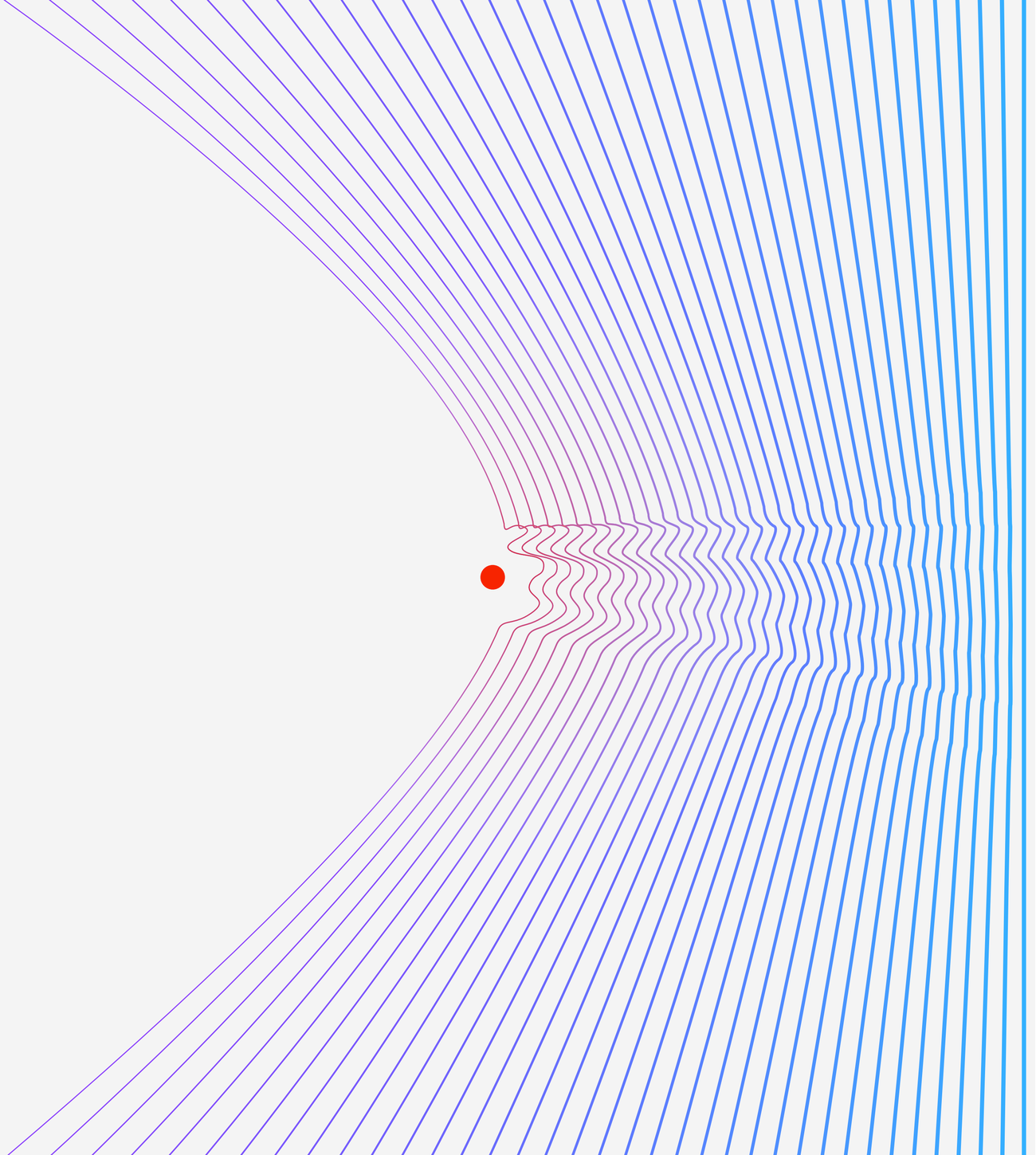
IBM **Security**

2023 年数据泄露成本报告



IBM

目录

01

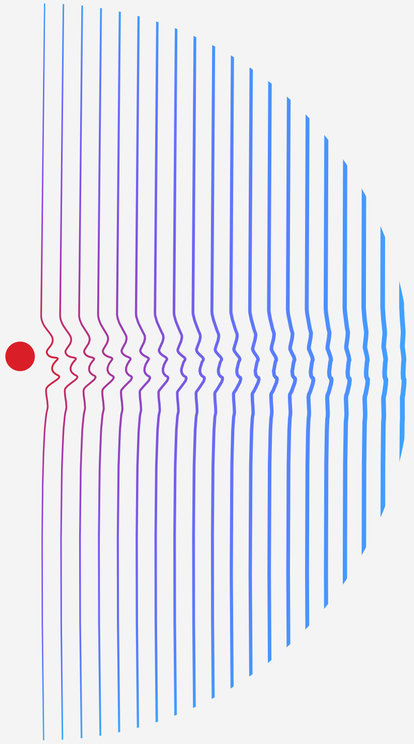
执行摘要

《数据泄露成本报告》为 IT、风险管理和安全主管提供了可量化的论据和佐证，以帮助各方更好地管理安全投资、风险情况和战略决策流程。2023 年版是该报告连续第 18 年发布的版本。

今年的研究由波耐蒙研究所 (Ponemon Institute) 独立进行并由 IBM Security® 发起、分析和发布，调研了 2022 年 3 月至 2023 年 3 月期间受数据泄露影响的 553 家组织。

本报告中提及的年份
是指报告发布的年份，
而不一定是泄露事件发生的年份。
所调研的泄露事件发生在
16 个国家和地区，涉及 17 个不同行业。

在本报告中，我们将研究数据泄露的根本原因以及短期和长期后果。我们还将探讨能让公司减少损失的各类因素和技术，同时避免采取那些会导致成本增加的因素和技术。



2023 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，覆盖新出现的内容，以匹配新技术、新兴策略和近期事件。今年的研究首次探讨了：

- 如何识别泄露行为：无论源于组织自身的安全团队、其他第三方还是攻击者
- 执法部门参与抵御勒索软件攻击而产生的影响
- 勒索软件运行手册和工作流程的影响
- 与监管罚款相关的特定成本
- 公司是否以及如何计划因泄露而增加安全投资
- 以下缓解策略产生的影响：
  - 威胁情报
  - 漏洞和风险管理
  - 攻击面管理 (ASM)
  - 托管安全服务提供商 (MSSP)

随着泄露成本不断增加，本报告可为各方提供重要洞察成果，可帮助安全和 IT 团队更好地管理风险并限制潜在损失。报告分为五个主要部分：

- 介绍重要结论和 2023 年新增内容的执行摘要
- 对完整调查结论的深入分析，包括按地理区域和行业划分的数据泄露成本
- IBM Security 专家根据本报告的结果提出的安全建议
- 组织统计数据与行业定义
- 研究方法，包括如何计算成本

重要结论

本报告所述主要结论基于 IBM Security 对波耐蒙研究所 (Ponemon Institute) 所汇编的研究数据的分析而得出。本报告中成本金额的计量单位为美元 (USD)。

445 万美元

泄露的平均总成本

2023 年，数据泄露的平均成本达到 445 万美元，创下历史新高。相较于 2022 年的 435 万美元，该成本增加了 2.3%。拉长时间线来看，平均成本较 2020 年报告中的 386 万美元增加了 15.3%。

51%

因数据泄露而计划增加安全投资的组织所占比例

虽然数据泄露的成本持续上升，但报告参与者在是否因数据泄露而计划增加安全投资的问题上几乎各持己见。确定需要额外投资的首要领域包括事件响应 (IR) 规划和测试、员工培训以及威胁检测和响应技术。

---

176 万美元

针对数据泄露造成的财务影响，广泛采用安全 AI 和自动化可获得良好的效果

在识别并遏制安全泄露事件方面，安全 AI 和自动化被证明是能够降低成本以及缩短时间的重要投资。广泛采用这些功能的组织在识别并遏制泄露方面耗费的时间平均缩短了 108 天。报告还指出，与不使用安全 AI 和自动化功能的组织相比，数据泄露成本降低了 176 万美元。

1/3

组织自身的安全团队或工具发现的漏洞数量
仅有三分之一的公司通过自己的安全团队发现了数据泄露事件，这凸显了亟需更好的威胁检测手段。67% 的漏洞是由良性第三方或攻击者自己报告的。当攻击者披露漏洞时，相较于内部检测，组织会损失近 100 万美元。

47 万美元

未让执法部门参与抵御勒索软件攻击的组织所承受的额外成本
今年的研究表明，将执法部门排除在勒索软件事件之外会导致更高的成本。虽然 63% 的回应者表示他们的数据泄露事件有执法部门介入，但 37% 的回应者表示没有执法部门介入，却还是多支付了 9.6% 的费用，并且泄露生命周期延长了 33 天。

53.3%

自 2020 年以来，医疗数据泄露成本增加了 53.3%
自 2020 年以来，受到严格监管的医疗保健行业的数据泄露成本大幅上升。根据报告，医疗保健行业数据泄露造成的损失已连续 13 年位居榜首，耗费的平均成本高达 1,093 万美元。

82%

涉及存储在云端（公共、私有或多个环境）中各类数据泄露所占比例
2023 年，云环境成为网络攻击者的常见目标。攻击者通常会入侵多个环境，39% 的漏洞跨越多个环境，造成的损失高于平均水平，达到 475 万美元。

168 万美元

通过采用高水平的 DevSecOps 部署来节省成本

软件开发流程 (DevSecOps) 中的集成安全性测试在 2023 年显示出可观的投资回报率。与 DevSecOps 采用率低或未采用的组织相比，采用率高的组织节省了 168 万美元。与其他降低成本的因素相比，DevSecOps 展示了最大的成本节省效果。

149 万美元

具备高水平的 IR 规划和测试的组织所节省的成本

除了成为组织的优先投资之外，IR 规划和测试还可成为控制数据泄露成本的高效策略。具有高水平 IR 规划和测试的组织比低水平的组织节省了 149 万美元。

144 万美元

安全系统复杂性较高的组织会产生更高的数据泄露成本

2023 年，依据报告统计，安全系统复杂性较低或不复杂的组织产生的平均数据泄露成本为 384 万美元。安全系统复杂性较高的组织平均成本为 528 万美元，增大了 31.6%。

102 万美元

发现并解决漏洞用时超过 200 天与用时不到 200 天的漏洞之间的平均成本差异

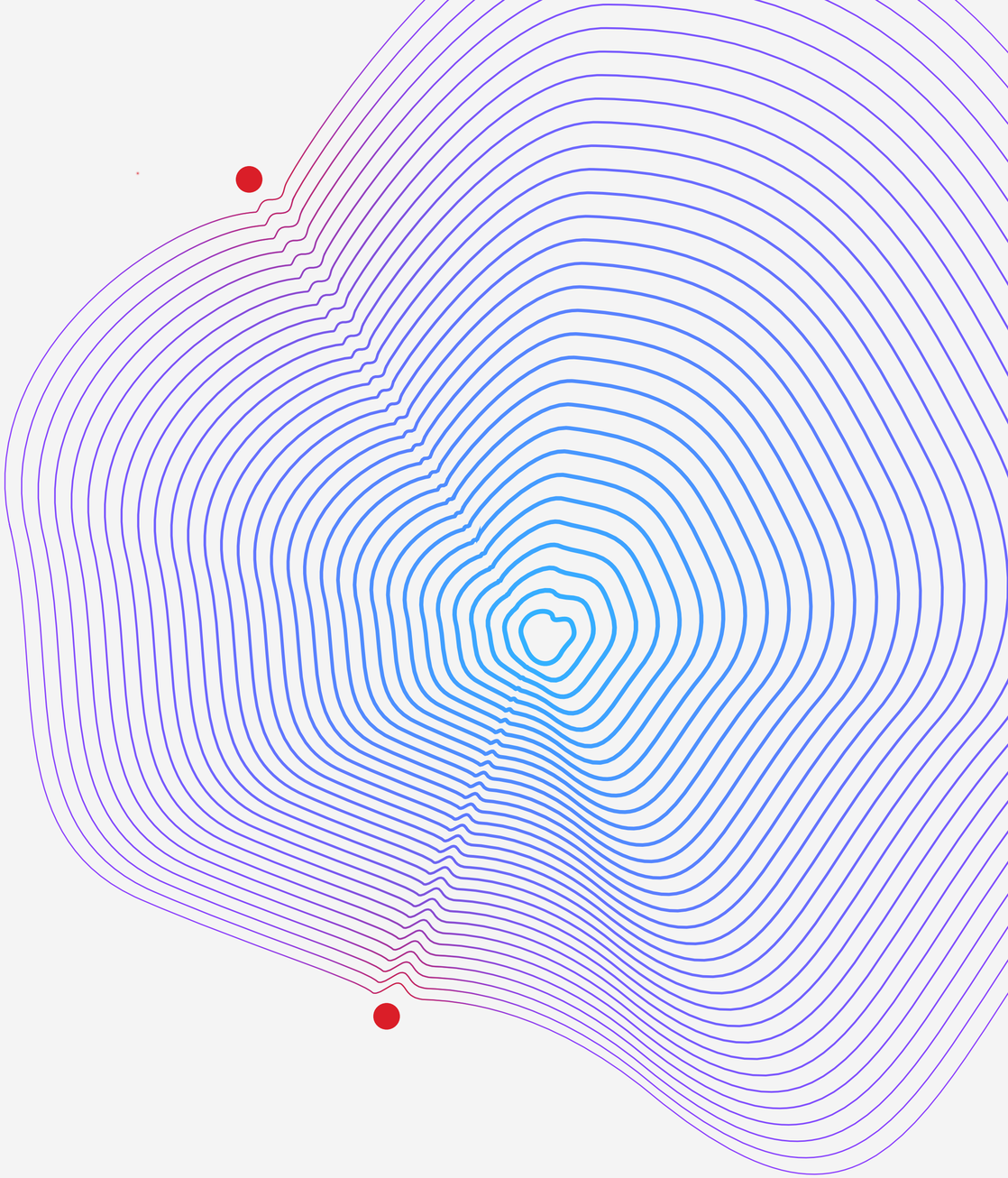
识别并遏制泄露所耗费的时间（称为泄露生命周期）仍然会对整体财务情况造成不可忽视的影响。对于那些识别并遏制泄露所耗费时间不到 200 天的事件，给组织造成了 393 万美元的损失。那些耗费时间超过 200 天的事件，成本为 495 万美元，相差 23%。

02

完整的结论

在这部分中，我们将整体内容划分为 18 个主题，详细介绍本报告得出的主要结论。主题安排顺序如下：

- 全球关注重点
- 初始攻击媒介
- 识别攻击
- 数据泄露生命周期
- 关键成本因素
- 勒索软件和破坏性攻击
- 业务合作伙伴供应链攻击
- 软件供应链攻击
- 监管环境
- 云泄露
- 大规模泄露
- 安全性投资
- 安全 AI 和自动化
- 事件响应
- 威胁情报
- 脆弱性和风险管理
- 攻击面管理
- 托管安全服务提供商



全球关注重点

《数据泄露成本报告》使用来自 16 个不同国家/地区、超过 553 起数据泄露的数据，并考虑了数百个成本因素，提供了数据泄露成本的全球概况。本节将阐述全球平均水平的关键指标。我们还会探讨国家/地区和行业之间每笔记录的平均比较成本。

445 万美元

数据泄露的全球平均总成本

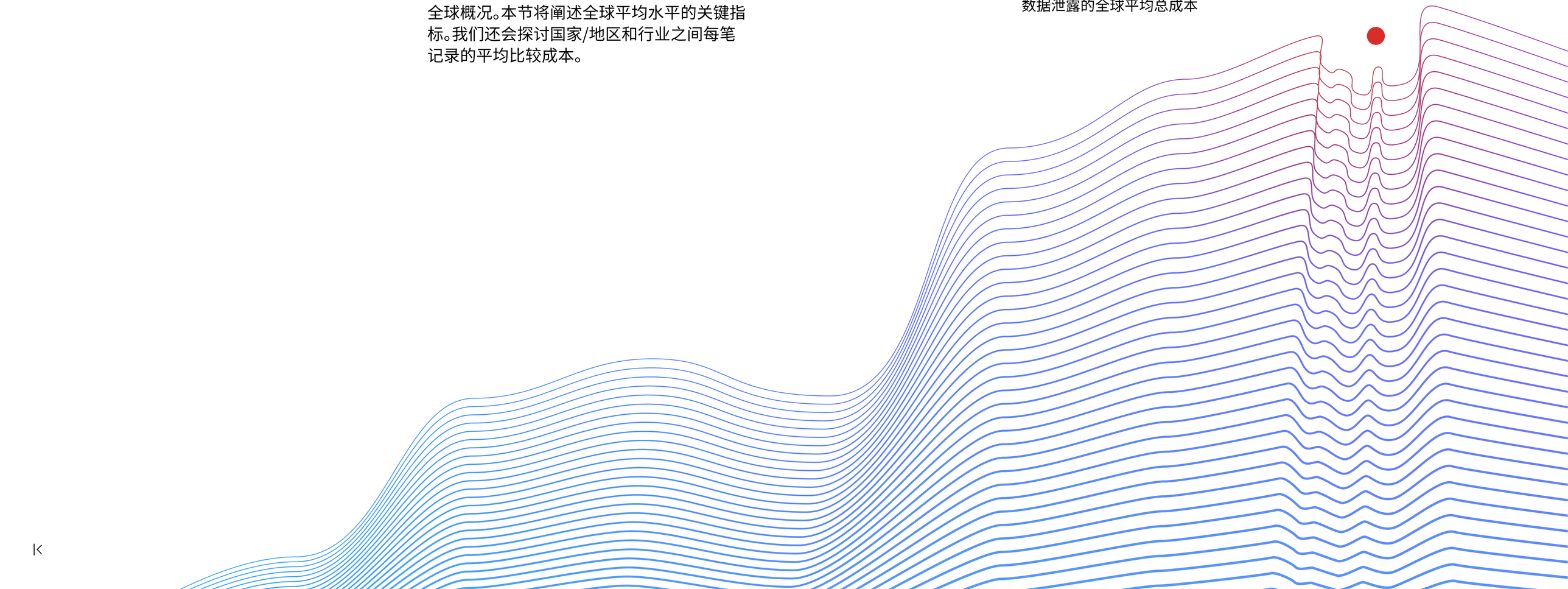


图 1：数据泄露的成本攀升至新高。
数据泄露的全球平均成本已上升至 445 万美元，比 2022 年增加了 10 万美元。相较于 2022 年的 435 万美元，平均成本增加了 2.3%。自 2020 年以来，数据泄露的平均总成本为 386 万美元，平均总成本增加了 15.3%。

图 2：数据泄露的每条记录成本也达到新高。
2023 年，数据泄露相关的每笔记录的平均成本为 165 美元，比 2022 年的平均成本 164 美元略有增加。这与 2021 年至 2022 年相对较小的增长相吻合，其中成本仅增长 3 美元。在过去七年中，每笔记录的平均成本最大增幅发生在 2020 年至 2021 年期间，平均成本从 146 美元上升到 161 美元，涨幅为 10.3%。这项研究调查了 2,200 至 102,000 笔记录规模不等的泄露情况。[1]

数据泄露的总成本

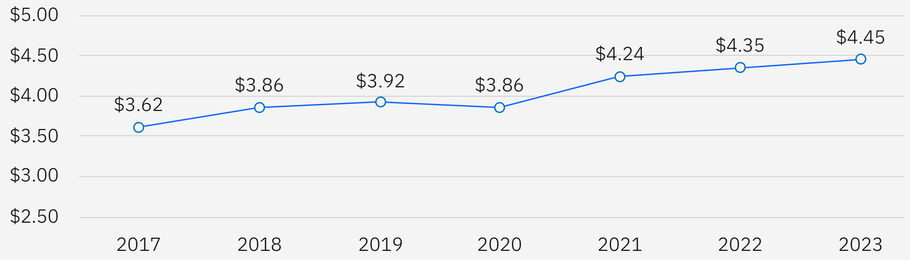


图 1：以百万美元为单位

数据泄露的每条记录成本

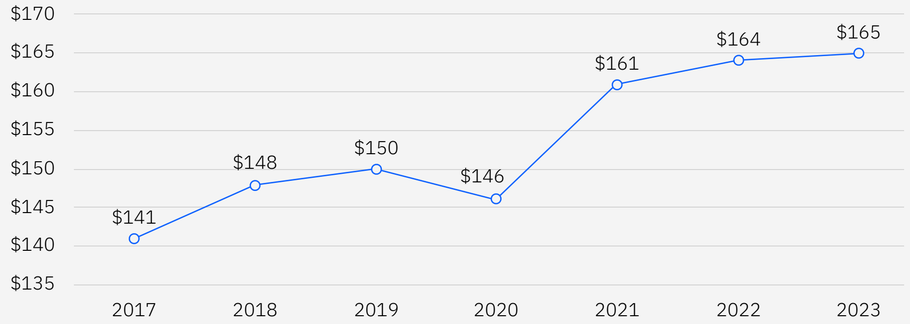


图 2：以美元为单位

图 3：美国连续 13 年成为数据泄露成本最高的国家。
数据泄露平均成本最高的前五个国家或地区与 2022 年相比发生了显著变化。

		2023 年	2022 年
1	↑	**美国** 948 万美元	**美国** 944 万美元
2	↑	**中东** 807 万美元	**中东** 746 万美元
3	↓	**加拿大** 513 万美元	**加拿大** 564 万美元
4	↓	**德国** 467 万美元	**英国** 505 万美元
5	↓	**日本** 452 万美元	**德国** 485 万美元

在今年的前五国家/地区名单中，日本是唯一不在 2022 年前五名单中的国家，去年排名第六。去年排名前 5 名的国家还包括英国 (UK)，其平均数据泄露成本为 505 万美元。今年，英国的平均成本大幅下降，为 421 万美元，比去年下降 16.6%，因此排在前五名之外。

美国再次成为数据泄露平均总成本最高的国家，为 948 万美元，比去年的 944 万美元增加了 0.4%。与去年相似，中东地区的数据泄露平均总成本位居第二，从 746 万美元增加到 807 万美元，增幅为 8.2%。

在加拿大，数据泄露的平均总成本从 564 万美元下降到 513 万美元，降幅为 9%。德国的平均成本也有所下降，从 485 万美元下降到 467 万美元，降幅为 3.7%。日本的平均成本略有下降，从 457 万美元下降到 452 万美元，降幅为 1.1%。

按国家或地区划分的数据泄露成本

图 3：以百万美元为单位

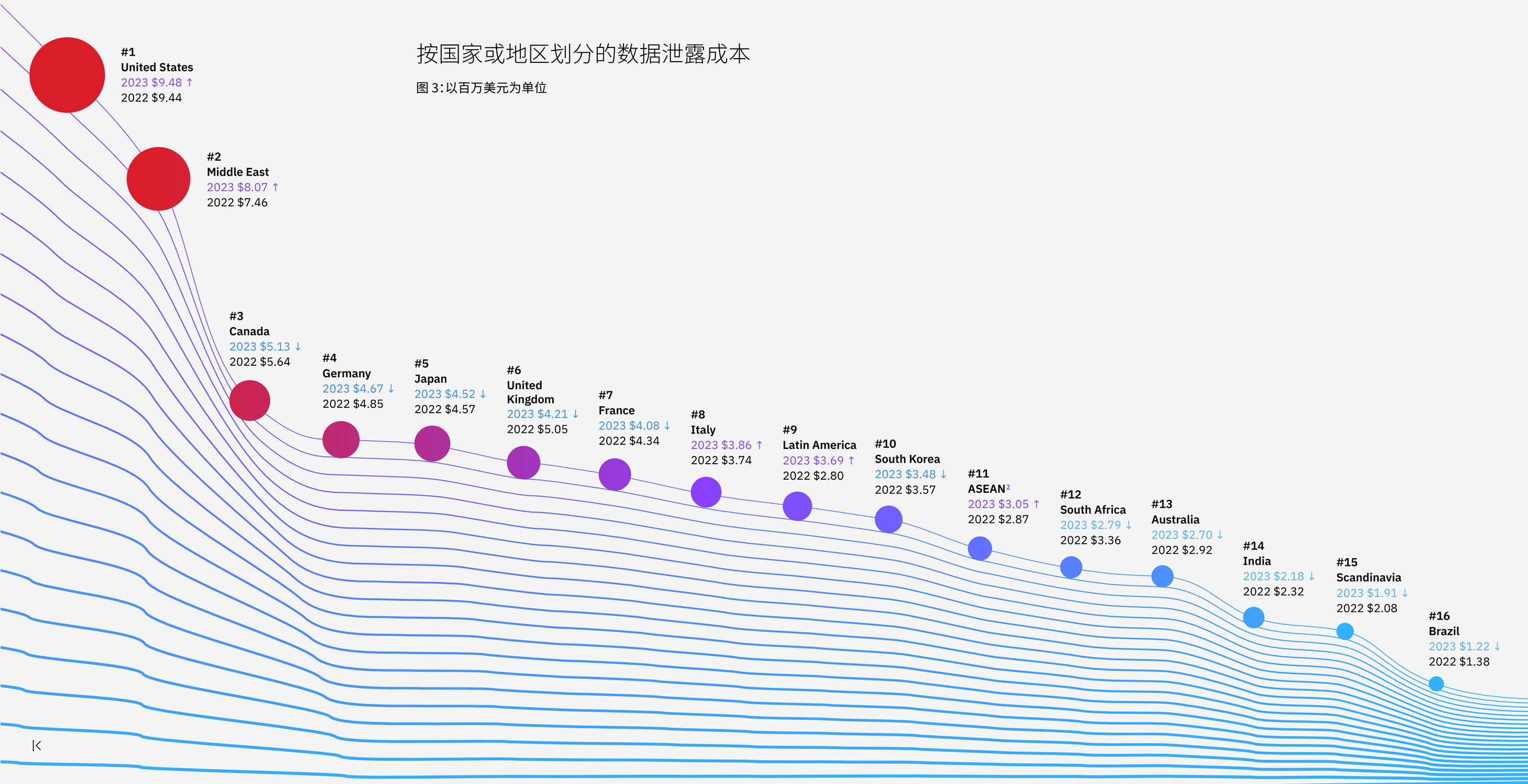


图 4：在各个行业中，医疗保健行业连续 13 年录得损失最高的数据泄露成本。
医疗保健行业的数据泄露成本仍为所有行业中最高，从 2022 年的 1,010 万美元增加到 2023 年的 1,093 万美元，增幅为 8.2%。在过去三年中，医疗保健领域数据泄露的平均成本增长 53.3%，与 2020 年的平均成本 713 万美元相比，增加 300 多万美元。医疗保健行业受监管程度很高，美国政府始终将之视为关键基础设施行业。自新冠疫情开始以来，该行业的平均数据泄露成本显著上升。

