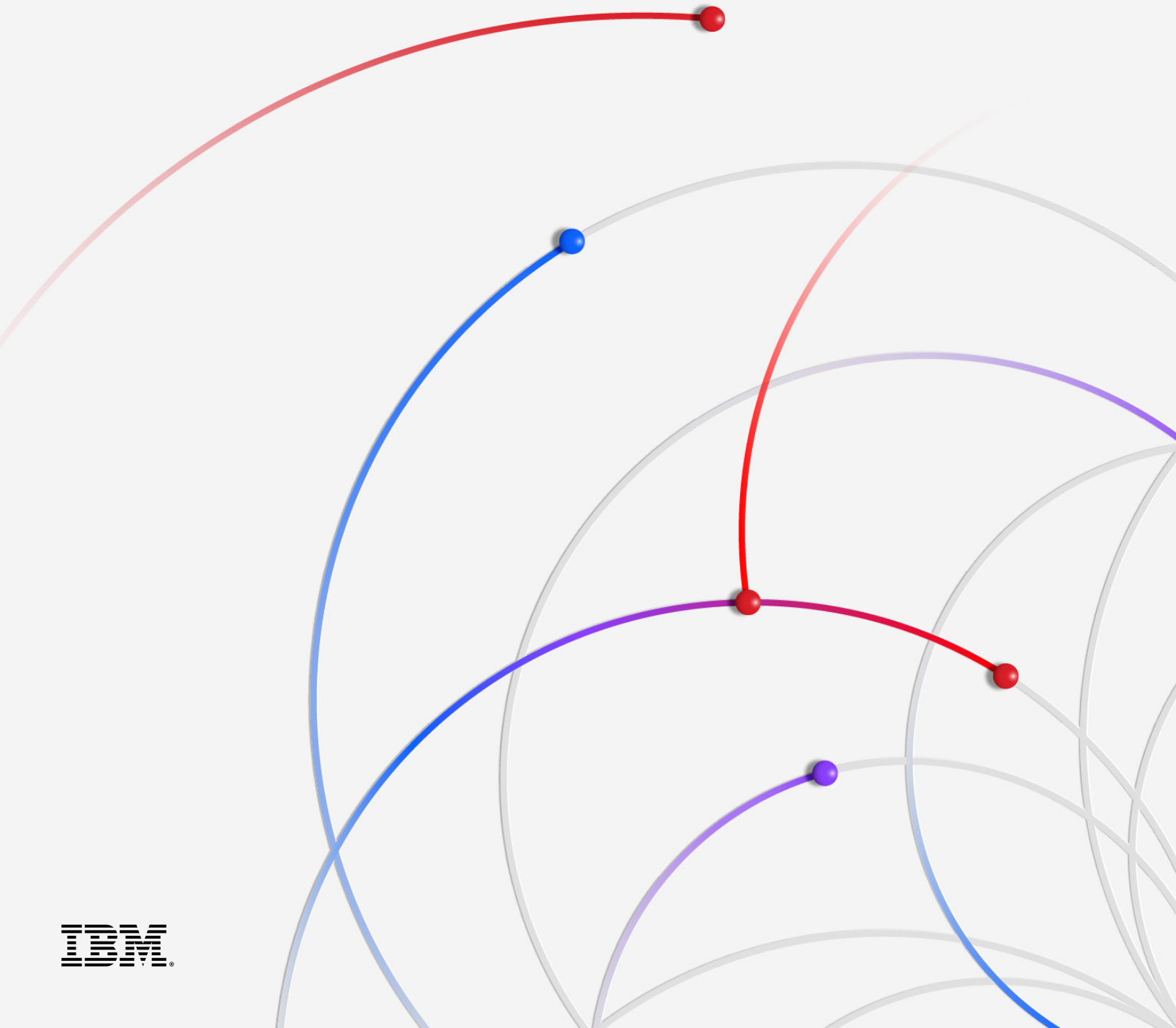
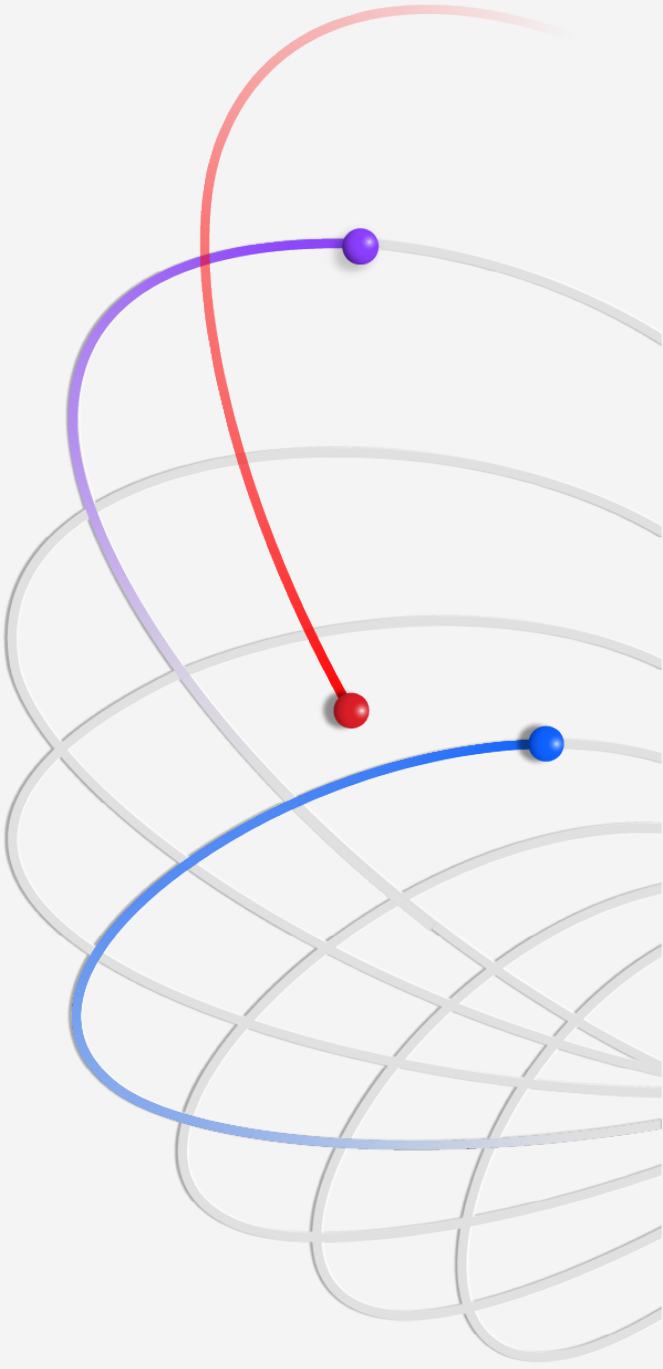
数据泄露成本报告
2024



IBM

目录

执行摘要



IBM 的年度《数据泄露成本报告》可为 IT、风险管理与安全领导者提供及时、可量化的证据，以便指导他们制定战略决策。此外，报告也有助于读者更好地管理风险状况和安全措施投资。本年度的报告为该系列的第 19 份报告，其中反映了技术变革带来的各种变化，例如影子数据（即驻留在未管理的数据源中的数据）的兴起，以及数据泄露所造成业务中断的范围和成本。

该报告的相关研究由波耐蒙研究所 (Ponemon Institute) 独立进行并由 IBM 发起、分析和发布，其中调研了 2023 年 3 月至 2024 年 2 月期间受数据泄露影响的 604 家组织。研究人员调查了 16 个国家或地区的 17 个行业的各大组织，而泄露的记录数量则从 2,100 条到 113,000 条不等。为了洞察分析实际状况，波耐蒙研究所的研究人员访谈了 3,556 名安全负责人与高管层领导，他们对其组织中发生的数据泄露事件均有第一手了解。

此项研究的成果为一份基准报告，可供业务领导者与安全负责人参考，有助于加强其安全防御并推动创新，尤其是如何在安全领域采用 AI，以及针对生成式 AI 举措如何实施安全保障。

在本年度的报告中，我们将主要介绍两大发展趋势。首先，一场数据泄露的全球平均成本较去年增长了 10%，达到 488 万美元，为新冠疫情以来的最大增幅。业务中断以及泄露后的客户支持与修复，是导致此成本飙升的主要因素。当被问及如何应对这些成本时，半数以上的组织表示会转嫁给客户。由于通胀导致的定价压力，市场竞争本已十分激烈，再让客户吸纳这些成本，很可能会引发问题。

其次，研究人员还发现，对于攻防双方的防御一方而言，将 AI 和自动化运用于安全领域，已经产生回报，且在一些实例中将泄露成本平均降低了 220 万美元。借助 AI 与自动化解决方案，可以缩短从识别到遏制泄露事件及其损害的整个过程所需时间。换言之，缺乏 AI 与自动化加持的防御方，可能需要更长时间来检测和遏制泄露事件，成本也会随之上升，且会高于已使用相关解决方案的组织。

正如我们在整个行业中所观察到的，网络安全团队普遍人手不足。本年度的研究发现，半数以上发生泄露的组织面临严重的安全专员短缺，且这一技能缺口相较去年的百分比增幅达到了两位数。随着威胁态势的蔓延，安全专业人员的短缺问题也变得日益严重。当组织中几乎所有职能领域不断竞相采用生成式 AI，可以预见随之而来的将是前所未有的风险，网络安全团队势必将要承受更大压力。

本报告将呈现源于此项研究的洞察和建议，旨在帮助读者降低数据泄露可能引发的财务和声誉损失。

2024 年报告新增内容

每年，我们都会不断改进《数据泄露成本报告》，以反映新的技术、新兴策略和近期事件。今年的研究首次探讨了：

- 组织是否长期受运营中断的困扰，例如无法处理销售订单、生产设施完全关停、客户服务无法有效开展
- 泄露事件是否涉及存储在未管理的数据源中的数据（也称为“影子数据”）
- 组织在安全措施运作的四个领域（预防、检测、调查和响应）中，使用了多少 AI 和自动化技术
- 敲诈攻击的性质如何，例如是否为敲诈加勒索软件攻击，还是仅为敲诈加数据渗漏
- 将数据、系统或服务恢复到泄露前状态所需的时间
- 有义务报告泄露事件的组织，实际用了多长时间来报告此类事件
- 遭受勒索软件攻击后，请执法部门介入的组织是否支付了赎金

重要结论

本报告所述的主要结论，均基于 IBM 对波耐蒙研究所汇总的研究数据的分析。

488 万美元

泄露的平均总成本

一场数据泄露的平均成本从 2023 年的 445 万美元上升至 488 万美元，增幅达 10%，创下自新冠疫情以来的最高。造成此成本上升的原因包括：业务损失（其中包括运营停机和客户流失）和泄露后响应成本（例如，配备客户服务帮助台人员和支付更高的监管罚款）。这些成本合计高达 280 万美元，创下过去 6 年以来业务损失与泄露后活动合计金额的新高。

220 万美元

预防环节广泛运用 AI，实现成本节省

三分之二的被调查组织表示，正在其安全运营中心全面部署安全 AI 和自动化技术，这一比例比去年提升了 10%。在攻击面管理 (ASM)、红队测试和态势管理等预防工作流中广泛部署 AI 的组织，泄露成本比未能运用 AI 的组织平均减少了 220 万美元。这是 2024 年报告中揭示的最大一项成本节省。

26.2%

网络技能缺口扩大

半数以上发生泄露的组织均面临严重的网络安全专员短缺问题。这一缺口比去年扩大了 26.2%，相当于泄露成本平均增加了 176 万美元。虽然有五分之一的组织表示已使用某种形式的生成式 AI 安全工具（有望提高产出和效率从而缩小缺口），但此技能缺口仍是一项不小的挑战。

1/3

涉及影子数据的泄露事件占比

35% 的泄露事件涉及影子数据，这表明数据的激增使跟踪和保护数据变得更加困难。影子数据被窃取，相应地导致了泄露成本增加 16%。研究人员发现，跨多种环境存储数据是一种常见的策略，并占到泄露事件的 40%。这些泄露事件也需要更长的时间来识别和遏制。相比之下，仅存储在一种环境中的数据发生泄露的频率较低，且无论该环境是公有云 (25%)、本地部署 (20%) 还是私有云 (15%)。

46%

涉及客户个人数据的泄露事件的占比

接近半数的泄露事件涉及客户个人身份信息 (PII)，其中包括税务识别 (ID) 号、电子邮件地址、电话号码和家庭住址。知识产权 (IP) 记录则紧随其后（43% 的泄露事件涉及）。与去年相比，知识产权记录的成本大幅增加，从去年报告中的每条记录 156 美元上升到今年的 173 美元。

292

识别和遏制涉及凭据被盗泄露事件的所用天数

在所有攻击媒介中，凭据被盗或泄露事件的识别和遏制用时最长（292 天）。利用员工和员工访问权限的类似攻击，也需要很长时间才能解决。例如，网络钓鱼攻击的平均持续天数为 261 天，社交工程攻击的平均持续天数则为 257 天。

499 万美元

恶意内部人员攻击的平均成本

较之其他攻击媒介，恶意内部人员攻击造成的损失最高，平均达 499 万美元。其他代价高昂的攻击媒介则包括：商业电子邮件诈骗、网络钓鱼、社交工程，以及凭据被盗或泄露。生成式 AI 在制造某些网络钓鱼攻击中可能起到了一定作用。例如，不会英语的人利用生成式 AI，能比以往更轻松地炮制出语法正确、令人信服的网络钓鱼消息。

100 万美元

遭受勒索软件攻击时，请执法部门介入可节省成本

涉及执法部门的勒索软件受害者最终将泄露成本平均降低了近 100 万美元，而这还不包括所支付赎金的成本。此外，借助执法部门的介入，识别和遏制泄露事件所用时间也从 297 天缩短到了 281 天。

830,000 美元

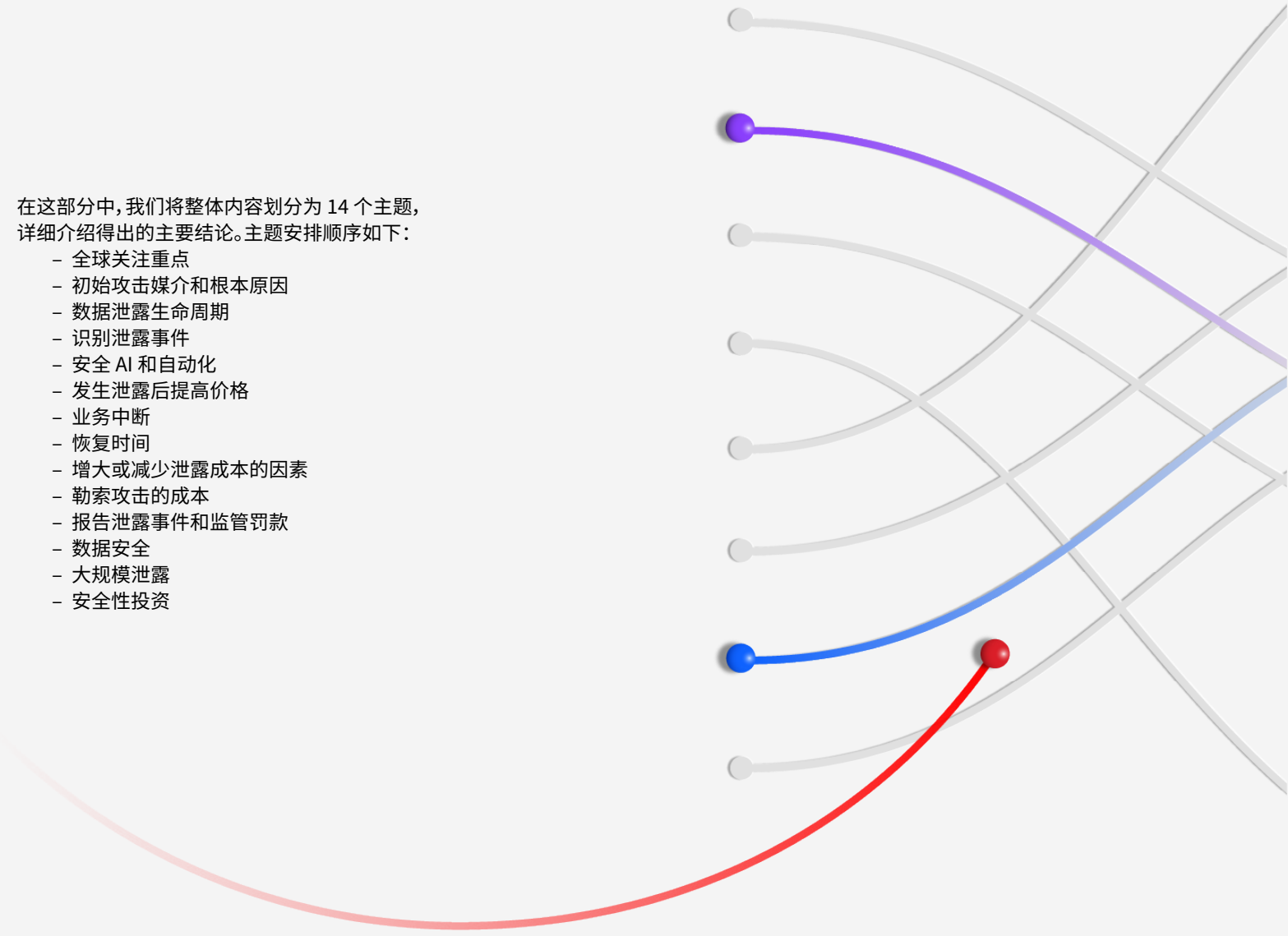
所有行业中最高的平均成本涨幅

在所有行业中，工业部门的成本涨幅最高。与去年相比，每次泄露事件的成本平均增加了 83 万美元。这一成本飙升的情况，或许表明工业组织需要准备好加快响应速度，因为这一行业对运营停机极为敏感。尽管如此，工业组织识别数据泄露所用时间为 199 天，遏制用时则为 73 天，仍高于所有行业的平均水平。

