五大应避免的常见数据安全陷阱

了解如何改善安全态势

IBM Security

目录

数据安全应该是企业的头等大事，而且理由很充分。

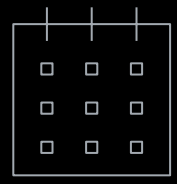
即便 IT 格局变得越来越分散、越来越复杂，我们也要知道非常重要的一点，即：许多安全漏洞是可以防范的。尽管不同企业的安全挑战和目标可能会有所不同，但他们在应对数据安全性时往往会犯一些相同的普遍错误。此外，许多企业领导者经常将这些错误视为正常的商业实践。

有几个内部和外部因素会导致成功的网络攻击，具体来说包括：

- 网络边界侵蚀
- IT 环境的复杂性增加导致攻击面扩大
- 云服务给安全实践带来的要求不断增多
- 网络犯罪日益高级化的性质
- 持续的网络安全技能短缺
- 员工缺乏数据安全风险意识

819 万美元

2019 年美国企业所遭受数据泄露事件的平均成本[1]



245 天

美国企业识别并遏制数据泄露所需的平均时间[1]

您的数据安全实践健全性如何?

让我们来看一下在数据安全方面会导致组织容易遭受潜在攻击的五个最普遍且可避免的错误做法，以及如何避免这些错误做法。

加速合规

集中管理安全性

确立所有权

评估漏洞

对活动进行优先排序

陷阱 1

未能超越合规

合规并不一定意味着安全。专注于通过有限的安全资源来确保符合审核或认证要求的组织会感到自满。即便是名义上完全合规的组织，也遭遇了许多大规模数据泄露事件。以下示例说明了仅仅关注合规性会如何降低有效安全性：

覆盖不完全
在进行年度审核之前，企业经常会“临阵磨枪”，解决数据库配置错误和过时的访问策略。企业应持续评估漏洞和风险。

投入最低
许多企业之所以采用数据安全解决方案，只是为了满足法律要求或业务合作伙伴的要求。这种“执行最低安全标准并重新将重点放在业务上”的思路，会有悖于良好的安全实践。有效的数据安全性是一场马拉松赛而非短跑比赛。

紧迫意识淡却
随着《萨班斯奥克利法案》(SOX)、《通用数据保护条例》(GDPR) 等法规不断成熟，企业会在其安全控件管理方面变得自满。随着时间的推移，领导者对受监管数据的隐私、安全性和保护的关注会不断淡却，但不合规相关的风险和成本仍然存在。

1.4 次/天

尽管《医疗保险可携性和责任法案》(HIPAA) 已经出台，但在 2019 年，估计每天发生了 1.4 起医疗保健数据泄露事件。[2]

无人监管数据的疏漏
知识产权等资产一旦丢失或与未授权人员共享，便会让组织面临风险。仅仅专注于合规会导致安全部门对重要数据的忽视及安全疏漏。

解决方案

认识并接受“合规是起点，而非目标”

数据安全部门必须制定战略计划，始终如一地保护其业务关键数据安全，而不是仅仅响应合规要求。

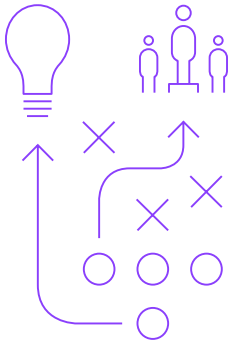
数据安全和保护计划应包括以下核心实践：

- **发现和分类**：发现内部数据存储和云数据存储中的敏感数据并对其进行分类。
- **评估风险**：基于情境式洞察力和分析来评估风险。
- **保护敏感数据**：通过加密和灵活的访问策略来保护敏感数据。
- **监控**：监控数据访问和使用模式，以快速发现可疑活动。
- **响应威胁**：实时响应威胁。
- **简化**：简化合规流程及其报告流程。

最后一个要素可以包括与合规相关的法律责任、企业可能遭受的损失以及这些损失的潜在成本（不包括违规罚款）。

最终，您应该从整体上考虑要保护的数据的风险和价值。

将合规性视为推动创新并提升安全标准，进而为业务提供支持的机会。



陷阱 2

未能识别对集中式数据安全性的需求

如果没有涵盖数据隐私和安全的更广泛的合规要求，组织领导者便会忽略对整个企业范围内一致的数据安全的需求。

对于具有不断变化且增长的混合多云环境的企业而言，每周或每天都会出现新的数据源，而且这些数据源会散播敏感数据。

已开始发展并扩展其 IT 基础架构的企业领导者会忽略不断变化的攻击面所带来的风险。当敏感数据在日益复杂且分散的 IT 环境中移动时，他们会缺乏对此类数据的足够可视性和可控性。如果未能采用端到端数据隐私、安全和保护控制措施（尤其是在复杂环境中），就会导致监督成本过高。

在数据孤岛中运行安全解决方案会导致出现其他问题。举例来说，已部署了安全运营中心 (SOC) 及安全信息和事件管理 (SIEM) 解决方案的组织会忽视向这些系统馈入从其数据安全解决方案中收集的洞察。同样，安全人员、流程和工具之间缺乏可互操作性也会阻碍任何安全计划的成功。

加密、业务连续性管理、将安全集成到软件开发流程 (DevSecOps) 之中及威胁情报共享，有助于降低数据泄露成本。[1]

解决方案

了解敏感数据所处的位置，包括内部存储库和云托管存储库

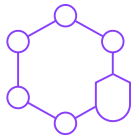
敏感数据的保护应与广泛的安全保护投入结合进行。除了了解敏感数据的存储位置之外，您还需要了解敏感数据的访问时间和方式，即便是在这些信息快速变化的情况下，亦应如此。此外，您应采取相应措施，将数据安全和保护洞察力及策略与总体安全计划集成到一起，以实现技术之间紧密一致的协同。关于这一点，部署跨不同环境和平台运行的数据安全解决方案会有所帮助。

那么，何时才是将数据安全作为更全面的安全实践的一部分，与其他安全控制措施集成到一起的适当时机？如果出现以下所列迹象，则表明您的组织需要采取这一措施：

丢失宝贵数据的风险
您的组织的个人数据、敏感数据和专有数据具有巨大的价值，因此，一旦此类数据丢失，就会严重损害企业的生存能力。

监管影响
您的组织依照相关法律要求收集和存储数据，比如信用卡号、其他付款信息或个人数据。

敏感数据的保护应与广泛的安全保护投入结合进行。



缺乏安全监督
随着您的组织的发展，您会面临难以跟踪和保护所有网络端点（包括云实例）的安全性的窘境。举例来说，您是否清楚地了解内部数据存储和云数据存储中数据的存储位置、存储/共享/访问时间和方式？

评估不足
您的组织采用片段化的方法，对所有安全活动的投入没有清晰的了解。举例来说，您是否拥有适当的流程来准确地衡量为降低数据安全风险而分配资源的投资回报 (ROI)？

如果您的组织出现前述任何一种情况，则应考虑部署将数据安全集成到更广泛的现有安全性实践中所需的安全技能和解决方案。

陷阱 3

未能确定数据责任人

许多公司即使意识到了数据安全的必要性，也没有委派专门的人员来负责保护敏感数据。组织在寻找真正的安全责任人方面面临着一些压力，这种情况在数据安全或审计事件期间通常会尤为明显。

高管们可能会求助于首席信息官（CIO），而首席信息官可能会说：“我的职责是确保关键系统能够正常运行。关于这个问题，您可以与我的 IT 员工谈谈。”这些 IT 员工可能要负责多个数据库，这些数据库中存储有敏感数据但缺乏安全预算支持。

通常而言，首席信息安全官（CISO）所带领团队的成员并不直接负责在整个企业中流动的数据。他们可能会向企业中的不同业务线（LOB）经理提供建议，但是在许多公司中，并没有明确的数据负责人。数据是组织最有价值的资产之一。不过，在没有所有权责任的情况下，适当保护敏感数据便会成为一个挑战。

74%

的受访组织表示，网络安全技能短缺已给其组织造成了影响。[3]

“2018 年，67.9% 的受访公司表示他们设立了首席数据官 (CDO)。不过，该角色的定义并不明确。”[4]

NewVantage 报告
2019 年大数据与 AI 高管调研 - 调研结果执行摘要

阅读案例研究 →

解决方案

聘请一名 CDO 或 DPO，专门负责敏感、关键数据集的管理和安全

在复杂的 IT 环境中，考虑以下各类数据至关重要：

跨业务部门共享的数据

位于混合多云基础架构中的数据

存储在移动设备上的数据

首席数据官 (CDO) 或数据保护官 (DPO) 可以负责处理这些事务。实际上，依照 GDPR 的要求，总部位于欧洲或与欧盟数据主体有业务往来的公司，都必须设立 DPO。这一要求意味着 GDPR 已经认可了敏感数据（即这种情况下的个人信息）具有超越使用此类数据的 LOB 的价值。此外，该项要求还强调企业应设立专门的角色来负责数据资产。在选择 CDO 或 DPO 时，应考虑以下目标和职责：

技术知识和业务意识
评估风险并提出实用的业务案例，同时确保即便是非技术性业务主管也能从适当的安全投资角度理解这些业务案例。

战略实施
在技术层面上引导安全计划的实施，通过检测、响应和数据安全控制措施来保护数据安全。

合规领导力
了解合规要求，并了解如何将这些要求映射到数据安全控制措施，确保企业合规性。

监控和评估
监控威胁格局并评估数据安全计划的有效性。

灵活性和扩展
了解何时以及如何调整数据安全策略，比如通过集成更多高级工具在新环境中扩展数据访问和使用策略。

劳动力事业部
与云服务提供商就服务水平协议 (SLA) 以及与数据安全风险和补救措施相关的责任设定预期。

数据泄露响应计划
最后一点，为承担关键职责做好准备，制定战略性数据泄露缓解和响应计划。

组织的每个成员都需要共同努力，确保有效地保护公司数据，因此，CDO 或 DPO 应负责领导各个团队之间以及整个企业内的数据安全协作。这种协作有助于 CDO 或 DPO 监督组织为确保其敏感数据安全而需要采取的计划和保护措施。

陷阱 4

未能解决已知漏洞

众所周知的企业数据泄露事件通常都是由于在补丁发布后仍未进行修复的已知漏洞所致。由于网络犯罪分子会主动寻找这些容易切入的弱点，因此如果未能快速修补已知漏洞，将会让组织的数据面临风险。

不过，由于 IT、安全和运营团队之间需要协调，因此许多企业会发现在快速实施补丁方面面临着挑战。此外，补丁通常需要进行测试，以查看它们是否破坏了流程，或是否会引入新漏洞。

在云环境中，某些情况下很难知道是否应修复合同项下的服务或应用组件。即使在某个服务中发现了漏洞，用户也常常缺乏对服务提供商进行的修复过程的控制。

51%

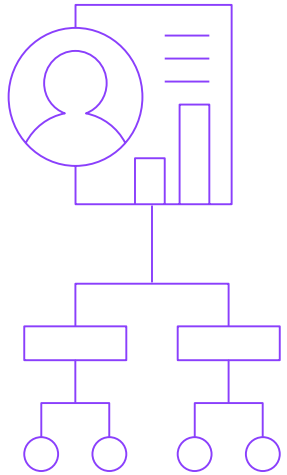
2019 年，51% 的数据泄露是由于恶意攻击造成的。恶意攻击是数据泄露事件最常见、成本最高的主要原因。[1]

解决方案

制定有效的漏洞管理计划，并采用适当的技术来支持此类计划的发展

漏洞管理通常涉及以下一些级别的活动：

- 维护数据资产的准确清单和基准状态。
- 对整个基础架构（包括云资产）进行频繁的漏洞扫描和评估。
- 考虑漏洞被利用的可能性以及安全事件对业务所产生的影响，划分漏洞修复的优先顺序。
- 与第三方服务提供商一同将漏洞管理和响应能力作为 SLA 的一部分纳入其中。
- 尽可能对敏感数据或个人数据进行模糊处理。您可以通过加密、令牌化和编修这三种方式来实现此目的。
- 采用适当的加密密钥管理，确保加密密钥安全地得以存储并适当循环，进而确保加密数据的安全。