与去年的排名相比，成本最高的五大行业发生了一些变化。科技行业跌出前五名，而工业部门则递补上来，从第七位上升到第五位，增幅为 5.8%。根据 IBM 威胁情报分析，制造业成为网络犯罪分子最常攻击的行业。

		2023 年	2022 年
1	↑	**医疗行业** 1,093 万美元	**医疗行业** 1,010 万美元
2	↓	**金融** 590 万美元	**金融** 597 万美元
3	↓	**制药** 482 万美元	**制药** 501 万美元
4	↑	**能源** 478 万美元	**科技** 497 万美元
5	↑	**工业** 473 万美元	**能源** 472 万美元

按行业划分的数据泄露成本

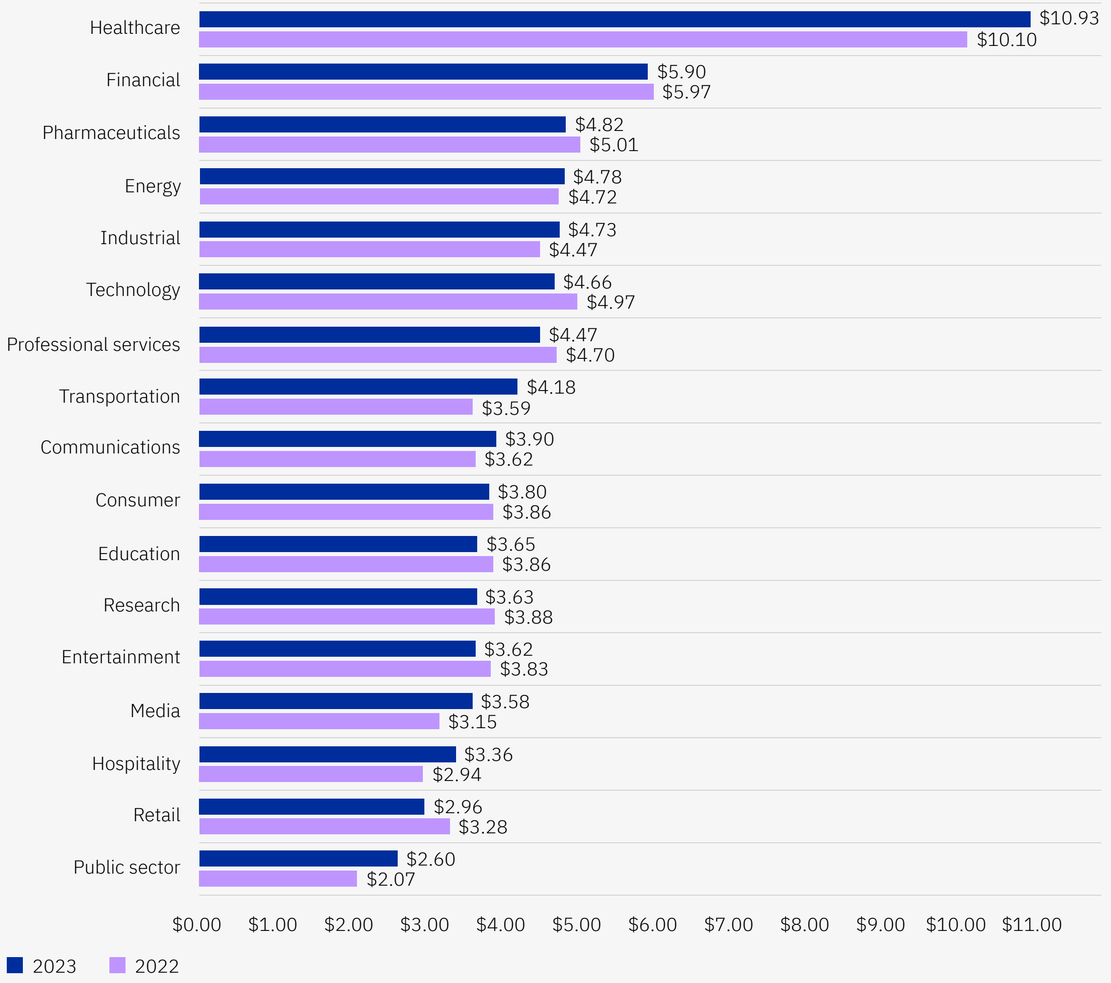


图 4：以百万美元为单位

图 5：识别和遏制泄露事件的平均时间大致相同。

与 2022 年相比，泄露事件的平均识别时间 (MTTI) 和平均遏制时间 (MTTC) 的变化微乎其微。平均识别时间是指组织识别安全泄露事件所需的时间。平均遏制时间是指识别安全泄露事件后解决所需的时间。

2022 年，各类组织需要 207 天才能识别泄露事件，而在 2023 年仅需 204 天。另一方面，组织在 2023 年平均需要 73 天来遏制泄露事件，而在 2022 年平均仅需 70 天。遏制和识别泄露事件的最长平均时间均发生在 2021 年，分别为 212 天和 75 天。

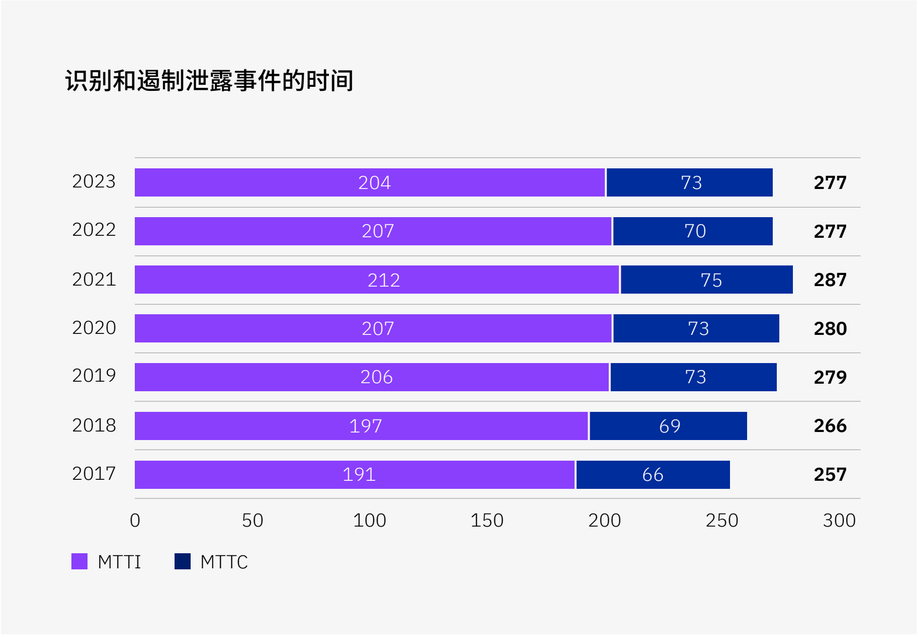


图 5：以天为单位

图 6：损失的业务成本达到五年来最低水平。
去年的报告显示，检测和上报成本上升为数据泄露费用中最昂贵的类别，这表明数据泄露调查正在转向用时更长、更为复杂的局面。今年这一趋势仍在继续，检测和上报成本仍然位居榜首，从 144 万美元上升到 158 万美元，差额 14 万美元，增幅为 9.7%。检测和上报成本包括支持公司合理检测漏洞的活动，并且可能包括取证和调查活动、评估和审计服务、危机管理以及高管和董事会沟通等。

数据泄露的其他关键成本部分（业务成本损失、泄露后响应和通知）与 2022 年相比也发生了变化。业务成本损失下降 8.5%，从 2022 年的 142 万美元下降到 2023 年的 130 万美元。业务成本损失包括系统停机造成的业务中断和收入损失、客户流失成本和获取新客户的成本以及声誉损失和商誉减少等活动。

值得注意的是，通知成本部分从 2022 年的 31 万美元上升到 2023 年的 37 万美元，增长 19.4%。泄露后响应成本仅增加了 20,000 美元。通知成本包括支持公司通知数据主体、数据保护监管机构和其他第三方的活动。

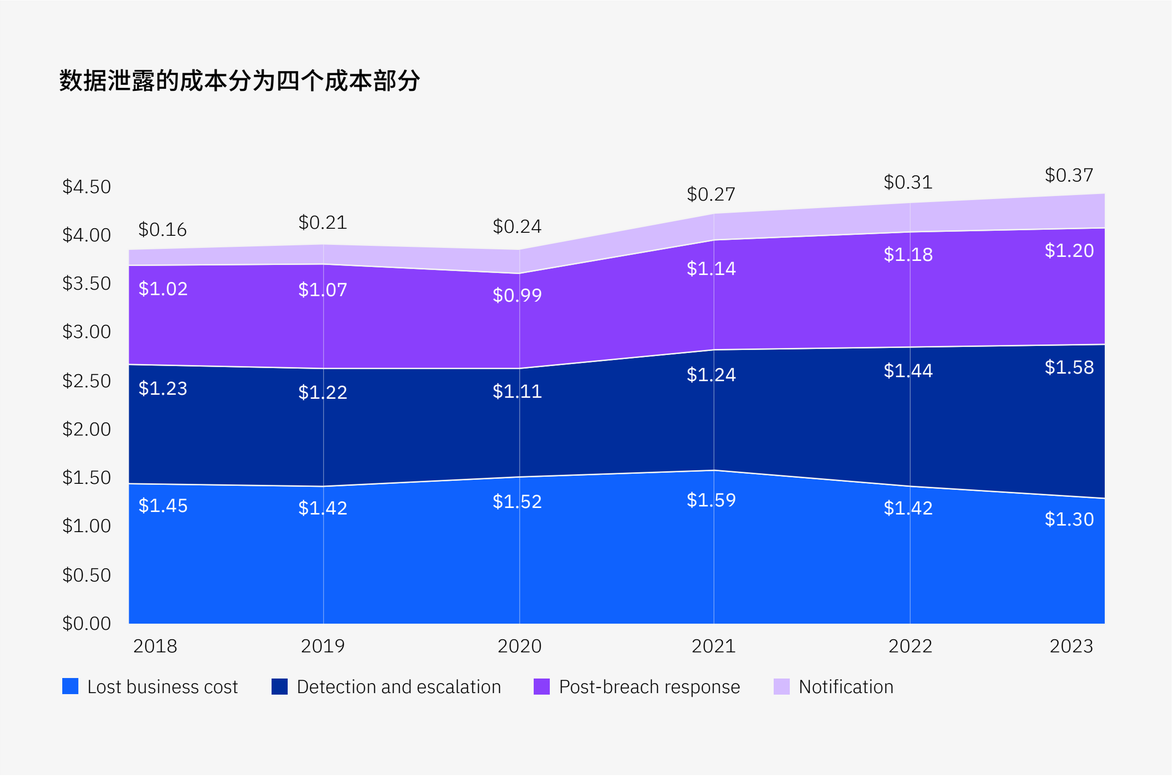


图 6：以百万美元为单位

图 7：与去年相比，规模较小的组织面临的数据泄露成本要高得多。
2023 年，拥有 5,000 名以上员工的组织的数据泄露平均成本较 2022 年有所下降。另一方面，员工人数不超过 5,000 名的公司的数据泄露平均成本显著增加。

员工人数少于 500 名的组织报告称，数据泄露事件的平均影响从 292 万美元增加到 331 万美元，增幅为 13.4%。员工人数为 500–1,000 名的组织从 271 万美元增加到 329 万美元，增幅为 21.4%。至于员工人数为 1,001–5,000 名的组织，数据泄露的平均成本从 406 万美元增加到 487 万美元，增幅近 20%。

在员工人数为 10,001–25,000 名的组织中，受访组织报告的平均成本为 546 万美元，比 2022 年的 556 万美元下降了 1.8%。员工人数超过 25,000 名的组织的平均成本从 2022 年的 556 万美元下降到 2023 年的 542 万美元，下降 14 万美元，降幅为 2.5%。

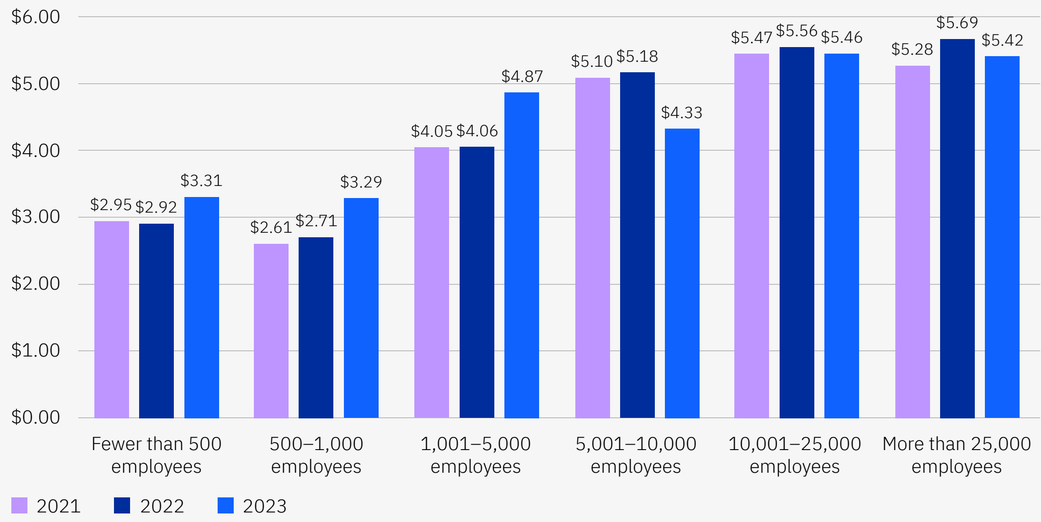


图 7：以百万美元为单位

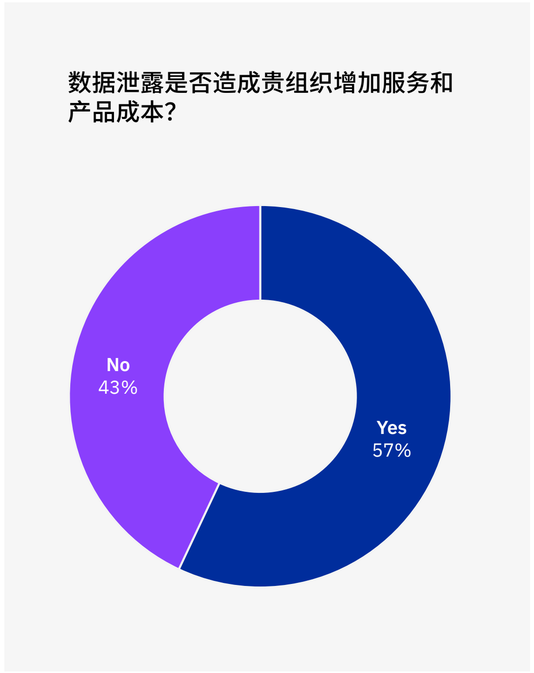


图 8:在已遭泄露组织总样本中所占份额

图 8:大多数组织会因数据泄露而继续提高服务和产品的价格。
大多数 (57%) 受访组织表示,数据泄露导致其业务产品定价上涨,将成本转移至消费者。这一发现与我们 2022 年的报告类似,其中 60% 的受访组织表示其提高了价格。

图 9a 和 9b：客户个人识别信息 (PII) 是成本最高、最常见的记录泄露事件。
在所有记录类型中，客户和员工个人识别信息 (PII) 的泄露成本最高。2023 年，客户 PII（如姓名和社会保障编号）每笔记录的成本为 183 美元，员工 PII 每笔记录的成本为 181 美元，紧随其后。泄露成本最低的记录类型是匿名客户数据，到 2023 年，组织每笔记录的成本为 138 美元。

与 2022 年和 2021 年的情况一样，客户 PII 是 2023 年最常遭受泄露的记录类型。52% 的泄露事件涉及某种形式的客户 PII。这比 2022 年增加了 5 个百分点，当时客户 PII 占所有泄露数据的 47%。第二最常见泄露的数据类型是员工 PII，占比为 40%。2021 年遭泄露的员工 PII 占所有泄露记录的 26%，自 2021 年以来，这一数值大幅增长。

自 2022 年以来，遭泄露的知识产权增长了三个百分点，而匿名（非 PII）数据比 2022 年下降了 7 个百分点，从 33% 下降到 26%。其他企业数据，如财务信息和客户名单，在遭泄露的数据中所占比例从 2022 年的 15% 上升到 2023 年的 21%。

遭泄露的数据类型

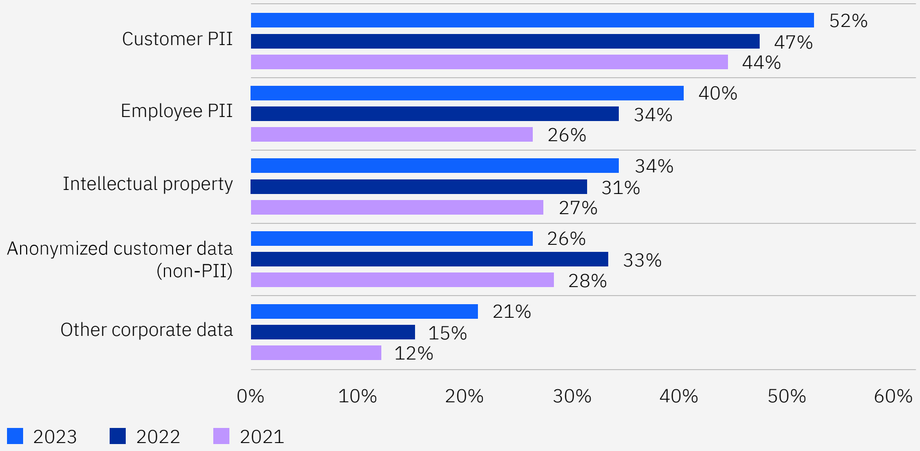


图 9a. 允许多个响应

按泄露记录类型划分的数据泄露对应的每条记录成本

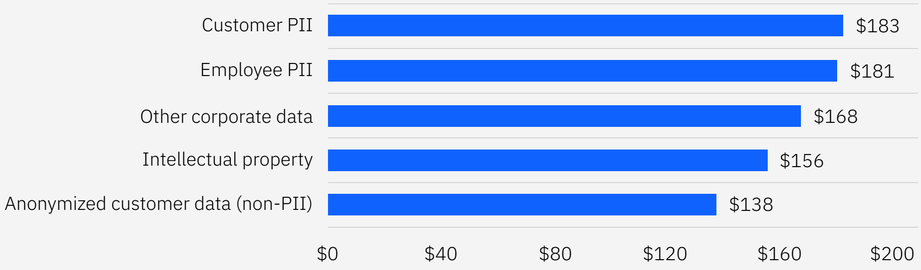
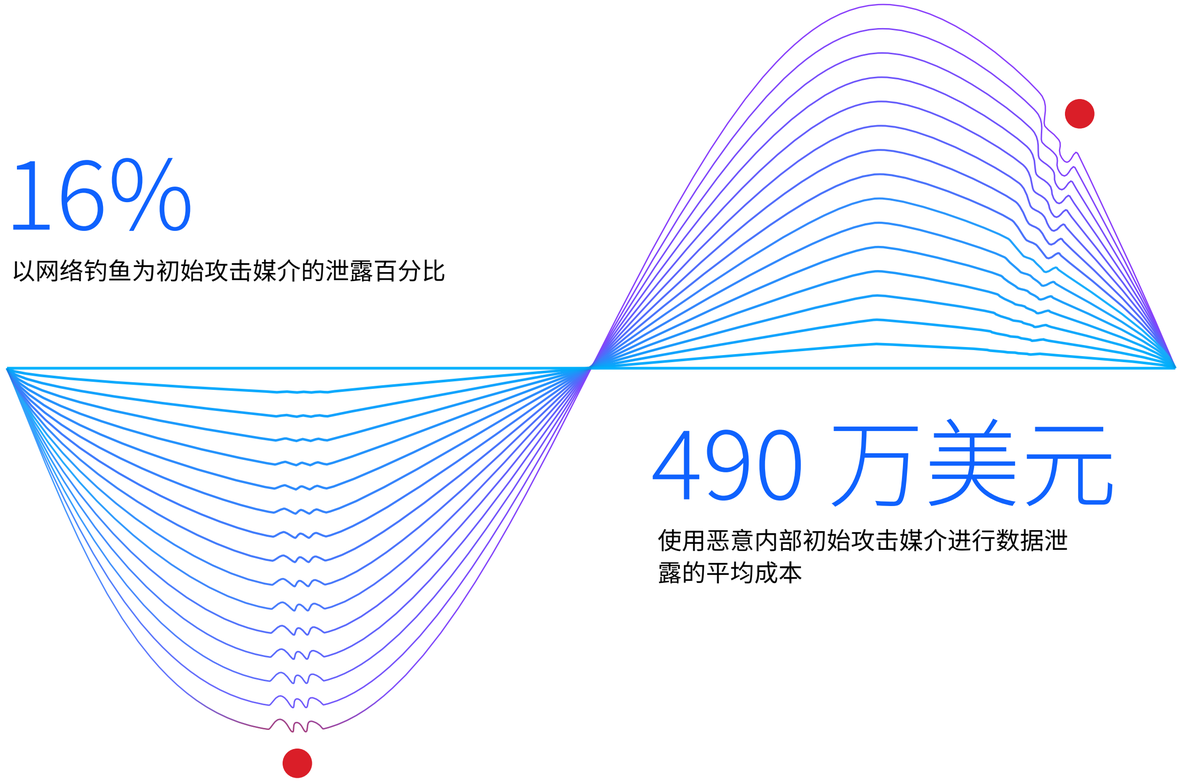


图 9b：以美元为单位

初始攻击媒介

本节探讨了研究中的数据泄露所采用的初始攻击媒介及其对泄露成本和时间线的影响。报告中确定了数据泄露的最常见根本原因，并比较了每个类别的平均泄露成本以及识别并遏制这些泄露的平均时间。网络钓鱼以及被盗或泄露的凭证是今年报告中最常见的两种攻击媒介，两者也都位居成本最高的四大事件类型之列。



16%

以网络钓鱼为初始攻击媒介的泄露百分比

490 万美元

使用恶意内部初始攻击媒介进行数据泄露的平均成本

图 10：网络钓鱼与凭证被盗或泄露是两种最常见的初始攻击媒介。
网络钓鱼与凭证失窃或泄露分别造成了 16% 和 15% 的数据外泄，网络钓鱼比凭证失窃略微靠前，成为 2022 年度报告中最常见的媒介。11% 的攻击所采用的初始媒介都属于云配置错误范畴，其次是企业电子邮件泄露，占 9%。今年，该报告首次审查了零日（未知）漏洞以及未修补的已知漏洞作为数据泄露的来源，并发现了所调研的数据泄露中有 5% 以上源于尚未修补的已知漏洞。

