# 全球数据安全观察

## 总第 132 期 2023 年第 13 期

（2023.04.03-2023.04.09）

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、《科技伦理审查办法（试行）》征求意见稿

4 月 4 日，科学技术部科技监督与诚信建设司公布《科技伦理审查办法（试行）》征求意见稿，对科技伦理审查的程序、标准、条件等进行规范，对覆盖各领域科技伦理审查作出综合性、通用性规定。其中，《审查办法》在涉及人类研究参与者的科技活动、以及涉及数据和算法的科技活动的要求中，明确了个人信息保护与数据安全的要求，加强了与个人信息保护法、数据安全法等法律法规的衔接。

https://www.most.gov.cn/tztg/202304/t20230404_185387.html

## 2、银保监会：将全面开展非银机构数据治理工作

4 月 3 日，银保监会组织召开政策通气会，解读近期发布的金融资产管理公司、保险集团（控股）公司和保险资产管理公司等三个监管数据标准化规范，要求非银机构开展数据治理工作，做到认好数、管好数、用好数、报好数。

http://www.cbimc.cn/content/2023-04/04/content_480867.html

## 3、《2023 年河南省大数据产业发展工作方案》印发

4 月 3 日，《2023 年河南省大数据产业发展工作方案》

印发，规定了完善数据基础设施、培育数据要素市场、推动产业链现代化、优化产业发展生态、提升数智治理水平、完善安全保障体系六个重点任务。其中在数据要素市场方面提出支持郑州数据交易中心做大做强，创建**国家级数据交易场所**；在安全保障体系方面提出要在装备制造、互联网服务等重点行业遴选一批典型企业，探索**开展 DSMM 贯标工作**，**打造一批 DSMM 贯标标杆企业**，总结经验，普及推广。

https://gxt.henan.gov.cn/2023/04-03/2718650.html

## 4、国家邮政局：推动邮政业高质量发展

4 月 7 日，国家市场监督管理总局（国家标准委）批准发布的《快递电子运单》（GB/T 41833-2022）和《通用寄递地址编码规则》（GB/T 41832-2022）两项国家标准于近日正式实施。《快递电子运单》国家标准设立专门章节，强化个人信息保护内容，其中包括**禁止显示完整的个人信息**，推荐对**个人信息进行全加密处理**，以及**规范个人信息相关内容的读取权限**等；《通用寄递地址编码规则》国家标准顺应我国邮政业数字化转型发展需要，提出了通用寄递地址编码的编码原则、编码规则和编码维护要求。

https://www.spb.gov.cn/gjyzj/c100015/c100016/202304/0b5b90ede55e4a399c2a3fa0fcf0c704.shtml

## 5、上海市地方标准《公共场所人脸识别分级分类应用规范》（征求意见稿）

3 月 30 日，上海市地方标准《公共场所人脸识别分级分类应用规范》（征求意见稿）和《人工智能标准化工作导则》（征求意见稿）公布。其中《公共场所人脸识别分级分类应用规范》（征求意见稿）聚焦于公共场所人脸识别系统建设前的分级分类评估及其应用要求：在明确公共场所人脸识别应用基本原则的基础上，对公共场所不同人脸识别应用场景进行分类，根据人脸识别应用目的、底库规模等风险因素进行分级，并基于分级分类针对性地提出应用和管理要求，为规范应用人脸识别技术、保护公民隐私、促进行业发展提供支撑。

https://mp.weixin.qq.com/s/eVIvrO2qsXl_hRlbYWs95Q

## 6、美国发布《促进数据共享与分析中的隐私保护国家战略》

3 月 31 日，美国白宫科技政策办公室（OSTP）发布《促进数据共享与分析中的隐私保护国家战略》，正式确立了政府的目标，即支持保护隐私数据共享和分析（Privacy-Preserving Data Sharing and Analytics, “PPDSA”）技术。PPDSA 技术是一种平衡数据收集、分析与伦理社会技术问题的解决

