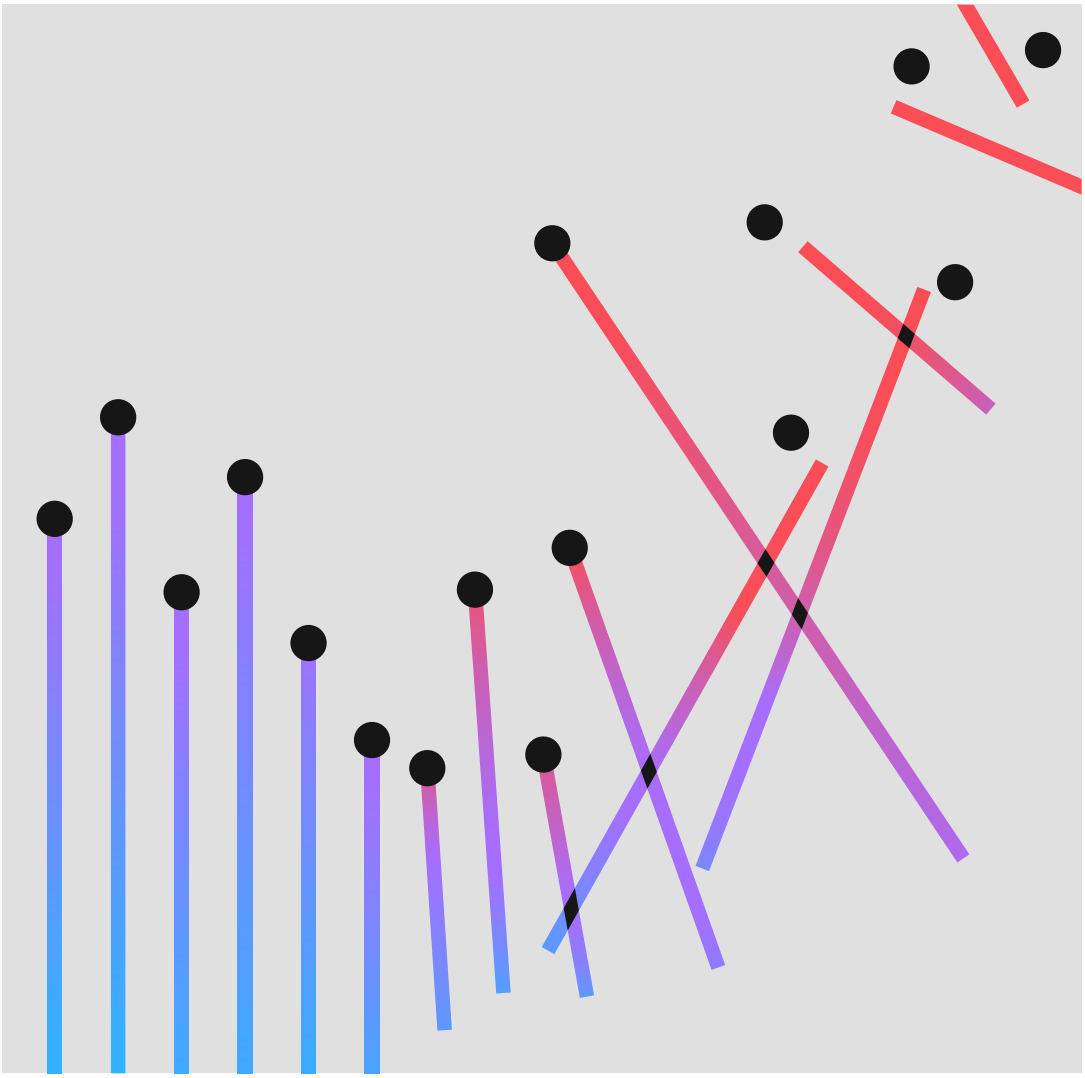
IBM **Security**

2022 年数据泄露成本报告：执行摘要



IBM

目录

执行摘要

“数据泄漏成本报告”让 IT、风险管理和安全主管能够从中了解那些会加快或有助于减缓数据泄漏成本上升的各种因素。

这项由波耐蒙研究所 (Ponemon Institute) 独立进行并由 IBM Security® 发起、分析和发布的研究已进入第 17 个年头，今年对 2021 年 3 月至 2022 年 3 月期间受数据泄露影响的 550 家组织展开了调研。这些数据泄露事件发生在 17 个国家和地区的 17 个不同行业中。

