和保留计划有助于了解容易被破坏的敏感和机密信息，并通过加密保护敏感信息。漏洞扫描、渗透测试和红队有助于发现云托管的数据库漏洞风险和错误配置。研究发现，所有这些解决方案都可降低数据泄露平均成本。

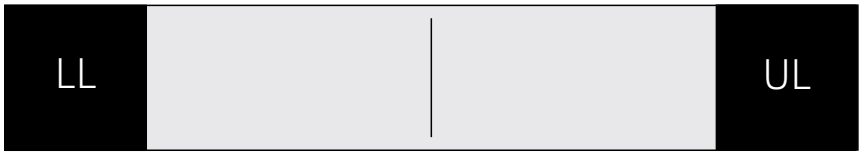
使用托管的安全服务有助于缩小安全技能差距。

研究中的组织发现，安全技能短缺是导致数据泄露成本增加的主要原因之一，而安全托管服务则有助于降低数据泄露平均成本。安全托管服务提供商利用持续的监控和集成的解决方案与服务简化安全与风险。



研究方法

为确保充分的机密性，基准工具不会捕捉任何公司特定的信息。数据收集方法不包含实际的会计信息，而是依赖各位参与者在数轴上标记范围变量来预估直接成本。参与者需要在每个数据泄露成本类别的上限和下限范围之间的一个点中标记一条数轴。



从数轴而不是各个已展示成本类别的点估计值来获得数值，保持了机密性，并确保较高的响应率。基准工具还要求参与者分别对直接成本和机会成本进行第二次预估。

为方便管理基准流程，我们尽量只预估我们认为是测量数据泄露成本必不可少的成本活动中心。在与众多专家探讨之后，最终确定的项目中包含固定的成本活动。收集基准信息之后，会重新仔细检查每件工具以确保一致性和完整性。

基准工具中包含的数据泄露成本项目的范围仅限于已知的成本类别，它们适用于各种处理个人信息的业务操作。我们相信，侧重于业务流程而非数据保护或隐私合规活动的研究会产生更高质量的结果。

数据泄露成本常见问题

什么是数据泄露？
数据泄露定义如下：电子格式或纸制形式的个人姓名和医疗记录和/或财务记录或借记卡面临潜在风险。本研究涉及的泄露中被破坏的记录在 3,400 至 99,730 条不等。

什么是被破坏的记录？
我们将记录定义为可以识别自然人（个人）的信息，该自然人的信息因为数据泄露而丢失或被盗。我们以数据库为例，其中保存了个人的姓名、信用卡信息及其他身份识别信息（PII），另一个示例是健康记录，其中保存了投保人的姓名和付款信息。

您如何收集数据？
我们的研究人员对 524 家在 2019 年 8 月至 2020 年 4 月期间经历过数据泄露的公司开展了 3,200 多次单独访谈，从中收集了大量深入的定性数据。我们从 2019 年 10 月开始招募组织，2020 年 4 月 21 日访谈正式结束。受访者中有 IT 专家也有合规和信息安全从业人员，他们对组织的数据泄露以及解决泄露问题所花费的成本都了如指掌。出于隐私考虑，我们没有收集组织特定的信息。

您如何计算成本？
要计算数据泄露的平均成本，我们收集了组织发生的直接和间接支出。直接支出包括聘请司法鉴定专家、外包热线电话支持，以及为将来的产品和服务提供免费的信用监控订阅和折扣。间接成本包括内部调查和沟通，以及营业额或客户获取率下降而造成客户流失的外推值。

本次研究只呈现了与数据泄露经历直接相关的事件。例如，组织可能因为《通用数据保护条例》（GDPR）和《加州消费者隐私法案》（CCPA）等新法规而决定加大对网络安全治理技术的投资，但这些投资并未直接影响本次研究中呈现的数据泄露成本。

为与前几年的研究保持一致，我们使用了相同的货币换算方法，而没有调整会计成本。

基准研究与调查研究有何不同？
数据泄露成本报告中的分析单位是组织。调查研究中的分析单位是个人。我们招募了 524 家组织来参与本次研究。

每条记录的平均成本能否用于计算涉及数百万份记录丢失或被盗的数据泄露的成本？
我们研究中的数据泄露平均成本不适用于灾难性的大型数据泄露，例如 Equifax、Capital One 或 Facebook。这些都不是许多组织都会经历的常见泄露。

