全球数据安全观察

总第 122 期 2023 年第 3 期

(2023.01.16-2023.01.29)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、国务院两部门：高效开展重要数据和个人信息出境安全评估

国务院办公厅近日转发商务部、科技部《关于进一步鼓励外商投资设立研发中心的若干措施》。《若干措施》提出了支持开展科技创新、提高研发便利度、鼓励引进海外人才、提升知识产权保护水平 4 方面 16 条政策举措。

《若干措施》在高效开展重要数据和个人信息出境安全评估方面提出：**支持研发数据依法跨境流动**。落实网络安全法、数据安全法、个人信息保护法等有关法律法规要求，加强数据跨境安全管理，保障国家安全和社会公众利益，保护个人信息权益。高效开展重要数据和个人信息出境安全评估，促进研发数据安全有序自由流动。

https://mp.weixin.qq.com/s/HoXJzY9NNvqMkt3htdN44g

2、人社部发布“数据安全工程技术人员国家职业标准”

1 月 17 日，为适应数字经济发展需要，加强数字技术人才培养，促进数字经济和实体经济深度融合，人力资源社会保障部办公厅发布《数据安全工程技术人员国家职业标准》《机器人工程技术人员国家职业标准》《密码工程技术人员

国家职业标准》《增材制造工程技术人员国家职业标准》4个国家职业标准的征求意见稿。现面向社会公开征求意见。其中，《数据安全工程技术人员国家职业标准》对数据安全工程技术人员的职业要求作出了规定，包括职业概况、基本要求、工作要求和权重表四部分。

https://mp.weixin.qq.com/s/08VbosIjHRTGoA8wdDxECg

3、全国首个获批数据出境安全评估案例落地北京

日前，首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目成为全国首个数据合规出境案例，该项目的审批通过，标志着国家数据出境安全评估制度在北京市率先落地，为强化医疗健康数据出境安全管理，促进国际医疗研究合作提供了实践指引。

https://mp.weixin.qq.com/s/3n5ObAlppZaUfcwCqfwWDw

4、团体标准《数据安全合规评估方法》发布

2023年1月20日，依据《深圳市信息服务业区块链协会团体标准管理办法》的规定，《数据安全合规评估方法》团体标准已通过审批，自2023年1月25日起实施。

http://www.ttbz.org.cn/Home/Show/50433

5、《互联网企业合规建设评价体系》团体标准发布

1 月 5 日，在第四届中国城市信用建设高峰论坛信用监管与互联网+监管融合创新主题论坛上，《互联网企业合规建设评价体系》团体标准发布。

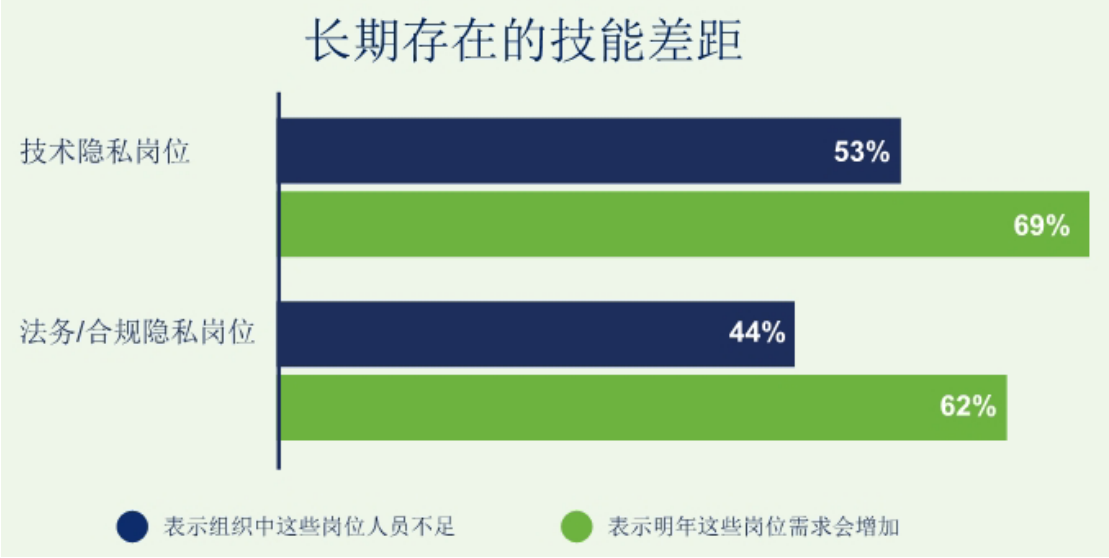
本标准是我国互联网领域第一部以合规建设评价为主的团体标准，从合规战略规划、合规主体责任、合规风险识别、合规整改措施四个方面构建指标体系，包含 4 个一级指标、18 个二级指标、87 个三级指标，主要适用于网络销售类、生活服务类、社交娱乐类、信息资讯类等互联网企业，有助于引导互联网企业依法经营、规范发展。