完整的结论

在这部分中，我们将整体内容划分为 14 个主题，详细介绍得出的主要结论。主题安排顺序如下：

- 全球关注重点
- 初始攻击媒介和根本原因
- 数据泄露生命周期
- 识别泄露事件
- 安全 AI 和自动化
- 发生泄露后提高价格
- 业务中断
- 恢复时间
- 增大或减少泄露成本的因素
- 勒索攻击的成本
- 报告泄露事件和监管罚款
- 数据安全
- 大规模泄露
- 安全性投资



488 万美元

数据泄露的全球平均成本激增

全球关注重点

放眼全球，虽然技能短缺问题仍为一项顽疾，但安全团队在检测和遏制泄露事件方面却做得很好。遭遇泄露的组织有半数以上正面临安全人员短缺问题，而安全领导者则正在利用 AI 与自动化解决方案来弥补技能差距。尽管他们颇为努力，但泄露成本仍在上升，而这主要因为在业务中断和发生泄露事件后，组织采取各种应对措施而产生的各种费用。在下一节中，我们将跨越行业、国家和地区来研究这些问题和其他问题，从而让安全领导者了解外部风险，以便您从中吸取教训。

全球数据泄露平均成本飙升

全球数据泄露的全球平均成本较去年增长了 10%，达到 488 万美元，为新冠疫情以来的最大增幅。业务中断以及泄露后的响应措施，是导致此年度成本上升的主要因素。请参阅图 1。

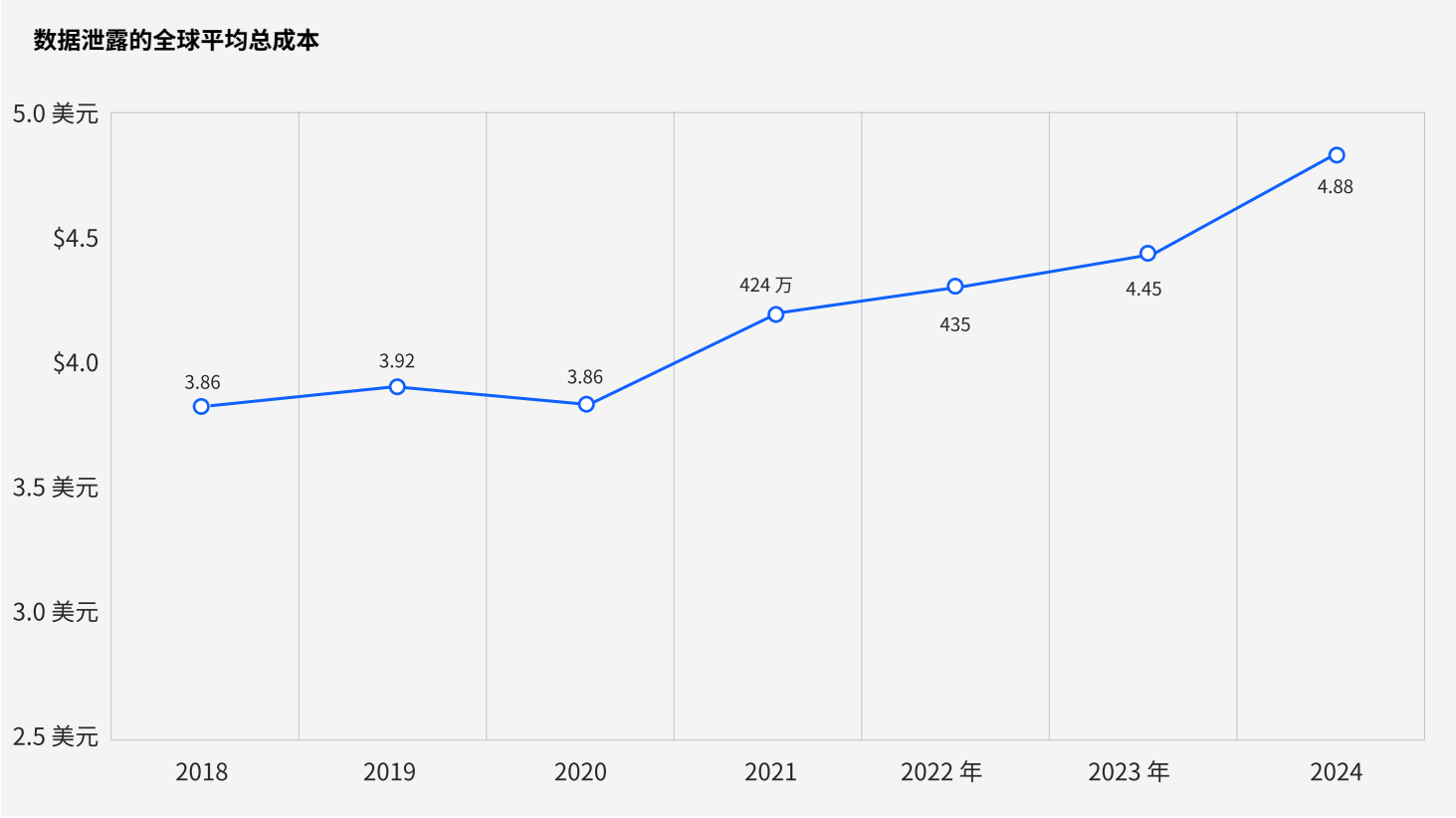


图 1：以百万美元为单位

美国的平均泄露成本位居世界首位
在所研究的 16 个国家或地区中，美国第 14 年平均数据泄露成本最高，达到 936 万美元。前五名则依次为中东、德国、意大利和比荷卢。比荷卢是指比利时、荷兰和卢森堡所组成的经济联盟，同时它也是今年新上榜的成员。值得注意的是，加拿大和日本的平均成本有所下降，而意大利和中东的平均成本则出现大幅上升。
请参阅图 2A 和 2B。

按国家或地区划分的数据泄露成本

#	国家或地区	2024	2023 年
1	美国	$9.36	$9.48
2	中东	$8.75	$8.07
3	比荷卢	$5.90	—
4	德国	$5.31	$4.67
5	意大利	$4.73	$3.86
6	加拿大	$4.66	$5.13
7	英国	$4.53	$4.21
8	日本	$4.19	$4.52
9	法国	$4.17	$4.08
10	拉丁美洲	$4.16	$3.69
11	韩国	$3.62	$3.48
12	东盟	$3.23	$3.05
13	澳大利亚	$2.78	$2.70
14	南非	$2.78	$2.79
15	印度	$2.35	$2.18
16	巴西	$1.36	$1.22

图 2A.以百万美元为单位

2024 年与 2023 年排名前 5 的国家和地区

#	成本变化	2024	2023 年
1	↓	**美国** $9.36	**美国** $9.48
2	↑	**中东** $8.75	**中东** $8.07
3	↑	**比荷卢** $5.90	**加拿大** $5.13
4	↑	**德国** $5.31	**德国** $4.67
5	↑	**意大利** $4.73	**日本** $4.52

图 2B.以百万美元为单位

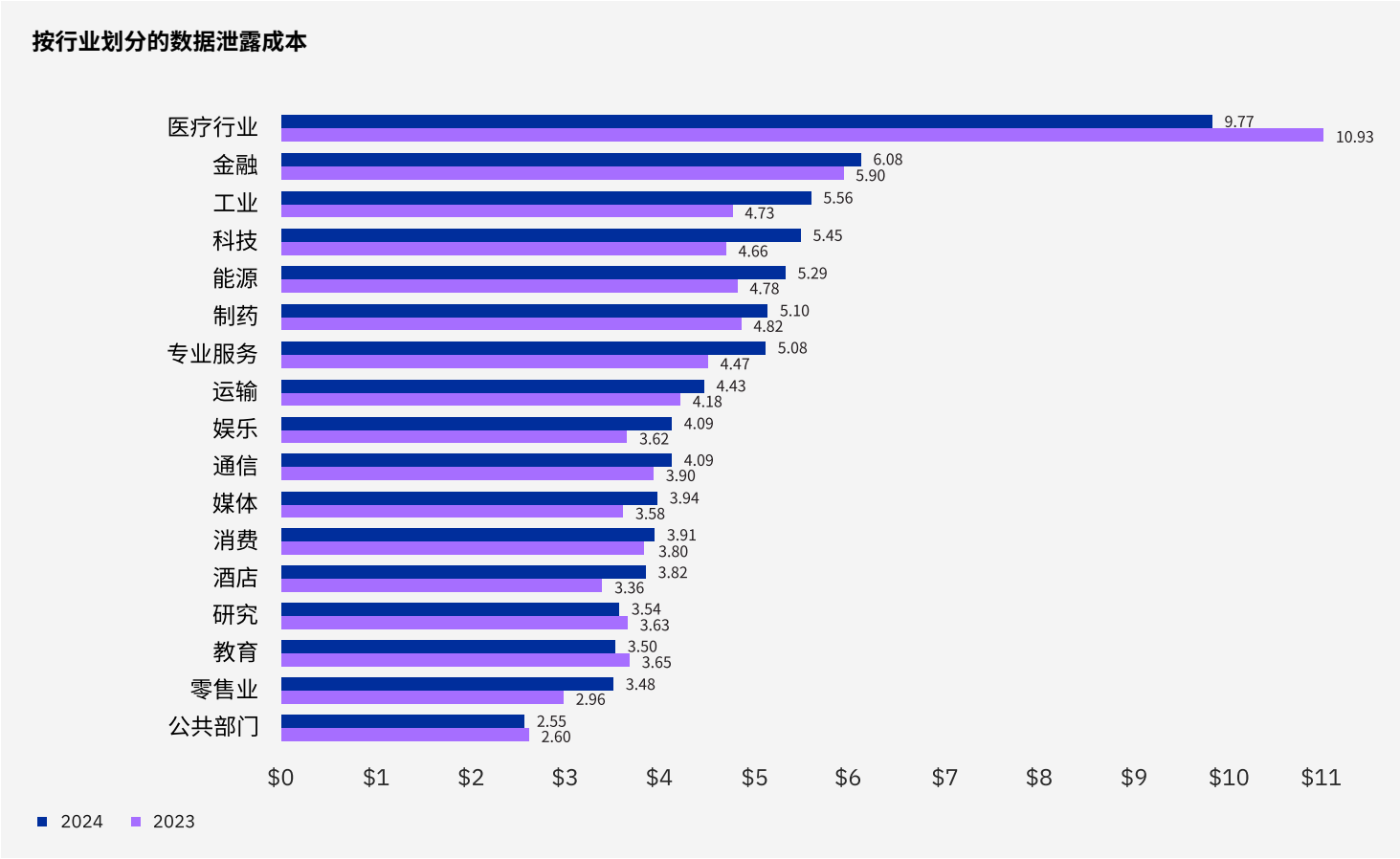


图 3：以百万美元为单位

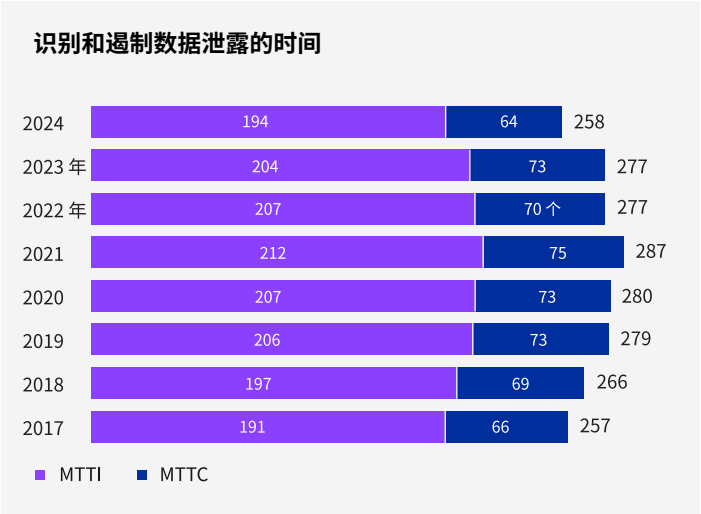


图 4. 以天为单位

医疗保健行业的平均泄露成本再次超越行业平均成本

医疗保健行业的平均泄露成本下降了 10.6%，降至 977 万美元。但这一因素尚不足以让其摆脱泄露成本最高行业的名声；因为自 2011 年以来，该行业便一直位居此列榜单。医疗保健行业仍是攻击者的一大攻击目标，因为该行业经常受到现有技术的影响，且极易发生中断问题，从而可能会危及患者的安危。请参阅图 3。

识别和遏制泄露事件的平均时间缩短

较之去年的 277 天，防御者识别和遏制泄露事件所用的平均时间降至 258 天，为 7 年来新低。注：平均识别时间 (MTTI) 和平均遏制时间 (MTTC) 的全球平均值不含比荷卢；这是因为，作为参与此研究的新地区，其影响力大于平均水平，且结果偏差较大。请参阅图 4。

业务损失成本和泄露后响应成本飙升

业务损失和泄露后响应产生的两类成本比去年增加了近 11%，而这也是泄露总成本大幅上升的原因之一。业务损失成本包括因系统停机造成的收入损失，以及客户流失和声誉受损的成本。泄露后成本可能包括为受影响的客户设立客户服务中心和信用监控服务的相关费用，以及缴纳的监管罚款。请参阅图 5。

以四种损失类别划分的数据泄露平均成本

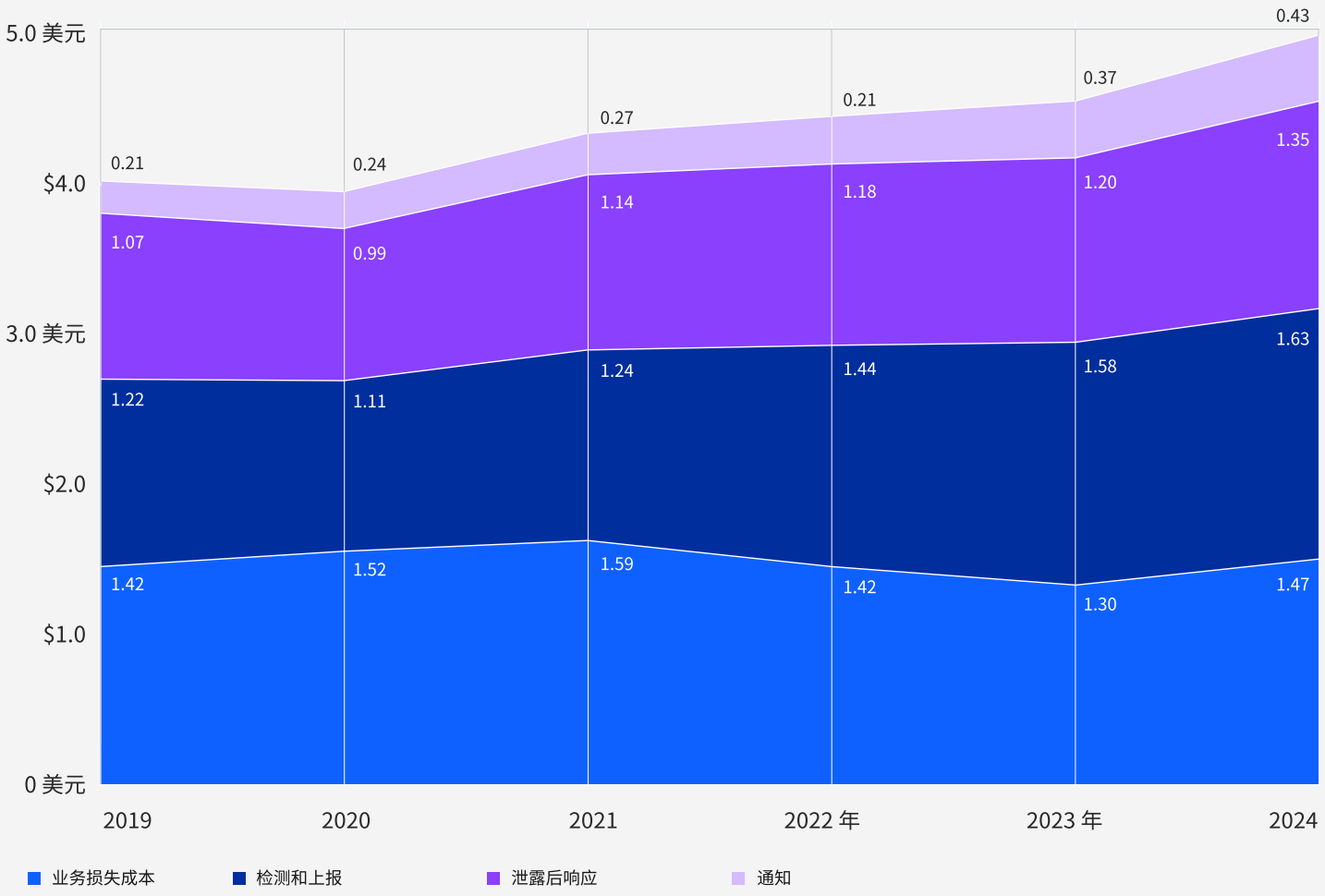


图 5. 以百万美元为单位

大多数泄露事件均涉及客户 PII
最常见的数据窃取或泄露类型为客户 PII，占到 46%。PII 可能包括税号、电子邮件地址和家庭住址，并可用于身份窃取和信用卡欺诈。所有被盗记录类型的全球平均成本飙升至高达 169 美元，其中员工 PII 的成本最高。请参阅图 6A 和 6B。

按百分比划分的遭泄露数据类型

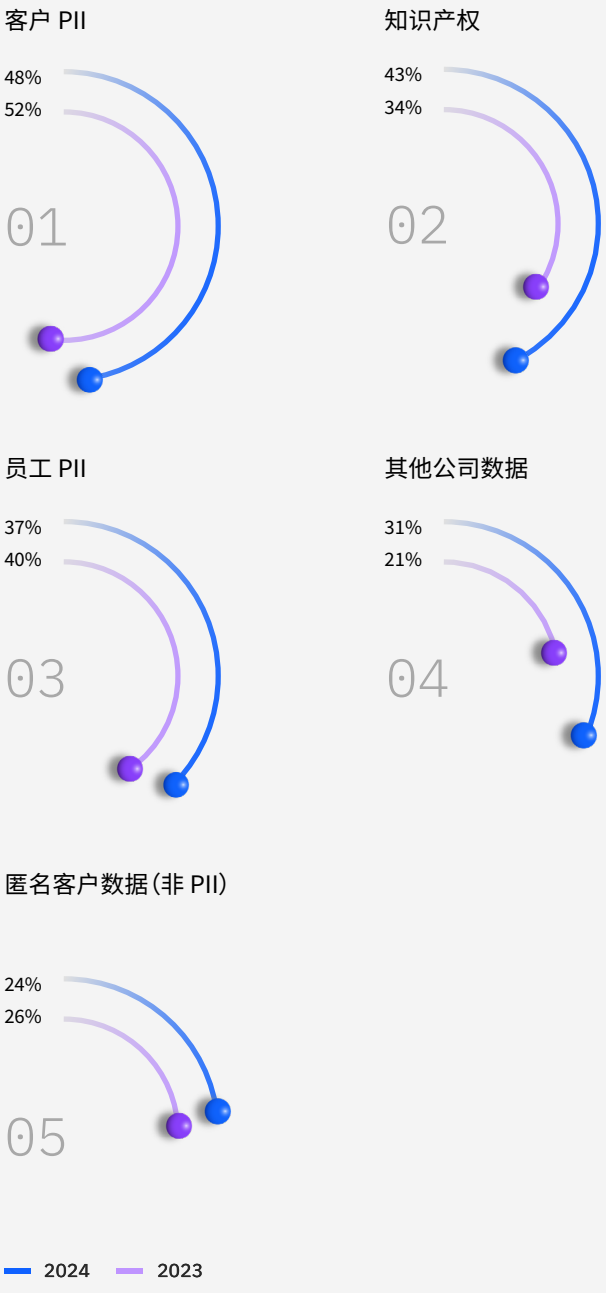


图 6A.允许多个响应

按泄露记录类型划分的数据泄露对应的每条记录成本

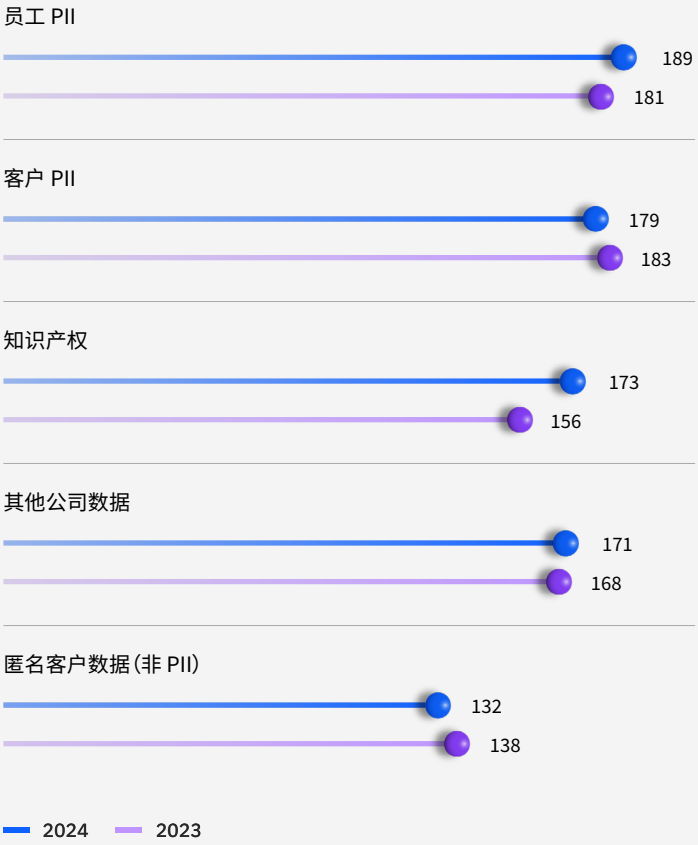


图 6B.以百万美元为单位

481 万美元

攻击者使用遭入侵的凭据所造成泄露事件的平均成本，而此类泄露事件在所研究的泄露案例中占 16%。

初始攻击媒介和根本原因

网络钓鱼和凭据失窃或泄露连续第二年成为最常见的两种攻击媒介。而这两类事件也是成本最高的前四类事件。除确定泄露事件的最常见根本原因之外，该研究还比较了每个类别的平均成本，以及识别和遏制这些泄露事件的平均时间。

凭据泄露位居初始攻击媒介之首

在 16% 的泄露事件中，攻击者均因使用了泄露的凭据而得逞受益。此外，凭据泄露攻击也会给组织带来高昂的成本，其中每次泄露平均会造成 481 万美元的损失。网络钓鱼则紧随其后，占到攻击媒介的 15%，但它最终造成的损失则更高，达到 488 万美元。恶意内部人员攻击造成的损失则最大，达到 499 万美元，但此类攻击仅占所有泄露途径的 7%。请参阅图 7。

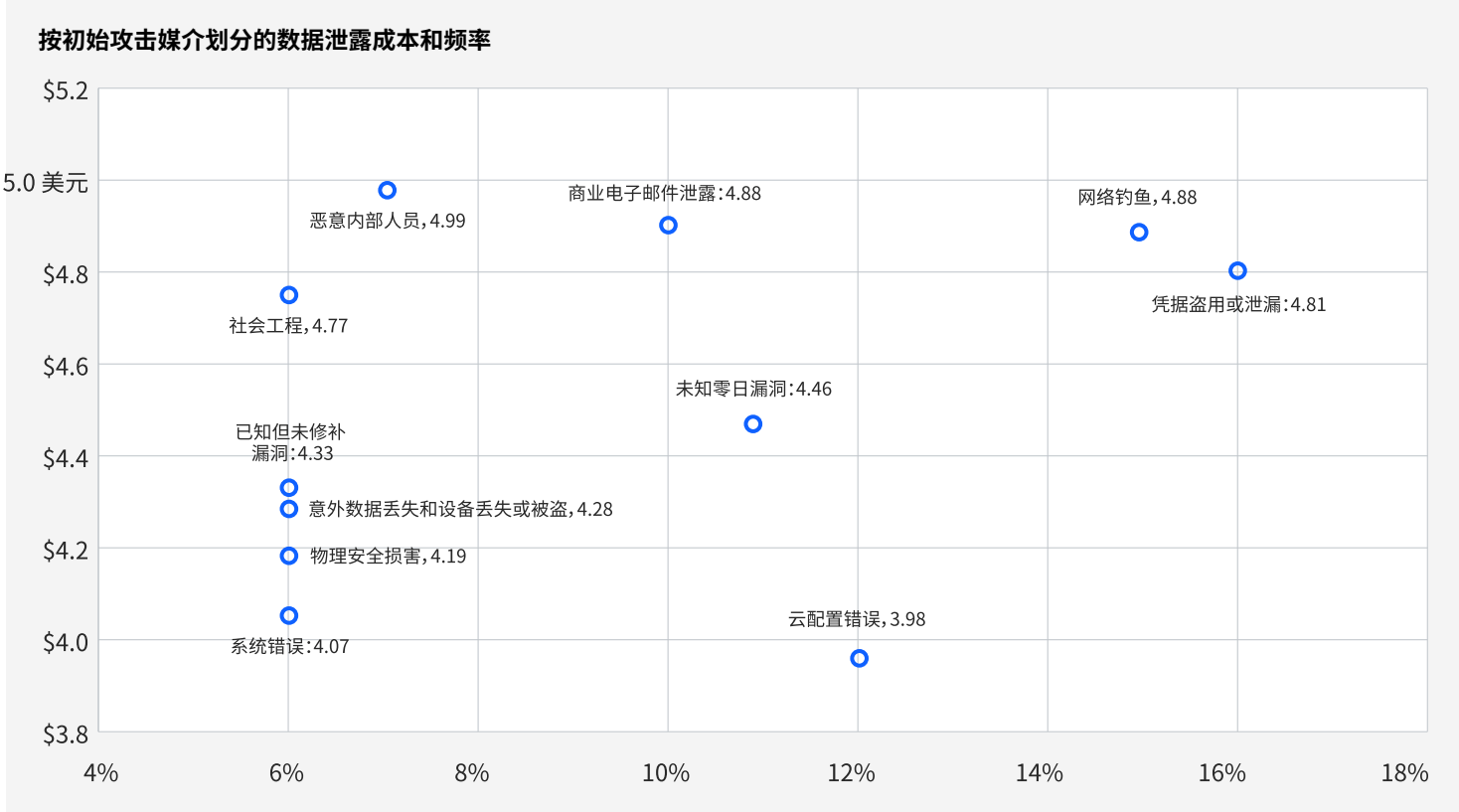


图 7. 以百万美元为单位；在所有泄露事件中的占比

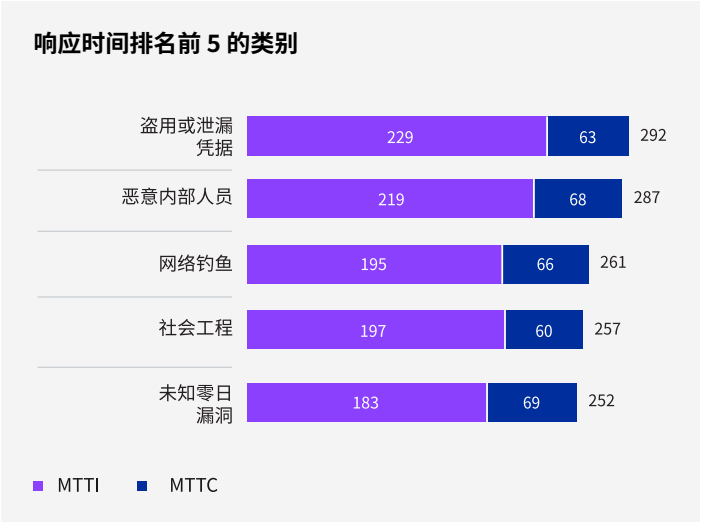


图 8. 以天为单位

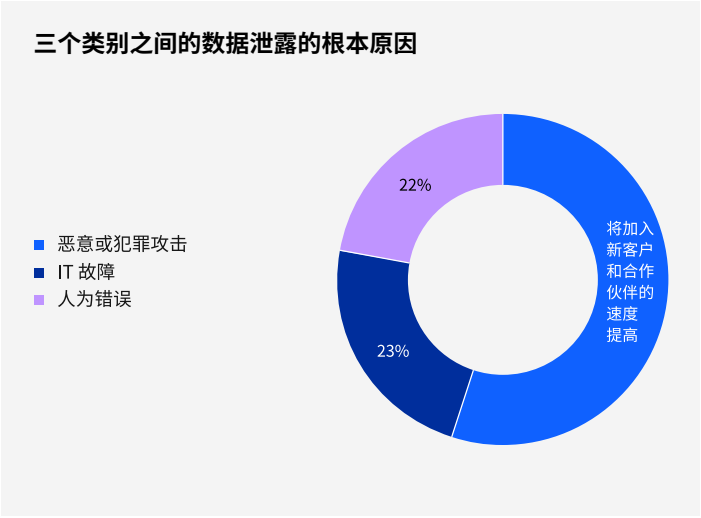


图 9.

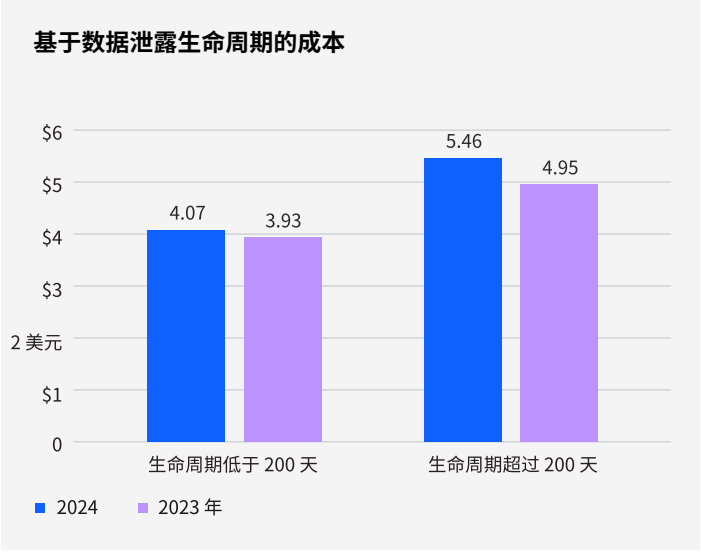


图 10：以百万美元为单位

基于凭据的攻击需要更长时间来来识别和遏制
无论是恶意内部人员窃取凭据还是使用凭据，攻击识别和遏制时间均呈上升趋势，其平均总时间分别达到 292 天和 287 天。由于防御者需对网络上的合法用户活动和恶意用户活动加以区分，因而更难识别相关威胁。另一方面，对利用零日漏洞的攻击加以遏制则最为耗时。请参阅图 8。

近半数的泄露事件源自各种 IT 故障或人为失误
恶意攻击（由外部攻击者或恶意内部人员发起的攻击）占到所有泄露事件的 55%。虽然这些泄露事件令人担忧，但更为重要的是要记住：其余 23% 的事件均源于 IT 故障，另有 22% 则源于人为失误。请参阅图 9。

数据泄露生命周期

根据我们 2024 与 2023 年的研究，在数据泄露中，时间就是金钱；而泄露事件的生命周期越长，其成本便越高。完整的泄露生命周期是指识别和遏制泄露事件的平均天数的组合。在这两份报告中，我们比较了完整生命周期不超过 200 天的数据泄露的平均成本与完整生命周期超过 200 天的数据泄露的平均成本。

更长的泄露生命周期会导致更高的成本
在本年度的报告中，研究人员发现：较之生命周期不超过 200 天的数据泄露，生命周期超过 200 天的数据泄露的平均成本最高，达到 546 万美元。这些研究结果与去年的结果一致。而值得注意的是，虽然今年较长数据泄露生命周期的对应成本比去年增加了 10.3%，但较短生命周期的对应成本也有所上升，但增幅较小 (3.6%)。请参阅图 10。

识别泄露事件

为了遏制数据泄露，首先需对其进行识别。谁负责对其进行识别以及识别速度有多快，会对最终的数据泄露成本产生影响。本年度，我们发现安全团队使用自己的工具提高了此方面的表现。在其他情况下，泄露事件则是由安全研究人员、执法机关和顾问等良性第三方或攻击者自己识别确认的。

安全团队识别出大多数泄露事件

较之良性第三方 (34%) 和攻击者自身 (24%)，安全团队及其工具检测到泄露事件的频率要高得多 (42%)。这一数字比 2023 年的报告有所提高，当时安全团队发现泄露事件的比例仅为三分之一。此变化表明安全团队能够加快检测速度。请参阅图 11。

如何识别数据泄露？

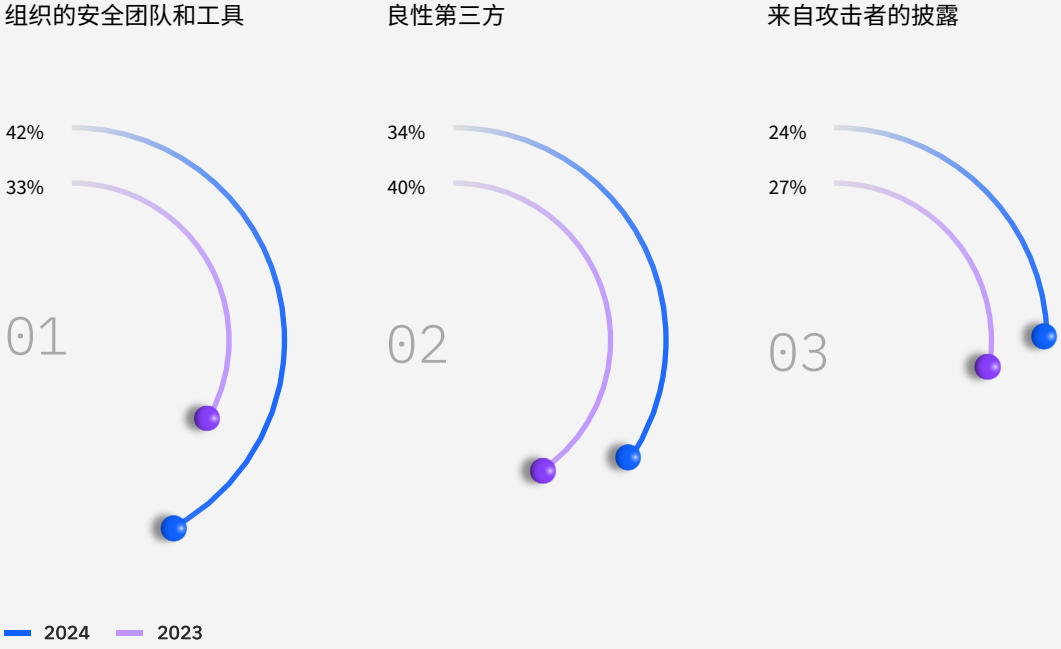


图 11.只允许单个响应

553 万美元

攻击者披露泄露事件时的平均泄露成本。

攻击者所披露泄露事件造成的损失更大

当攻击者披露某一泄露事件时，他们很可能已达到自身目的并已造成重大损失，从而会提高此泄露事件的总体成本。当攻击者披露某一泄露事件时，其平均成本为 553 万美元。另一方面，当安全团队发现某一泄露事件时，其平均成本为 455 万美元。请参阅图 12。

