《2025 年数据泄露成本报告》
AI 监管缺位

执行摘要

think report

IBM

执行摘要

欢迎阅读 IBM 年度《数据泄露成本报告》。值此报告发布之际，我们迎来了数据泄露研究二十载的里程碑。今年，我们将目光聚焦于本世代最根本的技术变革：AI 的普及。

通过 2025 年度报告，我们开始系统地对 AI 相关风险进行记录和量化。研究发现令人忧虑：众多企业为追求“快速上马”，跳过了 AI 安全治理环节。这些缺乏监管的系统更容易遭受攻击，且失陷后损失更为惨重。此现象实属意料之中。

自 2005 年起，本报告持续追踪不断扩张的技术版图及其伴生的威胁。波耐蒙研究所（Ponemon Institute）作为研究合作伙伴，不仅记录了新型威胁与攻击面的出现，更以企业安全与业务决策者能够理解并采取行动的财务指标来量化这些风险。综合来看，其研究人员累计分析了 6485 起数据泄露事件，访谈了 34652 位参与事件响应的技术、安全及业务负责人。

安全威胁态势经历了显著变迁。二十年前，近半数数据泄露事件 (45%) 是由笔记本电脑或 U 盘等设备丢失引发的，仅 10% 归因于“电子系统遭入侵”。如今，大多数泄露事件源于网络钓鱼、内部威胁等多样化的恶意活动。

十年前，云配置不当甚至都未被列为独立的威胁类别。而如今，云环境及其存储的数据已成为主要的攻击目标。在 2020 年新冠封控期间，勒索软件攻击才开始大量激增。次年，此类攻击平均造成了 462 万美元的损失，到本年度报告发布时，这一数字已攀升至 508 万美元。

波耐蒙研究所的研究工作始终如一。本年度的研究由波耐蒙研究所独立执行，IBM 提供赞助、分析与发布支持，涵盖 2024 年 3 月至 2025 年 2 月期间遭受数据泄露的 600 家企业。我们共同调研横跨 17 个行业、16 个国家地区的企业，分析事件涉及 2960 至 113620 条不等的失陷记录。为获取一线洞察，波耐蒙研究人员访谈了 3470 位掌握所在企业泄露事件第一手资料的安全负责人及企业高管。受访者涵盖首席执行官、运营总监、财务总监、IT 从业者、业务单元负责人、总经理以及风险管理与网络安全从业者。

本报告为商业、技术与安全领域的领导者提供了基准参考，有助于他们强化防御体系、优化资源配置并推动创新，特别是在 AI 项目的安全治理方面。

本年的关键发现：全球数据泄露成本五年来首次下降，降至 444 万美元，这得益于 AI 驱动的防御加速了事件的遏制。然而，在防御者取得进步的同时，攻击者也在同步升级——约 16% 的泄露事件涉及攻击者使用 AI 技术，这种情况常见于钓鱼攻击与深度伪造。尽管这场 AI 技术军备竞赛通过降低全球泄露成本使企业受益，但美国却呈现出逆势上扬的态势。受严厉监管处罚及不断攀升的检测成本驱动，该国的数据泄露成本已突破 1000 万美元。

我们还发现，AI 的应用速度已经快于监管跟进的速度。研究发现：97% 的 AI 相关安全事件源于缺乏完善访问控制的 AI 系统。多数遭遇攻击的企业承认，它们既未建立 AI 治理政策，也未防范“影子 AI”（未经企业批准或监管的 AI 应用）。影子 AI 的隐蔽使用与治理缺失共同推高了数据泄露成本。

2025 年报告新增维度

延续传统，《数据泄露成本报告》持续追踪新技术、新策略以及近期事件。本年度首次涵盖以下内容：

- AI 安全与治理现状
- 影子 AI 的普及率及风险特征
- AI 安全事件中的目标数据类型
- 泄露事件导致业务中断的持续时间
- 量子安全工具实现的成本节约
- AI 驱动攻击造成的泄露成本
- 转嫁至客户的泄露成本比例

重要结论

本文所述关键结论，是基于 IBM 对波耐蒙研究所独立汇编的研究数据进行的分析。

444 万美元

全球平均数据泄露成本

全球平均数据泄露成本从 2024 年的 488 万美元降至 444 万美元，降幅达 9%，回归至 2023 年的水平。成本下降主要得益于事件识别与遏制速度的提升——这主要归功于企业自有安全团队及安全服务商在 AI 与自动化技术的辅助下，能够快速识别与遏制事件。若非美国地区成本激增 9%，达到 1022 万美元（创下区域历史新高），全球平均值可能会更低。美国监管罚款增加以及检测升级成本上升是主要原因。

20 万美元

涉影子 AI 事件的附加成本

在今年接受调研的企业中，20% 表示遭遇了由影子 AI 相关安全事件引发的数据泄露。此类事件使得平均泄露成本增加了 20.0321 万美元。65% 的事件导致个人身份信息泄露，40% 造成知识产权失窃。这些数据常常存储于多种环境之中，这表明单个未受监控的 AI 系统就可能引发大规模的数据泄露。影子 AI 的迅猛发展已经取代安全人才短缺，成为本报告统计的三大高成本泄露因素之一。

49%

事件后追加安全投资的企业比例

在发生泄露事件后计划追加安全投资的企业比例显著下降，今年为 49%（去年为 63%）。在计划追加投资的企业中，不足半数将重点放在 AI 驱动的安全方案或服务上，例如威胁检测响应、事件响应（IR）规划测试、数据安全防护工具等。

13%

AI 相关安全事件占比

目前，企业 AI 系统直接引发的安全事件仍然相对有限。平均有 13% 的企业报告其 AI 模型或应用涉及泄露事件。但其中近全部（97%）都缺乏完善的 AI 访问控制。最常见的安全事件发生在 AI 供应链中，由受污染的应用程序、API 或插件引发。此类事件会引发连锁反应：它们导致了广泛的数据泄露（60%）和业务中断（31%）。这表明，AI 正成为高价值的攻击目标。

190 万美元

全面应用 AI 的安全成本节约

与未采用 AI 解决方案的企业相比，广泛运用 AI 与自动化的安全团队将事件处置时间缩短了 80 天，平均泄露成本降低了 190 万美元。近三分之一的企业表示在安全生命周期（防护、检测、调查、响应）中全面应用了这些工具。然而，这一比例较上年仅略有增长，暗示 AI 的应用可能陷入停滞。这也表明，多数企业仍未采用 AI 与自动化技术，因而无法获得相应的成本效益。

63%

缺乏 AI 治理政策的企业占比

多数遭遇泄露的企业（63%）尚未建立或仍在制定 AI 治理政策。即便已经制定了政策，也不足半数设置了 AI 部署审批流程，62% 的企业缺乏完善的 AI 系统访问控制。在已建立治理政策的企业中，仅有少数（34%）会定期审计未授权的 AI 应用。这表明，当应用速度超越安全与治理能力时，AI 基本处于失控状态。

492 万美元

恶意内部攻击平均成本

恶意内部攻击连续两年位居高成本初始威胁向量首位，平均造成 492 万美元的损失。第三方供应商与供应链攻击（491 万美元）紧随其后。其他高成本的攻击向量还包括漏洞利用和钓鱼攻击。不过，最高发的攻击类型仍是钓鱼攻击（占比 16%），其平均成本为 480 万美元。

63%

拒绝支付勒索赎金的企业比例

2025 年拒绝支付赎金的勒索受害者比例（63%）高于 2024 年（59%）。但勒索软件事件的平均成本仍居高不下，尤其是当攻击者主动披露事件时（508 万美元）。与此同时，上报执法机构的勒索受害者数量有所减少——今年 40% 的企业选择报案，而去年这一比例为 53%。

六分之一

涉及 AI 驱动攻击的泄露事件占比

攻击者利用生成式 AI 可以优化并扩大钓鱼攻击等社会工程攻击的规模。IBM 早前发现，生成式 AI 使编写高仿真钓鱼邮件的耗时从 16 小时锐减至 5 分钟。本年报告揭示了其影响：平均有 16% 的数据泄露涉及攻击者使用 AI 技术，最常见于 AI 生成钓鱼攻击（37%）和深度伪造冒充攻击（35%）。

建议

IBM 专家提出五项有效方案，助力预防数据泄露、降低损失成本，并保障 AI 模型、应用及使用的安全治理。

强化身份安全——涵盖人类与机器

众多企业存在访问控制松散、账户权限过度分配、关键系统访问者可视性不足等问题。不同部门及工具常常各自为政地管理身份访问（IAM）。这些漏洞正被攻击者利用，必须及时封堵。与此同时，AI 模型及基础设施的快速增长为攻击者提供了新型高价值攻击面。

借助 AI 与自动化技术加固身份安全，能够在不加重安全团队人力负担的前提下优化 IAM。随着 AI 智能体在运营中作用日益凸显，其身份保护需遵循与人类用户同等严格的标准。AI 智能体如同人类用户，日益依赖凭证访问系统以执行任务。因此必须实施强操作管控（或采用辅助服务），并全面监控所有非人类身份 (NHI) 活动。企业需能区分使用托管（保险库）凭证与非托管凭证的 NHI。

凭证纳入管理后，
必须强化生命周期治理。这包括凭证的分配、轮换、审计、保护及注销，以及监控 NHI 行为以确保其在预期参数内运行。此举可降低凭证滥用风险，维护安全合规环境。

如今多数攻击者通过登录凭证而非入侵系统得手。应对此威胁的关键在于阻断攻击者获取凭证的途径。最有效的方式之一是确保全员采用防钓鱼验证方法（如密钥），此类技术旨在消除传统密码和一次性验证码的漏洞，大幅增加攻击者截获或滥用凭证的难度。

提升 AI 数据安全实践

企业现已跨越生成式 AI 与 AI 智能体的实验阶段，将技术深度融入核心业务以实现创新。但应用速度已超过安全防护。本年报告显示，62% 的企业缺乏完善的 AI 系统访问控制。而数据作为 AI 的燃料，自然成为攻击者的首要目标。

保障 AI 数据安全不仅关乎隐私合规，更涉及保护数据完整性、维护企业信任及避免数据泄露。这要求超越表层管控，夯实数据安全基础：包括数据发现与分类及数据保护措施（访问控制、加密及密钥管理），还包括采用数据与 AI 安全服务。这些措施并非 AI 安全专属，但当 AI 兼具威胁载体与防御工具双重身份时，其重要性空前凸显。

打通 AI 安全与 AI 治理

AI 安全与 AI 治理实际上是一个互补的体系。若企业将二者割裂对待，将会推高风险、增加复杂度并提高成本。当前，AI 应用的普及速度已经超越了安全治理的建设速度：41% 的受访企业尚未建立相关制度，22% 的企业仍在制定中。

企业需确保首席信息安全官 (CISO)、首席营收官 (CRO)、首席合规官 (CCO) 及其团队定期进行协同合作。投资集成化的安全治理软件与流程，以聚合跨职能的利益相关者，可助力企业自动发现并管控影子 AI。此类投资还能：

- 洞悉所有 AI 部署的状态。
- 识别并修复漏洞。
- 防护因非预期使用而产生的提示词及数据。
- 运用可观测性工具提升合规检测与异常发现能力。

借助 AI 安全工具及自动化技术加速响应

攻击者已利用 AI 提升攻击效率——例如仅需少量提示词即可生成深度伪造内容，或将钓鱼信息制作时间从数小时压缩至数分钟。面对攻击者采用 AI 发动的自适应攻击，安全团队更应部署 AI 技术：通过提升威胁狩猎精准度、缩短响应时间等主动措施，减少或阻断攻击及其业务影响。

安全工具及托管安全服务（包括由 AI 和自动化驱动的解决方案），能够增强负担过重的安全团队能力。它们可以显著减少告警数量、识别存在风险的数据、更早发现安全漏洞与威胁、检测进行中的入侵事件，并实现更快速、更精准的攻击响应。

提高弹性

从长远来看，数据泄露是不可避免的。即便采取了强有力的预防措施，泄露事件依然可能发生。虽然努力阻挡威胁很重要，但这不应是企业的唯一关注点。企业还必须关注并制定计划，以便在攻击成功突破防线、发生泄露时，将损害降至最低。

构建弹性意味着能够快速发现问题、在其造成重大影响前加以遏制，并以最小的干扰迅速恢复运营。构建弹性的计划应包括：定期测试事件响应 (IR) 计划和备份恢复流程；确保危机响应期间（即使对非技术领导者）角色和职责清晰；限制高级别访问权限以缩小潜在问题的波及范围。面对面的或虚拟的培训对于帮助安全团队理解自身角色并在危机中有效执行至关重要。为增强应对攻击的能力，企业还可参与网络靶场危机模拟演练。

简介

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 ibm.com/cn-zh。

了解有关提升企业安全状态的更多信息：请访问 ibm.com/cn-zh/security。

加入 IBM Security 社区的对话。

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企业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