方案，它利用隐私增强技术进行数据分析、获取数据价值，同时确保用户隐私、秘密安全。

https://mp.weixin.qq.com/s/amhqMt-yHNpzfAo60C1kqA

## 7、意大利：从即日起禁止使用 ChatGPT

当地时间 3 月 31 日，意大利个人数据保护局宣布，从即日起禁止使用 ChatGPT，限制 ChatGPT 的开发公司 OpenAI 处理意大利用户信息，并开始立案调查。该机构认为，3 月 20 日，ChatGPT 平台出现了用户对话数据和付款服务支付信息丢失情况，该平台没有就收集处理用户信息进行告知，缺乏大量收集和存储个人信息的法律依据。机构要求 OpenAI 公司必须在 20 天内回应该机构的关切，否则将被处以最高 2000 万欧元或公司全球年营业额 4%的罚款。

https://www.chinanews.com.cn/cj/2023/04-08/9986208.shtml

# 技术、产品与市场

## 1、调查：IRM 计划也挡不住内部人造成数据泄露

一项数据暴露调查研究表明，尽管已经设置了专门的内部人风险管理（IRM）计划，大多数公司仍然难以阻止内部人事件造成的数据丢失。

研究揭示，内部人事件造成的数据损失平均同比增长32%。内部人事件包括源自企业现有内部员工造成的数据暴露、丢失、泄露和盗窃。

超过82%的首席信息安全官（CISO）承认担忧其所属企业的内部人风险及相关数据丢失问题。Gartner 分析师称：“员工、合作伙伴和承包商都有不同级别的访问权限，各具不同敏感性，但这些用户的行为却没有得到有效监控。IT 安全开支基本上集中在防范外部威胁和保护边界不受恶意侵入方面，未必会对受信内部用户施行相同等级的预防性数据保护控制措施，而且通常只在事后才会发现违规行为。”

内部人事件造成的数据丢失甚至更难检测，因为 75%的 CISO 表示自己在公司里没能做到这一点。在 CISO 看来，内部人风险（27%）是最难以检测的一种威胁，检测难度高于云数据暴露（26%）和恶意软件/勒索软件（22%）。

https://www.secrss.com/articles/53350

## 2、研究：Gartner 对企业网络安全建设和发展的 8 个预测

企业的 CISO 及其团队必须在专注于当前建设工作的同时，抽出时间来关注未来，看看今后几年可能会影响组织网络安全计划的变革因素会有哪些。以下预测是 Gartner 数字化研究团队在目前看到的一些主要趋势，建议企业管理者在制定新的网络安全发展战略时，应充分考虑并适应这些趋势。

预测一：到 2024 年底，尽管个人隐私保护的法规制度已经基本完善，能够覆盖大部分消费者数据，但或许只有不到 10%的企业能够将隐私保护转化为业务竞争优势。

预测二：到 2025 年，超过半数的 CISO 在尝试使用风险量化方法来推动网络安全决策时，会以失败而告终。

预测三：到 2025 年，超过半数的网络安全领导者可能会更换工作，主要原因是因为工作压力大，难以完成既定的工作目标。

预测四：尽管 CISO 的工作压力巨大，但企业对网络安全的重视度却会持续提升。到 2026 年，70%以上企业的董事会中都会包括一名具有网络安全专业知识的高级管理者。

预测五：到 2026 年，企业组织 60%以上的安全威胁检测、调查与响应能力将通过风险暴露面管理来实现和验证，并确定对威胁管理的优先级，而目前这个比例不到 5%。