即使在成熟的漏洞管理计划中，也没有系统能够做到尽善尽美。即使得到最佳保护的环境也可能会遭受入侵，因此您的数据还需要另一级别的保护。正确的数据加密技术和功能有助于保护您的数据免受新兴威胁的侵害。

陷阱 5

未能确定优先级并充分利用数据活动监控功能

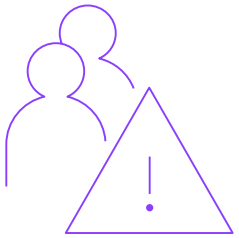
对于任何数据安全战略而言，数据访问和使用监控都必不可少。组织负责人需要知道访问数据的主体、访问方式和时间。此类监控应包括这些人员是否应具有访问权限、访问权限级别是否正确，以及此类访问是否会给企业增加风险。

特权用户身份是内部威胁的主要“元凶”。[5] 数据保护计划应涵盖实时监控功能，以检测被用于可疑活动或未经授权活动的特权用户帐户。为防止可能的恶意活动，数据安全解决方案必须能够执行以下任务：

- 基于违例情形阻止和隔离可疑活动。
- 基于异常行为暂停或终止会话。
- 在数据环境中使用预定义的法规特定工作流。
- 将可执行的警报发送到 IT 安全和运营系统。

内部人员威胁的全球平均成本为

1,145 万美元。[6]



组织在说明数据安全及合规相关信息，以及了解何时和如何应对潜在威胁方面困难重重。由于授权用户会访问多个数据源，包括数据库、文件系统、大型机环境和云环境等，因此监控和保存来自所有这些交互的数据似乎是一项艰巨的任务。挑战在于如何高效地监控、捕获、过滤、处理和响应大量数据活动。如果没有适当的计划，您的组织将会面对比合理处理能力更多的活动信息，进而会降低数据活动监控的价值。

解决方案

制定综合性数据安全检测与保护战略

为此目的，在启动数据安全之旅时，您需要确定监控的规模和范围，以适当地解决需求和风险。该活动通常会采用分阶段的方法，以支持在整个企业内开发和扩展最佳实践。此外，在流程的早期与业务和 IT 部门的关键利益相关者开展对话，了解短期和长期业务目标也至关重要。

此类对话还应包括获取为关键计划提供支持所需的技术。举例来说，如果业务部门计划结合使用内部数据存储库和云托管数据存储库在新的地理位置设立办事处，则在制定数据安全战略时，应评估该计划会对组织的数据安全性和合规性带来哪些影响。举例来说，公司拥有的数据将受限于新的数据安全与合规要求（例如 GDPR、《加利福尼亚消费者隐私法案》(CCPA)、巴西的 Le Geral deProteçãode Dados (LGPD) 等等）。

您还应确定优先级，并将重点放在可能具有最敏感数据的一个或两个来源上。在将这些实践扩展到基础架构的其余部分之前，应确保针对这些数据源的数据安全策略清晰明了。

2019 年，未部署安全自动化解决方案的组织所遭受数据泄露的全球平均总成本比部署此类解决方案的组织

高出 95%[1]

516 万美元 **（未部署自动化解决方案的组织）**[1]

265 万美元 **（完全部署了自动化解决方案的组织）**[1]

您应寻找一种具有丰富分析功能的自动化数据或文件活动监控解决方案，而且此类解决方案应专注于与特权用户相关的主要风险和异常行为。尽管在数据或文件活动监控解决方案检测到异常行为时必须能够接收自动警报，但在发现异常或偏离数据访问策略的情况时，您也必须能够迅速采取措施。保护措施应包括动态数据屏蔽或阻止。

在制定数据活动监控和保护计划时，考虑以下问题通常会有所帮助：

- 我最敏感的两个数据源是什么？
- 根据敏感数据量，我接下来应优先考虑哪些数据源（5 到 10 个）？
- 某些端点或云资产是否与高风险数据相关联？
- 敏感数据是否可以在内部环境、混合环境和云环境中自由来回移动？
- 应在哪些条件下授予哪些用户访问数据源的权限？
- 哪些高风险用户或特权帐户需要关闭或进行更严格的审查？
- 我的数据安全解决方案是否支持实时活动监控和自动数据保护功能？
- 是否部署了实时监控功能，用以跟踪数据存储（例如 Structured Query Lanuage (SQL) 数据库、Hadoop 分布、NoSQL 平台等）所含文件中的数据？
- 我的监控解决方案是否考虑了跨混合多云环境的数据存储？是否允许生成自定义报告，并在适当的时间发送给适当的人员？
- 我是否拥有高效地对风险、漏洞和补救工作进行优先排序所需的风险分析及经过筛选的监控功能？

您在监控优先事项和保护方面的要求越具体，此类解决方案就越能高效地支持您将其运用到可用的检测和响应资源。

下一步行动

您如何避免这些常见的数据安全陷阱，尤其是在越来越多的公司开始追寻混合多云环境的情况下？首先要认识到这一问题，并让您的组织做好准备，采取主动的全局式方法来保护数据，无论其位于何处。

如果贵企业拥有复杂的混合 IT 环境，孤岛式的数据安全方法将会无法奏效。您需要添加跨整个数据基础架构且支持所有数据类型的数据保护战略。

您可以立即采取的、用以保护组织宝贵数据的后续步骤包括：

- 制定支持组织的短期和长期业务与技术目标的数据安全战略
- 通过适当的人员、流程和工具实施该战略
- 规划相应资源，确保数据安全与合规计划可以随着贵组织对现代技术的采用而有效地进行扩展

IBM® Security Guardium® 数据保护平台旨在帮助组织采用更智能、更具适应性的方法来保护关键数据，无论其位于何处。了解为何该解决方案是贵组织的理想之选。

更多信息，敬请访问：
ibm.com/guardium。

超过 4 周

大多数组织在不到 1 个月的时间内便通过 Guardium 实现了价值。[7]

为什么选择 IBM Security?

IBM Security 可以提供最先进、集成的企业安全产品和服务组合。该产品组合由享誉全球的 IBM X-Force® 研究与开发团队提供支持，能够提供安全智能，帮助组织全面保护其人员、基础架构、数据和应用的安全。IBM Security 提供了各种解决方案，涵盖身份与访问管理、数据库安全、应用开发、风险管理、端点管理、网络安全等多个领域。这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。

IBM 作为全球覆盖范围最广的安全研究、开发和交付组织之一，每天对 130 多个国家/地区的超过

600 亿

次事件进行监控。

IBM 拥有 3,700 多项安全专利。

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2020 年 4 月

1 “Cost of a Data Rreach report 2019”，*IBM Security*。databreachcalculator.mybluemix.net/executive-summary

2 “Healthcare Data Breach Statistics”，*HIPAA Journal*。www.hipaajournal.com/healthcare-data-breach-statistics

3 Jon Oltsik，“The Life and Times of Cybersecurity Professionals 2018”，*Enterprise Strategy Group and Information Systems Security Association International*，2019 年 4 月。www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity- Professionals-Apr-2019.pdf

4 NewVantage Report，“Big Data and AI Executive Survey 2019 Executive Summary of Findings”，*NewVantage Partners*，2019 年。newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba，“Why Privileged Account Management Is Key to Preventing Insider Threats”，*Security Intelligence*，2018 年 6 月 20 日。securityintelligence.com/why-privileged-access-management-is- key-to-preventing-insider-threats

6 “Cost of Insider Threats:Global Report 2020”，*Ponemon Institute*，2020 年。www.ibm.com/security/digital-assets/services/cost-of- insider-threats/#

7 “Ponemon Report:Client Insights on Data Protection with Guardium”，*Ponemon Institute*，2019 年 8 月。www.ibm.com/account/reg/us-en/signup?formid=urx-40683

SEL03144-CNZH-02