因此，要通过了解数据泄露成本行为来得出有用的结论，我们把不超过 10 万份记录的数据泄露事件作为我们的研究目标。它与本研究不一致的地方在于，它使用每条记录的成本来计算单起或多起记录总数量达数百万之巨的泄露事件的成本。但今年的研究使用了模拟框架，它以 17 个此等规模的数据泄露为样本，衡量涉及 100 万份甚至更多记录（大型泄露）的数据泄露事件的成本影响。

为什么使用模拟方法来估算大规模数据泄露的成本？
17 家遭遇大型泄露的公司样本量太小，无法使用作业成本法执行有统计显著性的分析。为解决这一问题，我们部署了蒙特卡罗模拟法，利用它通过反复试验预估一系列可能（随机）的结果。

我们一共执行了 15 万多次试验。所有样本均值的总均值提供了各种规模的数据泄露最有可能的结果 — 被破坏的记录从 100 万份到 500 万份不等。

是否每年都跟踪相同的组织？
每年的研究都会涉及不同的公司样本。为了与之前的报告保持一致，我们每年招募的样本公司都有类似的特征，例如行业、员工人数、地理区域和数据泄露的规模等。从 2005 年起至今，我们已经研究了 3,940 家组织的数据泄露事件。

组织特征

今年的研究涉及到 524 个来自不同地域和行业且规模各异的组织。2020 年的研究抽样调查了 17 个国家或地区的 17 个行业。

今年的研究首次审查了位于拉丁美洲的组织集群地，其中包括墨西哥、阿根廷、智利和哥伦比亚。

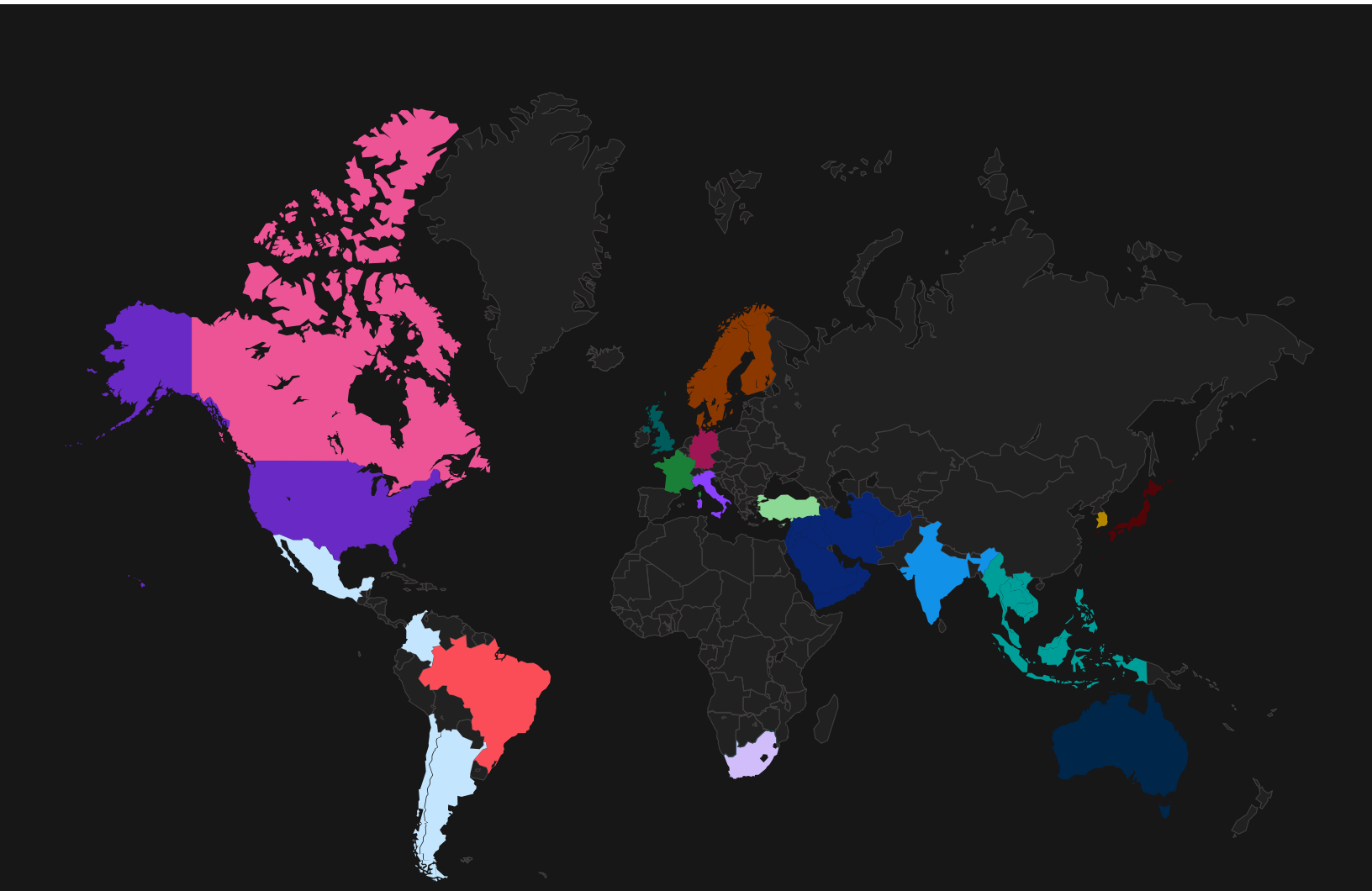
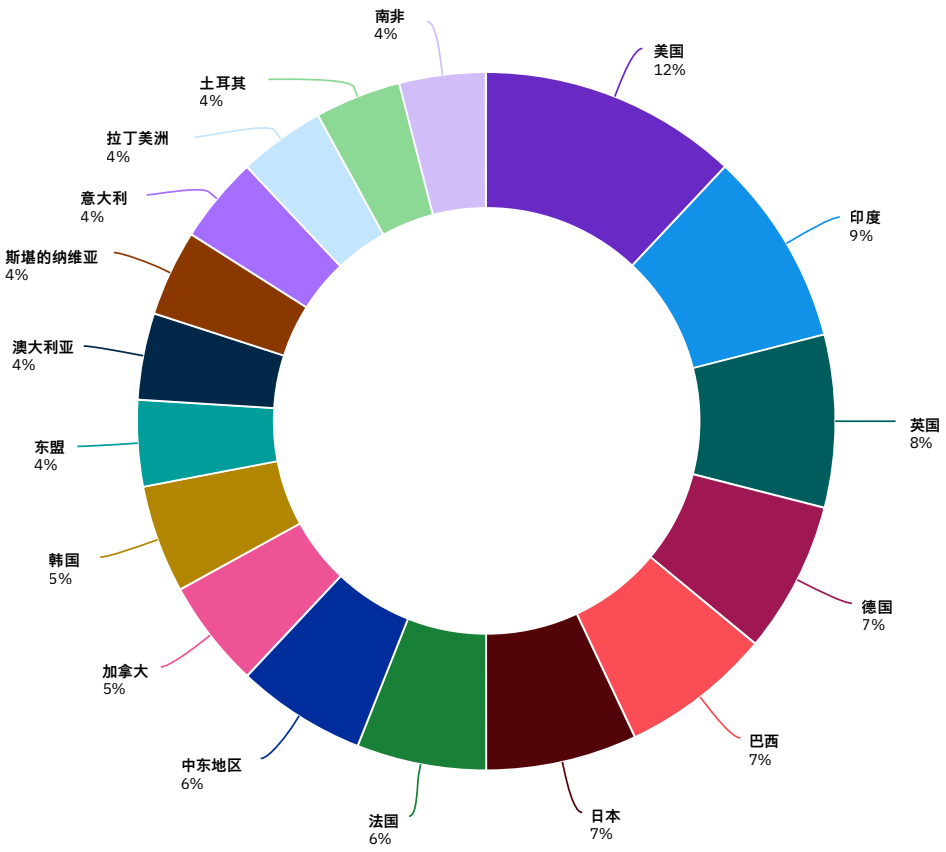