预测六：到 2026 年，将有超过 10%的大型企业组织能

够实际落地全面、成熟、可量化的零信任安全计划，目前这个比例还不到 1%。

预测七：到 2027 年，以人为本将会成为企业组织网络安全计划的基础性原则，安全管理者要尽量减小安全运营工作的阻力，并致力于提高安全管控措施的实际利用率。

预测八：到 2027 年，有 75%以上的企业员工将可以在不依赖 IT 部门的情况下添加、修改或应用数字化技术，而在 2022 年这个比例仅为 41%。

https://mp.weixin.qq.com/s/YPVLwan0Yzn39GdSuEqo1g

## 3、全国首个“交易激励计划”正式发布！

4 月 6 日，贵阳大数据交易所发布了全国首个以“百万激励星星之火，数据交易可以燎原”为主题的“交易激励计划”。根据总体安排，贵阳大数据交易所设立专项资金池，激励符合相应条件的市场主体：在 2023 年 1 月 1 日至 2023 年 12 月 31 日期间，参与数据交易的供需双方、促成交易的数据中介等市场主体、法人单位。激励类型包括：交易主体入场注册费用激励、数据产品及服务交易激励、数据中介专项激励、算法工具交易激励、算力资源交易激励五大类。

https://mp.weixin.qq.com/s/Gg1TDzx-4ih5OHsB6GbzEg

## 4、全国首个“算力资源专区”正式上线！

近日，由贵阳大数据交易所和贵州省算力科技有限责任公司合作共建的“算力资源专区”正式上线。“算力资源专区”以贵州枢纽算力运营调度平台为抓手，旨在推动算力跨地域、跨业务、跨平台集中高效调度，实现在算网资源层面的统一管理、编排和调度。目前，该专区涵盖了通用算力、智能算力、超算算力，目前共接入算力 29.7Pflops,存力 84P,运力 500G，同时还提供配套的安全资源和增值服务。

https://mp.weixin.qq.com/s/U6GzdzTdTHgB1E88SbVpEA

# 业界观点

## 1、国家发改委：从六方面发力，不断做强做优做大我国的数字经济

4 月 3 日，国新办举行第六届数字中国建设峰会新闻发布会。国家发展改革委创新和高技术发展司负责人孙伟出席发布会并回答记者提问。他表示，准备从六方面发力，不断做强做优做大我国的数字经济。

**一是加强政策制度建设**。加快构建“1+N”的数据要素基础制度体系，推动有条件的地方和行业开展数据要素流通使用先行先试，统筹构建多层次、多元化和场内场外相结合的数据要素市场体系。

**二是适度超前部署数字基础设施建设**。加快光纤网络扩容提速，5G 的商用部署和规模应用，深入实施“东数西算”工程，加快基础设施数字化、智能化的改造。

**三是大力推动数字产业创新发展**。培育一批具有核心竞争力的生态主导型企业，加快打造具有国际竞争力的数字产业集群，支持平台企业在引领发展、创造就业、国际竞争中大显身手。

**四是加快深化产业数字化转型**。强化各领域、各行业全方位、全链条数字化政策改造引领，提升“上云用数赋智”水

平，提升新一代的信息技术与一二三产业融合发展，支持龙头企业、第三方服务企业带动中小企业加快转型的步伐。

**五是持续提升数字公共服务水平**。提高公共服务资源的数字化供给和网络化服务水平，持续加大适老化的智能化产品供给，运用数字技术为弱势群体增加便利，持续推进智慧城市和数字乡村融合发展。

**六是不断深化数字经济国际合作**。积极提出“中国倡议”，落实全球发展高层对话会数字经济领域成果。积极提供“中国方案”，推进加入《数字经济伙伴关系协定》，开展双多边数字经济治理合作，构建良好的国际环境。

https://mp.weixin.qq.com/s/cDflCVRusrPoqFD2jTDJxA

## 2、周鸿祎：不发展才是最大的不安全

3 月 30 日下午，360 公司创始人周鸿祎在微博发布长文，对“马斯克请愿叫停 GPT-5 研发”发表了看法。

在周鸿祎看来，GPT 将引领一场新的工业革命，意义超越互联网和 iPhone 的发明。它将带来生产力的大幅提升，进而提升国家竞争力，因此中国一定要迎头赶上。

他也坦言，最近人工智能的指数级跃变确实让人有点措手不及。人类如何应对 AI 带来的未来安全挑战，谁也没法给出确定答案。

“人工智能的进化已经不以个人意志为转移了，哪怕是马斯克。”周鸿祎说，“我自己就是做安全的，但我坚定地认为，不发展才是最大的不安全。”