更快地识别和遏制泄露

本报告发现，无论如何发现泄露事件，各大组织在 2024 年识别和遏制此类事件时的平均速度均比去年更快。正如本报告下一节所示，AI 和自动化的使用可能促进了这类加速应用的进程。请参阅图 13。

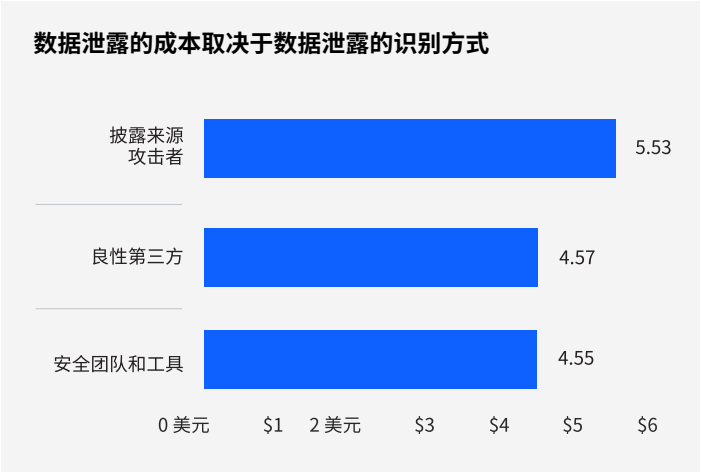


图 12：以百万美元为单位

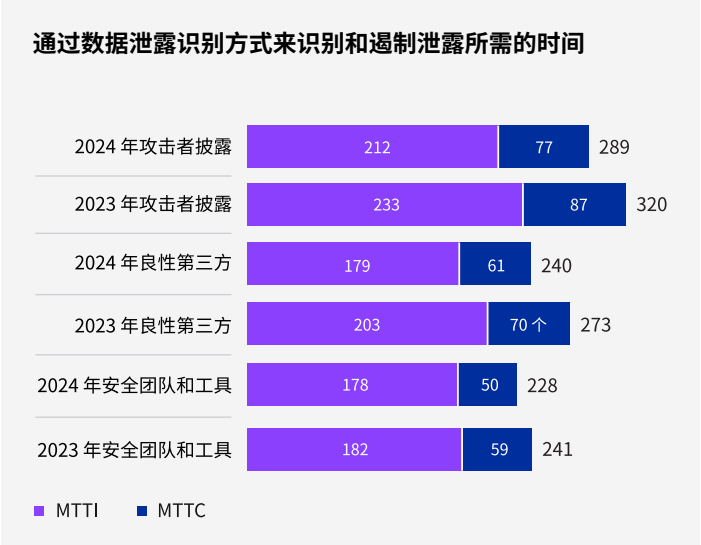


图 13：以天为单位

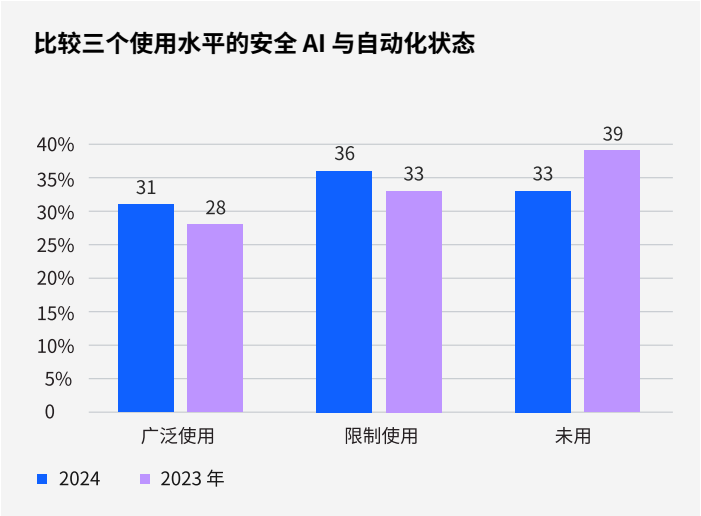


图 14：每个使用级别的组织所占比例

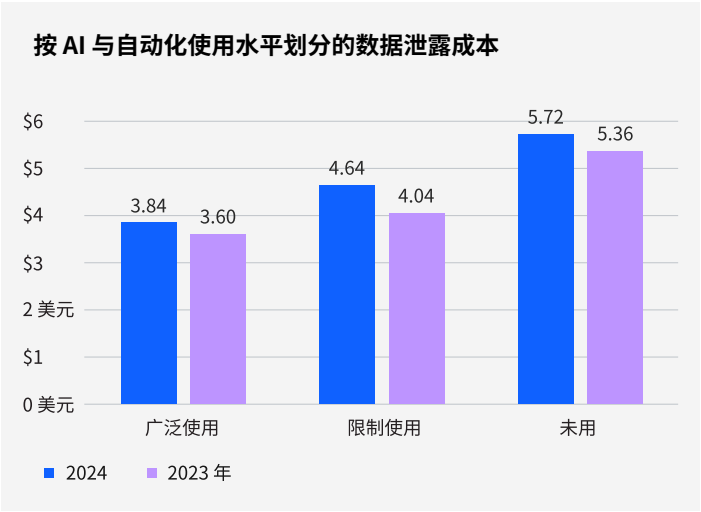


图 15：以百万美元为单位

安全 AI 和自动化

AI 和自动化正在改变网络安全世界。借助它们，恶意行为者可比以往更轻松地大举创建和发起攻击；但同时，它们还为防御者提供了新工具来快速识别威胁并自动响应。本年度的报告发现，这些技术可加快识别和遏制泄露事件并降低成本的相关工作。

AI 和自动化的使用率呈现增长

本年度的研究发现，广泛使用安全 AI 和自动化的组织数量已从去年的 28% 增长为 31%。虽然组织数量仅相差 3 个百分点，但使用率却上升了 10.7%。与此同时，有限使用 AI 和自动化的人数占比也从 33% 增长到 36%，增幅为 9.1%。请参阅图 14。

更多 AI 和自动化意味着泄露成本更低

组织使用的 AI 和自动化越多，其平均泄露成本就越低。此相关性非常突出，同时也是本年度报告的主要调查结果之一。未使用 AI 和自动化的组织的平均泄露成本为 572 万美元，而大量使用 AI 和自动化的组织的平均成本则为 384 万美元，节省了 188 万美元。请参阅图 15。

27%

在四个安全类别中使用 AI 和自动化的组织的占比。

更多 AI 等于更快地识别和遏制
广泛使用安全 AI 和自动化的组织在识别和遏制数据泄露时的速度比完全不使用这些技术的组织平均快了近 100 天。请参阅图 16。

安全团队已在各个职能部门均衡地部署 AI 和自动化技术
在表示已广泛使用 AI 和自动化的组织中，约有 27% 的组织在预防、检测、调查和响应等类别中广泛使用 AI。约有 40% 的组织已至少在一定程度上使用 AI 技术。请参阅图 17。

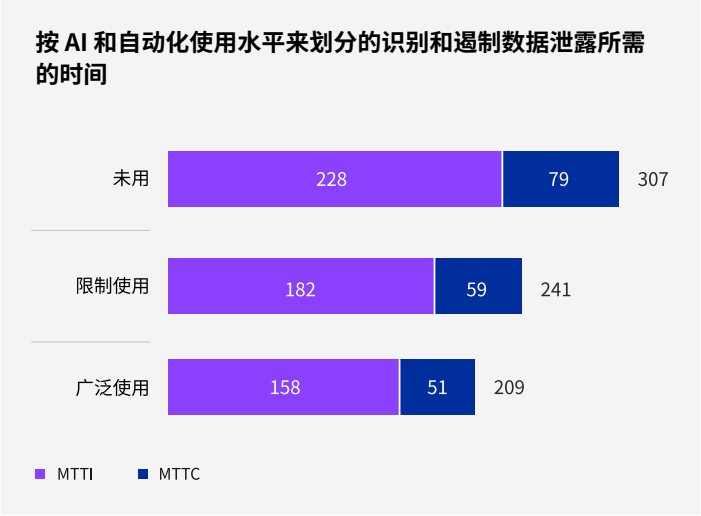


图 16：以天为单位

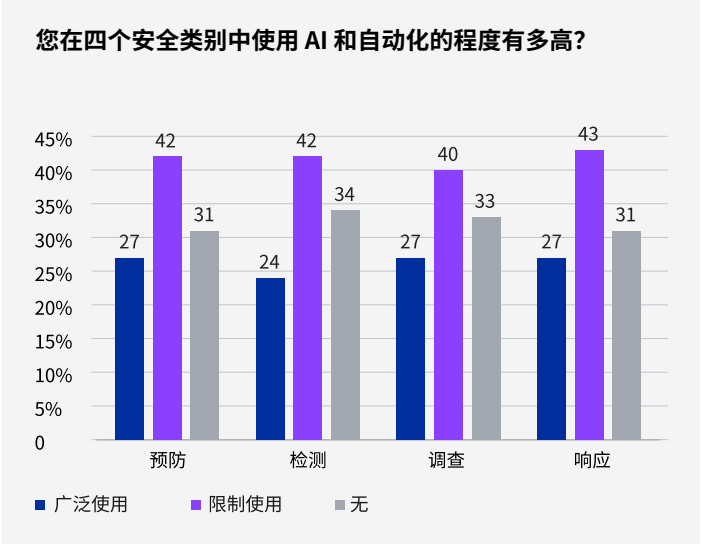


图 17.源自报告广泛使用 AI 和自动化的受访者；参考图 14

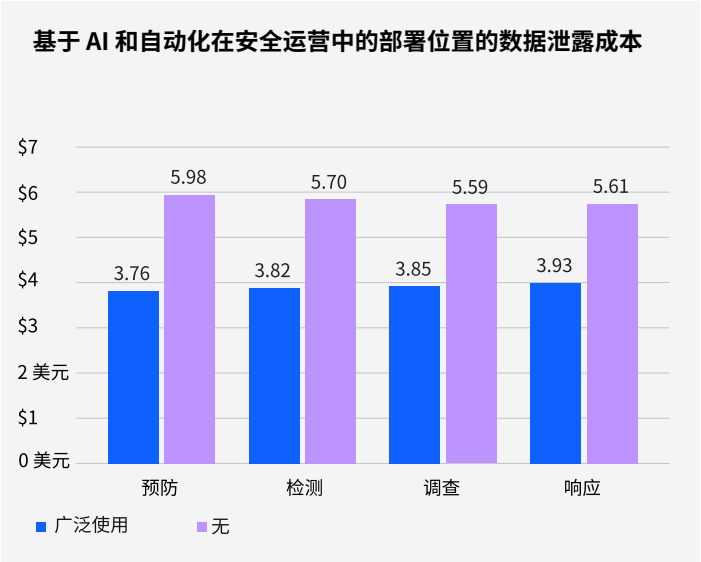


图 18.源自报告广泛使用 AI 和自动化的组织，以百万美元为单位；参考图 14

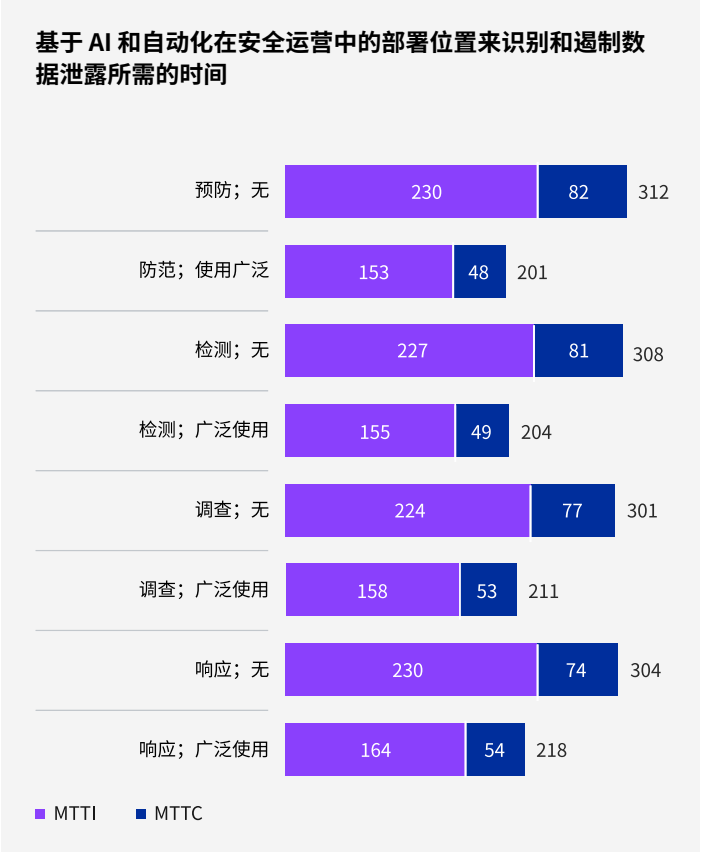


图 19.源自报告广泛使用 AI 和自动化的组织，以天为单位；参考图 14

广泛使用 AI 和自动化可降低成本

当 AI 和自动化在安全性的四个领域中得到广泛应用时，较之尚未在这些领域使用此类技术的组织，它可显著降低平均泄露成本。例如，当组织广泛使用 AI 和自动化进行预防时，其平均泄露成本为 376 万美元。与此同时，未使用这些工具进行预防的组织的成本则为 598 万美元，二者相差 45.6%。请参阅图 18。

AI 和自动化可加快识别和遏制泄露事件的时间

无论在何处应用 AI 和自动化，它们都会加快识别和遏制泄露事件的工作。在任意安全职能（预防、检测、调查或响应）领域广泛使用 AI 和自动化均可将数据泄露的平均 MTTI 和 MTTC 降低 33%（针对响应）和 43%（针对预防）。请参阅图 19。

70%

因泄露而遭受严重或非常严重的业务中断的组织的占比。

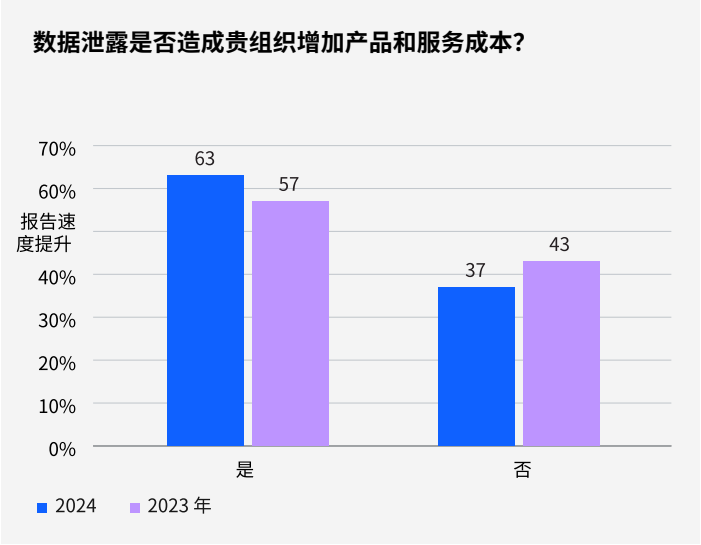


图 20:所有组织的占比

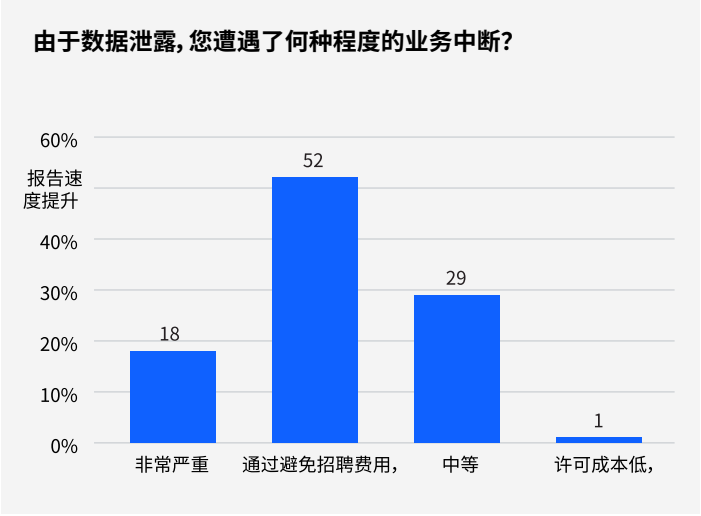


图 21.只允许单个响应

发生泄露后提高价格

就事件本身的性质而言,数据泄露的代价十分高昂。当组织发现自己背负着百万美元的成本时,它们可能会从其他方面来寻求弥补这些成本。其中一个选项是以涨价的形式将其转嫁给自己的客户,而这一趋势正变得日益显著。在已面临定价压力的市场中,提高价格可能会引发风险。

组织会将泄露成本转嫁给客户

大多数组织表示,它们计划在发生数据泄露后提高商品与服务的价格,从而将相关成本转嫁给客户。表示自身今年也有此计划的组织占比由去年的 57% 增至 63%,增幅达 10.5%。请参阅图 20。