图 47

样本分布(按国家或地区)



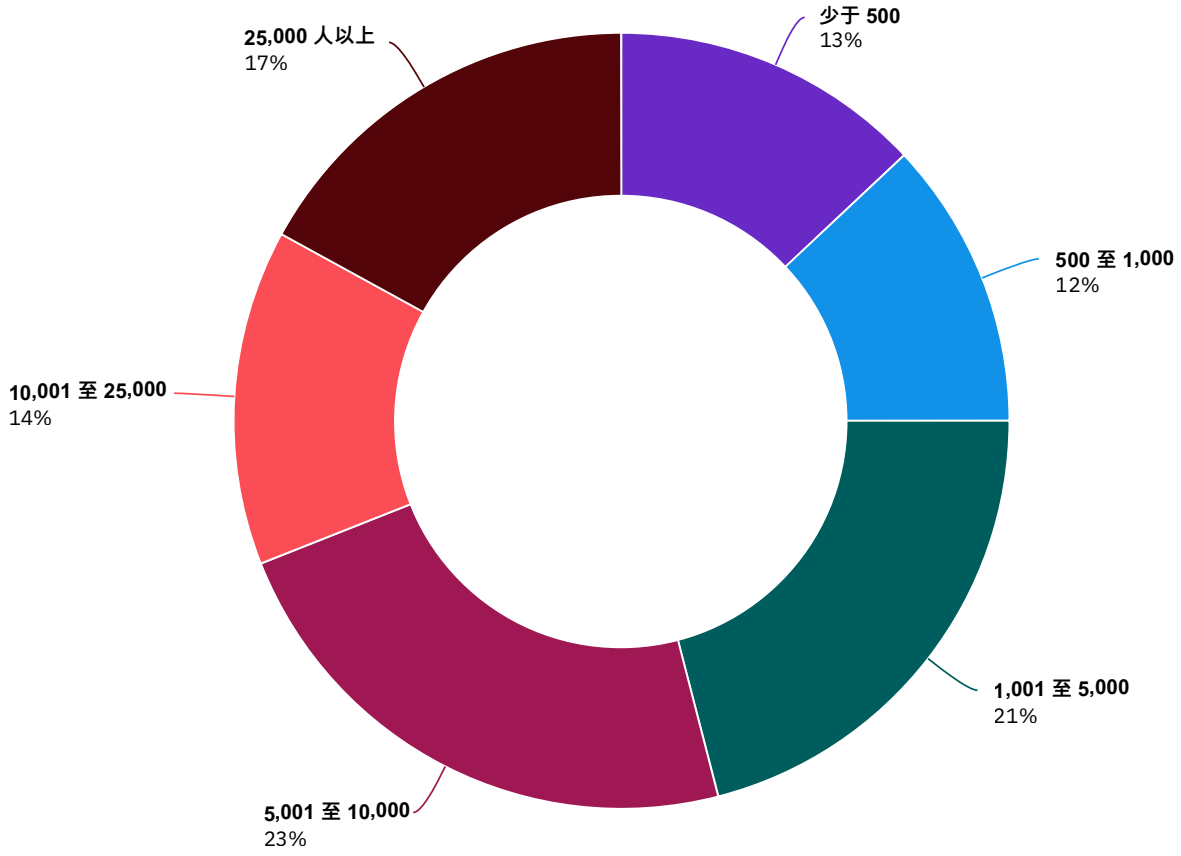
本次研究呈现了来自六大洲的国家/地区。

图 47 显示了基准组织的分布情况(按国家或地区划分)。美国以 12% 的代表比例高居榜首,印度和英国分别以 9% 和 8% 的比例紧随其后。代表比例最低的国家/地区是东盟、澳大利亚、斯堪的纳维亚、意大利、拉丁美洲、土耳其和南非。