对于人类如何与 AI 共处，周鸿祎将目前的观点概括为三派，分别是“降临派”、“幸存派”、“拯救派”。他表示自己比较认同“拯救派”的观点，即“**AI 不是来取代人类的，而是来升级人类的，人类将迎来工业革命之后最大的生产力解放**”。https://www.21jingji.com/article/20230330/herald/842e7569b3073511bd1314ad7757e00c.html

### 3、金中夏： 依法推进金融数据跨境流动，在开放中保障安全

中国人民银行国际司司长金中夏 4 月 4 日在 2023 中国金融学会学术年会暨中国金融论坛年会上表示：当前，不少国家已经出台数据管理规范和规制，一些区域和双边自贸协定也开始对金融数据跨境流动进行规范。“我国应以此为契机，在洞察国际大势的基础上，在制定完善本国相关规则的同时积极参与国际规则的讨论和制定。”

金中夏表示，下一步的任务就是如何根据金融行业的特点和发展要求来规范数据跨境流动。这个过程需要依法推进，**实现具体技术规程的细化、透明化、可预见性**，也需要在整

体上保持开放的心态。虽然在目前这个发展的早期阶段，由于数据法制框架刚刚搭起来、公众对之还不太熟悉，规范也有不明确之处，故而偶尔有一些触犯法条的新型案例冲击大家的神经，但总体而言，数据不应该是格外敏感的事物。在改革开放已经四十多年、中国从经济资源的跨境流动获取丰硕回报的今天，跨境流动本身不是一个禁忌，不应该有“尽量不给流动”的闭塞心态。不开放，绝不是安全的代名词。

金融数据的跨境流动只是金融数据整体流动的一环。无论对内对外，都应该**根据不同机构、不同类型、不同时段、不同用途的数据的特点分类施策**。对敏感数据限制、禁止流动和交易，对非敏感的数据允许在可控的范围内自由流动和交易。这里敏感和非敏感是有层次性的，不是简单的允许或禁止，还可以包括丰富的中间层。比如符合特定条件的特定类型的数据可以自由流动，或者是要在特定的许可、授权程序下流动。同一数据，在不同的时空条件下，面对不同的流动对象，也会存在不同的流动合规度。对规模量较小、性质更不敏感的数据，可以有更高的流动容忍度。对于合规度通过我国认证的境内外机构，也可以授予其更大的数据流动自由度和试点资格。

正在跨境流动的数据也可谓包括了法律知识本身。在世界多国正在探讨金融数据跨境流动规范的今天，我们当以数

据大国的进取姿态，以“通过开放促进安全”的自信心，积极主动地参与讨论、参与制定国际规则；可根据我国的实际情形需要，提出立场和互利互惠、互通有无的方案，同时吸收借鉴主流国家的通行规则，优化数据跨境流动的制度接口，从而实现有效博弈，缔造和拥抱能真正为我所用、利人利己的国际规范。

https://www.21jingji.com/article/20230406/herald/45f195affa19210cf8e2fa3f794b5b3d.html

## 4、高新民：解决数据流通问题需建立数据互操作基础设施，先导工程是数据共同体

近期，信息化百人会学术委员、国家信息中心原主任、国家信息化专家咨询委员会委员高新民在“2023 智慧中国年会”巡演第一站——“新时期数字政府创新发展专题暨评估指标专家研讨会”上发表演讲。

高新民提出数据通问题仍是当前发展难点，而发展出路是建设数据基础设施，他认为数字基础设施应该有第 5 个概念——数据互操作基础设施，即支撑所有数据互操作能力的设施。数据基础设施目前还没有很好的概念和清晰的架构，今天提出要重视政务数据基础设施的建设，具体建设可以探讨，但这个问题非常重要，否则政务通、数据通的根本问题