业务中断

业务的开展离不开数据。数据一旦泄露,业务便会中断。此类破坏可能为仅影响少数系统的小规模泄露,也可能是波及整个组织的长期运营中断后果。我们的研究深入了解了这些中断事件的严重程度,以及中断的严重程度与数据泄露成本之间的关联深度。

业务中断的态势十分严重

本年度的研究发现,70% 的组织会因泄露事件而遭受严重或非常严重的业务中断。其中,仅有 1% 的组织将其中断程度描述为较低。请参阅图 21。

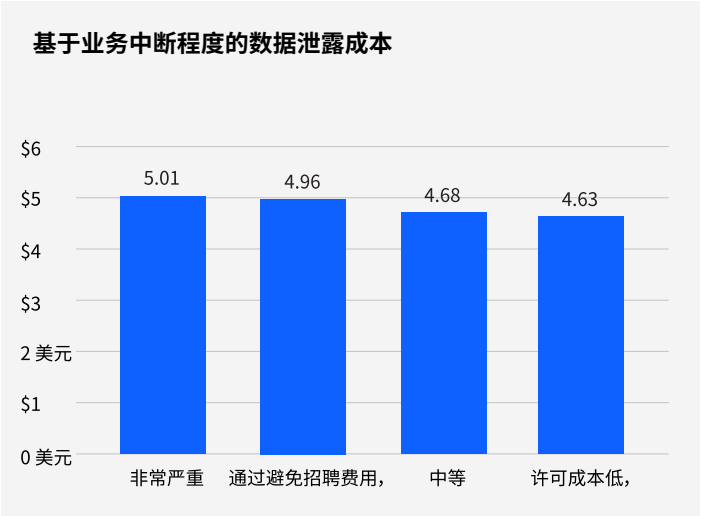


图 22：以百万美元为单位

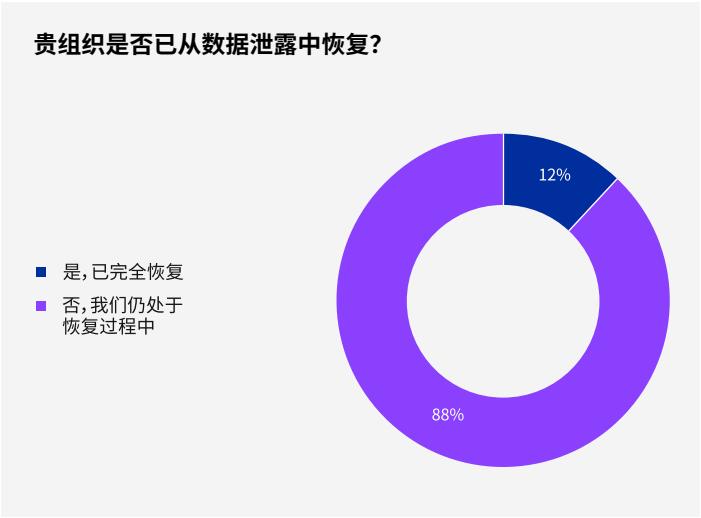


图 23.所有遭泄露组织的占比

泄露事件的平均成本会随中断的加剧而上升
业务中断的程度越深，平均泄露成本便越高。即使是报告其中断程度较低的组织，其平均数据泄露成本也高达 463 万美元。对于报告遭遇严重中断的组织，其平均成本则高出 7.9%，达到 501 万美元。请参阅图 22。

恢复时间

即使在遏制泄露事件后，恢复工作也仍在继续。在本研究中，恢复的含义为：

- 受泄露影响的地区的业务运营已恢复正常。
- 组织已履行合规义务，例如缴纳罚款。
- 客户的信心和员工的信任已得到恢复。
- 组织已采取或应用控制措施、技术和专业知识来避免未来的数据泄露。

此类工作的大部分内容（例如，重建客户信心）均涉及技术以外的多个因素。对于大多数组织，艰苦的恢复工作可能还需数月之久。

泄露恢复率较低
本年度的报告显示，受访组织中仅有 12% 表示其已从数据泄露中完全恢复。大多数组织表示其仍在努力解决这些问题。请参阅图 23。

完全恢复需用时超过 100 天

在已完全恢复的组织中，超过四分之三表示其为此花费的时间超过了 100 天。恢复是一个漫长的过程。在已完全恢复的组织中，约有三分之一表示它们花费了超过 150 天才得以恢复。仅有一小部分 (3%) 已完全恢复的组织得以在 50 天内实现此目标。请参阅图 24。

从数据泄露中恢复的平均时间

图 24.源自报告称已从事故中完全恢复的组织，以天为单位（参考图 23）

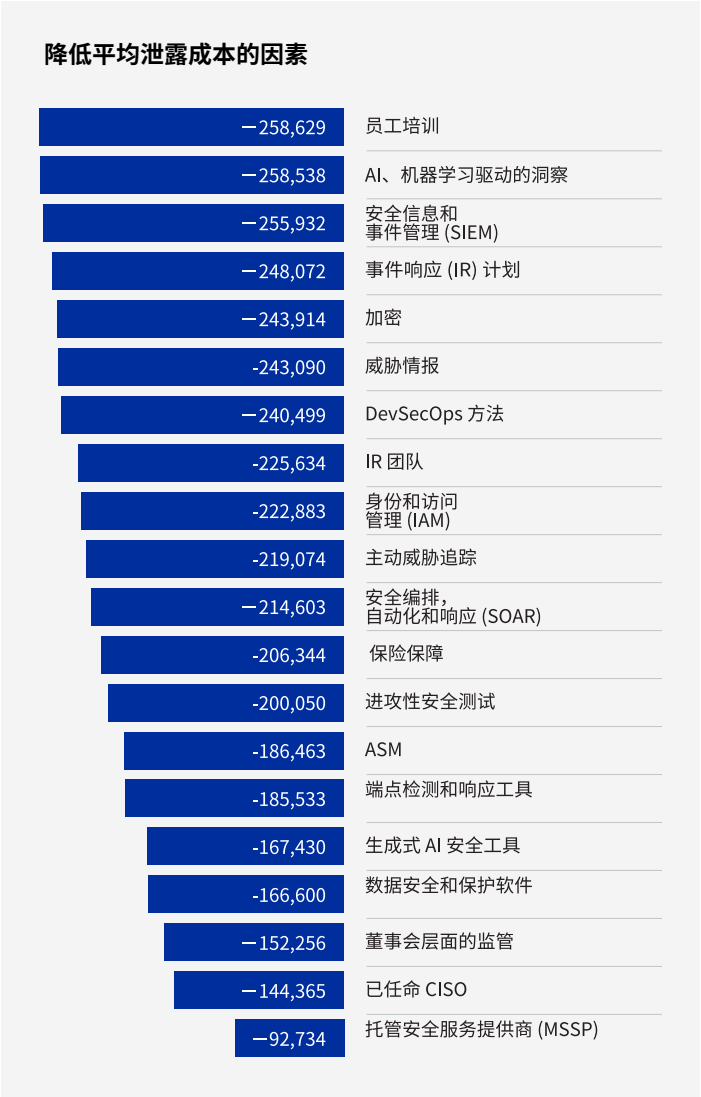


图 25.与 488 万美元平均泄露成本的差异；以美元为单位

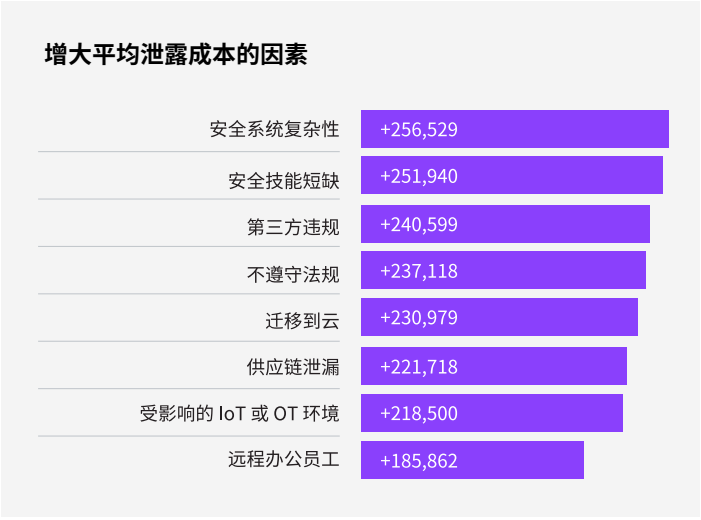


图 26.与 488 万美元平均泄露成本的差异；以美元为单位

减少或增大平均泄露成本的因素

分析成本时，了解哪些技术或事件会倾向于减少或增大成本会很有帮助。我们发现一个不变的事实：AI 和自动化可降低成本，而较为严重的网络技能短缺则会拉高成本。在此分析中，我们研究了 28 个促成因素。我们对照全球平均水平，单独研究了其中每个因素所造成的影响。然后，我们研究了经发现会导致平均数据泄露成本增大或减少的三大因素。

降低成本的关键因素
在此分析中，员工培训以及对 AI 与机器学习洞察信息的使用是降低平均数据泄露成本的首要因素。员工培训仍是网络防御战略中的一大要素，尤其是针对检测和阻止网络钓鱼攻击。AI 与机器学习洞察信息则紧随其后，位居第二。请参阅图 25。

增大成本的关键因素
在此分析中我们发现，导致泄露成本上升的三大因素分别为：安全系统复杂性、安全技能短缺和第三方泄露（其中可能包括供应链泄露）。请参阅图 26。

574 万美元

遭遇较严重安全技能短缺的组织的平均泄露成本。

关键成本放大因素的高低程度对比
当组织遭遇较为严重的安全技能短缺时，其平均泄露成本为 574 万美元，而技能短缺程度较低的组织则为 398 万美元。而其他两项关键成本因素领域也存在类似的差异。请参阅图 27。

关键成本下降因素的高低程度对比
当员工培训水平较低时，组织的平均泄露成本为 510 万美元，而员工培训水平较高的组织产生的平均泄露成本则降至 415 万美元。而其他两项关键成本因素领域也存在类似的差异。请参阅图 28。

数据泄露成本对比：三个成本增加因素程度较高的组织与三个成本增加因素程度较低的组织

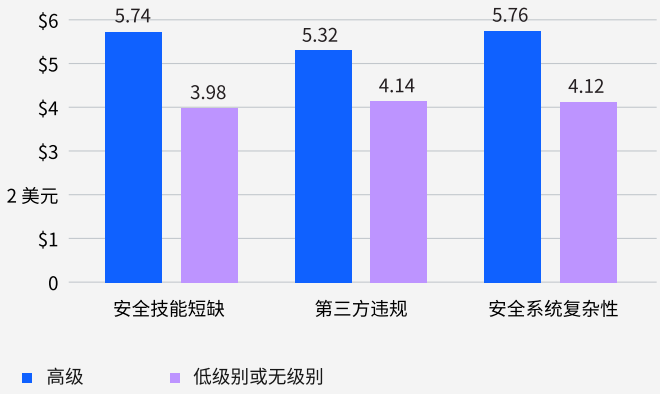


图 27：以百万美元为单位

数据泄露成本对比：三个成本缓解因素程度高的组织与三个成本缓解因素程度低的组织

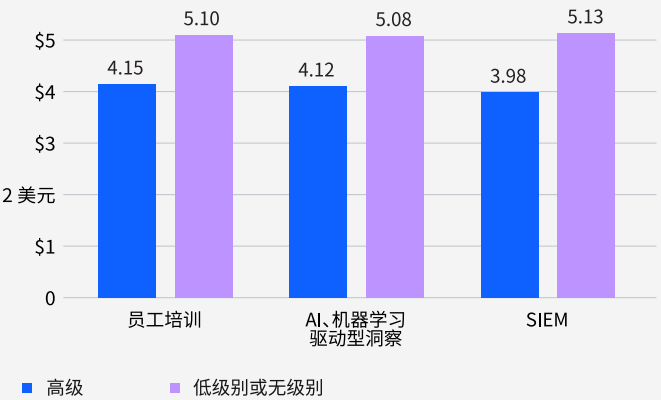


图 28：以百万美元为单位

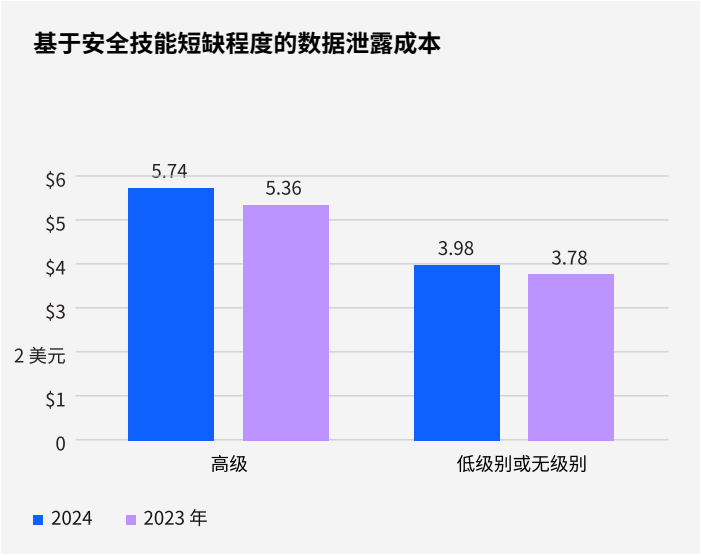


图 29：以百万美元为单位

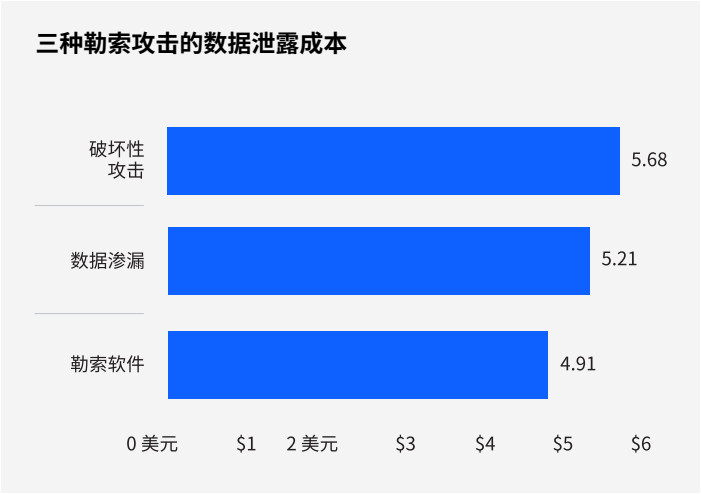


图 30.以百万美元为单位

安全技能短缺

面临熟练安全人员严重短缺的组织数量呈急剧上升趋势，从去年的 42% 上升至 2024 年的 53%。本年度的研究发现，技能短缺的加剧与数据泄露成本的上升之间存在密切联系。

技能短缺会导致泄露成本上升

2024 年，与较严重技能短缺相关的平均泄露成本将从去年的 536 百万美元跃升至 574 百万美元，增幅达 7.1%。这一涨幅比全球平均泄露成本高出了 860,000 美元。请参阅图 29。

勒索攻击的成本

组织在应对勒索攻击上花费的金额可能会根据攻击类型（勒索软件、数据渗漏和破坏性）以及组织的响应方式而各有不同。本年度的研究表明，如有寻求执法机构的帮助（当执法调查人员介入时，成本会大幅下降），此因素则尤其明显。我们对所有 3 种类型的攻击均进行了检查，其中包括勒索软件攻击（数据被加密且被要求支付赎金）、数据渗漏攻击（数据遭窃取且组织有时会遭到勒索）和破坏性攻击（攻击者出于自身目的而删除数据并破坏系统）。

破坏性攻击的成本高于其他勒索攻击

破坏性攻击（即，旨在造成持久且高昂损失的攻击）平均会造成 568 万美元的损失，因而它比勒索软件攻击或数据渗漏攻击的成本更高。请参阅图 30。

63%

涉及执法部门且免于支付赎金的勒索软件受害者占比。

识别和遏制 3 种勒索攻击的时间
所有这三种类型的攻击均需 284 到 294 天的时间来加以识别和遏制。请参阅图 31。

支付赎金
当组织成为勒索软件的受害者时，52% 的组织会寻求执法部门的帮助。而其中大多数组织 (63%) 最终并未支付赎金。请参阅图 32。

根据三种勒索攻击的发生情况来识别和遏制数据泄露所需的时间

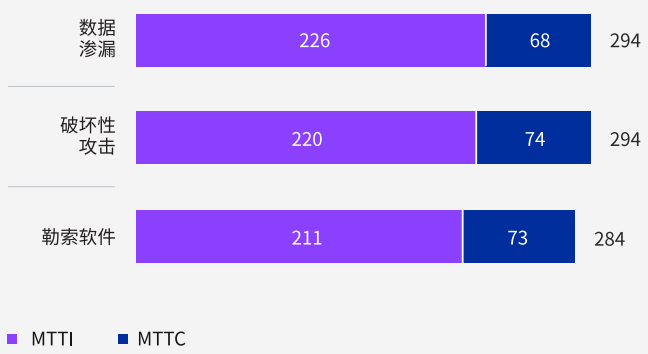


图 31：以天为单位

涉及执法部门但支付了赎金的勒索软件受害者占比

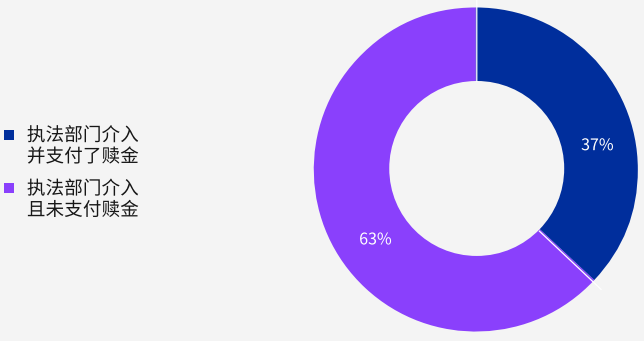


图 32：

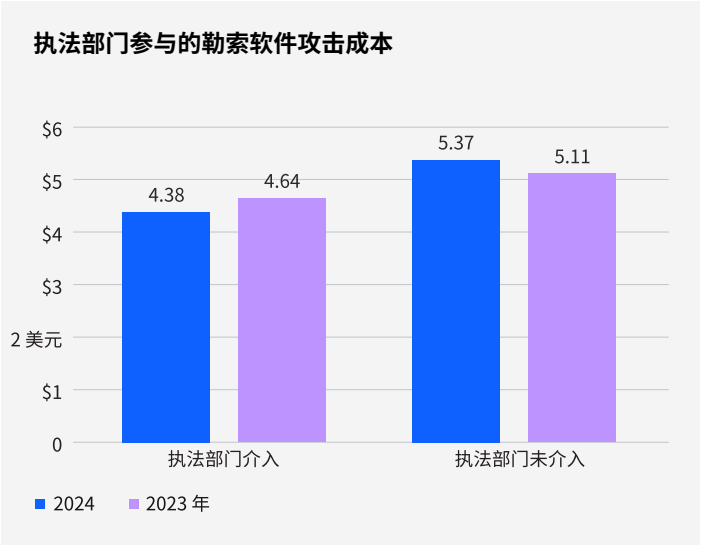


图 33：以百万美元为单位

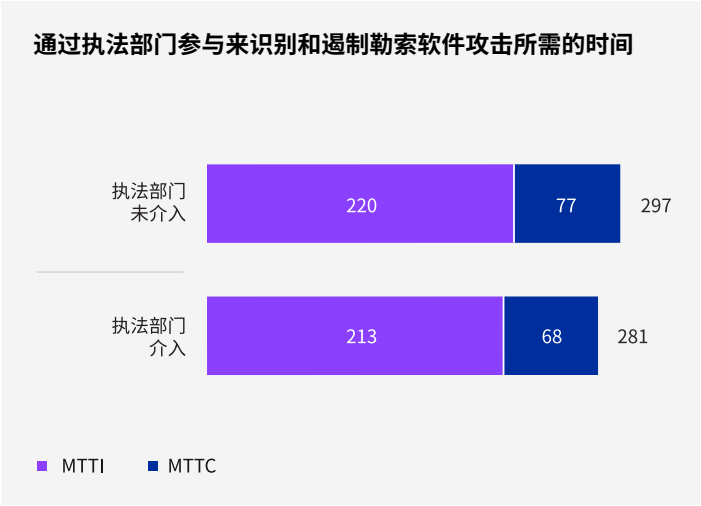


图 34：以天为单位

执法部门的参与可降低泄露成本

从有执法部门参与的 438 万美元到没有执法部门参与的 537 万美元，平均泄露成本各有不同，其成本差异超过了 20%（即，近 100 万美元）。注：这些成本数字并不包括赎金。请参阅图 33。执法部门的参与也加快了识别和遏制泄露事件所用的时间。请参阅图 34。

↑ 22.7%

缴纳 5 万美元以上罚款的组织的占比涨幅。

报告泄露事件和监管罚款

本年度的报告发现，大多数组织均向监管机构或其他政府机构报告了其泄露事件。其中约三分之一还缴纳了罚款。于是，报告和缴纳罚款已成为泄露后响应的常见组成部分。该研究调查了罚款金额，以及组织向监管机构披露泄露事件所花费的时间。大多数组织在几天内便报告了泄露事件。

平均泄露报告时间

超过一半的组织在 72 小时内便报告了其数据泄露，而 34% 的组织则在超过 72 小时后才报告。仅有 11% 的组织根本无需报告泄露事件。请参阅图 35。

监管罚款金额不断上升

缴纳较高监管罚款的组织增多；其中，缴纳 5 万美元以上罚款的较去年同期增长 22.7%，而缴纳 10 万美元以上罚款的则增长了 19.5%。请参阅图 36。

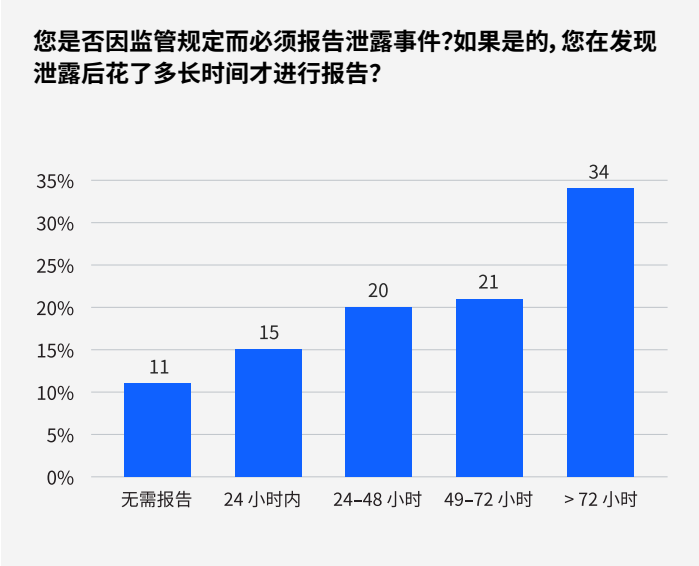


图 35.在所有泄露事件中的占比，只允许单个响应

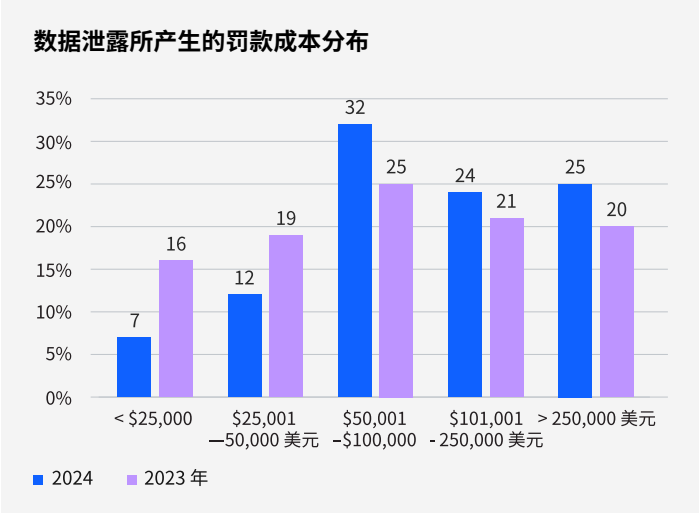


图 36.在遭受罚款的组织中，以美元为单位

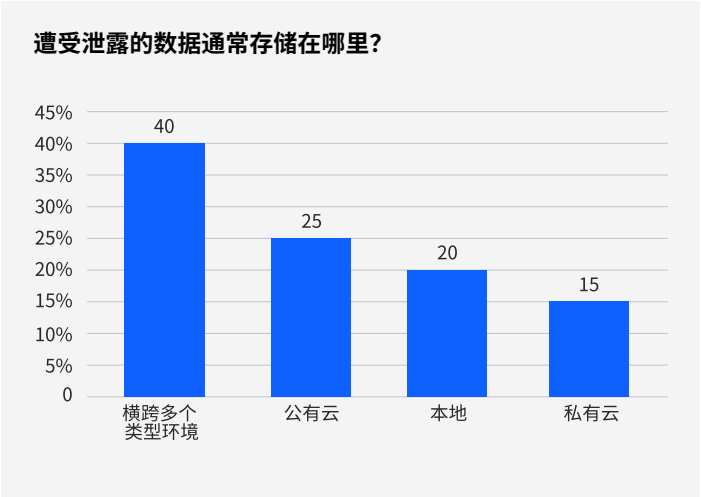


图 37. 在所有组织中的占比；允许单个响应

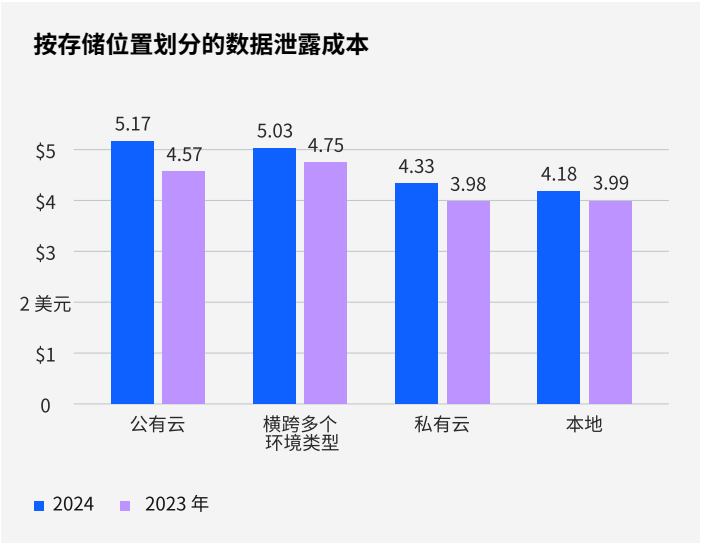


图 38：以百万美元为单位

数据安全

无论将数据存储在何处，均有可能遭遇泄露事件。本年度的研究表明，有些地方比其他地方更易受到攻击，而每次泄露的成本也更高。大多数泄露事件均涉及分布在多个环境或公有云中的数据。这两个存储选项均与较长的泄露生命周期和较高的泄露成本相关。

即使组织扩大并完善其数据管理战略，它们也常会忽视影子数据，即未受管理且可能对 IT 部门不可见的数据。这可能源于工作人员通过未经授权的应用程序来共享数据，或将数据上传到非官方云存储桶中。本报告发现，当泄露事件涉及影子数据时，其持续时间更长，导致的成本也更高。

云泄露

按数据位置划分的泄露事件
在所有泄露事件中，约有 40% 涉及分布在多个环境（例如，公有云、私有云和本地部署）中的数据。在此研究中，涉及仅存储在公有云、私有云或本地部署中的数据的泄露事件较少。随着数据在不同环境下变得更为多变和活跃，数据的发现、分类、跟踪和保护也变得更加困难。请参阅图 37。

按位置和成本划分的泄露事件
仅涉及公有云的数据泄露是成本最高一种数据泄露，其平均成本为 517 万美元，比去年上涨 13.1%。涉及多个环境的泄露事件更为常见，但其成本却比公有云泄露事件略低。本地泄露事件造成的损失最低。请参阅图 38。

527 万美元

涉及影子数据的数据泄露的平均成本。

与更快修复相关的集中控制
组织对数据的控制越是集中，它们就能越快地识别和遏制泄露事件。仅涉及本地所存储数据的泄露事件平均需 224 天才能加以识别和遏制，它比跨不同环境分布的数据泄露（需要 283 天）少了 23.3%。在私有云架构与公有云架构的比较中，也出现了同样模式的本地控制和泄露生命周期缩短。请参阅图 39。

影子数据

影子数据的泄露成本
涉及影子数据的数据泄露的平均成本为 527 万美元，比没有影子数据的平均成本高出 16.2%。请参阅图 40。

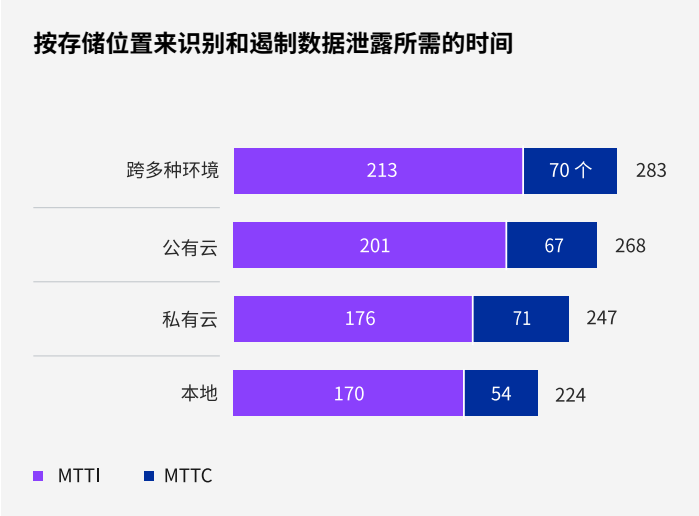


图 39：以天为单位

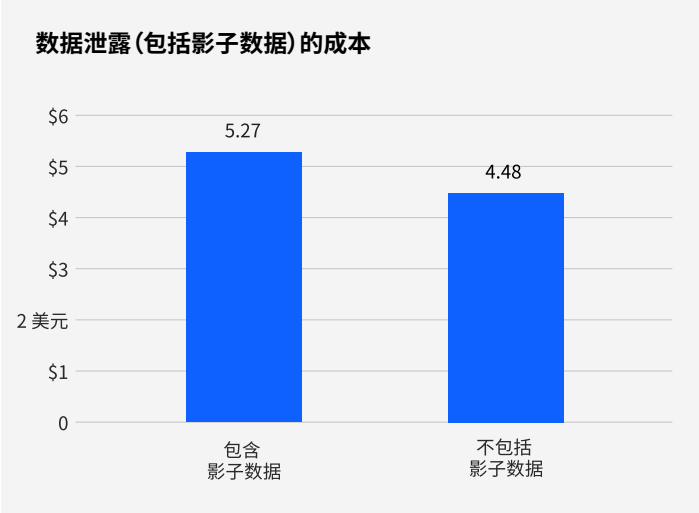


图 40：以百万美元为单位

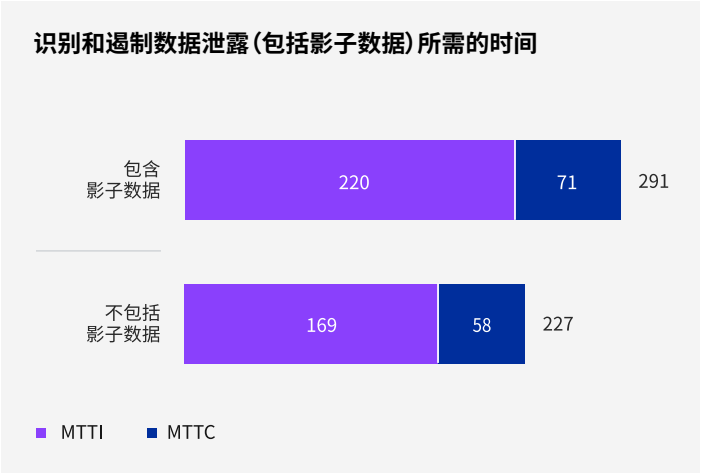


图 41:以天为单位

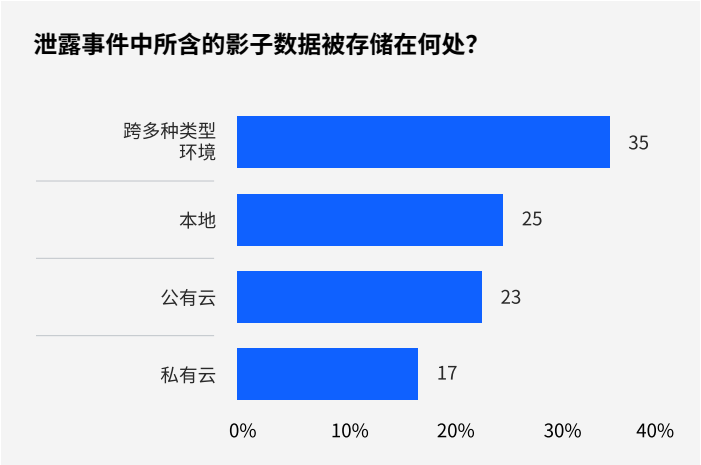


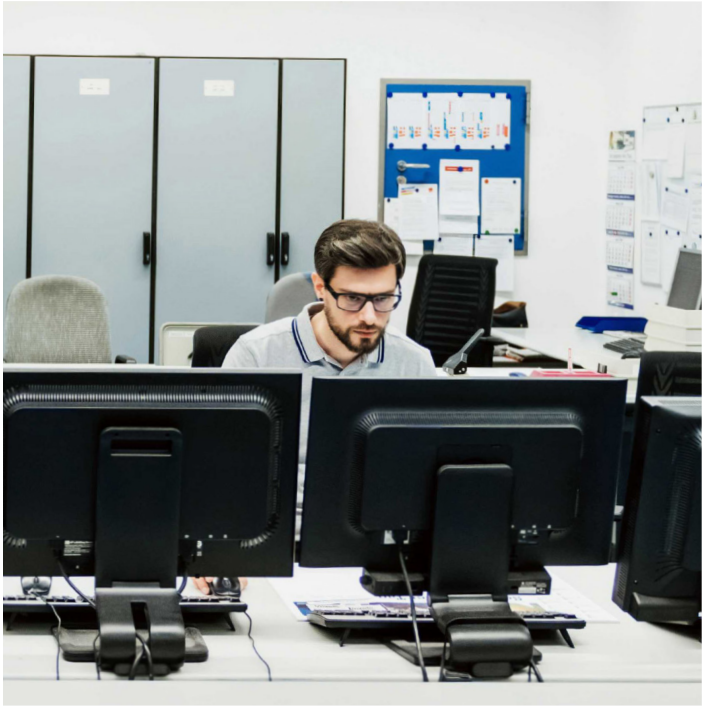
图 42.涉及影子数据的泄露事件的占比;允许单个响应

影子数据的泄露生命周期

较之不涉及影子数据的泄露事件,识别影子数据泄露平均需多用 26.2% 的时间,而遏制影子数据泄露平均需多用 20.2% 的时间。这些上涨的数据会造成平均生命周期达 291 天的数据泄露,而它比没有影子数据的数据泄露多出了 24.7%。请参阅图 41。

跨环境的影子数据

虽然影子数据存在于各种类型的环境中(公有云和私有云、本地部署以及跨多个环境),但涉及影子数据的泄露事件中有 25% 仅发生在本地。此调查结果表明,影子数据严格来说并非一个与云存储相关的问题。请参阅图 42。



大规模泄露

以超百万条受损记录为特征的大规模泄露事件相对罕见。因此，该研究会将它们与大多数其他泄露事件分开处理，而其中的部分原因在于：此举不会扭曲对更典型数据泄露的分析。

大规模泄露事件的成本上升

今年，所有超大泄露规模类别的平均成本均高于去年。在影响 5,000 万至 6,000 万条记录的最大泄露事件中，此涨幅最为明显。平均成本增加了 13%，且这些泄露事件的成本远高于一般的泄露事件。即使是规模最小的大规模泄露（涉及 100 万到 1,000 万条记录），其平均成本也达到全球平均成本 488 万美元的近 9 倍。请参阅图 43。

按丢失记录数量计算的大规模泄露成本

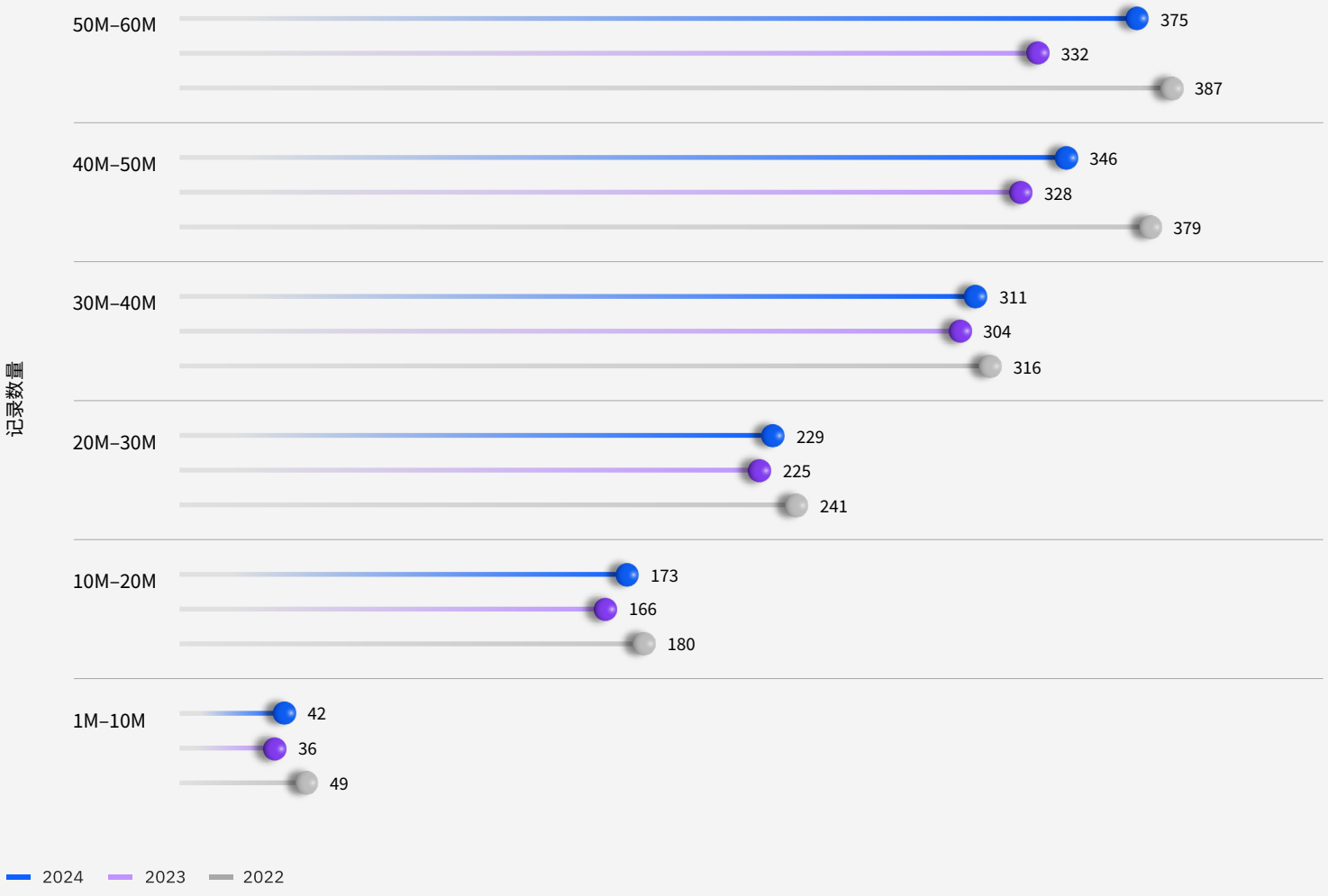


图 43：以百万美元为单位

↑ 23.5%

计划在发生泄露事件后增加安全投资的组织的占比涨幅。

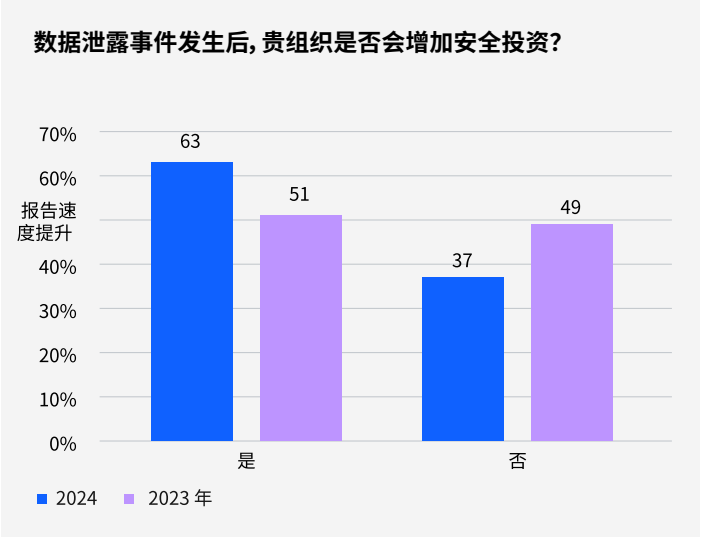


图 44：占所有组织的百分比

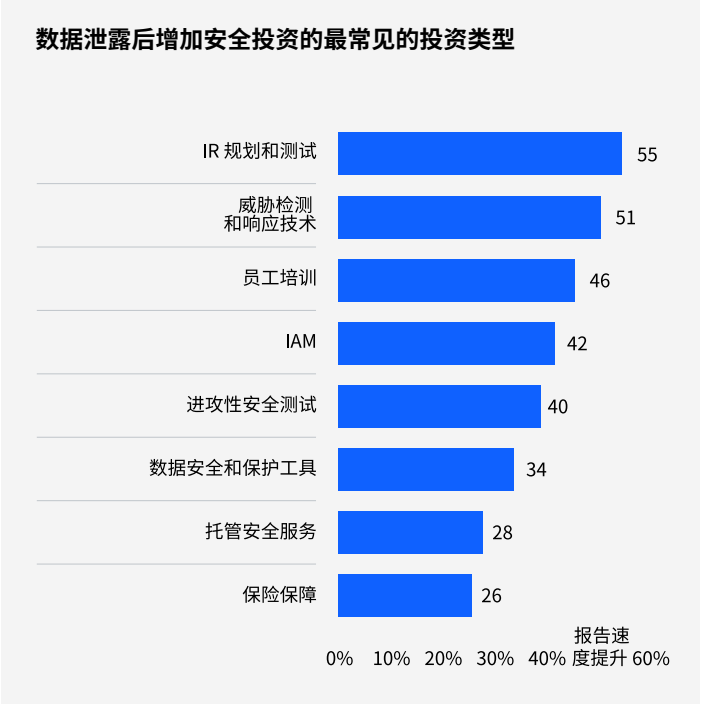


图 45.在增加安全投资的组织中的占比；允许多个响应

安全性投资

当某一组织遭遇泄露事件时，其业务与 IT 领导者通常会加大安全投资。本年度的研究询问了各组织关于未来安全支出的计划。与此同时，我们允许组织确定多个投资领域。

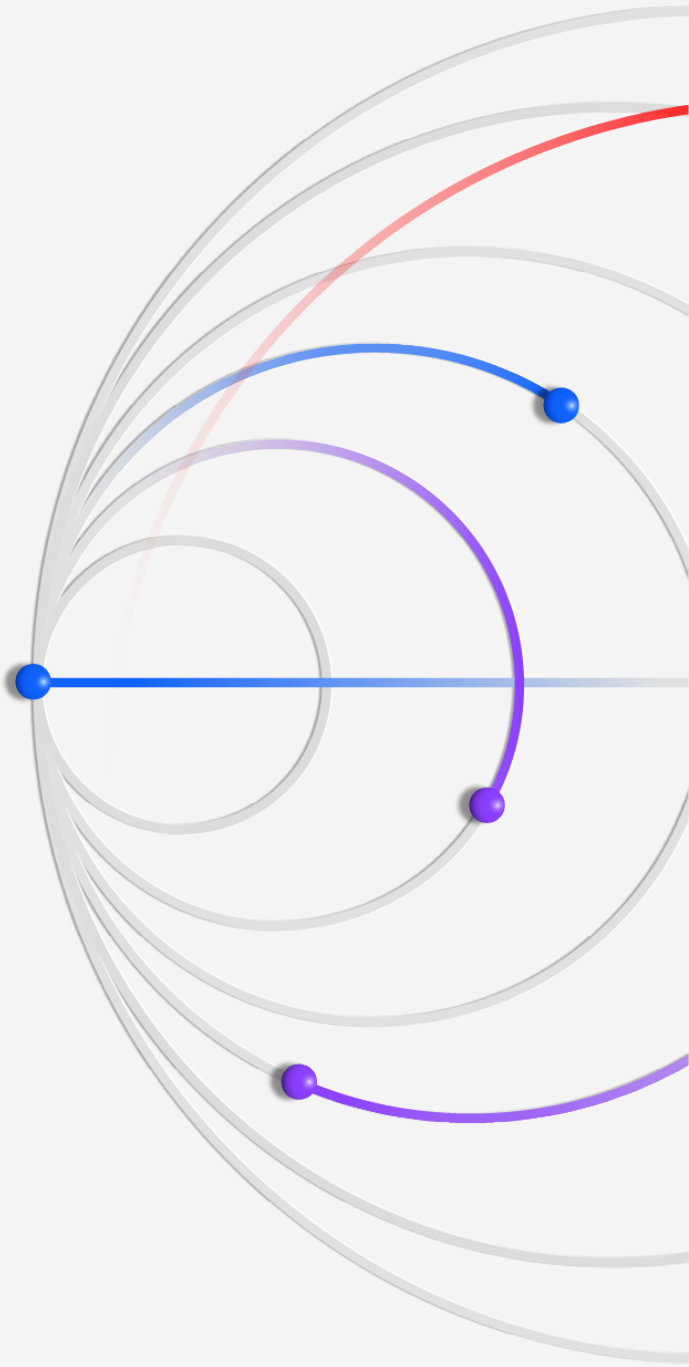
进行安全投资的组织占比上升

近三分之二的组织计划在发生泄露事件后加大安全投资，其金额则比去年增加了 23.5%。此增长可能反映出人们已意识到与业务损失和监管罚款相关的违约成本会继续增长，同时还可能会出现声誉损害现象。请参阅图 44。

安全投资的热门领域

今年报告的两个最热门的安全投资领域分别为：IR 规划和测试（占 55%）以及威胁检测与响应技术（占 51%）。前两大投资领域侧重于检测可疑事件和威胁，并更快地对其做出响应。很多组织还计划投资数据安全与保护工具（占 34%）和 IAM（占 42%）。请参阅图 45。

有助于降低数据泄露成本的几项建议



我们的建议包括成功的安全方法，这些方法可以帮助以更低的成本、更短的时间识别并遏制泄露事件。

了解自身的信息环境

大多数组织会将数据分布在多个环境中，其中包括本地数据存储库、私有云和公有云。然而，很多组织的数据存储库是不完整或过时的，这会使判断哪些数据遭泄露及其敏感或机密级别的过程被延误。此类延误可能会导致应对措施复杂化，并拉高泄露事件的成本。

安全团队应确保全面透视所有此类环境，以便在无论数据位于何处的情况下均可持续监控和保护数据。组织可在所有这些环境中应用数据安全状况管理 (DSPM) 和其他解决方案（如身份和访问管理 以及 ASM），以便提供一致且全面的保护。

安全团队必须特别关注混合环境和公有云。40% 的数据泄露涉及跨多个环境存储的数据，而当泄露的数据存储在公有云中时，导致的平均泄露成本最高（517 万美元）。安全团队必须更为深入地了解其所用每个云服务的具体风险和控制措施。

由于未管理的数据造成的影响，跨环境管理数据变得更为复杂。超过三分之一的数据泄露事件涉及影子数据。如今，安全团队必须假设其组织存在未管理的数据源。而非加密数据（包括 AI 工作负载中的数据）则会进一步加剧此风险。数据加密策略必须考虑数据的类型、用途和存储位置，以便在发生泄露事件时降低风险。

运用 AI 和自动化，增强预防策略

在整个组织中采用生成式 AI 模型和第三方应用程序，以及持续使用物联网 (IoT) 设备和“软件即服务” (SaaS) 应用程序，均会扩大攻击面，给安全团队带来压力。

将 AI 和自动化技术运用于支持安全预防策略（包括在 ASM、红队测试和态势管理中），往往可以通过托管安全服务来实现。在本年度的研究中，将 AI 和自动化技术运用于安全预防领域的组织，相比其他三个安全领域（检测、调查、响应），从其 AI 投资中受益最大。相较于未在预防技术中部署 AI 的组织，有部署的组织平均节省了 222 万美元。

采用生成式 AI，勿忘安全第一

虽然各大组织正在快速推进生成式 AI，但眼下却只有 24% 的生成式 AI 计划拥有相应的安全保障。安全措施不足，数据和数据模型暴露于泄露的风险之下，进而可能破坏生成式 AI 项目意在创造的优势。

随着生成式 AI 采用范围的不断扩大，组织需要一个框架来保护生成式 AI 数据、模型及其使用，并制定 AI 治理控制措施。为此，组织需防止其训练数据被窃取和操纵，从而确保这些数据的安全。组织可使用数据发现和分类方法，检测用于训练或微调的敏感数据。此外，组织还可在加密、访问权限管理和合规性监控的过程中，落实数据安全控制措施。

对于生成式 AI，组织面临的不仅是影子数据的增长及其风险，更涉及到影子模型。组织必须将态势管理扩展到 AI 模型本身，保护敏感的 AI 训练数据，同时洞悉未经批准的影子 AI 模型的使用情况，以及 AI 滥用或数据泄露的情况。

为了确保生成式 AI 模型开发过程的安全，需扫描开发管道中的漏洞、加固集成，并严格实施策略和访问权限。为了保证生成式 AI 模型的使用安全，安全团队需监控是否存在恶意输入（如提示注入）以及包含敏感数据的输出。此外，安全团队还必须部署 AI 安全解决方案，以检测和应对特定于 AI 的攻击，例如数据投毒、模型规避和模型窃取。制定响应策略，以实现拒绝访问，并隔离和断开遭泄露的模型，也是至关重要的。

在生成式 AI 和其他 IT 计划导致威胁态势不断蔓延的情况下，有必要为非安全从业人员提供安全培训，其中包括在 AI 团队中工作的数据科学家和数据工程师。

进一步加强网络安全响应培训

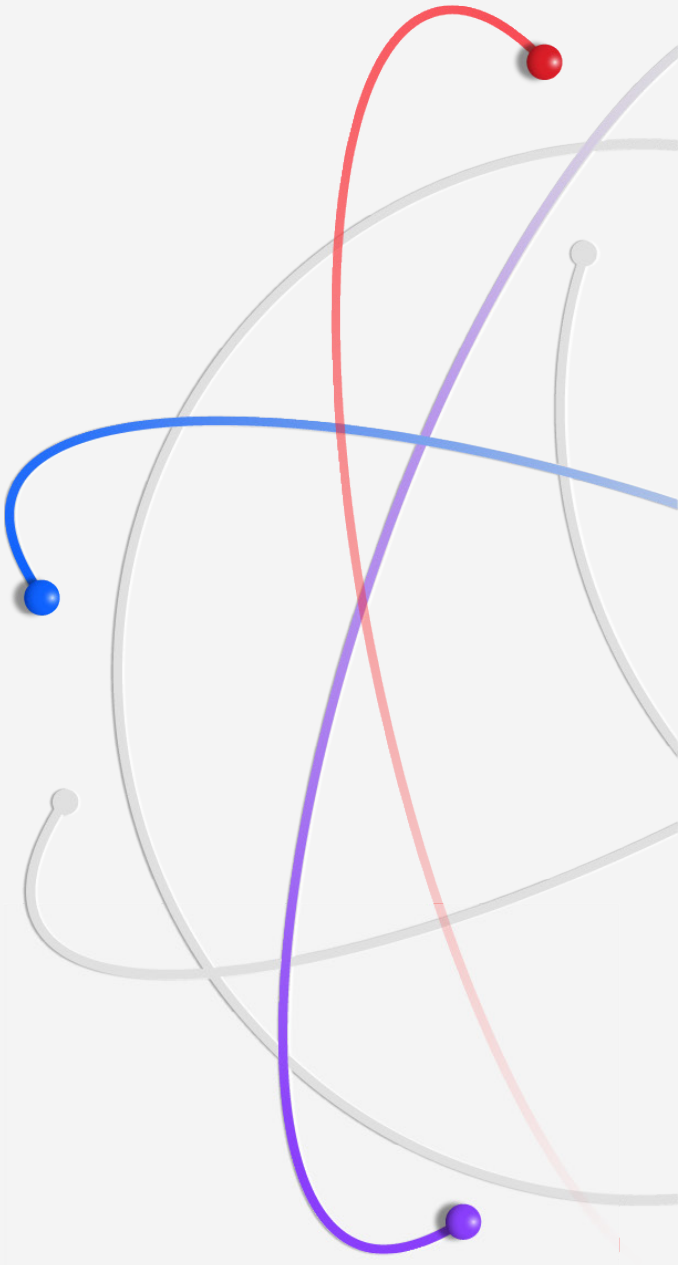
组织在泄露事件期间和之后如何应对，以及如何与企业领导、监管机构和客户进行沟通比以往任何时候都更为重要。为增强处理高影响力攻击的能力，组织可参加网络靶场危机模拟演习，形成针对泄露处置的肌肉记忆。

此类演习可涵盖安全团队和业务领导者，让整个组织均可提高检测、遏制和应对泄露事件的能力。安全负责人应提前与组织的各个业务职能部门和沟通团队开展合作，起草响应计划并加以测试。在生成式 AI 和其他 IT 计划导致威胁态势不断蔓延的情况下，有必要为非安全从业人员提供安全培训。此类人员包括在机器学习与 AI 团队中工作的数据科学家和数据工程师，以及负责在本地资产和云资产中维护 AI 工作负载连续性的人员。

组织通过投资于响应能力，可降低数据泄露所造成的成本高昂且极具破坏性的影响，为运营连续性提供支持，并帮助维护与客户、合作伙伴和其他关键利益相关者的关系。此外，在攻击的紧急阶段，由胸有成竹的领导团队开展处置、控制和沟通，实施经过演练的应对措施，可让员工感到安心，同时减少组织内部的压力、痛苦和摩擦。

组织统计数据

今年的研究调查了来自 16 个国家和地区以及 17 个行业的 604 个不同规模的组织。本节深入了解了本研究中按地理和行业划分的组织细分，并定义了行业分类。



地理统计数据

2024 年的研究已在 16 个国家和地理区域开展。比荷卢是今年新加入此研究的一个新地区，它是由比利时、荷兰和卢森堡组成的一个经济联盟。斯堪的纳维亚已从此研究中排除。

“东盟”是位于新加坡、印度尼西亚、菲律宾、马来西亚、泰国和越南的诸多组织的集群样本。“拉丁美洲”是位于墨西哥、阿根廷、智利和哥伦比亚的诸多组织的集群样本。“中东”是位于沙特阿拉伯和阿拉伯联合酋长国的诸多组织的集群样本。

全球研究速览

国家和地区	2024 年样本	样本总数占比	研究年限	货币
东盟	25	4%	8	新加坡元 (SGD)
澳大利亚	27	4%	15	澳元 (AUD)
比荷卢	32	5%	1	欧元 (EUR)
巴西	45	7%	12	巴西雷亚尔 (BRL)
加拿大	28	5%	10	加元 (CAD)
法国	36	6%	15	欧元 (EUR)
德国	47	8%	16	欧元 (EUR)
印度	53	9%	13	印度卢比 (INR)
意大利	29	5%	13	欧元 (EUR)
日本	42	7%	13	日元 (JPY)
拉丁美洲	28	5%	5	墨西哥比索 (MXN)
中东	39	6%	11	沙特阿拉伯里亚尔 (SAR)
南非	24	4%	9	南非兰特 (ZAR)
韩国	28	5%	7	韩元 (KRW)
英国	50	8%	17	英镑 (GBP)
美国	71	12%	19	美元 (USD)
总计	604	100%		

图 46.本研究中所有组织的占比

行业统计数据

本研究多年来始终会选择 17 个行业。今年，金融、工业、专业服务和科技这四大行业占到所研究 604 家组织的 47%。

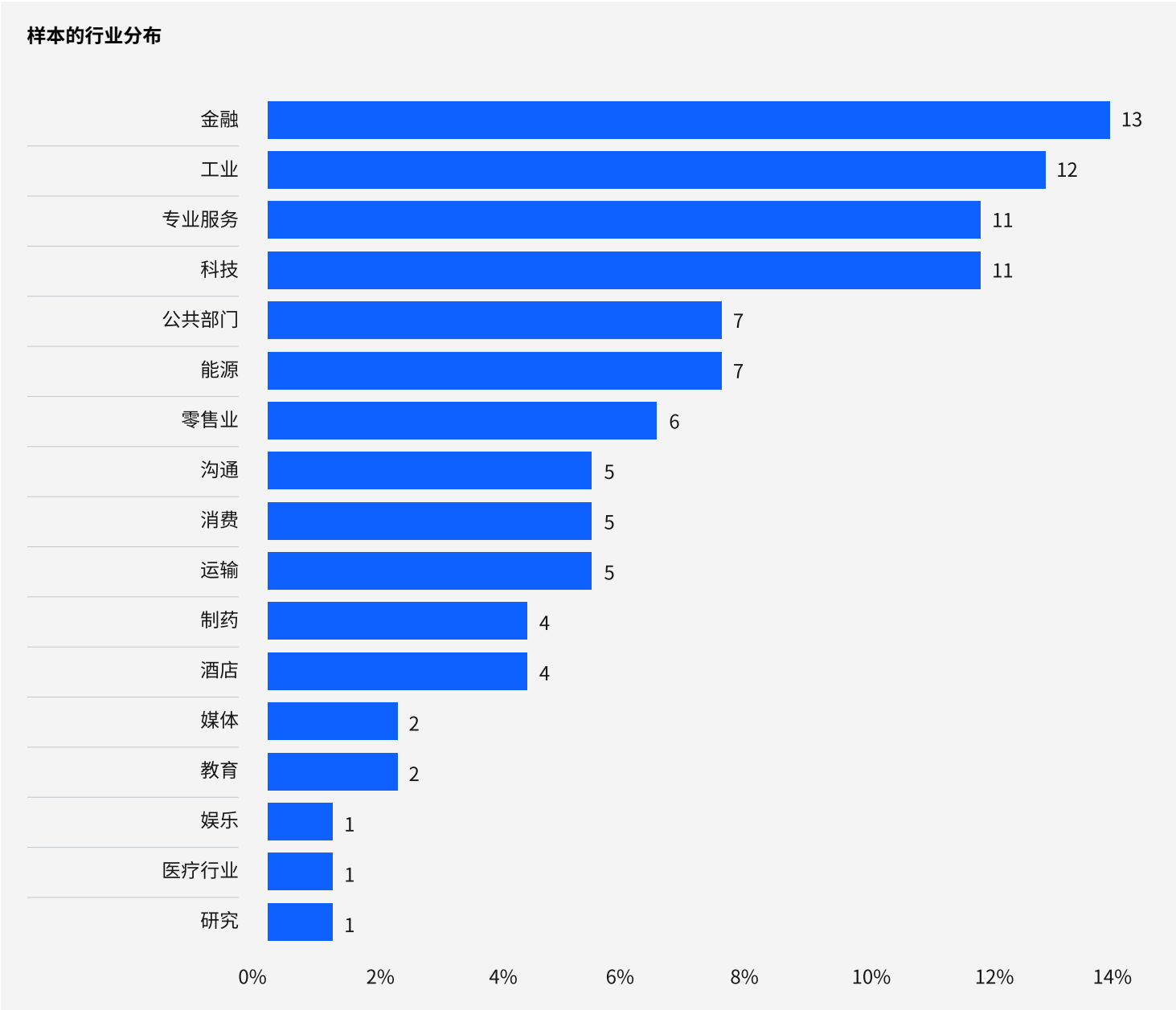


图 47.本研究中所有组织的占比

行业定义

医疗行业
医院和诊所

金融
银行、保险、投资公司

能源
石油和天然气公司、公用事业、替代能源生产商和供应商

制药
制药公司，包括生物医学生命科学公司

工业
化学加工、工程和制造公司

科技
软件和硬件公司

教育
公立与私立大学和学院、培训与发展公司

专业服务
法律、会计和咨询公司等专业服务

娱乐
电影制作、体育、博彩和赌场

运输
航空、铁路、货运与快递公司

通信
报纸、图书出版商、公共关系与广告公司

消费
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、餐饮连锁店、邮轮公司

零售业
实体店和电子商务

研究
市场调研、智库和研发

公共部门
联邦、州与地方政府机构和非政府组织

研究方法

出于保密目的，研究所使用的基准工具没有捕获任何公司的特定信息。数据收集方法排除了实际发生的会计信息，而是依靠参与者通过在数轴上标记一个范围变量来估计直接成本。参与者被要求在每个成本类别范围的下限和上限之间的某个位置标记数轴。

数值是通过数轴而不是对每个成本类别估计的点得出的，保留了机密性，并且确保了更高的响应率。基准工具还要求受访组织分别提供间接成本和机会成本的二次估计。

为顺利进行基准测试，需做好可管理数据集的维护工作，因此本报告仅包括那些对数据泄露成本有重要影响的成本活动中心。根据与专家的讨论，我们选择了一组固定的成本活动。在收集基准信息后，我们对每项基准工具都进行了仔细的重新审查，以确保其一致性和完整性。

数据泄露成本因素的范围仅限于应用于涉及个人信息的广泛业务运营的已知类别。我们选择关注业务流程，而不是数据保护或隐私合规活动，因为我们相信流程研究会产生更高质量的结果。

我们如何计算数据泄露的成本

在计算数据泄露的平均成本时，我们排除了非常小和非常大的数据泄露事件。2024 年的报告中，纳入调研的数据泄露事件规模均在 2,100 至 113,000 条受损记录之间。我们使用了单独的分析来研究大规模泄露的成本，报告中的“数据泄露常见问题解答”部分对该方法有深入的阐述。

我们采用了基于活动的成本计算，即确定活动并根据实际使用情况分配成本。有四种与流程相关的活动导致了与组织数据泄露相关的一系列支出：检测和升级、通知、泄露后响应和已丢失业务。

检测和上报
可帮助组织检测泄露事件的活动包括：

- 取证和调查活动
- 评估和审计服务
- 危机管理
- 与高管和董事会的沟通

通知
可帮助组织通知数据主体、数据保护监管机构和其他第三方的活动包括：

- 给数据主体的电子邮件、信件、出站呼叫通信或一般通知
- 确定监管要求
- 与监管机构的沟通
- 聘请外部专家

泄露后响应
帮助数据泄露事件的受害者与组织沟通的活动，以及对受害者和监管机构的补救活动，包括：

- 服务台和入站通信
- 信用监察和身份保护服务
- 签发新账户或信用卡
- 法律支出
- 产品折扣
- 监管罚款

业务损失
试图将客户流失、业务中断和收入损失降至最低的活动，包括：

- 因系统宕机而造成的业务中断和收入损失
- 失去客户和获得新客户的成本
- 声誉损失和商誉降低

数据泄露常见问题解答

什么是数据泄露?
数据泄露定义为包含 PII、财务或医疗帐户详细信息等;或者其他秘密、机密或专有数据的记录可能面临风险的事件。这些记录可以是电子或纸质格式。本研究中包括的数据泄露规模范围为 2,100 到 113,000 条受损记录。

什么是受损记录?
记录是指泄露机密或专有的公司、政府或财务数据,或识别在数据泄露事件中丢失或被盗的个人的信息。例如,包含个人姓名、信用卡信息和其他 PII 的数据库,或包含保单持有人姓名和付款信息的健康记录等。

如何收集数据?
我们的研究人员对 2023 年 3 月至 2024 年 2 月期间遭遇数据泄露的 604 家组织的个人进行了 3,556 次单独访谈,以此收集具有一定深度的定性数据。受访者熟悉所在组织的数据泄露事件,以及与解决泄露事件相关的成本。这些受访者包括首席执行官或高管、运营负责人、财务控制人或负责人、IT 从业者、业务部门领导和总经理,以及风险管理与网络安全从业者。出于隐私考虑,我们没有收集组织特定的信息。

数据泄露成本包括哪些项目?
我们收集了组织产生的直接与间接费用。直接费用包括聘请取证专家、外包热线支持,以及为未来的产品和服务提供免费信用监察订阅和折扣等费用。间接成本包括内部调查和沟通,以及因营业额或客户获取率下降而导致的客户损失的推断价值成本。

本研究只代表与数据泄露经历直接相关的事件。《通用数据保护条例》(GDPR) 和《加州消费者隐私法案》(CCPA) 等法规可能会鼓励组织增加对其网络安全治理技术的投资。然而,这种活动并没有直接影响本研究中的数据泄露成本。为了与往年保持一致,我们使用了相同的货币换算方法,而不是调整会计成本。

基准研究与调查研究有何不同?
《数据泄露成本报告》中的分析单位是企业或机构等组织。在调查研究中,分析的单位是个人。我们招募了 604 家组织参与这项研究。

每条记录的平均成本是否可以用来计算涉及数百万条丢失或被盗记录的数据泄露成本?
采用每条记录的总成本作为基准来计算总计数百万条记录的单起或多起数据泄露的成本,与本研究得出的结论并不一致。每条记录的成本根据我们对数百起数据泄露事件的研究总结得出,其中每起事件都最多有 113,000 条受损记录。为了衡量涉及 100 万条或更多记录的大规模泄露的影响,本研究采用模拟框架,以 17 起同等规模的事件为样本。

为什么要用模拟方法来估算大规模泄露的成本?
17 家经历过大规模泄露的组织的样本量不够大,无法使用基于活动的成本方法支持具有统计学意义的分析。为了解决这个问题,我们采用了蒙特卡罗模拟方法,通过重复的试验来估计一系列可能的、随机的结果。我们总共进行了超过 269,000 次试验。所有样本均值的总平均值提供了每种数据泄露规模的最可能结果,范围从 1 百万到 53 百万条受损记录。

此研究是否每年都跟踪相同的组织?
每年的研究均涉及不同的组织样本。为了与之前的报告保持一致,我们每年都会招募和匹配具有相似特征的组织,例如组织的行业、员工人数、地理足迹和数据泄露的规模。自 2005 年开始这项研究以来,我们已经研究了 6,184 家组织的数据泄露经历。

研究的局限性

我们的研究使用了一种机密且专有的基准方法，该方法已在早期研究中成功采用。然而，在从研究结果中得出结论之前，仍需要仔细考量这种基准研究所固有的局限性。

非统计结果
我们的研究利用了具有代表性的、非统计学的全球实体样本。鉴于这种抽样方法并不科学，统计推断、误差范围和置信区间等理论都不适用于这些数据。

无响应
未测试无响应偏差，因此，未参与的组织可能在潜在数据泄露成本方面存在显著差异。

抽样框误差
由于我们的抽样框属于判断性的，所以研究结果的质量会受到抽样框对被研究组织群体所代表程度的影响。我们认为，当前的抽样框偏向于拥有更成熟的隐私或信息安全计划的组织。

特定于组织的信息
研究中使用的基准没有捕获组织的识别信息。个人可以使用分类响应变量来披露有关组织和行业类别的统计信息。

未衡量因素
我们在分析中省略了某些变量，如主导趋势和组织特征。无法确定已省略的变量会在多大程度上解释基准测试结果。

推断成本结果
虽然可以将某些检查和平衡纳入基准流程，但受访者仍有可能未提供准确或真实的回答。此外，使用成本推断方法而非实际成本数据可能会无意中引入偏差和不准确因素。

货币换算
从当地货币换算成美元后，其他国家的平均总成本估计值会降低。为了与往年保持一致，我们决定继续使用相同的会计方法而不是调整成本。值得注意的是，此问题可能仅影响全球层面的分析，因为所有国家/地区层面的结果均以本地货币显示。本研究报告中使用的当前实际汇率由美联储于 2024 年 3 月 4 日公布。

关于 IBM 和波耐蒙研究所 (Ponemon Institute)

IBM

IBM 是全球领先的混合云、AI 与商业服务提供商，致力于帮助超过 175 个国家和地区的客户利用数据洞察、精简业务流程、降低成本，并在行业内获得竞争优势。所有这一切都离不开 IBM 在信任、透明、责任、包容和服务方面始终如一的努力付出。有关更多信息，请访问 www.ibm.com/cn-zh。

了解有关改善安全状况的更多信息：

请访问 ibm.com/cn-zh/security

加入 IBM Security 社区中的对话

波耐蒙研究所 (Ponemon Institute)

波耐蒙研究所 (Ponemon Institute) 成立于 2002 年，致力于通过独立的研究和教育活动，在企业和政府内部推进负责任的信息和隐私管理实践。我们的宗旨是针对影响个人和组织相关敏感信息管理和安全的关键问题，开展高质量的实证研究。

波耐蒙研究所坚持严格的数据保密、隐私与道德研究标准，而不会向个人收集个人身份信息 (PII)，也不会在商业研究中收集公司身份信息。此外，我们坚持履行严格的质量标准，绝不会向研究对象提出非必要、不相关或不恰当的问题。

如果您对本研究报告存有任何疑问或意见（包括获得引用或复制本报告的许可请求），请通过信函、电话 或电子邮件与我们联系：

Ponemon Institute LLC
研究部
1-800-887-3118
research@ponemon.org

国际商业机器（中国）有限公司
了解更多信息，欢迎访问我们的中文官网：
https://www.ibm.com/cn-zh
IBM Corporation
New Orchard Road
Armonk, NY 10504

美国出品
2024 年 7 月