https://mp.weixin.qq.com/s/WA00UQ90Jm-9RxTKXExRFA

技术、产品与市场

1、ISACA 发布《2023 年度隐私实践研究报告》：人才短缺形势依然严峻

1 月 28 日国际数据隐私日，ISACA 发布《2023 年度隐私实践研究报告》，报告显示坚持实施隐私设计的企业均大有收获，但由于隐私预算、人员配置和技能差距等问题，挑战依然严峻。ISACA 调查了全球 1890 位从事数据隐私工作或详细了解组织内的数据隐私功能的专业人员，报告总结了他们对隐私人员配置、组织结构、框架和政策、预算、培训和数据泄露的看法。



作为隐私行业的一大资源，隐私专业人员仍持续短缺，而明年对技术和法律/合规岗位的需求预计都将增加。技术隐私岗位仍然比法务/合规岗位更缺人。53% 的受访者表示所

在组织在一定程度上或在很大程度上缺乏人手，法务/合规岗位缺人的仅占 44%。调查还发现，许多企业的隐私岗位没招到人（34% 受访者表示技术隐私岗位有空缺，27% 表示法务/合规岗位有空缺）。此外，与法务/合规岗位（62%）相比，技术隐私岗位（69%）在未来一年的需求更有可能增加。

调查结果显示，发生隐私事故最常见的原因是缺乏培训（49%）、数据泄露（42%）和不使用隐私设计（42%）。为了解决以上问题，85% 的受访者表示所在组织为员工提供隐私意识培训，59%的受访者表示组织每年至少审查和修订一次隐私意识培训内容。衡量培训效果最常用的指标是完成培训的员工数量（65%）而非隐私事件的减少（54%），但 73%的受访者认为隐私培训对组织中的隐私意识产生了积极影响。

https://www.secrss.com/articles/51359

2、2022 年 GDPR 开出的累计罚款金额超 30 亿美元

2022 年违反欧洲通用数据保护条例（GDPR）的事件猛增，据律师事务所 DLA Piper 的分析发现，欧洲数据保护委员会在 **2022 年开出的罚款金额约为 29 亿欧元（约 31 亿美元），是 2021 年开出的罚款金额的两倍多**。

根据 2018 年 5 月 25 日全面生效的 GDPR，处理欧洲用户个人数据的组织必须遵守严格遵守 GDPR 关于数据

保护的相关规则，否则将面临最高至全球年收入 4% 或 2000 万欧元的罚款（取其中金额最高者）。根据统计，2022 年开出的最大单笔罚款，源自 9 月针对 Facebook 母公司 Meta 多次涉嫌未能保护儿童个人数据，罚金到达 4.05 亿欧元。

DLA Piper 认为 2022 年罚款金额的快速增长与欧洲数据保护委员会（EDPB）相关，这是一个独立的欧盟机构，负责确保各国在 GDPR 执法方面的一致性。EDPB 在 2022 年裁定的任何案件，没有一个案件的建议罚款金额被降低，DLA Piper 表示，这一趋势对罚款金额产生了“高度通胀的影响”。

https://www.51cto.com/article/745070.html

3、IDC：开源正在改写隐私计算商业逻辑

2022 年下半年以来，在隐私计算领域，开源的趋势愈加显现。蚂蚁集团、翼方健数等相继推出隐私计算开源平台，开放群岛开源社区、FATE 开源社区、百度、腾讯云、京东科技五家企业机构共同发起了“隐私计算开源协同计划”，还有更多隐私计算开源平台获得融资，以及更多基于开源平台研发的隐私计算产品推出。

近日，IDC 发布《IDC Perspective:中国隐私计算开源市

场洞察，2022》。报告通过调研中国市场上典型的在隐私计算领域进行开源实践的厂商、技术使用方以及尚未进行开源的隐私计算厂商，展现了 2022 年隐私计算在中国的开源实践以及未来的发展趋势。

IDC 经过研究发现，开源正在如下几个方面改变着该领域的商业逻辑：

（1）将隐私计算技术的门槛迅速降低——这一点正在动摇隐私计算领域商业逻辑的根本。

（2）改变隐私计算领域的人才供需状况。

（3）将催生更多数量的隐私计算产品的提供方出现，这将使得隐私计算赛道的竞争更加激烈。

（4）大量隐私计算产品的激烈竞争可能促使隐私计算产品价格迅速降低，从而进一步推动隐私计算领域的商业模式发生改变。

（5）新的行业格局与生态正在形成。

（6）在新的形势下，可能产生多种类型的隐私计算产品与服务提供商。与此对应，不同类型的提供商，在不同赛道上的致胜因素也将不同。

https://mp.weixin.qq.com/s/SGSKOqFAa8SdfbO3HGqCzA

4、九大热门 API 安全工具

鉴于 API 安全问题的严重性和紧迫性，近年来 API 安全工具的数量正在快速增加。目前市场上有数十种 API 安全商业工具以及数百种免费或开源工具。通常，根据 API 安全防护生命周期（上图），API 安全工具主要分为、检测、防护与响应、测试、发现、管理几大类；少数厂商宣称能提供完整覆盖 API 安全周期的平台工具，但如今最流行的 API 安全工具主要还是集中在“防护”、“测试”和“发现”三个环节。

CSOonline 基于全球用户和商业评论，评选出了目前九大热门顶级 API 安全工具：**APIsec、Astra、AppKnox、Cequence 统一 API 防护平台、Data Theorem API Secure、Salt Security API 保护平台、Noname Security、Smartbear ReadyAPI、Wallarm 端到端 API 安全平台。**

https://www.secrss.com/articles/51353

5、数据要素市场十大研判

近日，上海数据交易所研究院对数据要素市场发展做了十大研判，内容如下：

研判一：数商破圈成为年度关键词。2023 年“数商”将破圈成为年度关键词，数商不仅将成为创新创业的重要赛道和政府支持相关产业的重要门类，也将成为彰显时代特色的代

名词。

研判二：数据交易机构分化重组。仅在2022年，就有湖南、无锡、福建、郑州、苏州、广州、深圳、杭州等8地数据交易机构揭牌成立。2023年新设数据交易场所将变得困难，既有的数据交易场所将围绕全国统一要素市场目标进行功能分化和结构重组，形成国家-区域-行业-场外的多层次数据要素市场体系。

研判三：场内交易发挥基础设施功能。2023年将重点投入建设具有基础设施功能的数据交易场所，充分发挥场内交易的规范引导作用。

研判四：数据要素市场的逻辑和规则更为清晰。2023年数据要素市场的逻辑和规则将更为清晰，各类主体将在更为清晰的市场逻辑、更为明确的流通交易规则和创新容错规则中，让数据交易不再“棘手”。

研判五：数据要素流通标准体系逐步健全。2023年数据要素相关标准体系将逐步健全，形成分类齐全、层层递进的标准体系。

研判六：数据资产登记和入表走向现实。2023年数据资产登记和入表将分两步走实现，全国统一的数据资产登记机构将依托数据交易机构建立，在确权登记的前提下推动数据资产入表的第二步，从而为更为广阔的数据资产应用服务提

供基础。

研判七：数据产权结构性分置走向落地。2023 年将见证各层级各类制度和规范文件密集出台，推动数据产权结构性分置从理念走向落地。

研判八：公共数据授权运营激活场内交易。2023 年公共数据产品优先乃至应当进场交易将成为各地政策方向，通过公共数据产品激活场内交易，盘活带动整个数据要素市场。

研判九：数据跨境流通打通数字贸易外循环。2023 年数据跨境流通将实现更大发展，与东盟、“一带一路”国家之间的数据跨境流通将成为突破口，打通数字贸易外循环。

研判十：区块链+可信隐私计算赋能数据要素流通。2023 年区块链技术将被真正应用于数据交易系统中，可信隐私计算将继续迭代，为数据交易机构实现的更为广泛的数据要素流通提供安全可信的交付环境。

https://www.secrss.com/articles/51347

业界观点

1、构建公共数据有序开发利用的良好生态

《全国一体化政务大数据体系建设指南》指出，鼓励依法依规开展政务数据授权运营，积极推进数据资源开发利用，培育数据要素市场，营造有效供给、有序开发利用的良好生态，推动数据基础制度体系构建。在数字政府时代，公共数据已成为支撑数字化转型的重要基础资源和关键生产要素。然而，当下公共数据融合应用、政企联动开发、推进改革的模式还需进一步探索。如何在确保安全的前提下推进公共数据开发利用，助力数字经济、数字社会高质量发展显得尤为紧要。

公共数据开发利用是一项亟待探索的复杂系统工程。建议从以下三个环节入手，为公共数据开发利用提供保障，释放数据价值。

第一，加强政务数据平台支撑能力，打造公共数据高质量供给体系。一是推动数据资源“一数一源一标准”治理，加强全链路数据质量的管控。二是搭建元数据管理体系和数据标签管理系统，提高数据目录的好用易用水平。

第二，加强数字政府顶层设计，打造与公共数据开发利用相适配的组织架构。一是纵向上国家层面尽快成立大数据

管理机构，统筹推进国家大数据发展规划、管理和应用等工作。二是横向上有效协同数据治理机构与业务部门，促进公共数据跨部门、跨区域、跨行业安全高效共享。三是夯实基层和市、县（区）队伍基础、人才基础，完善支撑保障机制。

第三，加强数据基础制度体系建设，打造公共数据开发利用新模式。一是创新数据融合应用模式。二是创新数据产品服务模式。三是创新公共数据授权运营模式。

https://mp.weixin.qq.com/s/O5PVzzYK2ImCy2ifm2iWmg

2、魏亮：完善顶层设计，擘画数据安全产业发展蓝图

近日，工业和信息化部印发了《关于促进数据安全产业发展的指导意见》（以下简称“《指导意见》”）。

《指导意见》的出台对数据安全产业高质量发展具有重大意义。一是《指导意见》是贯彻落实国家战略规划与法律要求的关键举措。二是《指导意见》是合理规划数据安全产业发展路径的顶层引领。三是《指导意见》是加速数据要素市场培育和价值释放的重要保障。

《指导意见》为数据安全产业健康良好发展提供全方位、体系化的实践指引。《指导意见》承接《数据安全法》中关于数据安全产业的发展部署，明确数据安全产业发展总体要求，提出指导思想和基本原则，规划阶段性发展目标，聚焦产业

发展重点任务，细化了数据安全技术、产品、服务、标准、人才培养等关键领域的推进方向，为数据安全产业健康良好发展提供全方位、体系化的实践指引。

《指导意见》将全面强化数据安全对数字中国建设和数字经济健康发展的产业支撑。《指导意见》的制定全面贯彻了国家《数据安全法》中关于数据安全产业发展的总体要求，奠定了数据安全产业发展的政策基础，弥补了产业发展顶层设计尚存的不足。《指导意见》的发布，将指引数据安全技术、产品、服务、产业生态、人才等加速优化和发展，全面提升各行业各领域数据安全保障能力。

https://www.secrss.com/articles/51230

3、梅宏院士等：大数据技术的四大挑战与十大趋势

世界主要国家高度重视大数据发展，我国也将发展大数据作为国家战略，发展大数据技术具有重要意义。大数据技术涉及从采集、传输到管理、处理、分析、应用的全生命周期以及生命周期各阶段的数据治理。选取数据生命周期中的管理、处理和分析技术以及大数据治理技术来梳理国内外技术发展现状，特别是研判我国大数据技术发展与国际先进技术之间的差距。另外，在大数据应用需求的驱动下，计算技术体系正面临重构，从“以计算为中心”向“以数据为中心”

转型，在新的计算技术体系下，一系列基础理论和核心技术问题亟待破解，新型大数据系统技术成为重要发展方向。在计算体系重构的背景下，提出大数据技术发展的四大技术挑战和十大发展趋势。

http://cbdio.com/BigData/2023-01/09/content_6171574.htm

4、姚前：数据托管促进数据安全与共享

数据托管机构作为所有数据主体的受托者，对数据资产进行集中托管，可以有效保证数据安全、数据可控且高效利用。就像前台的股票交易需要后台的股票登记存管一样，数据托管机构刚好承担了大数据交易所的后台基础设施角色，从而与大数据交易所一道，构成了完整的大数据基础设施体系。数据托管机构可以是由相关机构组建的数据托管行业联盟，推动数据共建共享；亦可利用区块链技术，基于联盟链或有管理的公链，实现数据的链上托管、确权、交易、流转与权益分配。哪种方式更好，有待在未来实践中进一步探索验证。。

https://mp.weixin.qq.com/s/n9VUg9MlyH0ovj001GPQpw

5、智能化浪潮下 车企更须把好数据安全关

随着智能汽车的增多，汽车数据安全的重要性越发凸显。相较于传统汽车，智能汽车收集的数据范围更广、数据量更

大，数据泄露的风险也更高。确保数据安全，不仅是法律法规需要应对的课题，而且是车企必须高度重视和积极解决的现实问题。

国家工业信息安全发展研究中心此前的调研显示，一辆智能网联汽车每天至少收集 10TB 数据，不仅数量巨大，而且涉及到驾乘人员的出行轨迹、习惯、语音、视频等。这些数据可以实时传输到云端和服务器中，如果保护不当，就有可能被黑客窃取。一旦泄露，危害极大。因此，对于车企而言，必须切实守护数据安全，从多方面强化基础工作。

首先，要强化数据安全意识。从工作流程、技术规范、标准制定、车型设计、安全防范等方面着手，全方位提升数据安全性。

其次，要从技术上确保数据安全。要充分运用最新技术，做好数据安全防护设计，并进行相关配置的维护和升级。

再者，既要帮助用户提高防范意识，也要做好相应预案。一方面，要通过新车推荐和销售、说明书、光盘或随车硬盘等渠道，向用户宣传数据安全的重要性，提升用户重视数据安全、发现问题及时上报的能力；另一方面，要及时接收用户关于数据安全信息的反馈，并进行妥善处理。

https://www.pcauto.com.cn/hj/article/1815931.html

数据安全事件

1、Meta 旗下 WhatsApp 违反了欧盟隐私法，被 DCP 罚款 550 万欧元

DoNews1 月 20 日消息，由于进一步违反了欧盟隐私法，Meta 旗下 WhatsApp 于 1 月 19 日被欧盟主要隐私监管机构爱尔兰数据保护委员会（DPC）罚款 550 万欧元，并要求 WhatsApp 重新评估如何使用个人数据来改善服务。

https://www.donews.com/news/detail/1/3340082.html

2、俄罗斯科技巨头 Yandex 内部源代码全部泄露

安全内参 1 月 28 日消息，俄罗斯最大的 IT 科技公司之一 Yandex 的源代码仓库据传遭到前员工窃取，相关数据已在某个流行黑客论坛上以 BT 种子形式泄露。泄密者公开发布了一条磁力链接，宣称这是“Yandex git sources”，包含了 2022 年 7 月从 Yandex 公司窃取的 44.7 GB 文件。据称，这批数据包含了该公司除反垃圾邮件规则之外的全部源代码。

https://www.secrss.com/articles/51355

3、日本多个中央部门电邮地址遭泄露

据共同社网站报道，共同社记者 21 日采访日本内阁官

房情报安全中心（NISC）等处获悉，日本厚生劳动大臣加藤胜信的电子邮箱地址被泄露到了暗网。这是日本众院事务局分派的电邮地址，被用于注册推特账号。除加藤外，NISC 还发现多个中央部门的电邮地址泄露。

http://m.cankaoxiaoxi.com/world/20230122/2502527.shtml

4、警方称一荷兰黑客获得了几乎所有奥地利人的个人数据

奥地利警方上周披露，一名荷兰黑客于去年 11 月被捕，这名黑客窃取并出售几乎所有奥地利人的个人数据，包括全名、性别、完整地址和出生日期。这名黑客是于 2020 年 5 月在一个黑客论坛上出售这些数据，该数据集已被调查人员确认是真实的。它包含了近 900 万组数据，而奥地利人口为 910 万，因此几乎所有奥地利人都包含在内。该黑客还出售了意大利、荷兰和哥伦比亚等国的类似数据集。

https://www.anquanke.com/post/id/285699

5、美国证券交易委员会意外泄露加密矿工个人信息

PANews 1 月 18 日消息，据华盛顿观察家报报道，一份截图显示，美国证券交易委员会（SEC）于在调查去中心化电网区块链项目 Green 时无意泄露了加密矿工的个人信息。调查的部分内容包括该项目接触的消费者，询问他们购买

Green 产品的情况，并询问他们的体验。虽然 Green 的成员已经与 SEC 合作回答了所有相关问题，但该机构未能在 1 月 6 日将所有 650 名用户的电子邮件以密件方式发送，因此泄露了这些人的姓名和电子邮件。

https://web.panewslab.com/zh/sqarticledetails/lqe0zgxx.html

6、BlackCat 勒索软件团伙窃取了一家工业炸药制造商的秘密军事数据

1 月 27 日，据外媒报道，BlackCat 勒索软件组织声称已经入侵了 SOLAR INDUSTRIES INDIA 并窃取了 2TB 与武器生产相关的“秘密军事数据”，这些数据包括工程规格的完整描述、图纸、许多武器的审计等。

https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html

7、Zacks 投资研究公司数据泄露影响了数十万客户

1 月 25 日，据外媒报道，Zacks 投资研究公司披露了一起数据泄露事件，该安全事件可能影响了其 820,000 名客户的个人信息。该公司在 2022 年底发现了入侵，它认为未经授权的访问发生在 2021 年 11 月至 2022 年 8 月之间的某个时间。暴露的客户数据可能包括用于 Zacks.com 的姓名、

地址、电话号码、电子邮件地址和密码。

https://securityaffairs.com/141343/data-breach/zacks-investment-research-data-breach.html

8、法国橄榄球俱乐部 Stade Français 泄露源代码

1 月 25 日，据外媒报道，Cybernews 最近发现托管官方 Stade Français 网站的服务器正在通过可公开访问的 .git 目录泄露其源代码。该网站为球迷提供每日新闻更新、即将到来的比赛、比赛评论、票务服务和商品商店。对 .git 目录的访问控制不佳可能使威胁行为者能够对俱乐部的服务器进行未经授权的更改。如果威胁行为者利用了该漏洞，它可能会对用户的数据构成风险，并可能导致服务器被接管。

https://securityaffairs.com/141318/data-breach/french-rugby-club-stade-francais-leaks-source-code.html

9、数字情报公司 Cellebrite 的 1.7TB 数据被发布在 DDoSsecret

媒体 1 月 15 日称，以色列数字情报公司 Cellebrite 的 1.7TB 数据泄露。它是数字取证领域的领先公司之一，执法部门和情报机构使用其服务 UFED 来解锁和访问移动设备上的数据。这家公司和另一家瑞典的取证公司 MSAB 的数据已

被 Enlace Hacktivist 团伙泄露，后来通过 DDoSsecret 平台公开。泄露数据通过 Torrent 分享，包括整个 Cellbrite 套件，以及用于软件本地化和客户技术指南的大量文件。

https://securityaffairs.com/140838/data-breach/cellebrite-software-leaked-online.html

10、T-Mobile 遭遇新数据泄露，3700 万个账户被盗

1 月 20 日报道，T-Mobile 遭遇新的数据泄露，威胁者窃取了 3700 万当前后付费和预付费客户帐户的个人信息。

电信公司于 2023 年 1 月 5 日发现入侵，攻击者未经授权通过单一应用程序编程接口（“API”）获取数据。泄露的数据包括姓名、账单地址、电子邮件、电话号码、出生日期、T-Mobile 帐号以及帐户线路数和计划功能等信息。

https://securityaffairs.com/141086/data-breach/t-mobile-data-breach-5.html

11、PayPal 通知 34942 名用户因撞库攻击导致数据泄露

1 月 20 日报道，PayPal 宣布，在 12 月 6 日至 12 月 8 日期间，有 34942 个客户的账户遭到入侵。该公司补充说，未经授权的访问是撞库攻击的结果，其系统并未遭到破坏。

该公司正在向受影响的客户发送违规通知信，威胁行为者可以访问姓名、地址、社会安全号码、个人税号、PayPal用户的出生日期，当然还有交易历史记录。

https://securityaffairs.com/141072/data-breach/paypal-data-breach-credential-stuffing.html