无法解决。

高新民指出现阶段数据的操作是通过单个的人或主体来操作，我们推荐通过数据共同体的概念从局部去推进数据的互操作。对此他倡导领域数据共同体：数据共同体将是国家数据基础设施的重要组成部分，也是基础设施的先导工程，它与数据交易市场体系互为补充和支撑，也是数据安全保障体系的基石之一。数据共同体是由业务强关联单位参与、以共建共享为原则、标准架构支撑的能够实现机器访问、识别的共同体。互操作不等于共享，国家提出的“共享是原则，不共享是例外”，政务数据共同体成熟后，我认为应该为“互操作是原则，不互操作是例外”。在互操作的基础上共享是有原则的：一是，需求驱动，拿了数据干什么用。二是，共享过程要确保数据主权者知情，是否收费另论。三是，安全可控，不能出现泄密、篡改等安全事故。四是，应用场景确有需要。

具体有三条建议：一是，重视数据要素的流转不建议只考虑交易这一条路，要重视数据流转的多元化建设，尤其政府的数据要开放、共享。二是，数据的流转和开发利用是一个相当复杂的工程，需要强化数据基础设施建设，即要建好数据技术架构和制度架构两大支柱。三是，数据共同体将是基础设施的先导工程，它与数据交易市场体系互为补充和支撑，也是数据安全保障体系的基石之一。可从政务领域数据

共同体建起，共同探索，建设可操作可实现的数据基础设施体系。

http://www.cbdio.com/BigData/2023-04/07/content_6172543.htm

## 5、特斯拉被曝分享用户隐私信息 如何平衡技术创新与数据安全

近日，据媒体报道，前特斯拉员工透露，特斯拉内部团队在 2019-2022 年期间，经常在内部消息系统中分享客户车载摄像头记录的视频和图像，其中包括了一些车祸、客户路怒症的录影。

北京大成律师事务所高级合伙人邓志松告诉记者，新能源汽车通常搭载了更多的数字化服务功能，以增加与传统油车竞争的优势，而这些服务的运行需要海量的数据支撑，这使得新能源汽车更像一个“数据收集器”。

“新能源车企作为数据处理者负有告知义务，在处理敏感个人信息时应征得个人同意，同时应当采取相应数据安全保护措施防止数据泄露。”邓志松指出。

新能源车企在设计功能时，应如何平衡技术创新与数据安全？在邓志松看来，技术创新要以保障数据安全为前提，这就要求企业内部建立一个**完备的数据安全保障体系**。“数据安全是至关重要的，新能源车企应高度自律，坚守安全发

展底线，对个人信息保护持敬畏之心，在汽车数据收集、存储、使用、加工、传输、提供、公开等各个环节都严格执行相关规定。同时，数据保护也不应成为企业创新发展的桎梏，相关制度设计应为企业的技术进步和创新发展预留空间。”
https://www.21jingji.com/article/20230408/herald/ffef7797c0153277c98e2bb7834d890b.html

# 数据安全事件

## 1、英国监管机构因“滥用儿童数据”对 TikTok 处以 1600 万美元罚款

4 月 5 日，据路透社披露，英国数据监管机构以短视频社交媒体平台 TikTok 未经家长同意便使用 13 岁以下儿童的个人数据，违反数据保护法为由，对 TikTok 处于 1270 万英镑（1590 万美元）的罚款。

据信息专员办公室 (ICO) 估计，TikTok 在 2020 年允许多达 140 万英国 13 岁以下儿童使用其平台，尽管它规定 13 岁为创建帐户的最低年龄。

https://www.reuters.com/technology/tiktok-fined-16-mln-by-uk-watchdog-misusing-childrens-data-2023-04-04/