图 48

按公司规模划分的样本分布情况

按员工人数测量

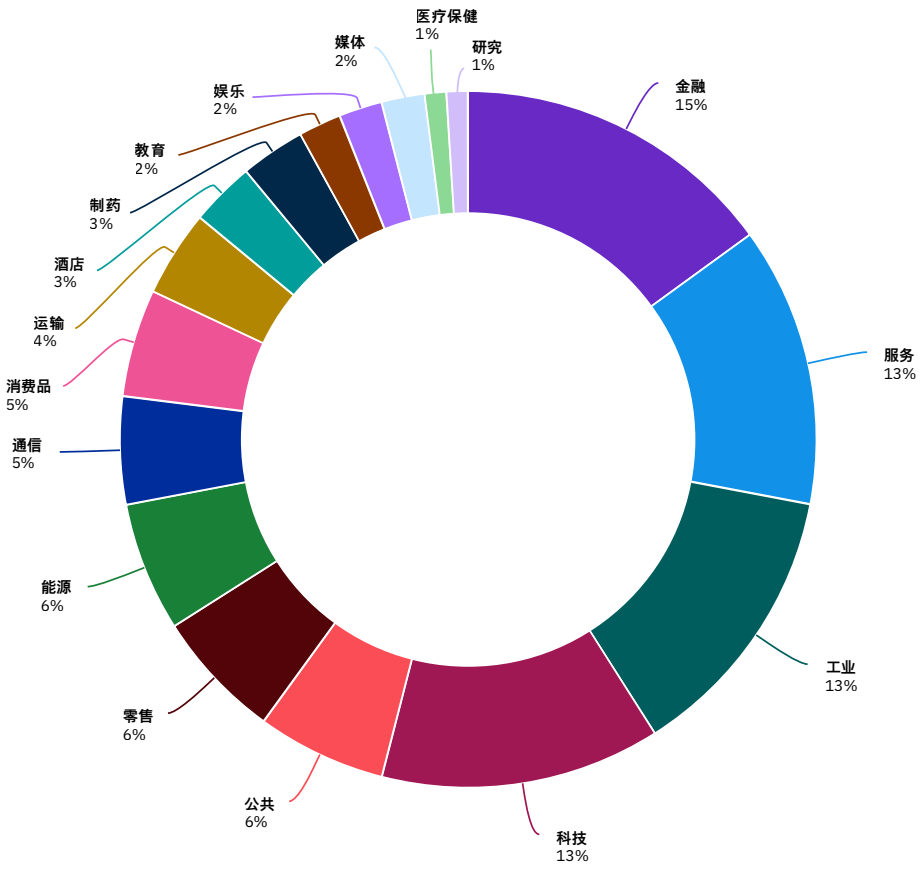


涵盖了大中小型组织。

图 48 显示了样本中 524 个按员工数量划分的组织的分布情况，员工数量代表着公司规模。该样本略偏重于中等规模的组织，有 58% 的组织员工人数在 1,001 至 25,000 人之间，有 25% 的组织员工人数少于 1,000 人，还有 17% 的组织超过 25,000 人。

图 49

各行业的样本分布情况



行业代表倾向于几个较大的行业。

图 49 显示了基准组织的分布情况（按行业划分）。今年的研究涉及十七个行业。最大的行业是金融、服务、工业和科技。我们单独解释了工业的定义。

行业的定义

医疗保健
医院，诊所

金融
银行、保险、投资公司

能源
石油和天然气公司，公用事业，替代能源制造商和供应商

制药业
制药，包括生物医学生命科学

工业
化学工艺、工程和制造公司

科技
软件和硬件公司

教育
公立和私立大学和学院，培训和发展公司

服务
专业服务，例如法律、会计和咨询公司

娱乐
电影制作、体育、游戏和娱乐场

运输
航空、铁路、卡车和运输公司

通信
报纸、图书出版商、公共关系和广告公司

消费品
消费品制造商和分销商

媒体
电视、卫星、社交媒体和互联网

酒店
酒店、联锁餐厅、游船公司

零售
实体店和电子商务

研究
市场研究、智囊团、研发

公共
联邦、州和地方政府机构以及非政府组织

研究限制

我们的研究利用了专有的机密基准方法，在之前的研究中都得到了成功部署。但是这种基准研究也存在固有的限制，在从研究结果中得出结论之前必须认真考虑这些限制。

非统计结果
我们的研究对象是全球实体的代表性非统计样本。考虑到我们的取样方法不够科学严谨，因此统计推论、误差幅度和置信区间不能用于这些数据。

非响应
无反应偏差未经测试，因此未参与研究的公司可能在潜在数据泄露成本方面有本质上的不同。

抽样框架偏差
我们的抽样框架带有评判性，因此，框架在多大程度上代表了被研究公司的群体，会影响到结果的质量。我们认为当前的抽样框架偏向于制定了更成熟的隐私或信息安全计划的公司。

公司特定的信息
基准不会捕捉可识别公司身份的信息。个人也可利用它使用类别响应变量披露关于公司和行业类别的地理信息。

未测量的因素
我们在分析中省略了一些变量，例如主要的趋势和组织特征等。省略的变量可以在多大程度上说明基准结果，这一点我们无法确定。

外推成本结果
尽管可以将某些制衡原则纳入基准流程，但受访者仍有可能不提供准确或真实的回答。此外，使用成本外推方法而不是实际的成本数据也可能造成误差和不准确性。

外推成本结果
今年美元表现强势，极大地影响了全球成本分析。从本币换算成美元降低了每项记录的成本和平均总成本预估。为了与前些年保持一致，我们决定继续使用相同的会计方法而不是调整成本。

Ponemon Institute 和 IBM Security 简介

*数据泄露成本报告*由 Ponemon Institute 和 IBM Security 联合发布。本次研究由 Ponemon Institute 单独开展，IBM Security 对结果提供了赞助、分析并予以报告和发布。

Ponemon Institute 致力于开展独立研究和培训，在企业和政府内部推广负责任的信息和隐私管理实践。对影响个人和组织敏感信息管理和安全的重要问题开展高质量的实证研究，是我们肩负的使命。

Ponemon Institute 遵从严苛的数据机密性、隐私和道德研究标准，不会从个人那里收集个人身份信息（也不会在我们的业务研究中收集可识别公司身份的信息）。此外，Ponemon Institute 还遵从严格的质量标准，确保受试者不会被问及不相关或不恰当的问题。

IBM **Security**

IBM Security 是最先进的集成式企业安全产品与服务组合之一。得益于享誉世界的 IBM® X-Force® 研发团队的支持，该产品组合提供安全解决方案，帮助组织将安全融入其业务流程，在充满不确定的环境中也能蓬勃发展。

IBM 是全球最广泛、最深入的安全研发和交付组织之一。IBM 每月监控 130 多个国家/地区的两万多亿起事件，并拥有 3,000 多项安全专利。如需了解更多信息，请访问：ibm.com/security.

如果您对本研究报告有任何问题或意见（包括引用或重用此报告的权限），请通过信函、电话或电子邮件与我们联系：

Ponemon Institute LLC

收件人：研究部门2308
US 31 NorthTraverse City,
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

采取后续行动

网络安全服务

借助咨询、云和托管安全服务降低风险

[了解更多 →]

身份和访问管理

将每位用户、API 和设备安全地连接至每款应用程序

[了解更多 →]

数据安全性

发现、分类并保护敏感的企业数据

[了解更多 →]

安全信息和事件管理

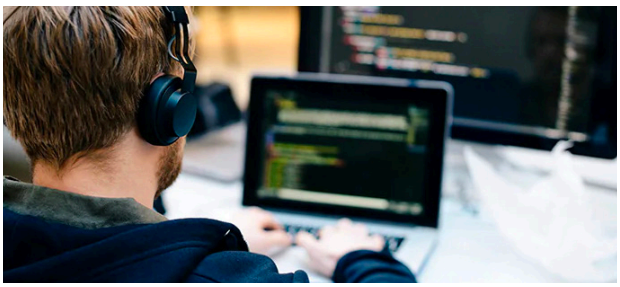
获得可见性，及时检测、调查并响应威胁

[了解更多 →]

安全编排、自动化和响应

借助编排和自动化加快事件响应

[了解更多 →]



云安全

将安全性整合到您的混合多云之旅

[了解更多 →]

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印制
2020 年 7 月

IBM Security