尽管由恶意内部人员发起攻击的概率相对较低（仅占 6%），但这类攻击造成的损失却是最高的，平均为 490 万美元，比每次数据泄露的全球平均成本 445 万美元高出 9.6%。网络钓鱼是最常见的攻击媒介，所造成的损失金额高居第二位，达 476 万美元。因系统错误造成的数据外泄所导致的损失最低，平均为 396 万美元，也是最不常见的，发生概率仅为 5%。

按初始攻击媒介划分的数据泄露成本和频率

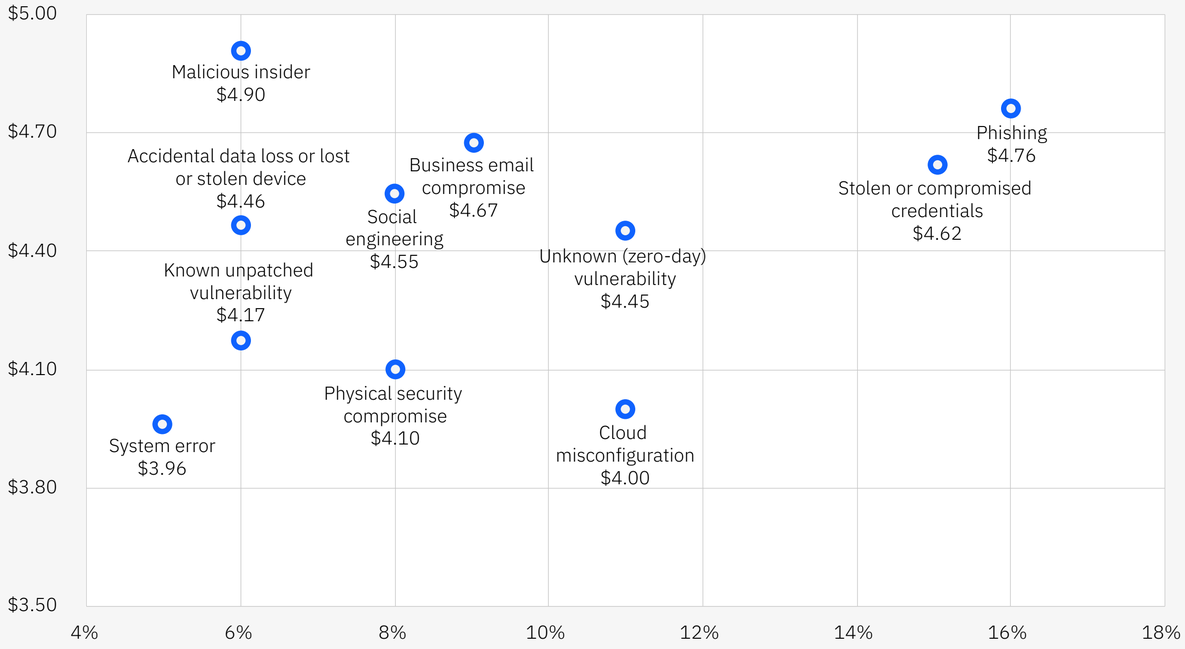


图 10：以百万美元为单位

图 11：因凭证失窃或泄露以及恶意内部人员引发的数据泄露解决起来最为耗时。
今年，识别和遏制因凭证失窃或泄露而导致的数据泄露事件平均耗费近 11 个月（328 天），而解决由恶意内部人员引发的数据泄露则耗费约 10 个月（308 天）。这两种媒介，以及网络钓鱼和商业电子邮件泄露，造成的损失最高。

相比之下，识别和遏制数据泄露的总体平均时间为 277 天或刚超过九个月。过去几年中，报告的这一数字一直保持相对稳定。

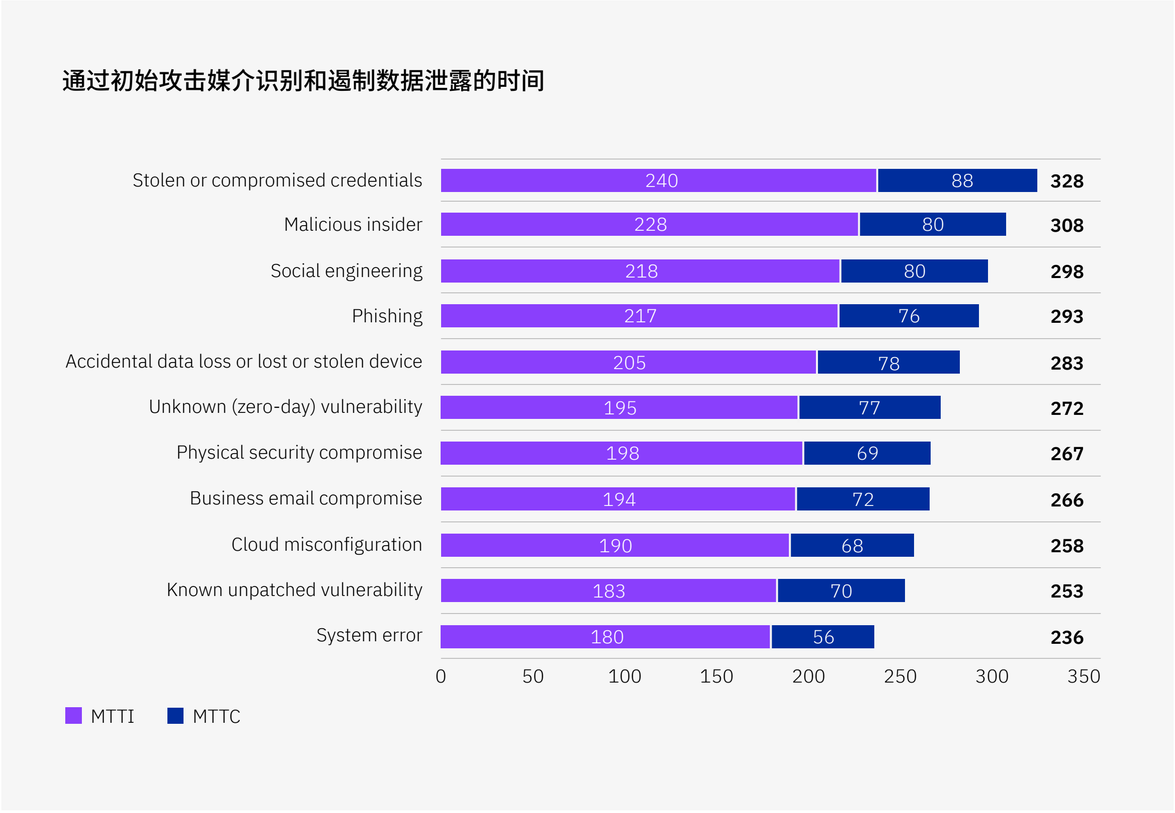
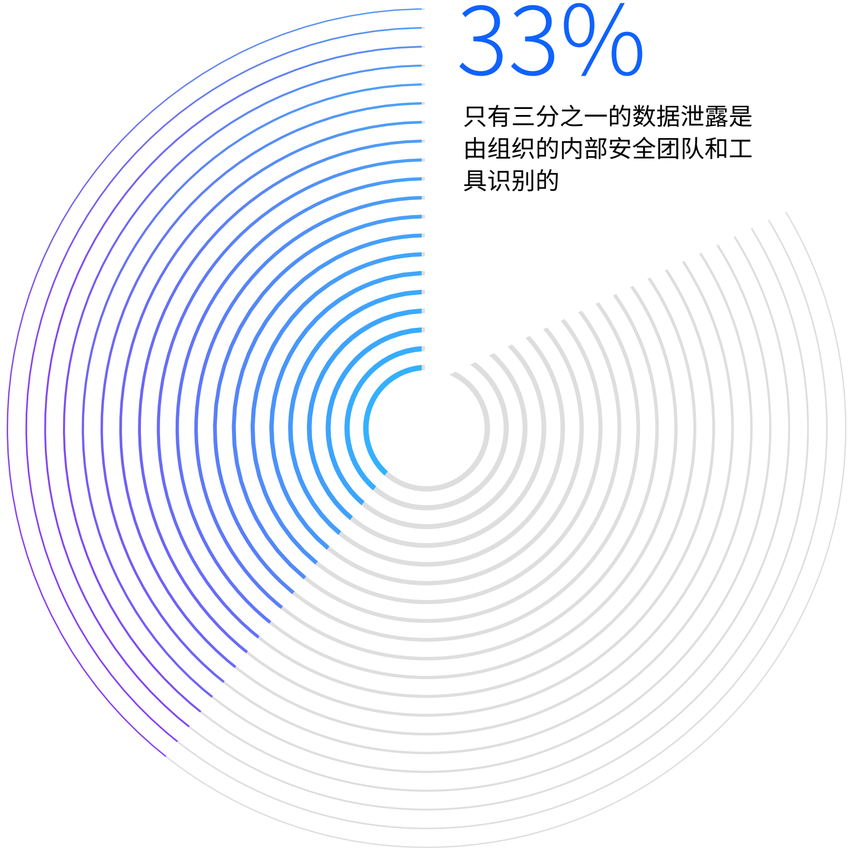


图 11：以天为单位

标识攻击

本节讨论了如何识别数据泄露以及不同的识别方法下成本和遏制时间的差异，这些分析都属于今年首次报告的内容。识别数据泄露的方式分为三类：由组织的内部安全团队和工具识别，包括托管安全服务提供商 (MSSP)；由善意友好的第三方（如安全研究人员或执法人员）识别；以及由攻击者披露（如勒索软件）。



33%

只有三分之一的数据泄露是由组织的内部安全团队和工具识别的

图 12：数据泄露通常由良好的第三方确定。
40% 的数据泄露是由善意友好的第三方或外部人员识别的，而 33% 的数据泄露是由内部团队和工具识别的。超过四分之一 (27%) 的数据泄露是攻击者在勒索软件攻击中披露的。

图 13：由攻击者披露的数据泄露（例如勒索软件）所造成的损失要高得多。
由攻击者披露的攻击造成的平均成本为 523 万美元，比通过内部安全团队或工具识别的数据泄露平均成本 430 万美元高出 19.5%（即 93 万美元）。此外，由攻击者披露的数据泄露造成的损失比 2023 年的平均数据泄露成本 445 万美元高出 16.1%（即 78 万美元）。由组织自己的安全团队和工具所识别的数据泄露的损失要低得多，比由攻击者披露的事件少了近 100 万美元。

如何识别数据泄露？

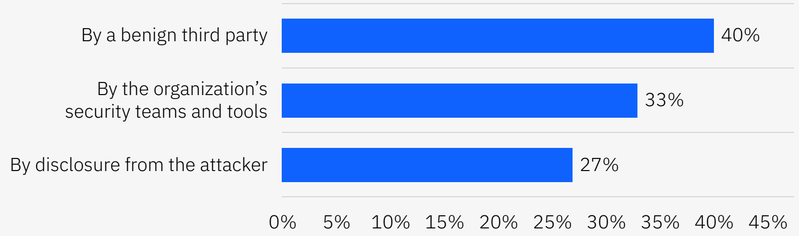


图 12：只允许单个响应

数据泄露的成本取决于数据泄露的识别方式

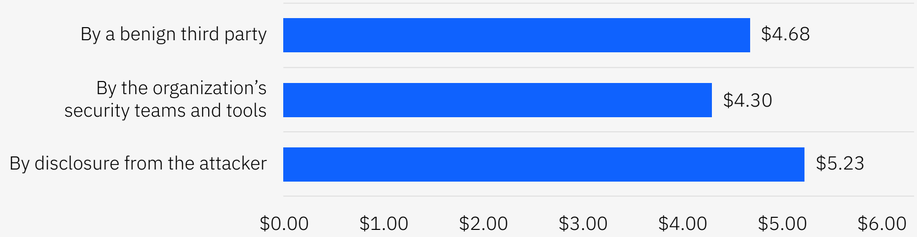


图 13：以百万美元为单位

图 14：识别和遏制由攻击者披露的数据泄露耗费的时间最长。
响应者平均需要耗费 320 天来识别和遏制由攻击者披露的数据泄露。与内部识别的数据泄露相比，这一时间又长了 80 天（即增加 28.2%），后者平均需要耗费 241 天才能进行识别和遏制。与善意友好的第三方识别的数据泄露相比，识别和遏制由攻击者披露的数据泄露的平均时间长了 47 天（即增加 15.9%）。

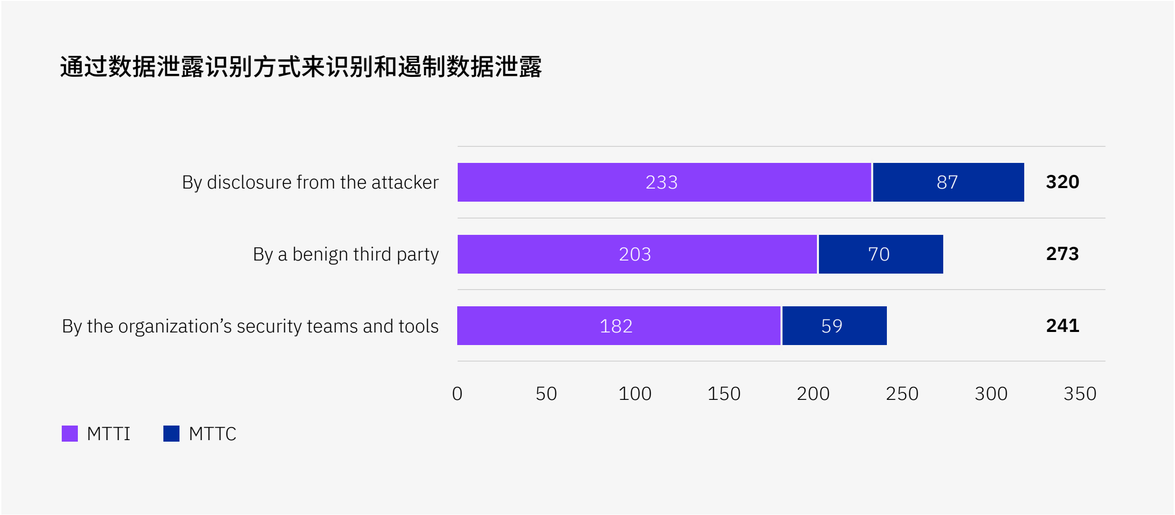


图 14：以天为单位

数据泄露生命周期

数据泄露生命周期定义为从最初发现漏洞直至遏制数据泄露所经过的时间。“识别时间”描述了其发现一个事件所需的天数。“遏制时间”是指组织解决这个情况并在检测到数据漏洞之后恢复服务所需的天数。这两个指标有助于确定组织事件响应 (IR) 和遏制过程的效率。

277 天

识别和遏制数据泄露的时间

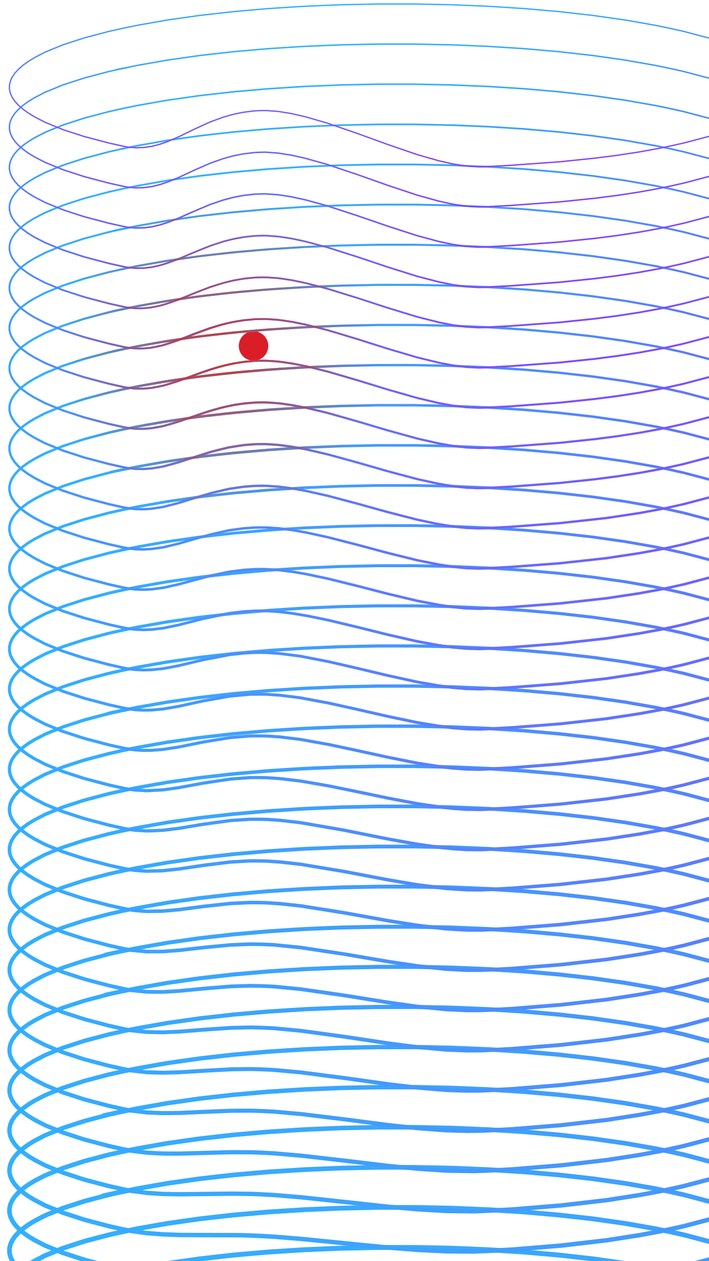


图 15：数据泄露生命周期越短，数据泄露成本越低。
生命周期少于 200 天的数据泄露造成的平均成本为 393 万美元，而生命周期超过 200 天的数据泄露造成的平均成本为 495 万美元。两者之间存在着 23% 的差异，相对较短的生命周期减少了 102 万美元的成本。

回顾前几年，基于生命周期为 200 天的数据泄露造成的平均成本虽然有所变化，但相对稳定。

对于生命周期少于 200 天的数据泄露，其 2023 年所造成的损失为 393 万美元，比上一年的平均成本 374 万美元增长了 5.1%。对于生命周期超过 200 天的数据泄露，其 2023 年所造成的损失为 495 万美元，比上一年的平均成本 486 万美元增长了 1.9%。2023 年报告的平均成本节约为 102 万美元，与 2022 年的成本节约金额 112 万美元相比，下降了 8.9%。

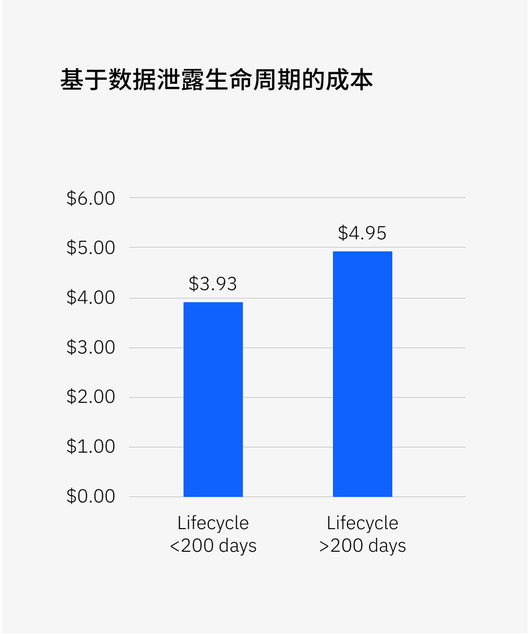


图 15：以百万美元为单位

关键成本因素

组织内部采用的安全技术和实践的类型是影响数据泄露平均成本的众多因素之一。本节量化了 27 个成本因素，以帮助安全和风险决策者了解这些因素在多大程度上会增加或降低成本。这些因素并不具备累加效应，因此，将多个成本因素相加来计算数据泄露的可能成本会与本研究方法有所不同。

今年，《数据泄露成本报告》考虑了几个新因素，包括供应链数据泄露、ASM 工具、数据安全和保护软件、端点检测和响应 (EDR) 工具、威胁情报、主动威胁追踪、IR 团队以及安全业务流程、自动化和响应 (SOAR) 工具等。

536 万美元

安全技能严重短缺的
组织产生的数据泄露平均成本

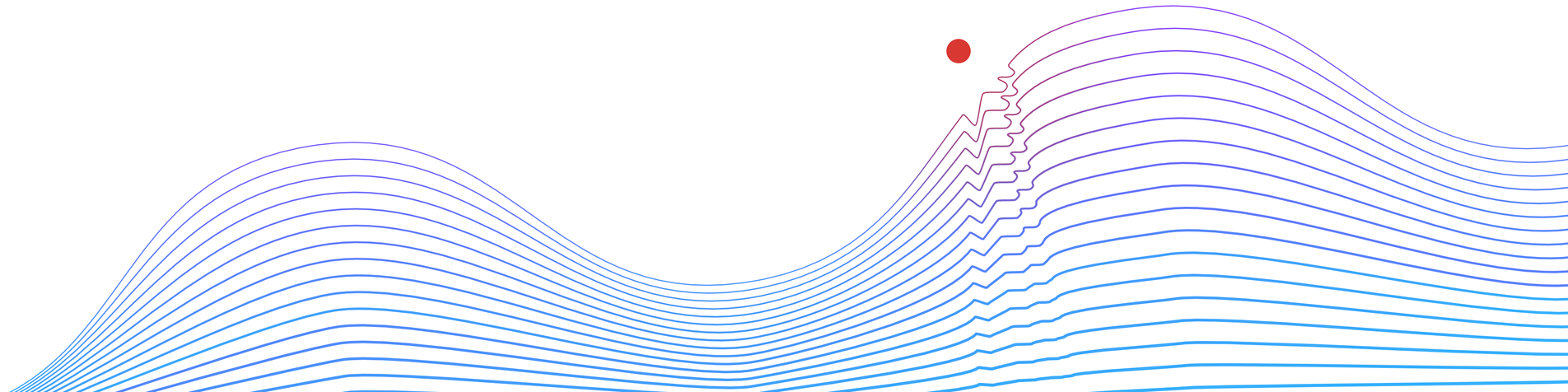


图 16：27 个因素对数据泄露平均成本的影响。
该图表展示了具备这些成本影响因素的组织的数据泄露平均成本与 445 万美元的数据泄露平均成本之差。成本降低因素描述了与数据泄露成本低于平均水平相关的因素，而成本增加因素则与高于平均水平的数据泄露成本有关。

最有效的三个成本降低因素（与最大程度降低成本相关的因素）分别是采用 DevSecOps 方法、员工培训以及 IR 规划和测试。例如，采用 DevSecOps 方法的组织发生数据泄露所造成的平均成本约为 420 万美元，比 2023 年的平均数据泄露成本（445 万美元）低 24.9 万美元。

最大的成本增加因素是安全系统的复杂性、安全技能短缺和不合规情形。例如，安全系统复杂的组织发生数据泄露所造成的平均成本约为 469 万美元，比 2023 年的平均数据泄露成本（445 万美元）高 24.1 万美元。

关键因素对数据泄露总成本的影响

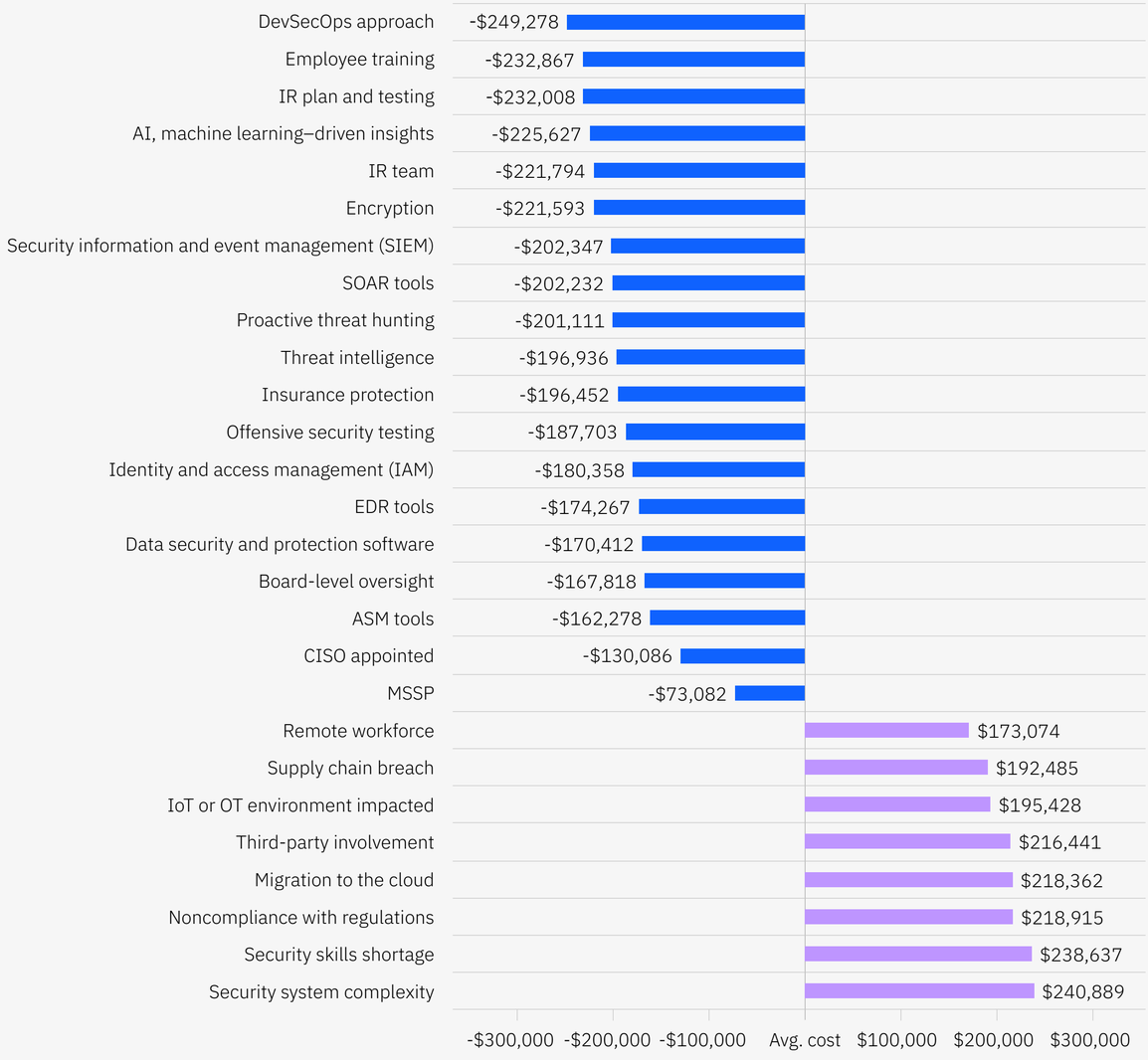


图 16：以美元为单位

图 17：27 个因素中最具影响力的三个成本增加因素。
此图表将具备最强成本增加因素的组织与具备最弱成本增加因素的组织进行了比较，在某些情况下，可能意味着没有相同因素的实例。这种比较不同于先前的分析（图 16），在先前的分析中，是将这些因素的大量存在所导致的成本增加与成本平均值进行比较。安全技能短缺程度高低之间存在 158 万美元（即 34.6%）的成本差异。安全系统复杂性程度高低之间存在 144 万美元（即 31.6%）的成本差异。不合规程度高低之间存在着 104 万美元（即 23%）的成本差异。

安全技能严重短缺的组织的平均成本为 536 万美元，比数据泄露的平均成本高出 91 万美元，增加 18.6%。安全系统复杂性高的组织的平均成本为 528 万美元，比数据泄露的平均成本高出 83 万美元，增加 17.1%。不合规程度较高的组织的平均成本为 505 万美元，比数据泄露的平均成本高出 56 万美元，增加 12.6%。

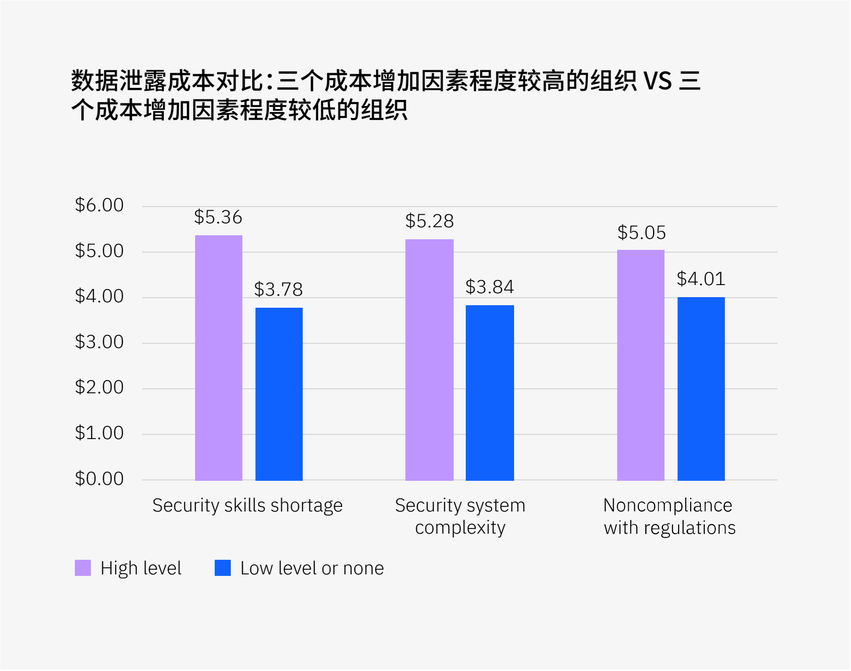


图 17：以百万美元为单位

图 18：在 27 个因素中，三个最具影响力的成本降低因素。
此图表将具备最强成本降低因素的组织与具备最弱成本降低因素的组织进行了比较，在某些情况下，可能意味着没有具备相同因素的实例。DevSecOps 方法采用程度高低不同，导致组织间数据泄露平均成本存在 168 万美元（即 38.4%）的差异。高采用率与几乎没有 IR 规划和测试之间相差 149 万美元（即 34.1%）。最后，员工培训程度高低之间相差 150 万美元（即 33.9%）成本。

成本降低因素较强的组织的数据泄露成本显著低于平均水平。DevSecOps 方法使用率高的采用者的平均成本为 354 万美元，比数据泄露的总体平均成本低 91 万美元（降低幅度为 22.8%）。DevSecOps 方法使用率低的组织的平均成本为 522 万美元，比数据泄露的平均成本明显高出 77 万美元（增加幅度为 15.9%）。

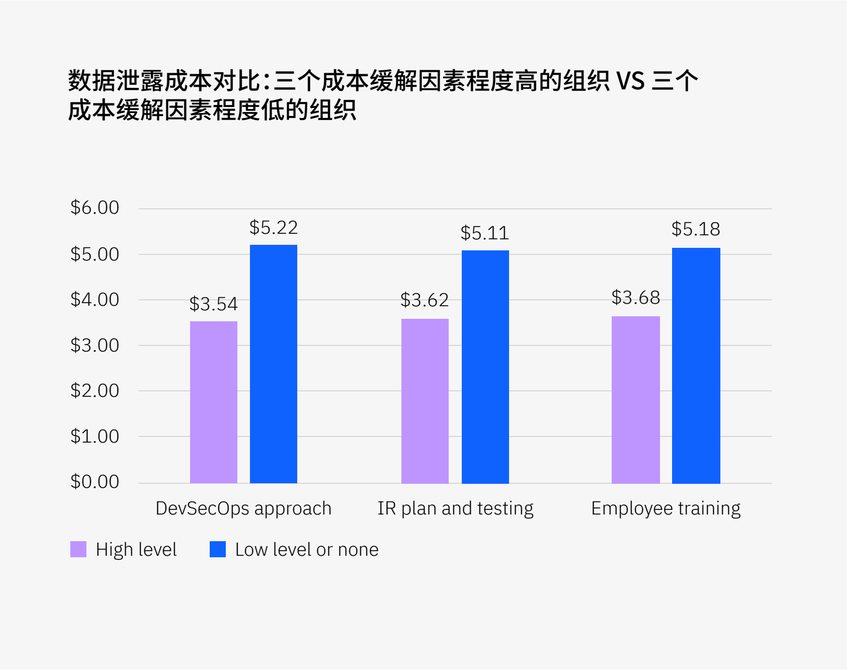
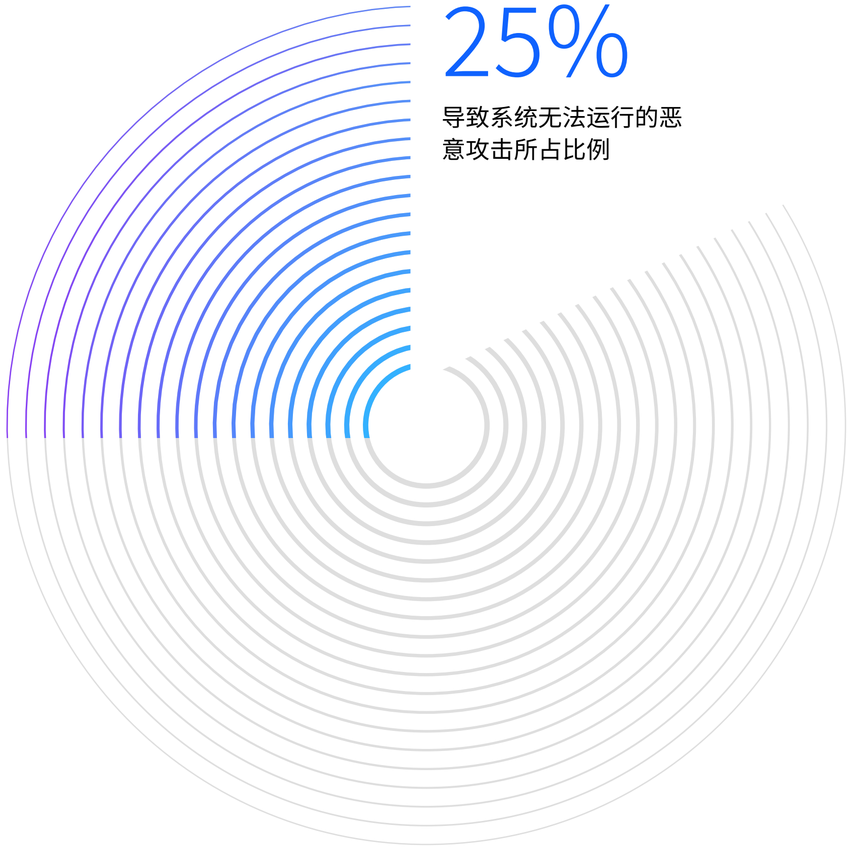


图 18：以百万美元为单位

勒索软件和破坏性攻击

今年，勒索软件和破坏性攻击[3]分别占恶意攻击的 24% 和 25%。

与 2022 年的报告一样，我们研究了此类泄露事件的生命周期，以及支付赎金与不支付赎金的影响对比。本研究在计算泄露总成本时不包括赎金成本。在 2023 年报告中，我们首次研究了执法部门参与遏制勒索软件攻击造成的影响。



25%

导致系统无法运行的恶意攻击所占比例

图 19：近四分之一的攻击涉及勒索软件。
每四次攻击中就有一次是导致系统无法运行的破坏性攻击，另有 24% 的攻击涉及勒索软件。业务合作伙伴和软件供应链攻击分别占攻击总数的 15% 和 12%。

图 20：勒索软件攻击成本显著增加。
2023 年报告中，勒索软件攻击的平均成本为 513 万美元，较 2022 年报告中的 454 万美元增加了 13%。2023 年报告中，破坏性攻击的平均成本为 524 万美元，也较 2022 年报告中的 512 万美元增加了 2.3%。

按恶意攻击类型划分的泄露总数所占比例

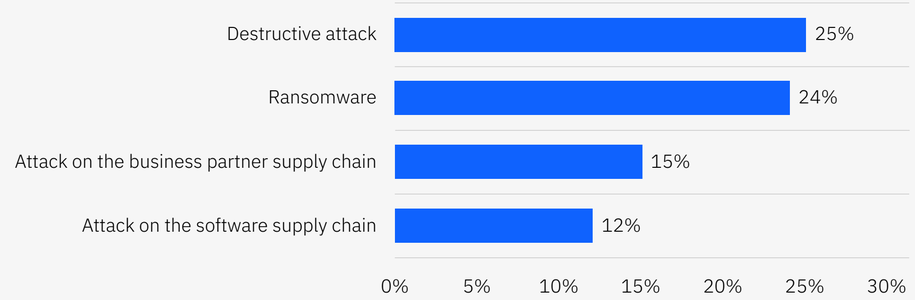


图 19：显示的每种攻击类型占泄露总数的百分比；条形统计总和不会达到 100%

勒索软件或破坏性攻击的成本

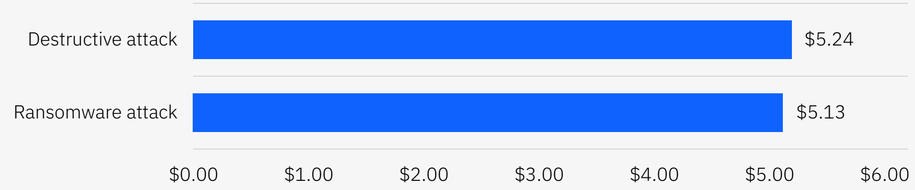


图 20：以百万美元为单位

图 21 和 22：涉及执法部门的组织节省了大量的时间和成本。
37% 的勒索软件受害者选择不让执法部门介入以便遏制勒索软件泄露事件，但选择介入的勒索软件泄露受害者总体上所经历的勒索软件泄露成本较低。不涉及执法部门时，勒索软件泄露的平均成本为 511 万美元；而涉及执法部门时，勒索软件泄露的平均成本为 464 万美元，相差 9.6%（即 47 万美元）。

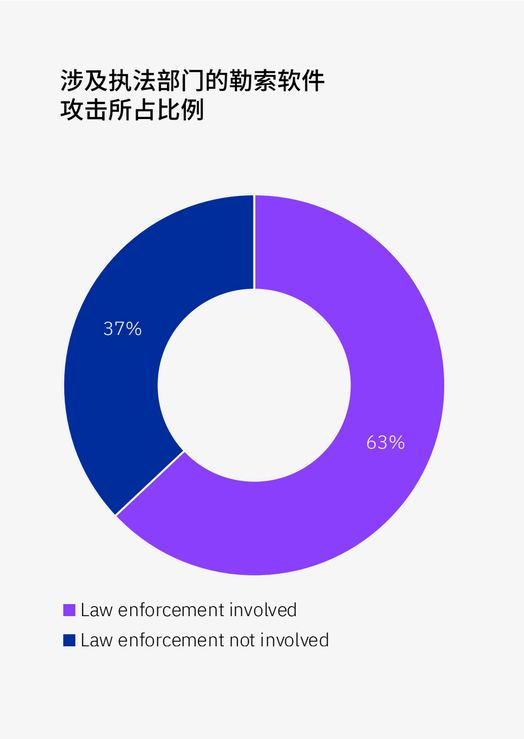


图 21：所有勒索软件攻击所占比例

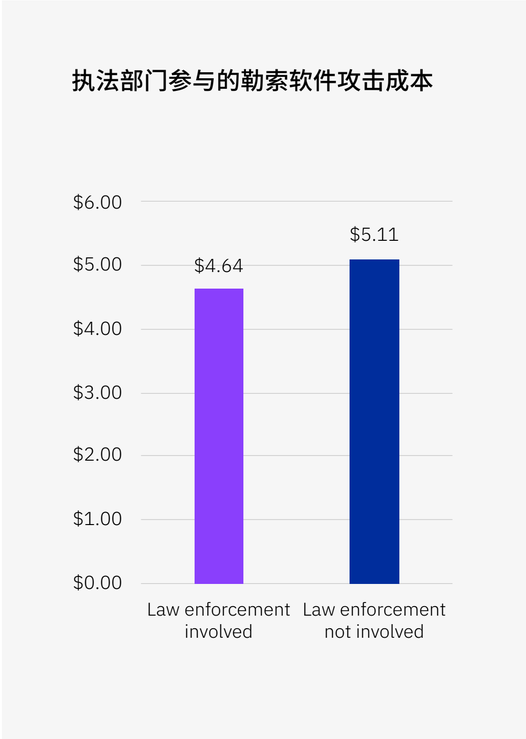


图 22：以百万美元为单位

图 23：执法部门帮助缩短了识别和遏制勒索软件漏洞的时间。
在执法部门的参与下，识别和遏制勒索软件泄露的总时间缩短了 11.4%（即 33 天），总时间为 273 天，而此前为 306 天。执法部门介入时，遏制勒索软件泄露的平均时间为 63 天，比执法部门未介入时的 80 天缩短了 23.8%。很明显，执法部门的参与可以帮助降低勒索软件泄露的成本和持续时间。

在执法部门参与下识别和遏制勒索软件攻击所需的时间

图 23：以天为单位

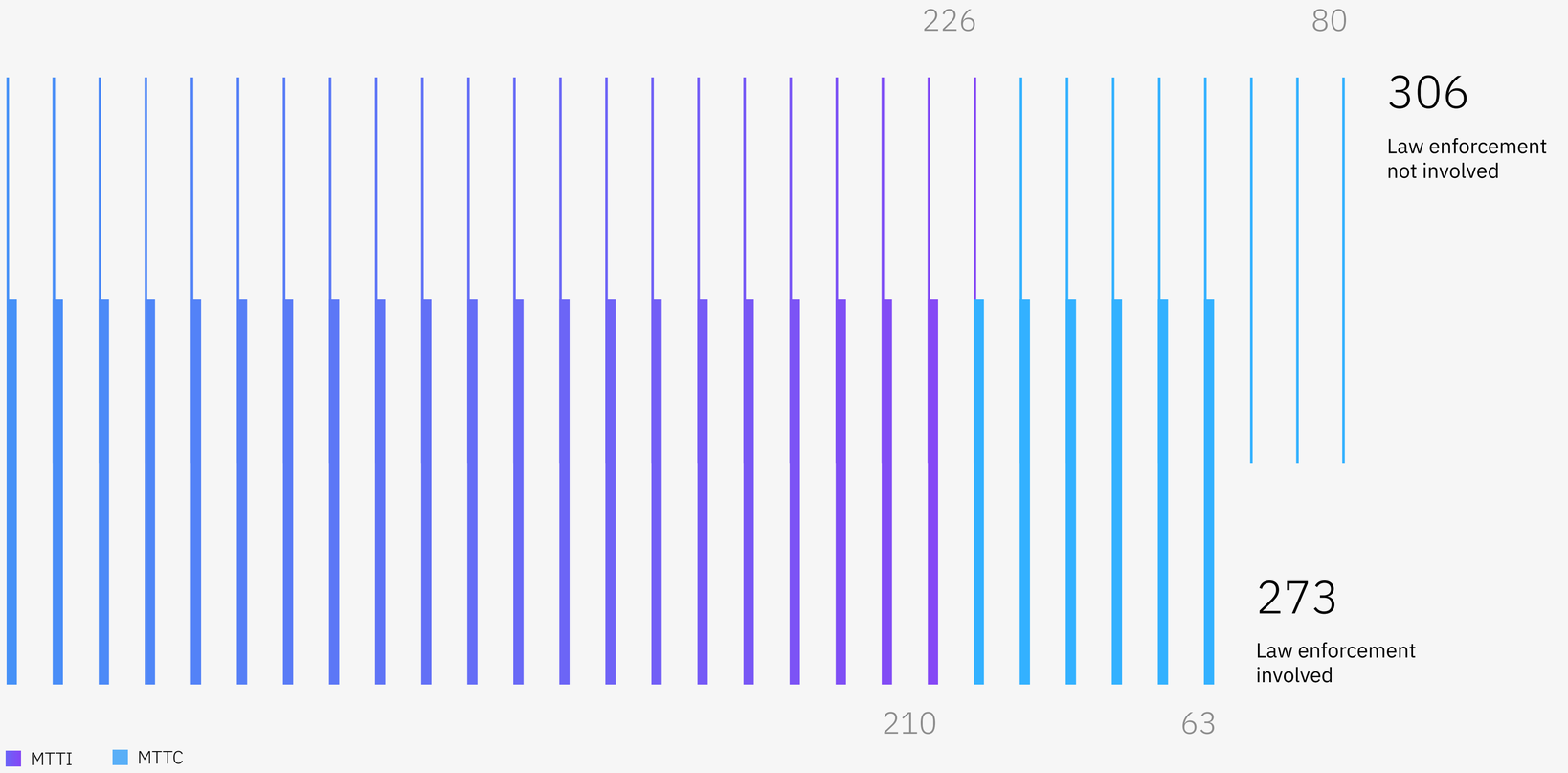


图 24：自动响应运行手册或工作流程可缩短遏制勒索软件漏洞的时间。
在经历过勒索软件攻击的组织中，那些拥有专门针对勒索软件攻击而设计的自动响应运行手册或工作流程的组织能够在 68 天之内遏制勒索软件攻击，比没有自动响应运行手册或工作流程的组织平均减少了 80 天，减少了 16%。

图 25：支付赎金只能实现最低程度的成本节约。
在勒索软件攻击期间支付赎金的组织的总成本为 506 万美元，与 517 万美元的成本相比，仅相差 11 万美元 (2.2%)。但是，此计算不包括赎金本身的成本。鉴于大多数勒索软件要求支付的成本很高，支付赎金的组织最终的总支出可能超过未支付赎金的组织。在 2022 年的报告中，总成本节约为 630,000 美元，总成本差异为 13.1%，同样，不包括赎金本身的成本。数据显示，总体而言，支付赎金的优势越来越小，与 2022 年至 2023 年的报告相比，节省的费用减少了 82.5%。

勒索软件自动响应运行手册或工作流程对遏制勒索软件泄露事件的影响

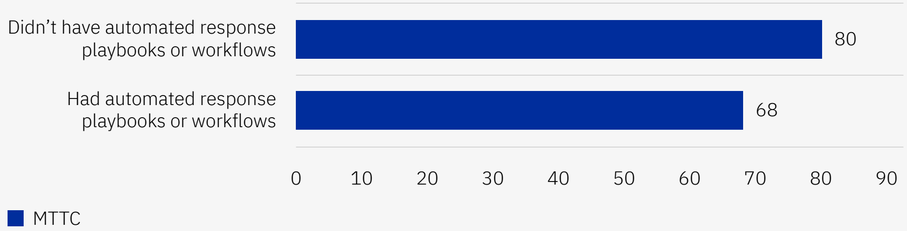


图 24：以天为单位

基于是否支付赎金的勒索软件攻击成本

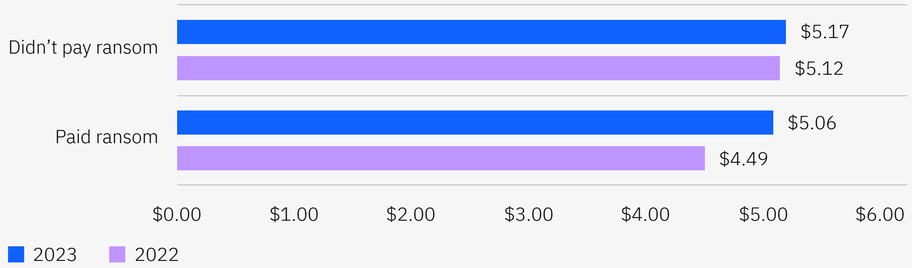


图 25：以百万美元为单位（不包括赎金成本）

业务合作伙伴供应链攻击

业务合作伙伴供应链泄露是源于对业务合作伙伴的攻击而产生的一种数据泄露。在今年的研究中，15% 的组织认为供应链泄露是数据泄露的根源。

图 26 和图 27：与其他泄露类型相比，业务合作伙伴供应链泄露的成本高出 11.8%，识别和遏制时间要长 12.8%。
业务合作伙伴供应链入侵造成的数据泄露成本平均为 476 万美元，比其他原因造成的数据泄露平均成本（423 万美元）高出 53 万美元（即 11.8%）。

组织平均需要 233 天来识别业务合作伙伴供应链入侵，并且需要 74 天来遏制业务合作伙伴供应链入侵，总生命周期为 307 天。该平均生命周期比其他原因造成的数据泄露的平均生命周期（270 天）长 37 天（即 12.8%）。

由于业务合作伙伴供应链入侵而导致的数据泄露成本

图 26：以百万美元为单位

根据业务合作伙伴出现的供应链数据泄露事件，来识别和遏制数据泄露所需的时间

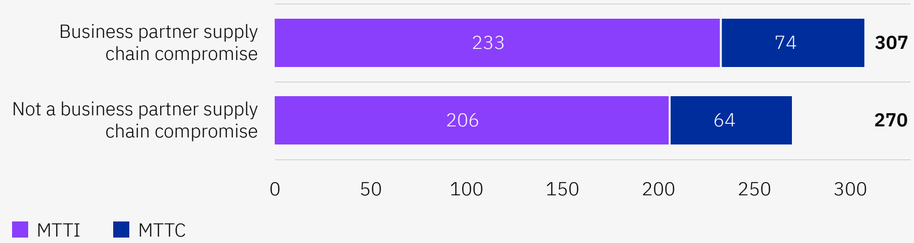
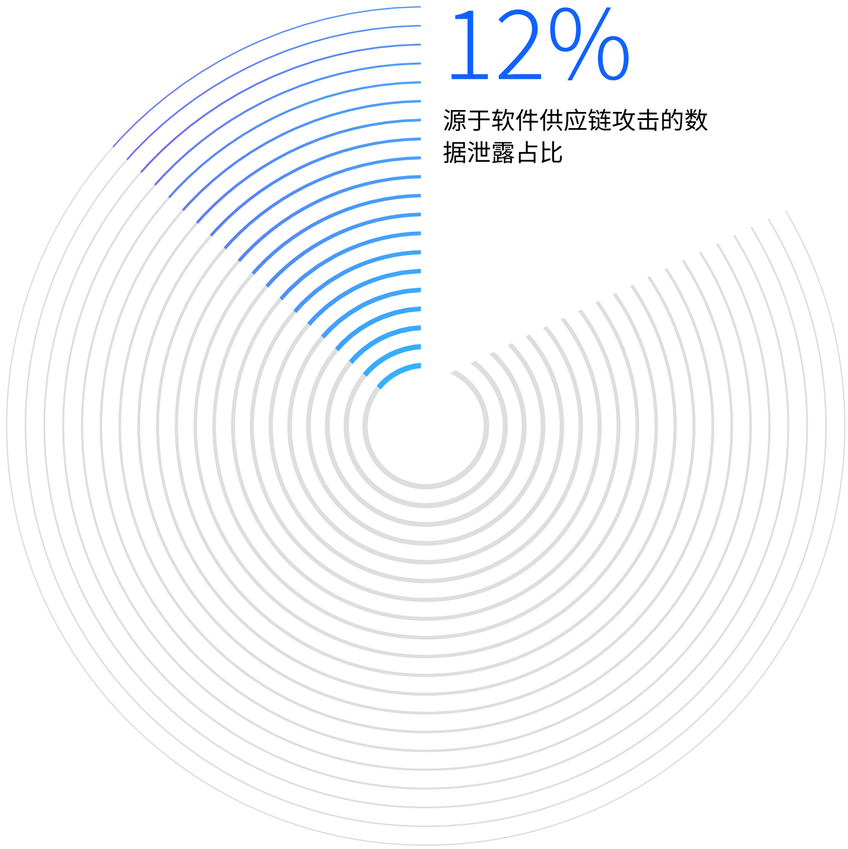


图 27：以天为单位

软件供应链攻击

今年，该研究还首次研究了源自软件供应链攻击的入侵事件。在这种攻击中，攻击者入侵软件供应商的网络并部署恶意代码，企图侵入软件，然后再将其发送给客户。遭受入侵的软件会攻击客户的数据或系统。在今年的研究中，12% 的组织认为软件供应链是数据泄露的根源。



12%

源于软件供应链攻击的数据泄露占比

图 28 和图 29：与其他泄露类型相比，软件供应链泄露的成本高出 8.3%，识别和遏制时间长 8.9%。

软件供应链入侵造成的数据泄露成本平均为 463 万美元，比其他原因造成的数据泄露平均成本（426 万美元）高出 37 万美元（即 8.3%）。与其他原因造成的数据泄露（269 天）相比，软件供应链入侵造成的数据泄露的生命周期（294 天）长 8.9%。

尽管源自软件供应链内部的供应链泄露比源自业务合作伙伴的供应链泄露成本更低，但两者仍比平均数据泄露成本更高且耗时更长。

根据软件供应链泄露的发生计算的数据泄露成本

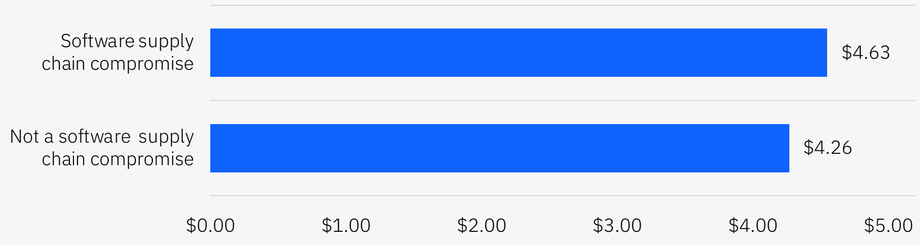


图 28：以百万美元为单位

根据软件供应链泄露的发生情况，来识别和遏制数据泄露所需的时间

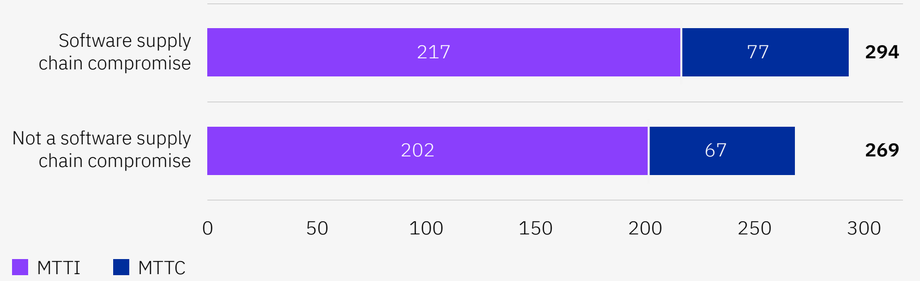


图 29：以天为单位

法规环境

研究探讨了数据监管程度对数据泄露成本的影响。在数据监管水平较高的环境中，58% 的成本在第一年后持续增加。在低监管环境中，64% 的泄露相关成本更有可能在第一年内得到解决。

数据泄露的成本往往会随着泄露发生后的时间推移而变化。在识别和遏制泄露以及恢复或修复遭受入侵的数据时，泄露的每个阶段都可能会产生不同的成本。

250,000 美元

经历过数据泄露的组织中有 20% 已支付该金额或更昂贵的罚款

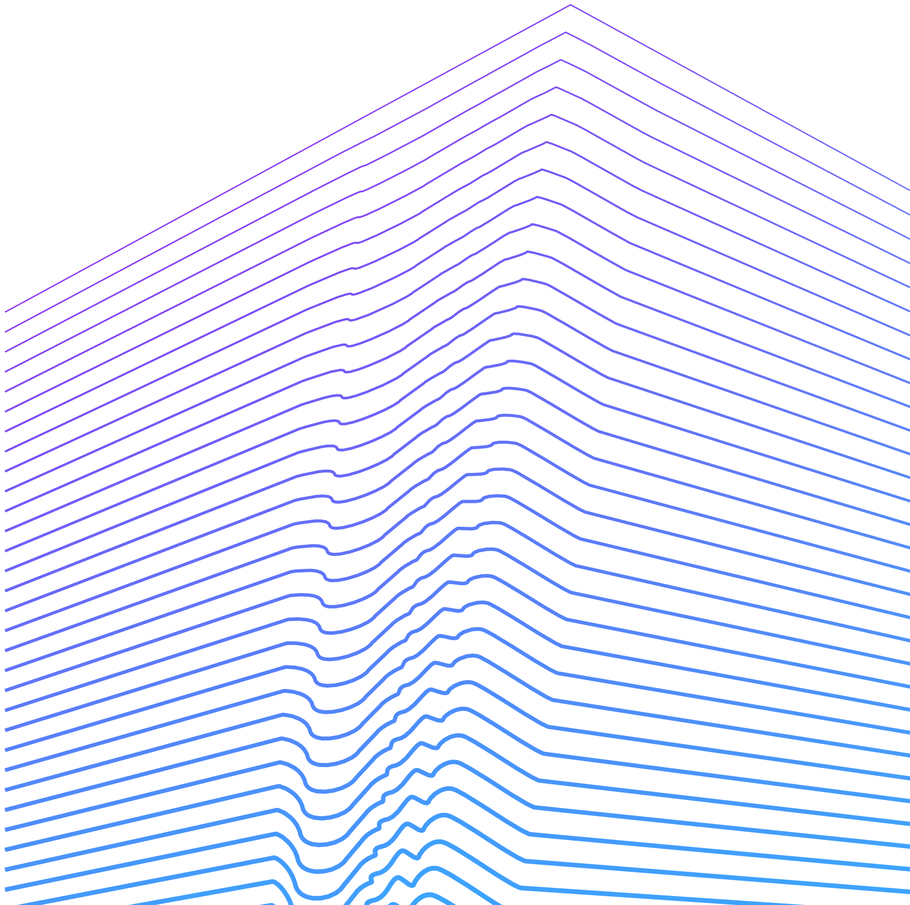


图 30a 和图 30b：在高数据监管环境中识别数据泄露超过两年后，成本达到峰值。
处于低监管环境中的组织在第一年就支付了将近三分之二的数据泄露成本，而处于监管严格环境中的组织在第一年支付的数据泄露成本不到一半。低监管环境中的数据泄露成本在 6–9 个月的时间范围内达到峰值，占总成本的 21%。监管严格环境中的数据泄露成本在两年后达到峰值，占总成本的 21%。在低监管环境中，大部分数据泄露成本会在早期飙升，并随着时间的推移而逐渐减少。在监管严格环境中，识别泄露事件发生两年后，成本出现波动并持续上升。

低数据监管环境与高数据监管环境下的数据泄露成本随时间的分布情况

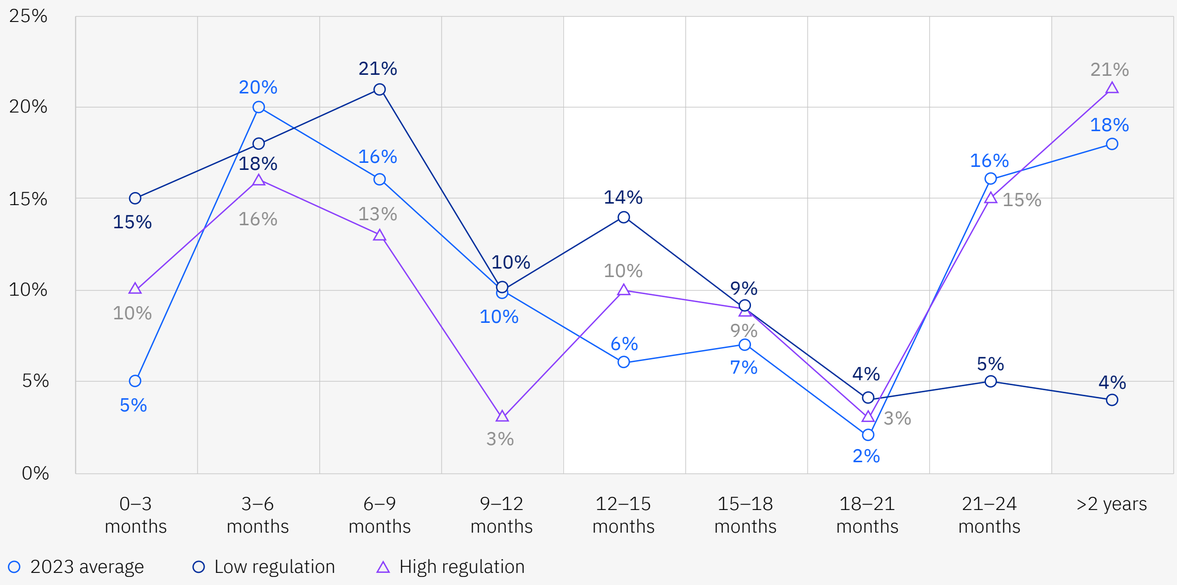


图 30a：在三个月时间间隔内累积的总成本百分比

低数据监管环境与高数据监管环境中每年数据泄露成本的分布

泄露后已用时间	占总成本的百分比		
	2023 年平均值	低监管	高监管
第一年	51%	64%	42%
第二年	31%	32%	37%
超过两年	18%	4%	21%

图 30b：占历年总成本的百分比

关键基础架构行业与其他行业的数据泄露平均成本对比

图 31：以百万美元为单位

图 31：关键基础架构行业的数据泄露成本超过 500 万美元。
关键基础设施组织包括金融服务、工业、科技、能源、运输、通信、医疗保健、教育以及公共部门等行业的企业和机构。这些组织的数据泄露成本比其他行业组织的平均成本（378 万美元）高出 126 万美元，相差 28.6%。这 504 万美元的成本还反映出，与 2022 年报告的关键基础设施行业的数据泄露平均成本 482 万美元相比费用增加了 4.6%。

图 32 和图 33：三分之一偏弱的组织因数据泄露而遭受罚款，其中 80% 的罚款金额为 25 万美元或以下。
在所研究的组织中，31% 的组织因数据泄露而遭受罚款，其中只有 20% 的罚款超过 25 万美元。在 2023 年的报告中，金额为 25 万美元的罚款占数据泄露平均总成本的 5.6%。

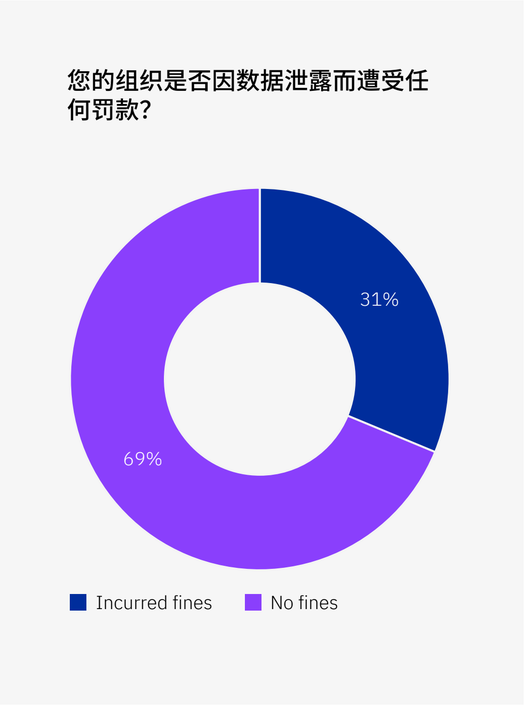


图 32：所有组织的占比

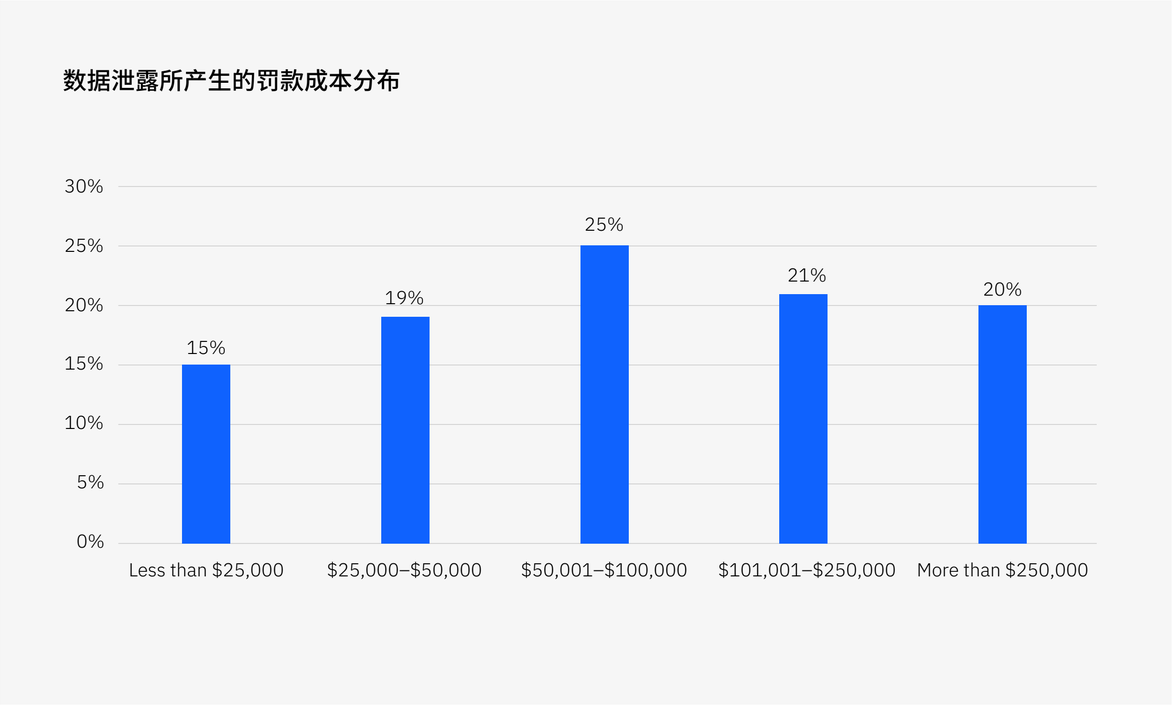
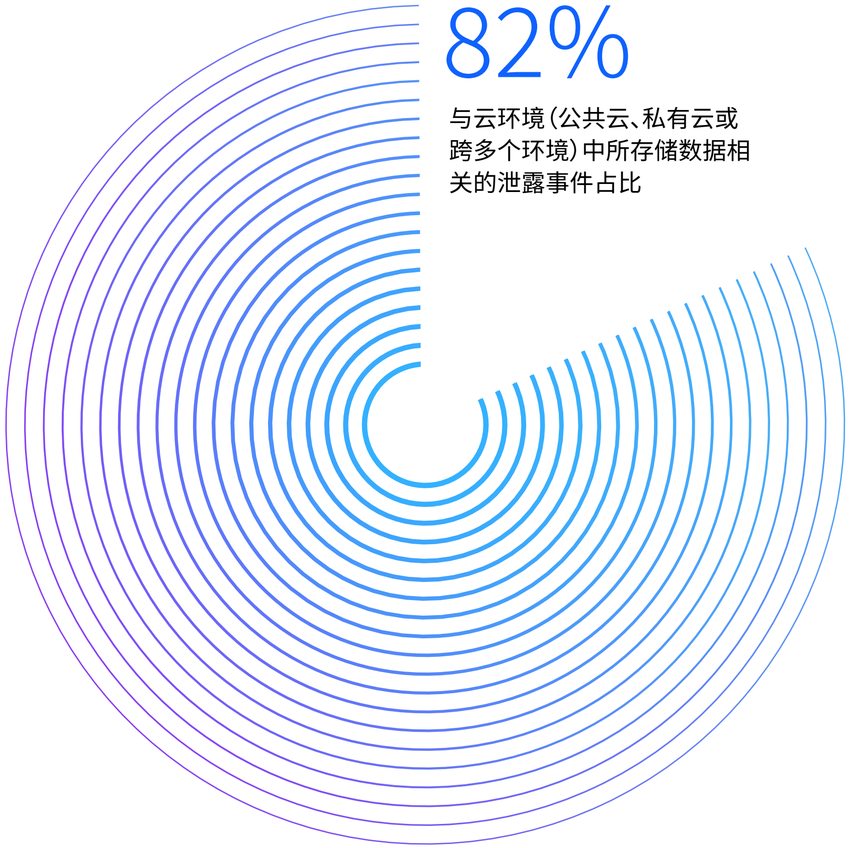


图 33：在遭受罚款的组织中（以美元为单位）

云泄露

数据泄露的成本和持续时间因数据存储位置而异。最常见的是，所研究的泄露事件包括跨越多个环境（包括云环境和本地环境）的数据，而此类泄露事件还导致了更高的成本以及需要更长的时间来识别和遏制数据泄露。



82%

与云环境（公共云、私有云或跨多个环境）中所存储数据相关的泄露事件占比

图 34：泄露事件对跨多个环境存储的数据造成影响最多。
其中与跨多个环境所存储数据相关的泄露事件比例最大，为 39%，其次是公共云中所存储数据相关的泄露事件，占比为 27%。跨多个环境发生的泄露数量超过了仅在私有云或本地环境中发生的泄露总数的 34%。

图 35：公共云和多个环境中的数据泄露成本更高。
在 2023 年的报告中，跨多个环境的数据泄露成本达到 475 万美元，在所分析环境中成本最高，比私有云环境中数据泄露成本（所分析环境中泄露成本最低，为 398 万美元）高出 17.6%。跨多个环境的数据泄露成本也比数据泄露的平均成本（445 万美元）高出 6.5%。

遭受泄露的数据通常存储在哪里？

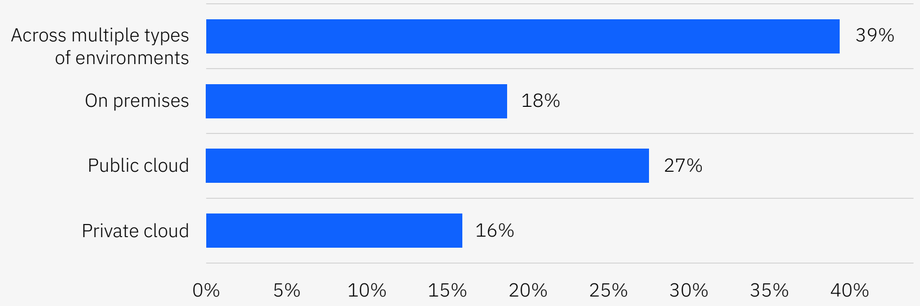


图 34：所有泄露事件的占比

按已泄露数据的存储位置划分的数据泄露成本

图 35：以百万美元为单位

图 36：使用公共云和多个环境也是导致数据泄露生命周期延长的因素。
与跨多个环境数据存储相关的识别和遏制泄露事件所需时间最长，为 291 天。此时间间隔比识别和遏制泄露事件的最短时间（在私有云环境中为 235 天）多了 56 天（即增加 21.3%）。另外值得注意的是，使用多个环境是唯一超过 2023 年报告的识别和遏制数据泄露平均时间（277 天）的模式，二者之间差值为 14 天（即相差 4.9%）。

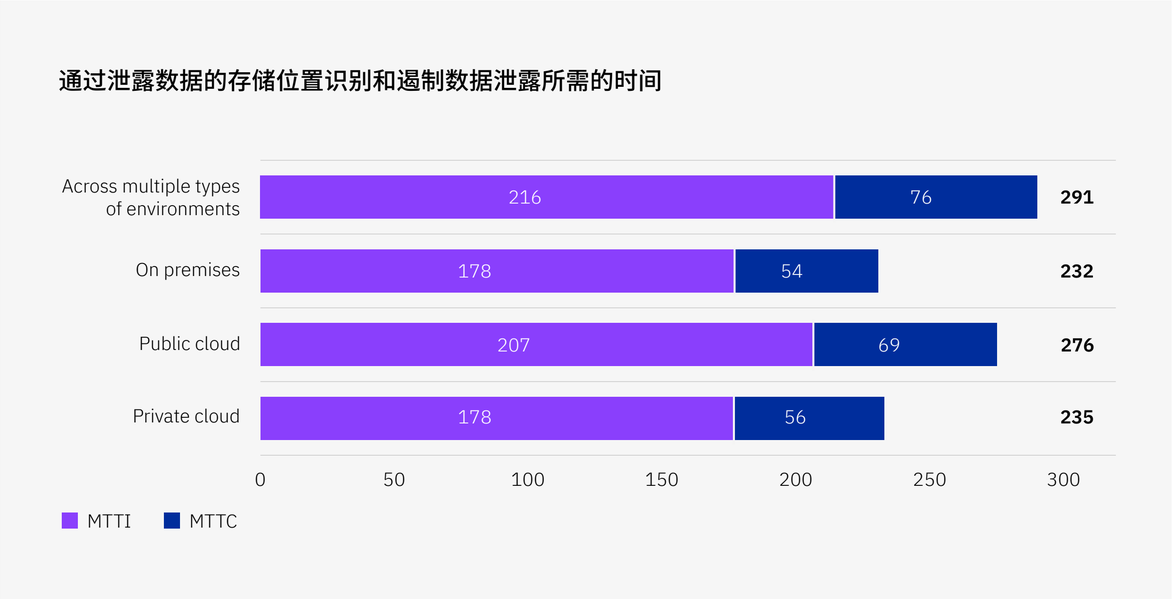
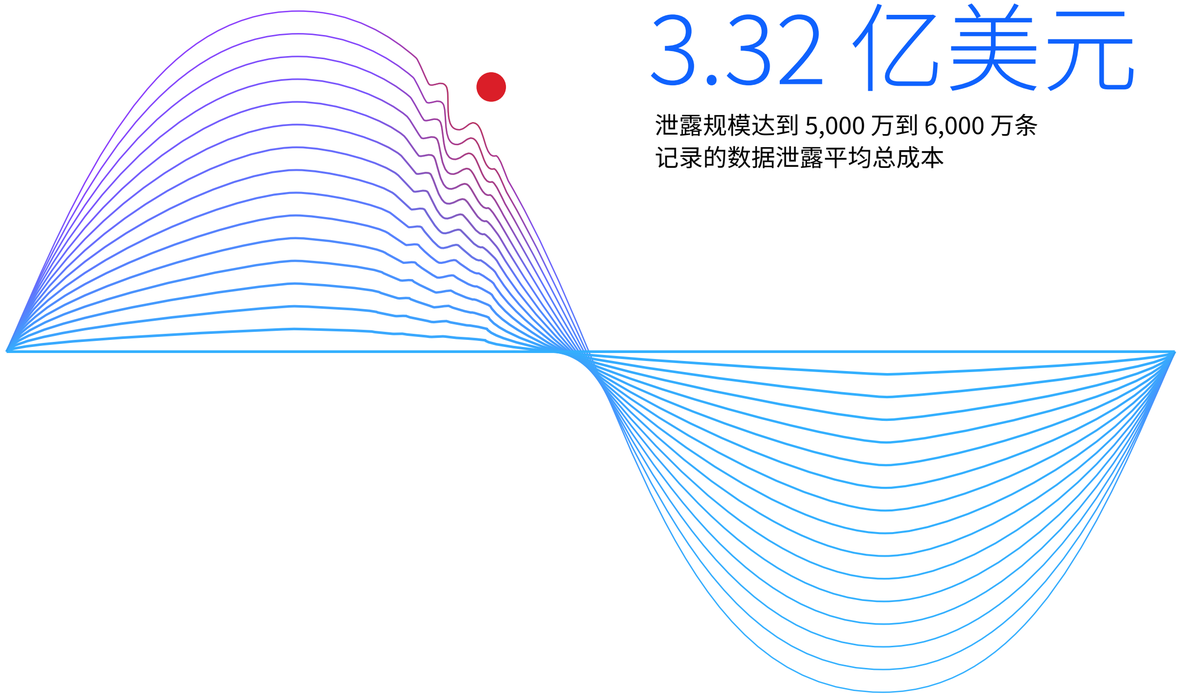


图 36：以天为单位

大规模泄露

以超过百万条受损记录为特征的大规模泄露事件相对罕见。但是，由于其规模庞大，此类事件可能会产生深远的影响。

今年的研究包括 20 个组织，这些组织因数据泄露而遭受了 100 万至 6,000 万条记录的丢失或被盗。该研究采用一种独特的方法来检查这些大规模泄露，将其与该研究的其他 553 起泄露事件分开考虑，每起泄露事件包括不超过 101,200 条丢失或受损的记录。有关研究方法的完整说明，请参阅本报告末尾的数据泄露常见问题解答。



3.32 亿美元

泄露规模达到 5,000 万到 6,000 万条记录的数据泄露平均总成本

图 37：在 2023 年的报告中，大规模泄露的成本有所下降。
在所有数据泄露规模群组中，大规模数据泄露的平均成本都有不同程度的下降。降幅最高的是 100 万至 1,000 万条记录群组，从 2022 年报告中的 4,900 万美元下降到 2023 年报告中的 3,600 万美元，降幅达 26.5%。降幅最小的是 3,000 万至 4,000 万条记录群组，从 2022 年报告中的 3.16 亿美元下降到 2023 年报告中的 3.04 亿美元，降幅达 3.8%。在 5,000 万至 6,000 万条记录群组中，2022 年报告的成本为 3.87 亿美元，减少了 5,500 万美元（即 14.2%），与 2023 年报告的 3.32 亿美元相当。

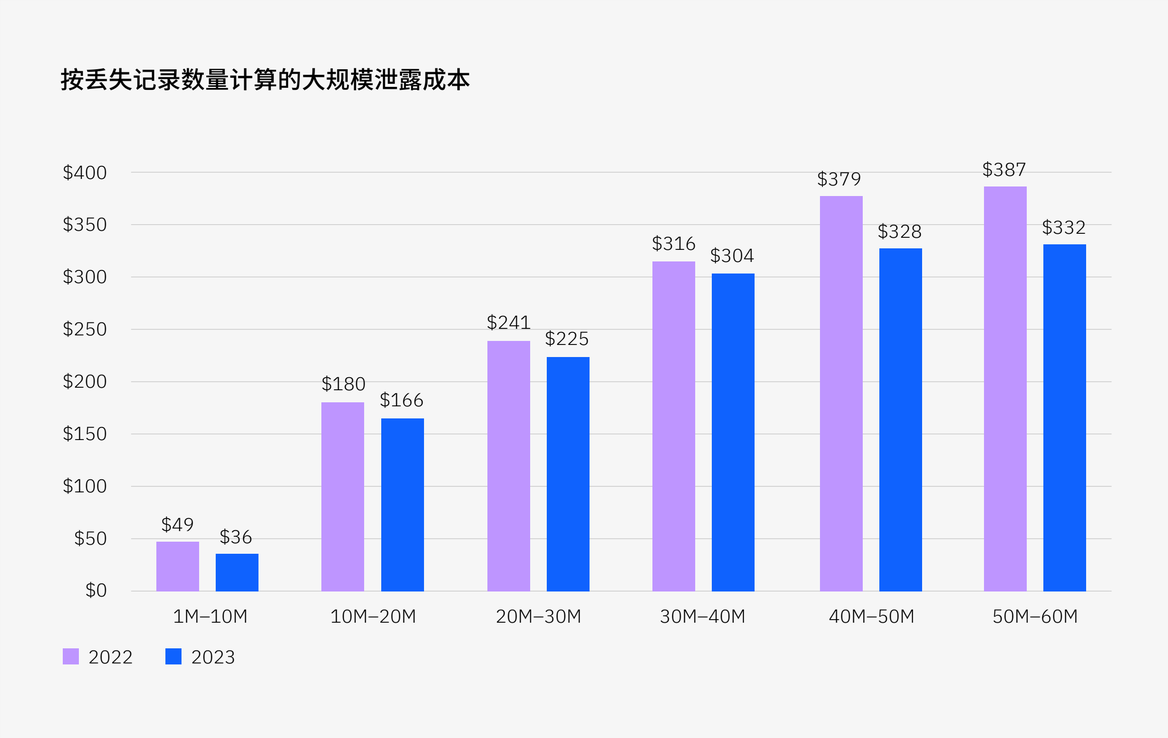


图 37：以百万美元为单位

安全性投资

本节将探讨各组织在遭受数据泄露后采取的安全投资策略。我们将探讨组织在泄露事件后增加支出的频率以及他们如何选择分配资金。

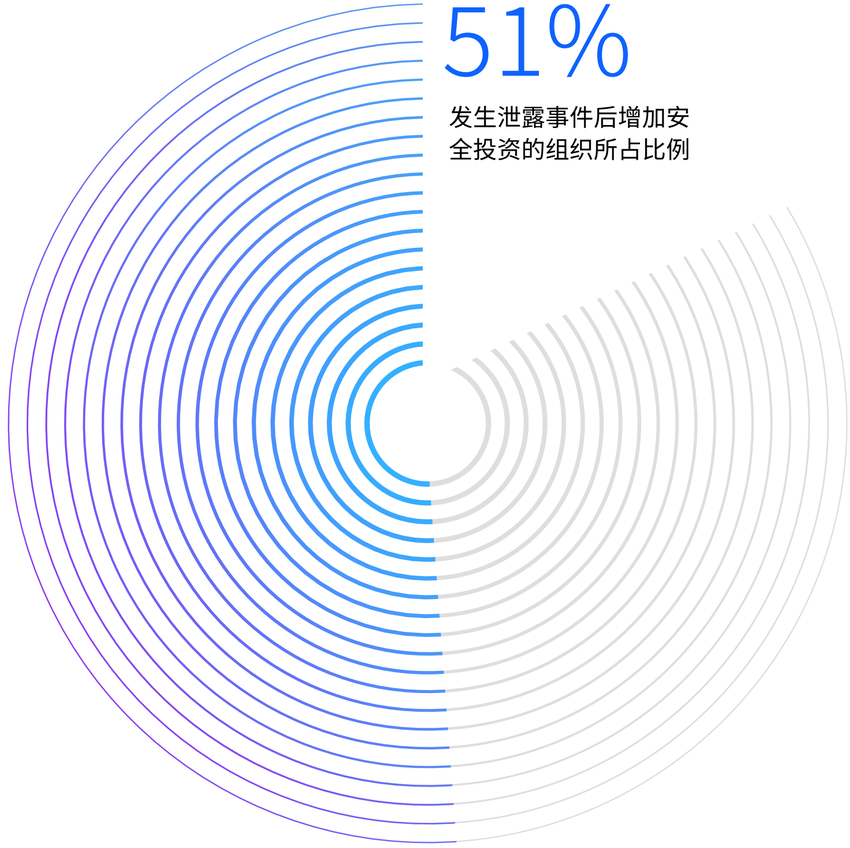


图 38：泄露事件发生后，受访者在增加安全投资方面存在分歧。

尽管数据泄露的全球成本不断增加，但研究参与者对事件发生后增加安全投资的看法存在分歧。51% 的受访者表示，他们计划在泄露发生后增加安全支出。

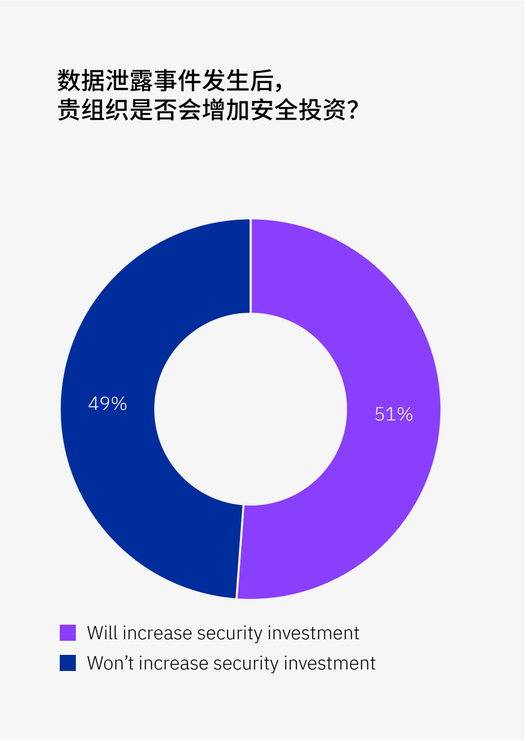


图 38：占所有组织的百分比

图 39：泄露事件发生后，组织投入了大量资金开展 IR 规划和测试以及员工培训。
在数据泄露后增加支出的 51% 组织中，最常见的投资是 IR 计划和测试 (50%)，紧随其后的是员工培训 (46%)。威胁检测和响应技术位居第三（占 38%），在本节讨论的技术或工具投资中排位靠前。值得注意的是，在本年度报告“关键成本因素”部分中，我们探讨了与降低数据泄露成本相关的多个首要因素，而这三项投资就与之关联甚为密切。仅 18% 的受访者认为保险保障是数据泄露后最不常见的投资。

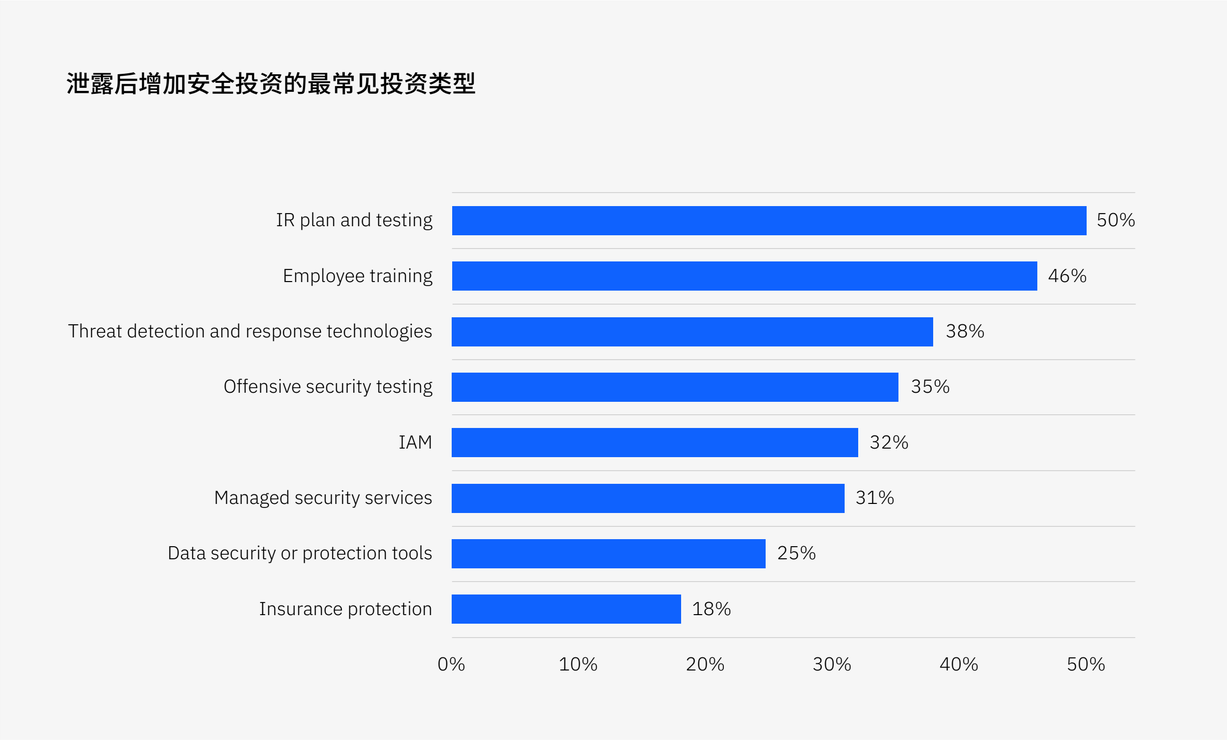


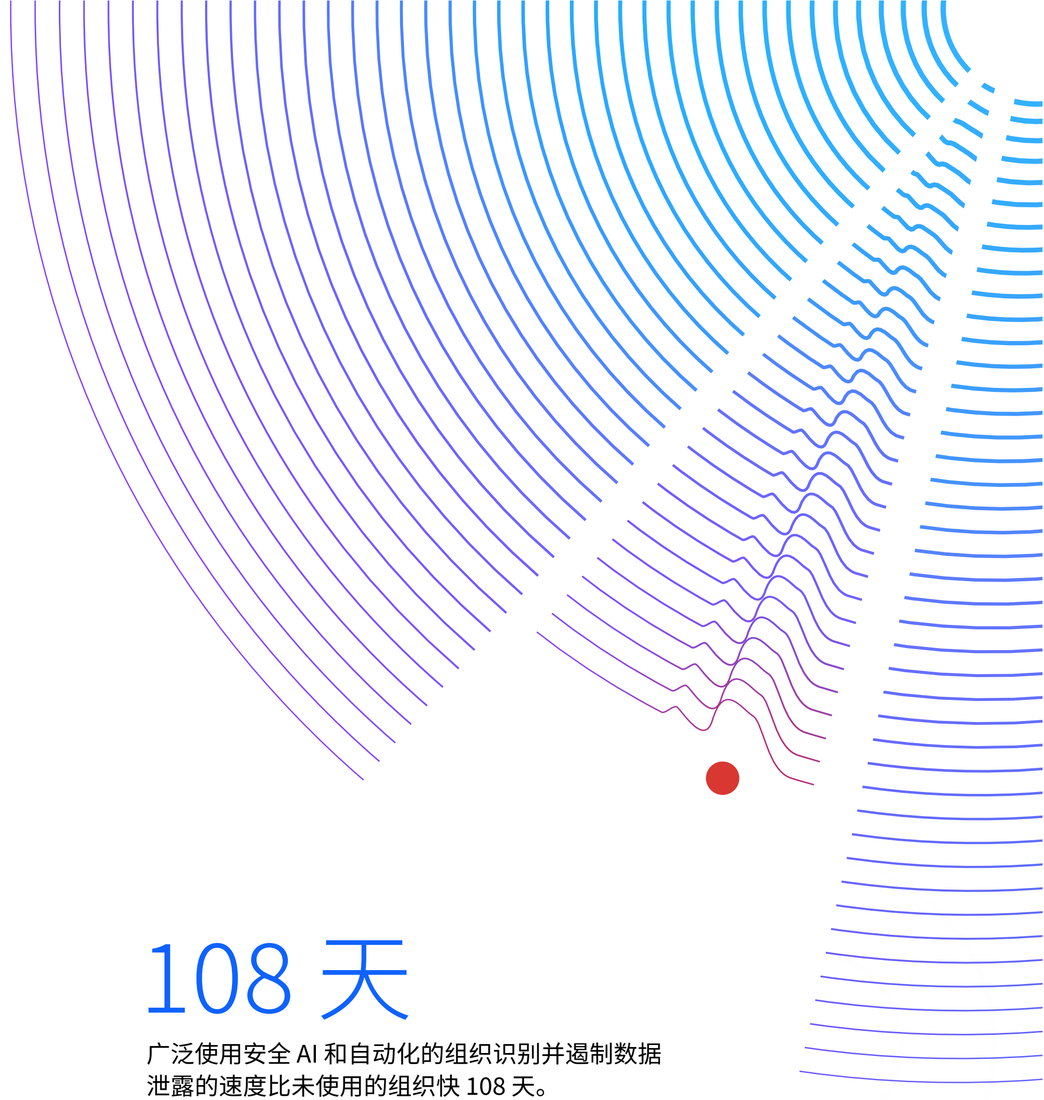
图 39：在增加投资的组织中各项所占比例（可纳入多个响应策略）

安全 AI 和自动化

随着安全行业的安全 AI 和自动化用例的不断发展，本报告研究了这些技术对数据泄露成本和时间线的影响。示例包括使用 AI、机器学习、自动化和业务流程，来增强或取代在威胁检测和调查以及响应和遏制过程中的人为干预。与之相对的是基于人工输入而运行的流程，这种流程往往需要运用几十种工具和复杂的非集成式系统，并且这些工具和系统之间并没有设立数据共享的机制。

尽管这是调查 AI 和自动化对网络安全影响的第六年，但今年我们引入了新标准，这些标准考虑了 AI 在整个组织安全流程中的渗透，而非前几年数据中的部署水平（从未部署到部分或完全部署）。

- “广泛使用”是指在整个运行过程中集成安全 AI 和自动化，包括多种不同的工具集和功能。
- “有限使用”是指将 AI 仅应用于安全运营中的一个或两个用例。
- “未使用”是指仅通过手动输入执行实施的安全流程。



108 天

广泛使用安全 AI 和自动化的组织识别并遏制数据泄露的速度比未使用的组织快 108 天。

图 40：61% 的大多数组织采用一定程度的安全 AI 和自动化。
仅 28% 的组织在其网络安全流程中广泛使用安全 AI 和自动化工具，而 33% 的组织采取“有限使用”的方式。这导致近四成的人员在安全运营过程中完全依赖手动输入。

图 41：广泛使用安全 AI 和自动化，成功节省了近 180 万美元的成本。
相对而言，广泛使用安全 AI 和自动化的组织所节省的成本最高，数据泄露的平均成本为 360 万美元，比不使用的组织减少了 176 万美元，相差 39.3%。即便是有限使用安全 AI 和自动化的组织，数据泄露的平均成本达到 404 万美元，但仍比“未使用”组织的成本减少了 132 万美元，相差 28.1%。未使用安全 AI 和自动化的组织的数据泄露平均成本为 536 万美元。这比 2023 年数据泄露的平均成本（445 万美元）高出 18.6%。

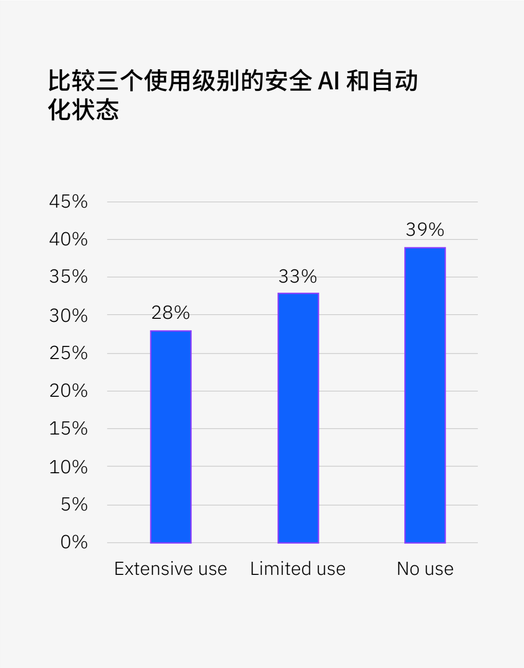


图 40：每个使用级别的组织所占比例

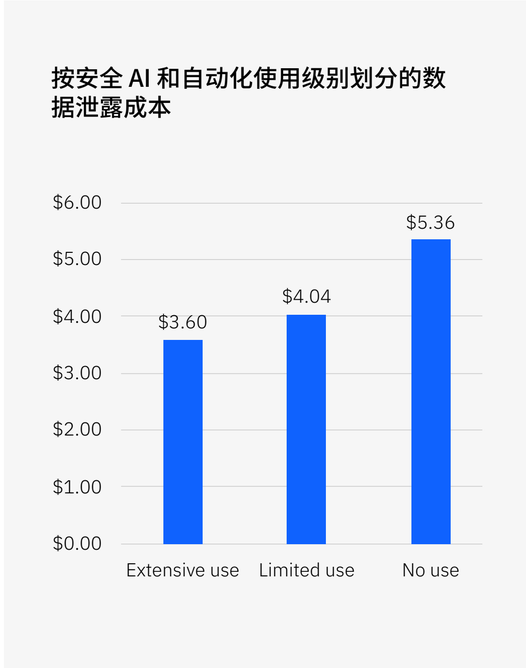


图 41：以百万美元为单位

图 42：广泛使用安全 AI 和自动化，可将识别和遏制泄露的时间大幅缩短，超过了 100 天。广泛运用安全 AI 和自动化的组织的受访者表示，他们能够在 214 天内识别并遏制泄露事件，比未使用安全 AI 和自动化的组织缩短 108 天。这意味着，在广泛运用安全 AI 和自动化的情况下，识别和遏制泄露事件所需的时间仅为没有应用 AI 和自动化的组织所需时间的 66%。即便有限的应用也产生了重大影响，识别和控制泄露的平均时间为 234 天，比未使用的组织缩短 88 天。显然，即使是将安全 AI 和自动化集成至安全工作流程中的有限努力，也能显著加快识别和遏制泄露的时间，并大幅降低成本。

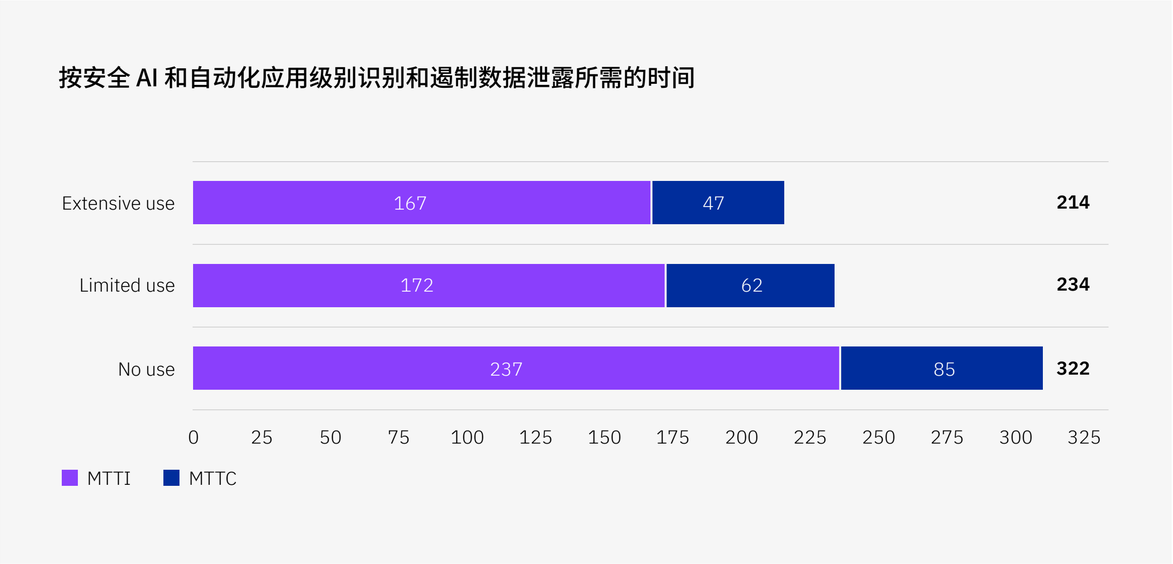
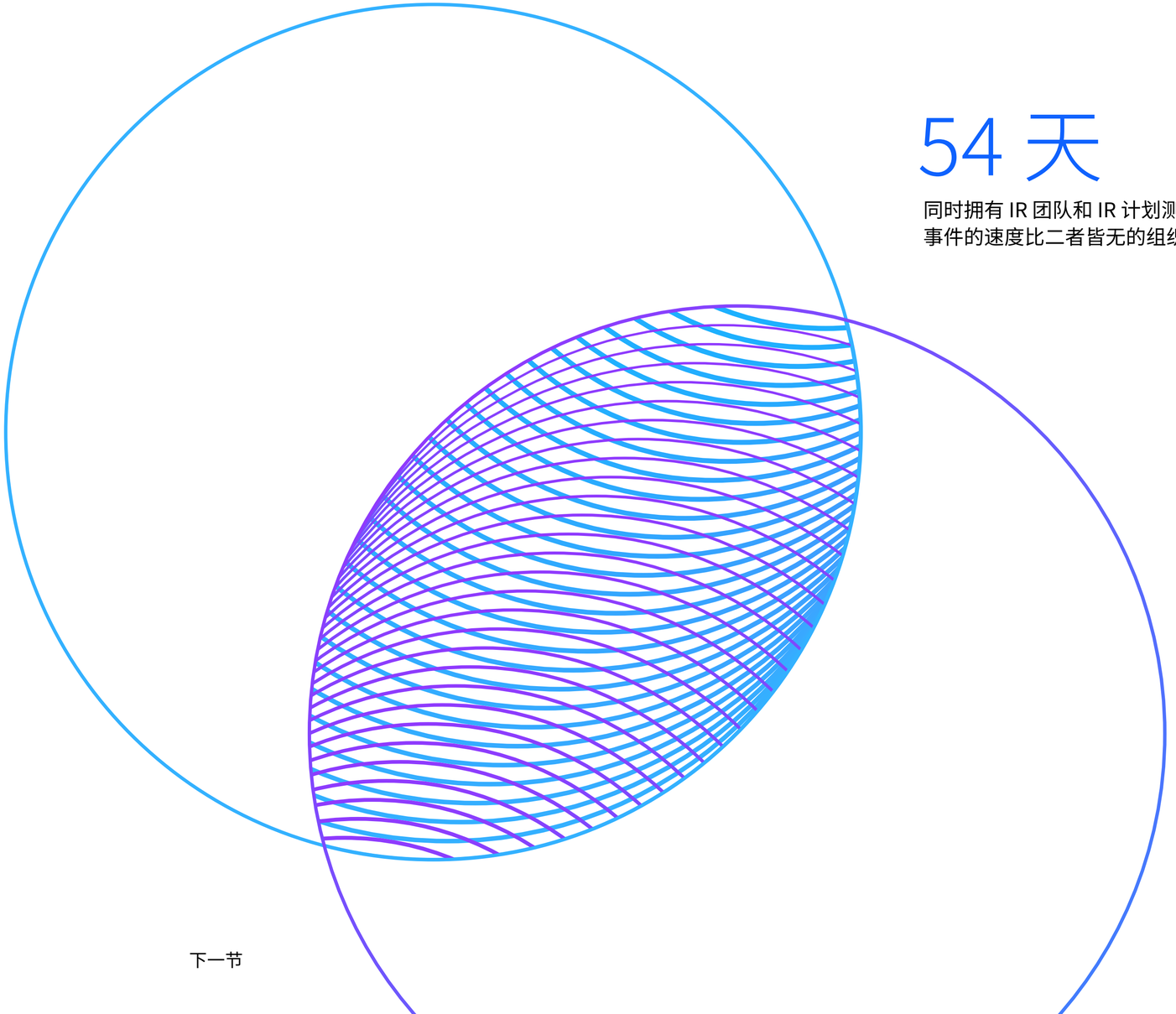


图 42：以天为单位

事件响应

IR 战略和策略在减少数据泄露影响方面发挥了重要作用。缩短数据泄露持续时间的最有效 IR 策略是将组建 IR 团队与测试 IR 计划相结合。不过，有些组织只采用这两种战略中的一种。单独的 IR 计划测试工作在减少识别和遏制泄露事件的总时间方面比仅组建 IR 团队更有效。



54 天

同时拥有 IR 团队和 IR 计划测试的组织，识别泄露事件的速度比二者皆无的组织要快 54 天。

图 43：合并的 IR 策略在识别和遏制泄露方面节省了 54 天的时间。
事实证明，采用组建 IR 团队和 IR 计划测试的双重策略，识别和遏制数据泄露的时间更短（252 天），而没有采用这两种方法则需要 306 天，相差 54 天（即 19.4%）。在不组建团队的情况下 IR 计划测试几乎同样有效，但二者相差 48 天（即 17%）。

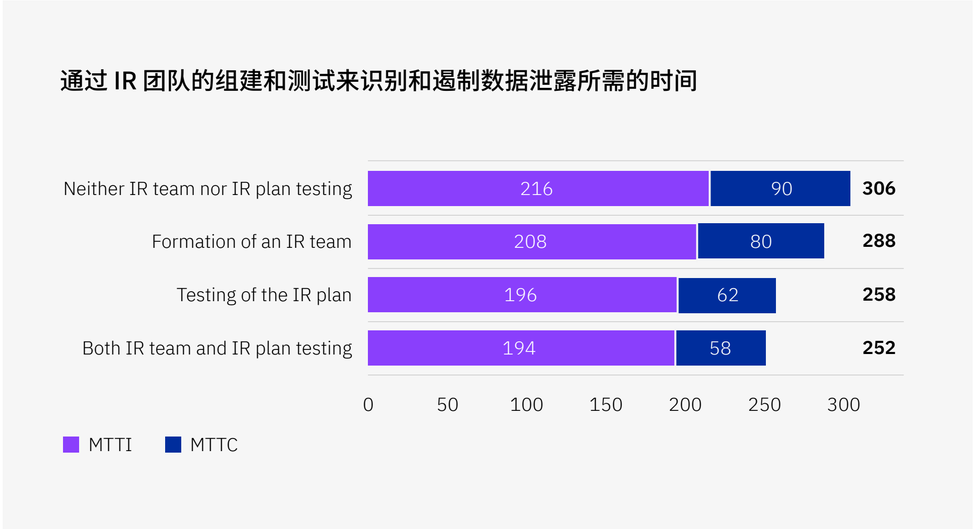
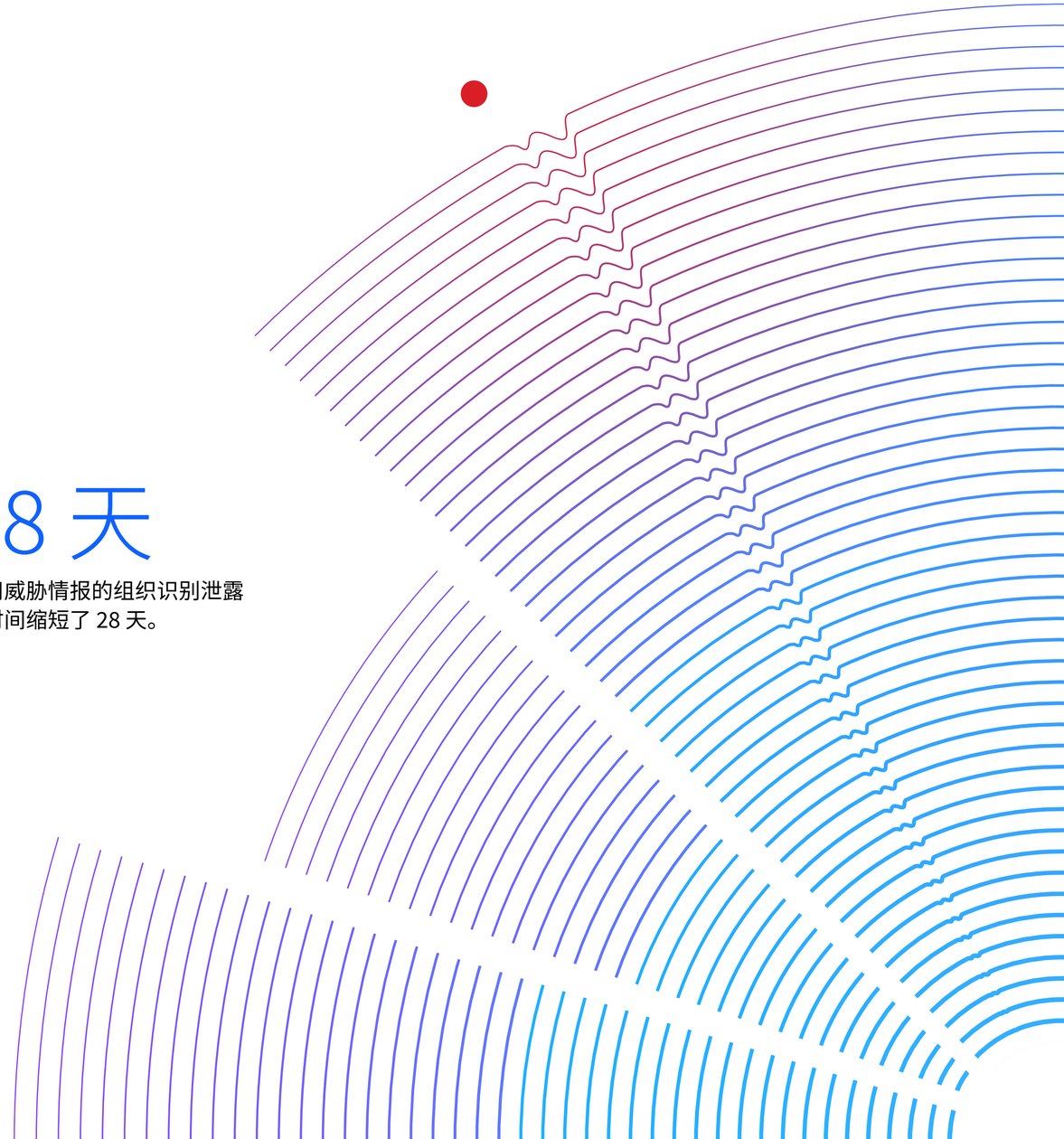


图 43：以天为单位

威胁情报

今年的报告新增了威胁情报服务对识别泄露事件所需平均时间的影响。威胁情报服务为安全领导者提供有关网络威胁和泄露的信息和洞察分析，有助于其改善组织的安全状态。



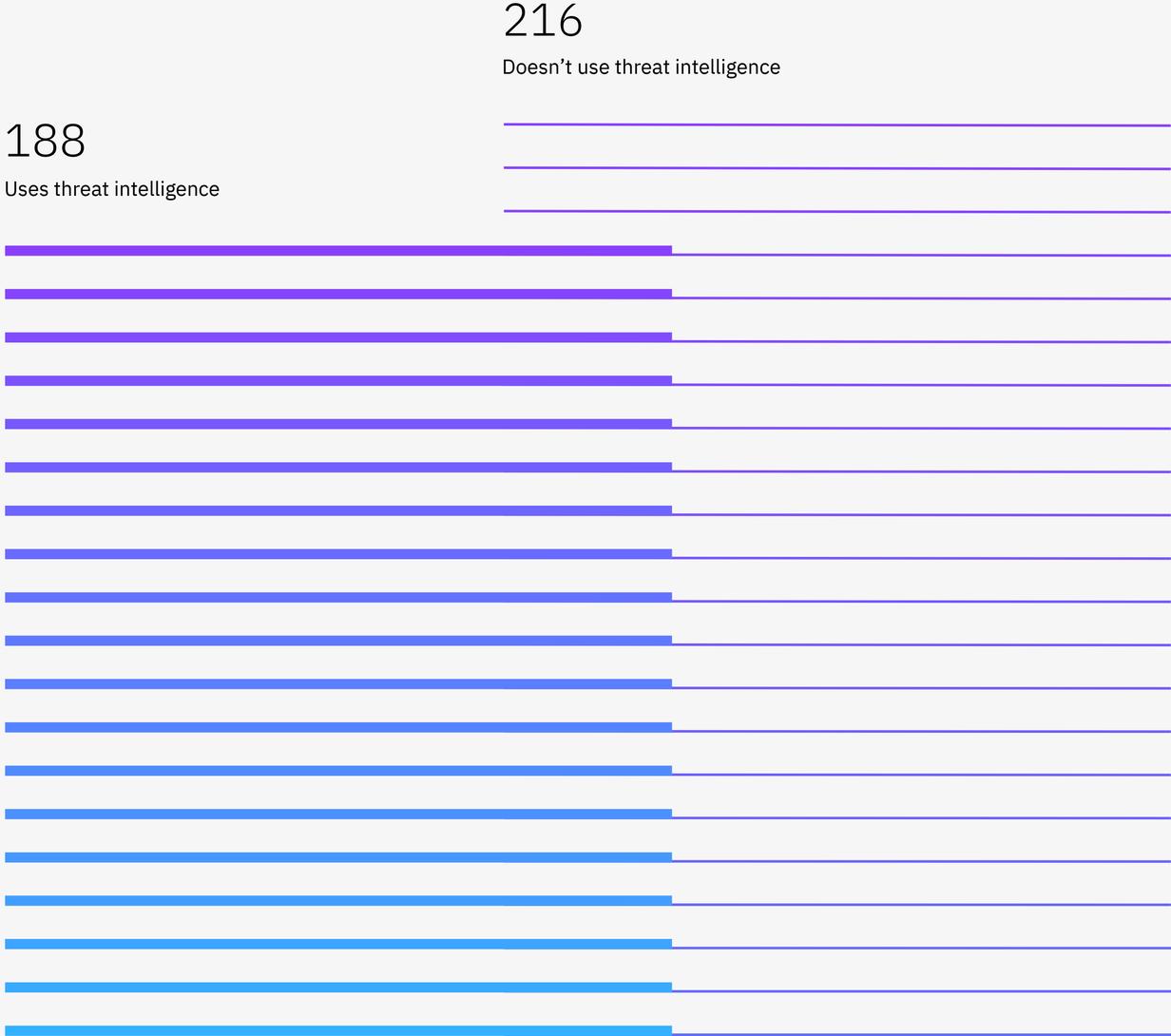
28 天

使用威胁情报的组织识别泄露的时间缩短了 28 天。

图 44：采用威胁情报服务可缩短泄露识别时间。
今年的研究表明，威胁情报用户发现泄露的时间比没有实施威胁情报投资的用户少 13.9%，相差 28 天。与今年 204 天的全球 MTTI 相比，采用威胁情报服务的组织识别泄露事件所需时间缩短 16 天（即 8.2%）。未使用威胁情报的受访者识别泄露的时间比全球平均水平长 5.7%（12 天）。

采用威胁情报服务识别数据泄露所需的时间

图 44：以天为单位的 MTTI



漏洞和风险管理

今年的新研究调查了组织如何对风险和漏洞进行优先排序，以及这如何影响数据泄露的成本。与仅依赖行业标准通用漏洞和暴露 (CVE) 术语表和通用漏洞评分系统 (CVSS) 的组织相比，采用更主动和基于风险的漏洞管理（例如漏洞测试、渗透测试或红队）的组织所承受的数据泄露成本低于平均水平。通常，主动风险管理工作包括组织的 IT 安全团队从潜在攻击者的角度来确定哪些漏洞可利用、哪些漏洞可能造成最大的危害。

398 万美元

已部署基于风险的强力分析工具的组织所产生的数据泄露成本

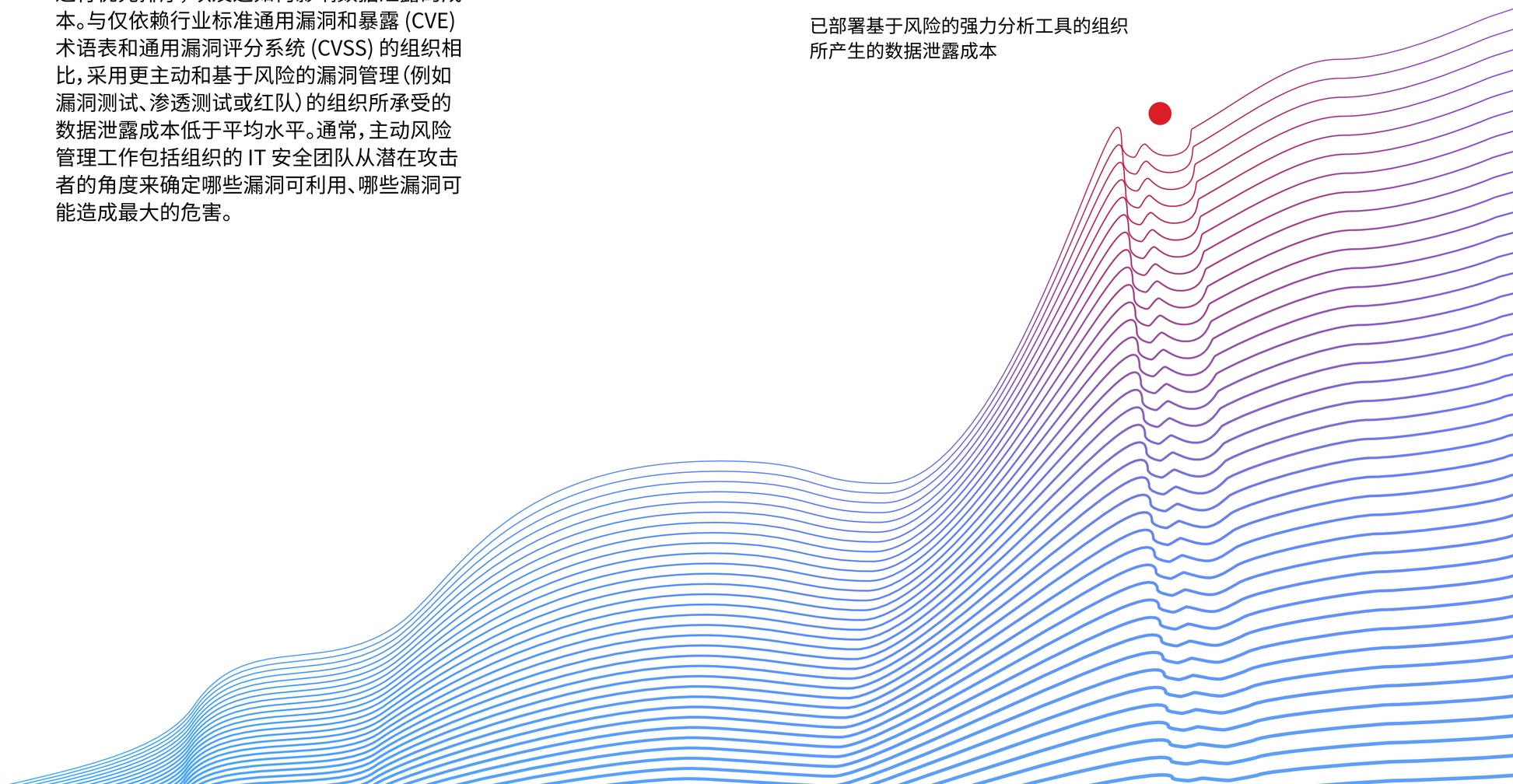


图 45 和图 46：将 CVE 评分以外的活动划分优先级的组织的泄露成本较低。
超过三分之一 (36%) 的组织仅依靠 CVE 评分来划分漏洞的优先级，而大多数组织 (64%) 更多地使用基于风险的分析方案。2023 年的研究表明，这两个群体之间的数据泄露成本存在显著差异。部署更密集、进行基于风险分析的组织的数据泄露平均成本为 398 万美元，而仅依赖 CVE 评分的组织的数据泄露平均成本为 478 万美元，相差 18.3%。

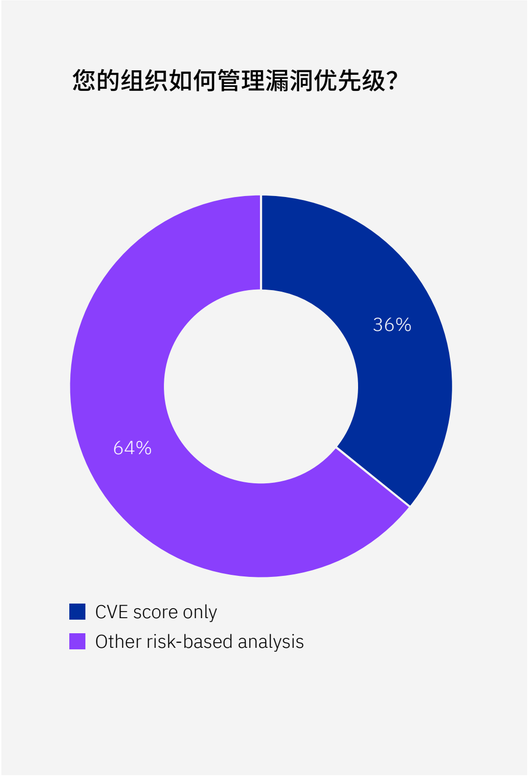


图 45：占所有组织的百分比

图 46：以百万美元为单位

攻击面管理

ASM 是一组有助于发现、分析、修复和监视组织潜在攻击面或漏洞的流程。与未部署 ASM 解决方案的组织相比，已部署 ASM 解决方案的组织仅需 75% 的时间就能识别和遏制数据泄露。

图 47：ASM 帮助将识别和遏制数据泄露的总时间缩短了近 12 周。
如果没有 ASM 解决方案，组织首先需耗费 260 天来识别数据泄露，然后又要投入 77 天来遏制数据泄露，总共需要 337 天（约 11 个月）。部署 ASM 解决方案的组织在 193 天内成功识别泄露事件，并在 61 天内完成遏制操作。识别和遏制泄露的总时间为 254 天，相对缩短了 83 天（约 12 周），因此识别和遏制数据泄露所需的时间仅为未部署 ASM 解决方案的组织所耗费时间的 75%。

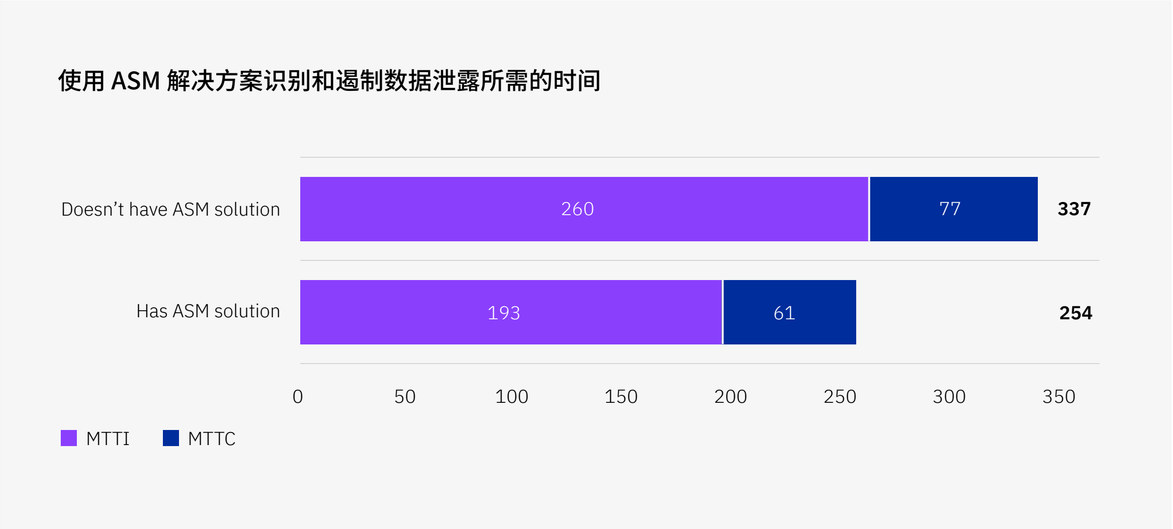


图 47：以天为单位

托管安全服务提供商

我们的研究首次探讨了与 MSSP 合作对识别和遏制泄露事件的影响。MSSP 为组织提供外包安全监控和管理的能力，通常会投入具备高可用性的安全运营中心来提供全天候服务。MSSP 可以帮助组织增强安全保障状态，而无需增加员工数量或投资内部资源培训。

图 48：拥有 MSSP 的组织的数据泄露生命周期缩短了 21%。

在 2023 年报告中，与没有 MSSP 的组织相比，拥有 MSSP 的组织识别和遏制泄露事件所需的时间仅为 80%。与 2023 年报告的全球平均 204 天相比，与 MSSP 合作的组织识别泄露的速度快了 16 天，识别时间缩短了 8.2%。那些没有 MSSP 的组织则多需 28 天（即 12.8%）的时间。没有 MSSP 的遏制时间比 2023 年报告的全球平均时间（73 天）长 5 天（即 6.6%）。在 MSSP 的协助下，遏制时间缩短了 10 天（即 14.7%）。

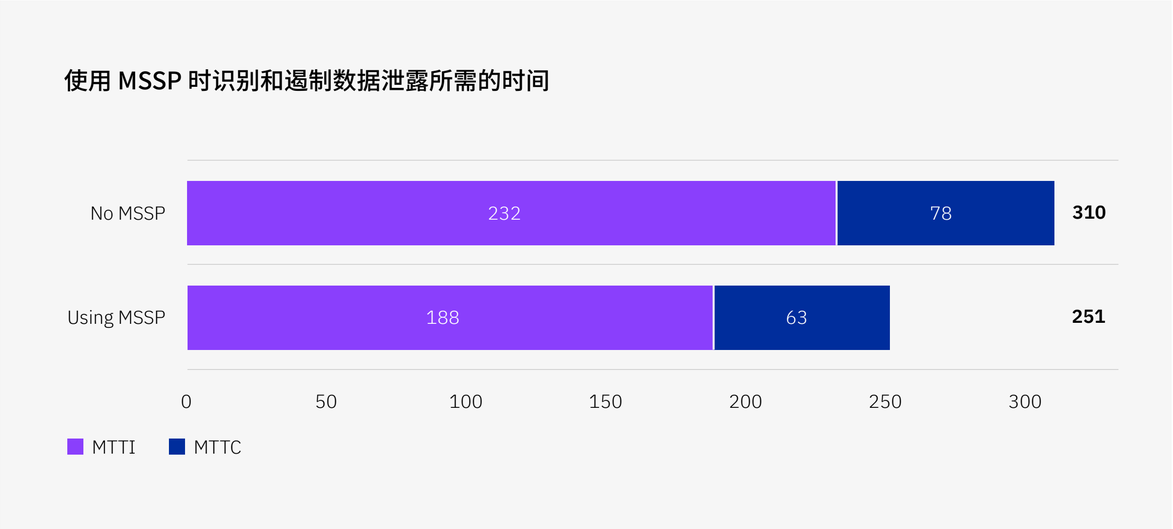


图 48：以天为单位

03

有助于降低数据泄露成本的几项建议

在本部分中，IBM Security 概括介绍了组织可采取哪些措施来降低数据泄露事件造成的财务成本，以及减少给组织声誉带来的不良影响。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。

1. 在软件开发和部署的每个阶段建立安全机制，并定期进行测试
2. 跨混合云实现数据保护现代化
3. 使用安全 AI 和自动化来提高速度和精度
4. 通过了解攻击面态势和实践 IR 来增强恢复弹性

有助于降低数据泄露成本的几项建议

1

将安全性融入到软件开发和部署的每个阶段，并定期进行测试

法规要求日益复杂，尤其当技术与日常活动交织在一起并且软件功能变得更加丰富和复杂时。DevSecOps 方法（2023 年报告中对 27 个因素进行的特别分析中，这是首要的成本缓解因素）对于将安全性构建到组织的工具或平台中至关重要，这些工具或平台是组织的员工投入工作流程或客户参与商业互动所不可或缺。

所有类型的组织都应该确保安全性处于正在开发的软件和正在部署的商业现货软件的最前沿。应用程序开发人员必须继续加速采用设计安全原则和默认安全原则，以确保安全性是数字化转型项目初始设计阶段考虑的核心要求，而不是简单地在事后解决。同样的原则也适用于云环境以支持云原生应用开发，认真努力保护用户隐私并最大程度地减少攻击面。

从攻击者的角度进行应用程序测试或渗透测试还可以让组织有机会在漏洞变成泄露之前标识和修补漏洞。没有任何技术或应用程序是完全安全的，添加更多功能会带来新的风险。持续的应用程序测试可以帮助组织标识新的漏洞。

2

跨混合云实现数据保护现代化

跨越各种多云环境，采取前所未有的规模创建、共享和访问数据。新云应用程序和服务的快速采用模式加剧了“影子数据”（敏感数据未被跟踪或管理）的风险，从而增加了安全和合规风险。本报告中的大多数 (82%) 数据泄露涉及云环境中存储的数据，而 39% 的泄露涉及跨越多种环境类型的数据。不断演变的法规矩阵以及对不合规的严厉惩罚加剧了这些数据泄露的成本和风险。

面对这些挑战，获得数据在混合云中传播的可见性和控制应该是所有类型组织的首要任务，并应将焦点放在强度加密、数据安全和数据访问政策上。公司应寻求数据安全以及适用于所有平台的合规技术，使其能够在混合云环境中部署的数据库、应用程序和服务之间移动时保护数据。数据活动监控解决方案可以帮助确保在积极执行这些政策的同时实施适当的控制，例如尽早发现可疑活动以及阻止对关键数据存储的实时威胁。

此外，数据安全状态管理等较新的技术可帮助在云中查找未知和敏感数据，包括云服务提供商、软件即服务 (SaaS) 属性和数据湖中的结构化和非结构化资产。这有助于识别和缓解底层数据存储配置、授权和数据流中的漏洞。

随着组织继续深入混合多云运营，部署强大的身份和访问管理 (IAM) 策略至关重要，其中包括多因子认证 (MFA) 等技术，特别注重管理具有较高访问级别的特权用户帐户。

3

使用安全 AI 和自动化来提高速度和准确性
在 2023 年报告中，只有 28% 的组织在运营中广泛使用安全 AI 和自动化，这意味着许多组织有很大机会提高速度、准确性和效率。与未使用安全 AI 和自动化的组织相比，广泛使用安全 AI 和自动化可节省近 180 万美元的数据泄露成本，并将识别和遏制泄露事件的时间缩短 100 天以上。

通过将安全 AI 和自动化嵌入工具集，安全团队可从中受益良多。例如，在威胁检测和响应工具中，使用安全 AI 和自动化可以帮助分析师更准确地检测新威胁，并更有效地对安全警告进行情境处理和分类。这些技术还可以自动处理部分威胁调查流程，或者建议执行有助于加快响应速度的操作。此外，由 AI 驱动的数据安全和身份识别解决方案，可识别高风险交易、以最小的用户摩擦提供保障服务，并更有效地将可疑行为拼接起来，统筹管理，从而助力实现颇具前瞻性的主动安全状态。

将 AI 运用于安全运营时，应寻找能够提供值得信赖和成熟用例的技术，要具备经过验证的精度、效能和透明度，以消除潜在的偏差、盲点或漂移。随着威胁和技术能力的发展，组织应规划一种旨在推动 AI 采用的运营模式，支持持续学习。

组织还可从各种核心安全技术的紧密集成部署中受益，实现更顺畅的工作流程，并在通用数据池中共享洞察成果。首席信息安全官 (CISO) 和安全运营 (SecOps) 负责人还可以借助威胁情报报告，针对新兴威胁展开模式识别，并实现威胁的可视化管理。

4

通过了解攻击面态势和实践 IR 来增强恢复弹性

了解您所在行业和组织最容易受到的攻击，并据此确定安全策略的优先级。ASM 等工具或对手模拟等技术可帮助组织从攻击者的角度了解其独特的风险情况和漏洞，其中包括那些易被利用的漏洞。

此外，事实证明，如果一个团队已精通适当的协议和工具、可以响应事件，则该团队可显著降低成本，缩短识别和遏制泄露事件的时间。

在 2023 年报告中，IR 规划和测试不仅是三大成本缓解因素，而且数据还显示，在实施这些对策水平较高的组织中，数据泄露成本降低了 149 万美元；与水平低或没有对策的组织相比，解决事件的速度快了 54 天。组建专门的 IR 团队，起草 IR 运行手册，并定期在桌面练习或模拟环境（如网络靶场）中测试 IR 计划。确保获取 IR 供应商的长期服务保障，也有助于加快响应泄露事件的时间。

最后，组织应力求实施和落实网络分区段操作方案，以限制攻击的传播及其可能造成的损坏程度，从而增强整体网络弹性，并减少相关的恢复工作。

安全措施建议仅供教学培训使用，不保证任何结果。

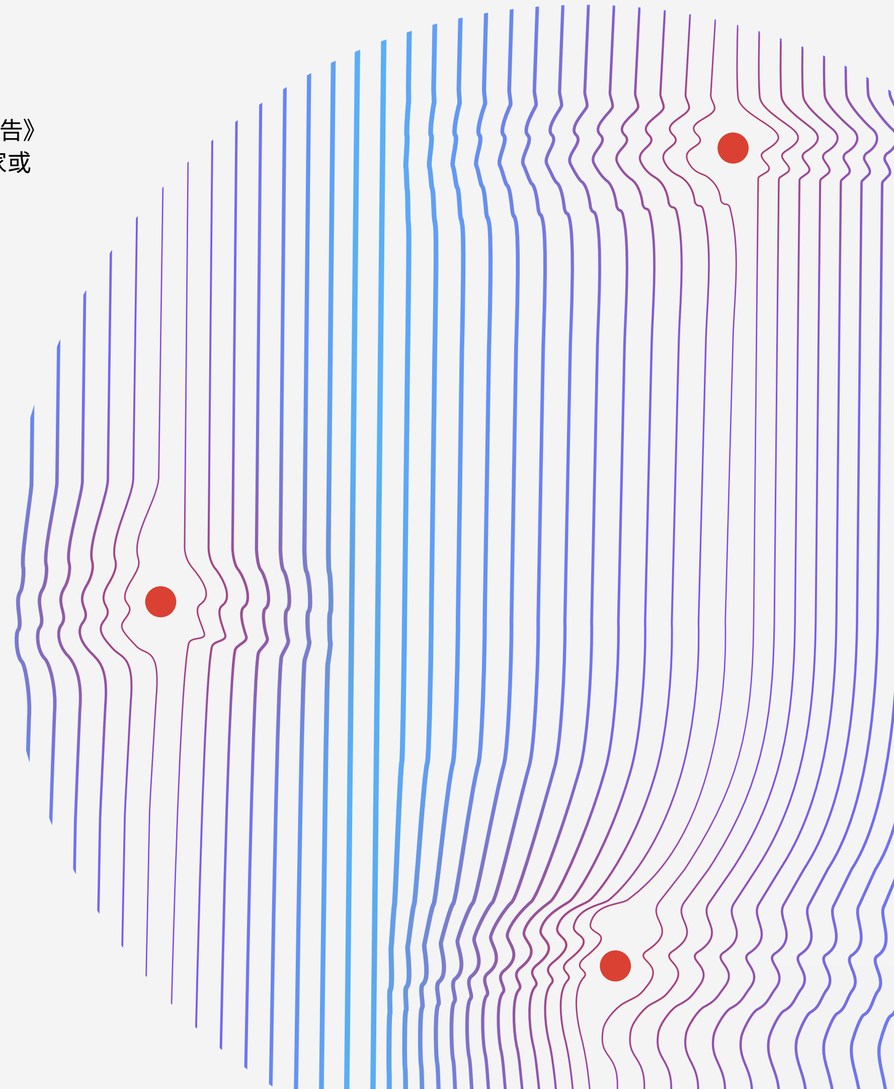
04

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 553 个不同规模的组织。本节按照地理和行业对所研究的组织进行了划分，并针对行业分类予以定义。

18 年

美国已被列入《数据泄露成本报告》18 年，在该报告涉及的所有国家或地区中时间最长。



地理统计数据

2023 年的研究在 16 个不同的国家和地区之间进行。

全球研究速览

国家/地区	2023 年样本	百分比	货币	2023 美元汇率[7]	研究年限
东盟	23	4%	新加坡元	1.3294	7
澳大利亚	24	4%	澳元	1.4916	14
巴西	43	8%	巴西雷亚尔	5.0702	11
加拿大	26	5%	加元	1.3525	9
法国	34	6%	欧元	0.9198	14
德国	45	8%	欧元	0.9198	15
印度	51	9%	印度卢比	82.19	12
意大利	24	4%	欧元	0.9198	12
日本	42	8%	日元	132.75	12
拉丁美洲[4]	23	4%	墨西哥比索	18.025	4
中东[5]	36	7%	沙特里亚尔	3.7037	10
斯堪的纳维亚[6]	22	4%	挪威克朗	10.4445	5
南非	21	4%	南非兰特	17.73	8
韩国	23	4%	ZRW	1303.8	6
英国	49	9%	英镑	0.8085	16
美国	67	12%	美元	1.00	18
总计	**553**	**100%**			

图 49：所研究的所有国家/地区一览表

行业统计数据

所选定的 17 个行业多年来一直被纳入本报告的调研范围。

五个行业合计占今年研究样本组织的 55%。

14% 金融

12% 服务

11% 技术

10% 工业

8% 能源

样本的行业分布

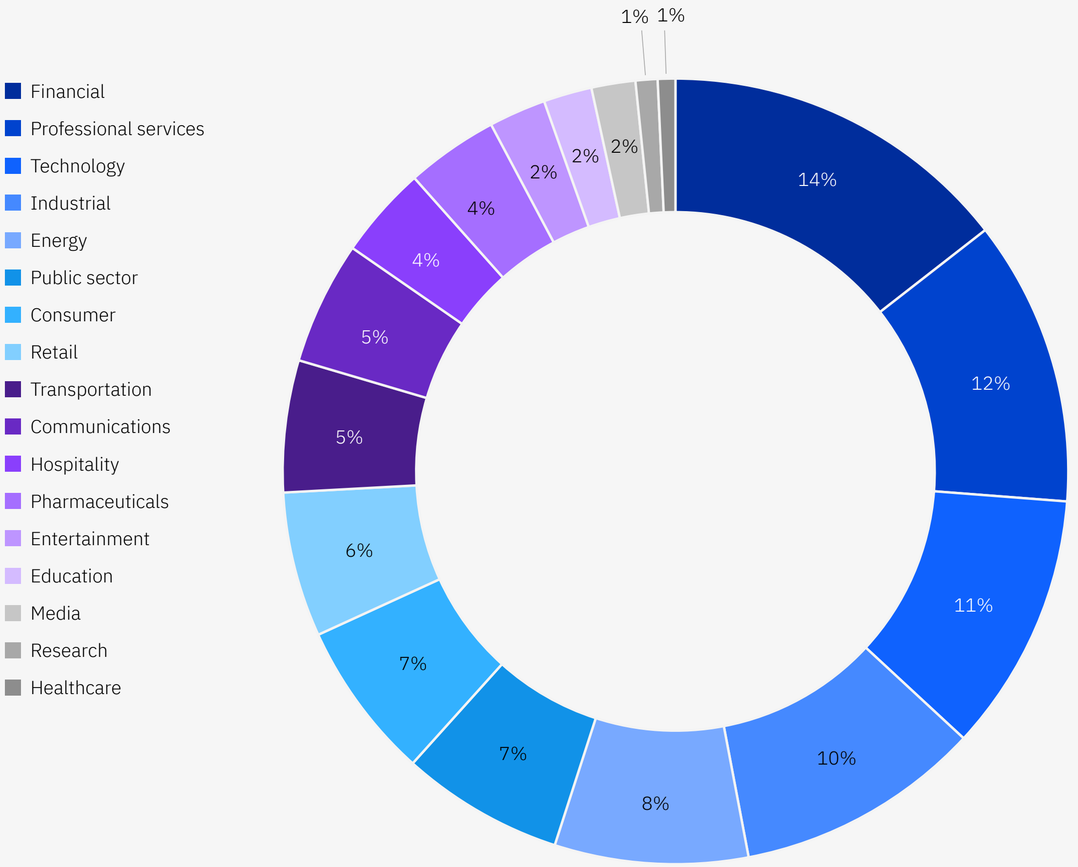


图 50:行业的百分比

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，包括生物医学与生命科学

工业
化学加工、工程和制造公司

科技
软件和硬件公司

教育
公立和私立大学和学院、培训和发展公司

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、货运和快递公司

通信
报纸、图书出版商、公共关系和广告公司

消费
消费品制造商和分销商

媒体
电视、卫星、社交媒体、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
市场研究、智库和研发 (R&D)

公共部门
联邦、州、地方政府机构和非政府组织 (NGO)

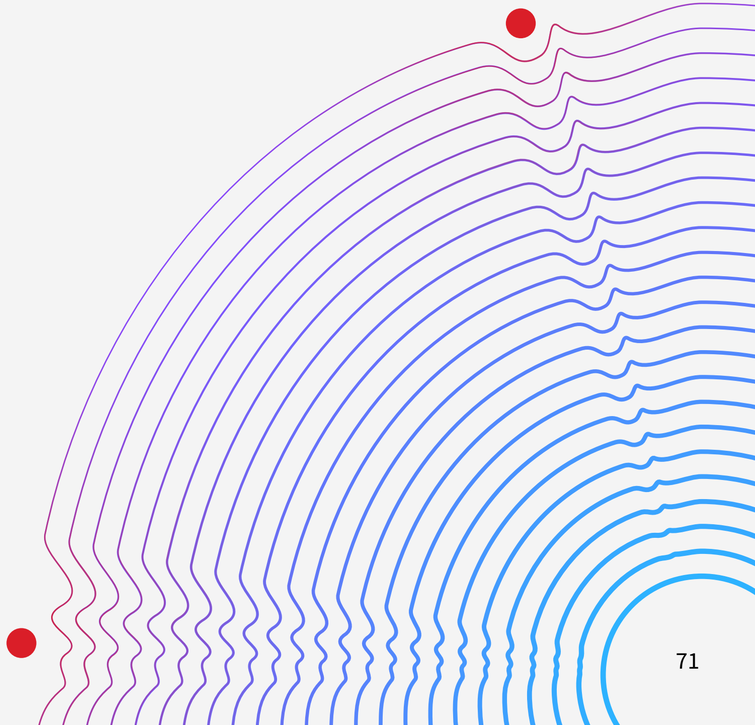
研究方法

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。

为了顺利进行基准测试，需要做好可管理数据集的维护工作，因此我们只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，我们选择了一组项目固定的成本活动。在收集基准信息后，我们仔细地重新检查了每项基准工具的一致性和完整性。

在涉及个人信息的广泛业务运营中，有一些已知的成本因素类别，我们将数据泄露成本因素限定在这些已知类别中。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，本研究排除了非常小和非常大的数据泄露事件。2023 年的报告中，纳入调研的数据泄露事件规模均在 2,160 至 101,200 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。

本研究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
确保公司能够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
确保公司能够通知数据主体、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公司沟通的活动，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?
泄露定义为包含个人身份信息 (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 2,200 到 102,000 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?
我们的研究人员通过对 2022 年 3 月至 2023 年 3 月期间遭遇数据泄露的 553 家组织中的个人进行 3,475 多次单独访谈,以此收集具有一定深度的定性数据。受访者包括 IT、合规和信息安全从业人员,他们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。出于隐私考虑,我们没有收集组织特定的信息。

如何计算数据数据泄露的平均成本?
我们收集了组织产生的直接和间接费用。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。

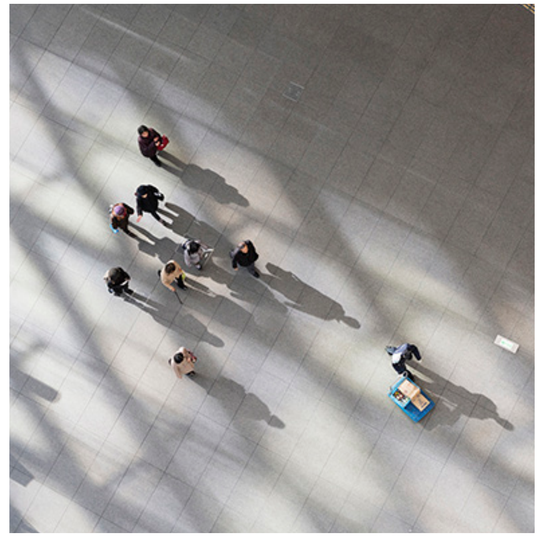
为了与往年保持一致,我们使用了相同的货币换算方法,而不是调整会计成本。

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 553 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，其中每起事件都有 101,200 条或更少的受损记录。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 20 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?
20 家经历过大规模泄露的公司的样本量不够大，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 250,000 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 100 万到 6,000 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公司样本。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公司，例如公司的行业、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 5,580 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，未参与的公司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公司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公司。

公司特定信息
研究中使用的基准没有捕获公司的识别信息。个人可以使用分类响应变量来披露有关公司和行业类别的统计信息。

未衡量因素
我们在分析中省略了一些变量，如主导趋势和组织特征。无法确定已省略的变量可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 2023 年 3 月 31 日公布。

06

波耐蒙研究所 (Ponemon Institute) 和 IBM Security 简介

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 (Ponemon Institute) 坚持严格的数据保密、隐私和道德研究标准，不会向个人收集个人可识别信息，也不会在商业研究中收集公司可识别信息。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。

IBM Security
IBM Security 通过融入动态安全 AI 和自动化功能的集成安全性产品服务组合，帮助全球规模最大的企业和政府强化安全措施。该产品组合得到了世界知名的 IBM Security X-Force® 研究的支持，使组织能够预测威胁、保护移动中的数据，并快速准确地应对威胁，同时不会阻碍业务创新。IBM 受到数千家组织的信赖，成为其评估、制定策略、实施和管理安全转型的合作伙伴。

IBM 管理和运营全球覆盖面最为广泛的安全研发与交付组织，每天在 130 多个国家/地区监测超过 1,500 亿次安全事件，已在全球范围内获得了超过 1 万项安全专利。

如果您对本研究报告有任何疑问或意见（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
收件人：研究部门
2308 US 31 North
Traverse City
Michigan 49686 USA
1.800.887.3118
research@ponemon.org

了解有关提升企业安全状态的更多信息

请访问 ibm.com/security。

加入 IBM Security 社区的对话。

采取下一步行动

AI 网络安全解决方案
加快安全响应时间，提高工作效率。
了解更多

威胁检测和响应解决方案
为安全团队赋能，确保团队能够快速、准确、高效地战胜威胁。
了解更多信息

云安全解决方案
在企业转型至混合多云的旅程中，实现安全集成化运营。
了解更多信息

勒索软件解决方案
管理网络安全风险和漏洞，以最大程度降低勒索软件的影响。
了解更多信息

身份和访问管理解决方案
安全连接每位用户、每个 API 和每台设备至每个应用程序。
了解更多信息

事件响应和威胁检测服务
主动管理和应对安全威胁。
了解更多

数据安全和保护解决方案
跨混合云保护数据并简化合规性。
了解更多

攻击面管理
管理数字足迹的扩展范围，快速提高组织的网络弹性。
了解更多信息

统一端点管理解决方案
通过保护和管理任何设备来壮大您的移动员工队伍。
了解更多信息

治理、风险与合规服务
通过集成的治理、风险和合规方法提高网络安全成熟度。
了解更多信息

安排一对一咨询
与 IBM Security X-Force 专家会面以讨论您的需求。
了解更多信息

申请参加 IBM 安全与框架发现研讨会
获得有关实现安全计划现代化的帮助。

了解更多信息

1. 采用每条记录的成本来计算规模超过 102,000 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。更多信息请参见“研究方法”部分。

2. “东盟”是位于新加坡、印度尼西亚、菲律宾、马来西亚、泰国和越南的公司构成的集群样本。

3. 破坏性攻击定义为导致系统无法运行并难以复原的攻击。不一定涉及赎金。

4. “拉丁美洲”是位于墨西哥、阿根廷、智利和哥伦比亚的公司构成的集群样本。

5. “中东”是位于沙特阿拉伯和阿拉伯联合酋长国的公司构成的集群样本。

6. “斯堪的纳维亚”是位于丹麦、瑞典、挪威和芬兰的公司构成的集群样本。

7. 外汇汇率 - H.10，2023 年 3 月 31 日。

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
2023 年 7 月

本文档为自最初公布日期起的最新版本，IBM 可能随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

以上所有引用或描述的客户实例的展示取决于部分客户使用 IBM 产品的方式以及他们可能取得的结果。实际的环境成本和性能特征会因具体客户配置和情况而有所不同。无法提供通用的预期结果，因为每个客户的结果将完全取决于客户的系统和订购的服务。本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议条款和条件获得保证。

良好安全实践声明：IT 系统安全涉及通过预防、检测和响应企业内部和外部的不当访问来保护系统和信息。不正当访问可导致信息被更改、破坏、盗用或滥用，也可能导致系统被损坏或滥用，包括用于攻击他人。任何 IT 系统或产品都不应被视为完全安全，任何单一产品、服务或安全措施都不能完全有效防止不正当使用或访问。IBM 系统、产品和服务旨在成为合法、全面的安全措施的一部分，这必然涉及其他操作程序，且可能需要借助其他系统、产品或服务才能发挥最大作用。IBM 不保证任何系统、产品或服务可免于或使您的企业免于受到任何一方恶意或非法行为的影响。

客户负责确保遵守适用的法律和法规。IBM 不提供任何法律咨询，也不声明或保证其服务或产品经确保客户遵循任何法律或法规。关于 IBM 未来方向、意向的声明仅仅表示了目标和意愿而已，可能会随时更改或撤销，恕不另行通知。