## 2、知名台企微星疑遭勒索攻击，被索要 400 万美元巨额赎金

4 月 6 日，据外媒报道，台湾个人电脑零部件制造商微星国际（MSI）被列入一个名为“Money Message”的新勒索软件团伙的勒索门户网站，该团伙声称从该公司的网络中窃取了源代码。

威胁行为者声称从 MSI 的系统中窃取了 1.5TB 的数

据，并在其数据泄露网站上发布了他们声称属于微星的 CTMS 和 ERP 数据库以及包含软件源代码、私钥和 BIOS 固件的文件的屏幕截图。Money Message 威胁要在大约五天内公布所有这些据称被盗的文件，除非 MSI 满足其 400 万美元的赎金支付要求。

https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/

## 3、Medusa 勒索软件团伙对塞浦路斯开放大学进行了攻击，学生数据遭泄露

4 月 6 日，据外媒报道，Medusa 勒索软件团伙声称对塞浦路斯开放大学 (OUC) 进行了网络攻击，导致该组织的运营严重中断。

近日，Medusa 勒索软件组织在其数据泄露网站上添加了 OUC，并给该机构 14 天的时间来响应其 100,000 美元的勒索赎金要求。数据样本也已经被泄露，这些泄露的文件包括含有个人身份信息的学生名单、研究项目承包商的财务细节等等。

https://www.bleepingcomputer.com/news/security/medusa-ransomware-claims-attack-on-open-university-of-cyprus/

## 4、Noteboom 遭到 BlackCat 的攻击并被勒索 175 万美元

媒体 4 月 5 日报道称，德克萨斯州的律师事务所 Noteboom 遭到了 BlackCat 的勒索攻击。BlackCat 向 Noteboom 发送电子邮件，通知其在 3 月 24 日发生了数据泄露。邮件还称他们已入侵系统并停留了 7 天，下载了超过 400Gb 的数据，并加密了所有服务器和数据。泄露数据包括保密协议、未决案件的文件、涉及诉讼的医疗记录以及员工数据等。BlackCat 透露赎金要求为 1750000 美元，但 Noteboom 根本没有回应他们。

https://www.databreaches.net/noteboom-the-law-firm-hit-by-blackcat/

## 5、UnitedLex 遭到 d0nut 勒索攻击超过 200GB 数据泄露

据 4 月 4 日报道，UnitedLex 公司遭到了 d0nut 的勒索攻击。d0nut 声称，他们已从 UnitedLex 的系统下载了超过 200GB 的数据，包括涉及付款、合同和其他与众多组织和个人有关的机密文件。UnitedLex 表示近期在系统上发现了可疑活动，正在确定活动的性质和范围。据悉，d0nut 曾要求 500 万美元的赎金，这与谈判中提到的 60 万美元的要求明显不同。UnitedLex 已被添加到了 BlackCat 的网站，研究人员正试图确定这些是否与 D0nut Leaks 泄露的数据相同。

https://www.databreaches.net/unitedlex-hit-by-d0nut-ransomware-team-200-gb-of-corporate-files-leaked/

## 6、身份验证厂商 OCR Labs 数据泄露，危及大量银行客户

4 月 6 日，据 Cybernews 报道，全球知名数字身份验证工具提供商 OCR Labs 近日曝出敏感数据泄露事件，导致大量银行和政府客户面临严重风险。

OCR Labs 提供的服务被宝马、沃达丰、澳大利亚政府、西太平洋银行、澳新银行、汇丰银行和维珍货币等知名企业使用。因公司系统配置错误将敏感凭据暴露给公众，该数据泄露事件影响了多个国家的多家金融机构。使用泄露的数据，黑客能够入侵 OCR Labs 的后端基础设施，从而渗透到其客户的基础设施。由于金融服务是网络犯罪分子的主要目标，因此该数据泄露事件对企业及其客户的威胁极为严重。