我们对来自受数据泄漏影响的组织的人员进行了 3,600 多次采访。采访中，我们提出了一些问题，以确定组织在应对数据泄露事件时，因采取各种即时和长期响应策略而产生的各种成本。

与往年的报告一样，今年的数据同样向我们展示了诸多因素如何影响数据泄露发生后不断增加的成本。此外，本报告还研究了数据泄露的根本原因、短期和长期后果以及有助于企业降低损失的缓解因素和技术。

重要结论

本报告所述之重要结论基于 IBM Security 对波耐蒙研究所 (Ponemon Institute) 所汇编的研究数据的分析得出。[1]

435 万美元

数据泄露的平均总成本

2022 年，数据泄露的平均成本达 435 万美元，创历史新高。这一数据相比去年增加了 2.6%，去年的数据泄露平均成本是 424 万美元。相比 2020 年所报告的 386 万美元攀升了 12.7%。

83%

不止一次发生数据泄露事件的组织所占百分比

83% 的受访组织曾不止一次发生数据泄露事件，仅有 17% 的组织表示这是他们的首次数据泄露事件。60% 的受访组织表示，他们因数据泄露而提高了服务或产品的价格。

482 万美元

关键的基础设施数据泄漏平均成本

受访的关键基础设施组织的数据泄露平均成本为 482 万美元，比其他行业组织的平均成本多 100 万美元。关键的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、教育以及公共部门行业的组织。28% 的组织曾遭受破坏性或勒索软件攻击，而 17% 的组织曾因业务合作伙伴被入侵而发生数据泄露。

305 万美元

因全面部署安全 AI 和自动化而节省的平均成本

与未部署安全 AI 和自动化的组织相比，已全面部署安全 AI 和自动化的组织的数据泄露成本减少了 305 万美元。数据泄露平均成本相差 65.2%（全面部署为 315 万美元，未部署为 620 万美元），是本研究中成本节省最多的情况。此外，与未部署安全 AI 和自动化的公司相比，已全面部署的公司发现和控制数据泄露的时间（称为数据泄露生命周期）平均缩短了 74 天（分别为 323 天和 249 天）。安全 AI 和自动化的使用率从 2020 年的 59% 上升到了 2022 年的 70%，两年内大幅增长了近 1/5。

1. 本报告中的成本金额单位为美元。

454 万美元

勒索软件攻击的平均成本，不包括赎金本身的成本

本研究中 11% 的数据泄露是因勒索软件攻击造成的，比 2021 年的 7.8% 增长了 41%。勒索软件攻击的平均成本从 2021 年的 462 万美元减少至 2022 年的 454 万美元，略有下降。这一成本略高于数据泄露的平均总成本 435 万美元。

19%

因凭证被盗或泄露而造成的数据泄露频率

使用被盗或已泄露的凭证仍然是数据泄露最常见的原因。在 2022 年的研究中，19% 的数据泄露事件的主要攻击媒介是被盗或泄露的凭证，而在 2021 年的研究中，被盗或泄露的凭证也是最主要的攻击媒介，造成了 20% 的数据泄露事件。凭证被盗或泄露造成的数据泄露的平均成本达 450 万美元。这些泄露事件的生命周期最长，发现泄露需要 243 天，而控制泄露还需要 84 天。网络钓鱼是数据泄露的第二大常见原因，占比为 16%，成本最高，平均成本高达 491 万美元。

59%

未部署零信任架构的组织所占百分比

在本研究中，仅有 41% 的组织表示他们部署了零信任安全架构。其他 59% 的组织未部署零信任安全架构，与已部署的组织相比，他们的数据泄露成本平均高出 100 万美元。在关键基础设施组织中，未部署零信任架构的组织所占比例甚至更高，达 79%。这些组织的数据泄露平均成本为 540 万美元，比全球平均水平高出 100 万美元。

100 万美元

因远程工作导致数据泄露与不是因远程工作导致数据泄露的平均成本差异

因远程工作导致数据泄露与不是因远程工作导致数据泄露相比，成本平均高出近 100 万美元（分别是 499 万美元和 402 万美元）。与远程工作相关的数据泄露平均成本比全球平均成本高约 60 万美元。

45%

在云中发生的数据泄露所占比例

在本研究中，45% 的数据泄露发生在云中。然而，混合云环境中发生数据泄露的平均成本为 380 万美元，而私有云中发生数据泄露的成本为 424 万美元，公有云中数据泄露的成本为 502 万美元。混合云数据泄露和公有云数据泄露之间的成本差异为 27.6%。此外，与仅采用公有或私有云模式的组织相比，采用混合云模式的组织拥有的数据泄露生命周期更短。

266 万美元

与事件响应 (IR) 团队和定期测试 IR 计划相关的平均节省成本

在本研究中，近 3/4 的组织表示他们制定有 IR 计划，而其中 63% 的组织称会对该计划进行定期测试。拥有 IR 团队和定期测试的 IR 计划大大节省了成本。与没有 IR 团队且不对 IR 计划进行测试的企业相比，设有 IR 团队并对 IR 计划进行测试的组织平均降低的数据泄露成本高达 266 万美元，两项数据分别是 326 万美元和 592 万美元，成本节省高达 58%。

29 天

实施扩展检测和响应 (XDR) 技术的组织可节省的响应时间

44% 的组织实施了 XDR 技术。这些组织在响应时间方面具有相当大的优势。与未实施 XDR 的组织相比，这些部署了 XDR 的组织的数据泄露生命周期平均缩短了大约一个月。具体来说，部署 XDR 的组织发现和控制数据泄露事件需要 275 天，而未部署 XDR 的组织需要 304 天。这表明二者的响应时间相差 10%。

12 年

医疗保健行业数据泄露平均成本连续高居榜首的时间（年）

医疗保健行业数据泄露成本再创历史新高，平均成本高达 1,010 万美元，增加了近 100 万美元。医疗保健行业数据泄露耗费的成本已连续 12 年高居榜首，自 2020 年报告以来增长了 41.6%。金融组织的成本居第二位，平均 597 万美元，其次是制药行业 501 万美元，科技行业 497 万美元，能源行业 472 万美元。

944 万美元

美国的数据泄露平均成本，高于其他任何国家

数据泄露平均成本最高的五个国家和地区分别是美国 944 万美元、中东 746 万美元、加拿大 564 万美元、英国 505 万美元以及德国 485 万美元。美国已连续 12 年高居榜首。同时，与去年相比，增长率最快的国家是巴西，从 108 万美元增加到 138 万美元，增长了 27.8%。

如下建议可最大限度减少因数据泄露事件造成的财务影响

在这部分中，IBM Security 概括介绍了组织可采取哪些措施来降低数据泄漏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。这些建议包括本研究中受访组织所采用的各种成功的安全保障方法。

采用零信任安全模型可防止人员未经授权访问敏感数据。
研究结果表明，尽管只有 41% 的组织实施了零信任安全措施，但如果部署周全，仍可助力组织节省高达 150 万美元的数据泄露成本。随着各组织采用远程工作方式和构筑混合多云环境，零信任策略可通过限制相关的可访问性，并要求提供上下文背景凭据来助其保护数据和资源。

这些安全工具能在不同系统之间共享数据并可集中进行数据安全操作，进而确保安全团队可跨越混合多云复杂环境，检测出各种数据泄露事件。开放式安全平台有助于促进实施零信任策略，通过该平台，您可获得更加深刻的洞察成果、降低风险并加快响应速度。此外，您可将数据留存在原处，同时利用现有投资，让您的团队运作做到更加高效和协调。

采用策略和加密保护云环境中的敏感数据。
随着托管于云环境中的数据量和数据价值持续增加，组织应采取有力措施保护云托管数据库。与未采用云安全措施相比，采用成熟的云安全措施可节省数据泄露成本高达 72 万美元。采用数据分类架构和保留方案有助于建立可视化管理，有效减少易于泄漏的总体敏感信息数量。利用数据加密和全同态加密来保护敏感信息。采用内部审计框架、全面评估企业风险并跟踪了解合规措施是否符合治理要求，有助于提高检测数据泄露和升级遏制措施的能力。

投资安全统筹、自动化与响应 (SOAR) 策略以及扩展检测和响应 (XDR) 技术，可帮助组织缩短检测和响应时间。
连同安全 AI 和自动化的运行部署，XDR 功能还可显著减少数据泄露平均成本、缩短数据泄露生命周期。根据本研究的结果，与未实施 XDR 的组织相比，已部署 XDR 的组织可缩短数据泄露生命周期平均高达 29 天，节省成本 40 万美元。SOAR 和安全信息及 事件管理 (SIEM) 软件、托管检测和响应服务以及 XDR 技术等可通过自动化、流程标准化以及与现有安全工具的集成，助力组织加快事件响应速度。

采用有助于保护和监测端点和远程员工的工具。
在本研究中，因远程工作导致数据泄露与不是因远程工作导致的数据泄露相比，成本高出近 100 万美元。统一端点管理 (UEM)、端点检测和响应 (EDR) 以及身份和访问管理 (IAM) 产品和服务可为安全团队提供深入的可视化管理，监测相关的可疑活动。这种监管涉及自带设备 (BYOD) 和公司笔记本电脑、台式机、平板电脑、移动设备和物联网等，其中包括组织无法物理访问的诸多端点。UEM、EDR 和 IAM 可缩短调查和响应时间，从而隔离和控制完全或部分因远程工作而导致的数据泄露损失。

创建和测试事件响应运行手册，以提高网络弹性恢复能力。
降低数据泄露成本最有效的两种方法是组建事件响应 (IR) 团队和对 IR 计划进行全面广泛的检测。与没有 IR 团队或不对 IR 计划进行测试的组织相比，设有 IR 团队并定期对 IR 计划进行测试的组织所节省的数据泄露成本高达 266 万美元。通过制定详细的网络事件运行手册，组织可做到快速响应，控制数据泄露造成的后果。通过桌面演练定期对计划进行测试，或者在模拟环境（如网络靶场）中运行数据泄露场景。

对手模拟演练（也称为红队演习）可帮助 IR 团队发现他们可能未察觉的攻击路径和技术，以及在检测和响应能力方面的差距，从而增强 IR 团队的运行效率。攻击面管理解决方案可通过模拟真实攻击体验，找到之前未曾发现的漏洞，助力组织改善安全状态。

安全措施建议仅供教学培训使用，不保证结果。

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

波耐蒙研究所 (Ponemon Institute)

波耐蒙研究所致力于通过独立研究和教育促进企业和政府机构内部构建和推进负责任的信息和隐私管理实践。我们的宗旨是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、隐私和道德研究标准，不会向向个人收集个人可识别信息或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无关联、不相关或不恰当的问题。

IBM Security

IBM Security 提供的集成式企业安全产品和服务组合属于业界最为先进的配置组合。该组合由世界知名的 IBM Security X-Force® 研究作为强大后盾，提供安全解决方案，助力组织将安全纳入业务架构，确保在充满不确定性的市场环境中蓬勃发展。

IBM 运营着全球最广泛、最深入的安全研发和交付组织之一。IBM 每月在 130 多个国家或地区监控超过 4.7 万亿起事件，拥有 1 万多项安全专利。如需了解更多信息，请访问 ibm.com/cn-zh/security。加入 IBM Security 社区的对话。

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），请通过信函、电话或电子邮件与我们联系：

Ponemon Institute LLC
收件人：Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

采取后续步骤

零信任安全解决方案
时刻守护每位用户、每台设备、每次连接的安全。
了解更多信息

身份和访问管理
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

数据安全
发现、分类和保护敏感企业数据。
了解更多信息

安全统筹调度、自动化和响应
部署统筹调度和自动化技术，提高事件响应速度。
了解更多信息

安全信息和事件管理
部署可视化管理，检测、调查和应对各种威胁。
了解更多信息

云安全
将安全性集成至企业转型至混合多云的旅程中。
了解更多信息

端点安全
保护设备、用户和组织免受复杂攻击。
了解更多信息

网络安全服务
借助咨询、云和托管安全服务，降低安全风险。
了解更多信息

事件响应和威胁情报
积极管理和应对安全威胁。
了解更多信息

预约 IBM Security X-Force 专家，进行一对一咨询
立即预约

国际商业机器(中国)有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编:100020

美国出品
2022 年 7 月