https://www.secrss.com/articles/53466

## 7、奥克兰证实 2 月勒索软件攻击后第二次大规模数据泄露

4 月 6 日消息，奥克兰市官员本周证实，2 月份袭击该市的勒索软件组织在暗网上发布了更多数据。

据称，Play 勒索软件组织在上个月发布了首批 10GB 的城市数据后，又发布了 600GB 属于奥克兰市的城市数据。

该市还承认第一批被泄露的数据范围广泛——其中包括从市警察局和市政府其他办公室窃取的大量文件，甚至市长的个人资料也被泄露了。

除了被盗数据外，自攻击开始以来，关键的城市服务也已瘫痪。直到上周半，该市才得以恢复其 311 电话线、在线许可中心和城市合同系统，支付停车罚单和营业税的平台仍在恢复中。

https://therecord.media/oakland-confirms-massive-second-data-leak

## 8、存储巨头西部数据遭入侵：多个内部系统被访问，My Cloud 网盘服务中断

4 月 4 日报道，西部数据宣布其网络遭到入侵，未授权黑客已获得公司多个系统的访问权限。

这家总部位于美国加州的计算机硬盘驱动器制造商与数据存储服务商在新闻稿中表示，“在发现事件之后，公司实施了事件响应措施，并在领先外部安全与取证专家的协助下启动了调查。”根据目前发现的证据，西数公司认为入侵者已经访问到了部分内部数据，目前正在努力了解数据的具体性质和范围。

https://www.secrss.com/articles/53423

## 9、Uber 律师事务所将司机数据泄露给黑客

4 月 5 日，据外媒报道，一家代表 Uber 的律师事务所已通知数量不详的司机，包括他们的姓名和社会安全号码在内的敏感数据已被网络攻击者窃取。这是这家网约车巨头在六个月内发生的第三次数据泄露事件。

位于新泽西州纽瓦克的律师事务所 Genova Burns LLC 在 1 月底首次注意到可疑活动，并且在外部专家进行调查后发现其系统遭到破坏，一些未公开数量的 Uber 司机的数据被盗。Genova Burns 没有解释为什么律师事务所需要司机的个人身份信息 (PII)，也没有回应多项评论请求。

https://www.darkreading.com/attacks-breaches/law-firm-uber-loses-drivers-data-hackers-breach

## 10、荷兰皇家足协称黑客窃取了员工数据

4 月 5 日，据外媒报道，荷兰皇家足球协会（KNVB）的管理机构表示，黑客在网络攻击期间窃取了其员工的个人信息。

该组织拥有超过 120 万会员，是该国最大的体育协会。“被盗数据的细节正在调查中。网络入侵已报告给荷兰数据保护局。尽管我们有安全系统，但 KNVB 现在也成为了受害者，我们感到特别抱歉。” 该组织没有回应关于该事件是

否涉及勒索软件以及有多少员工受到影响的评论请求。

https://therecord.media/netherlands-dutch-football-association-cyberattack-soccer

## 11、美国消费贷款公司 TMX 披露重大数据泄露事件

4 月 3 日报道，美国消费贷款公司 TMX Finance 披露了近三个月前首次发现的严重泄露客户数据的事件。

这家公司在向缅因州总检察长办公室提交的违规通知信中表示，违规行为可能始于 2022 年 12 月初。但是，该公司直到 2023 年 2 月 13 日才发现。“超过 480 万客户受到影响。涉及的个人信息可能包括客户的姓名、出生日期、护照号码、驾照号码、联邦/州身份证号码、税号、社会安全号码和/或财务账户信息，以及电话号码、地址和电子邮件地址。”

TMX Finance 声称事件现已得到控制，它已重置所有员工密码，并通过额外的端点保护和监控增强了防御性安全态势。

https://www.infosecurity-magazine.com/news/consumer-loans-tmx-reveals-major/

# 《全球数据安全观察》周报

**政策形势：** 政策法规/地方动态/标准动态

**技术、产品与市场：** 技术研究/行业洞察/市场趋势

**业界观点：** 大咖观点/业界报告

**数据安全事件：** 合规事件/数据泄露/数据勒索

**编委会：** 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn