全球数据安全观察

总第 87 期 2022 年第 15 期

（2022.05.02-2022.05.08）

目录

政策形势

1、北京拟明确数据财产性收益、建立数据要素登记、评估、入表等资产化制度

为促进数字经济高质量发展，助力打造全球数字经济标杆城市，北京市经济和信息化局会同北京市司法局、北京市人大常委会财经办、北京市人大常委会法制办等部门制定了《北京市数字经济促进条例(征求意见稿)》。

关于数据资源：目前对数据目录定位和编制主体责任进行了规定；明确公共数据、各类数据资源共享与数据开放的渠道与规则；明确各主体有权对其合法收集的数据进行处理，并享有受法律保护的数据财产性收益；建立数据要素登记、评估、入表等资产化制度，建立健全数据要素市场生态，支持北京国际大数据交易所发展，促进数据资源的高效流通。关于数字经济安全：明确任何单位和个人在北京市从事数据处理活动，都要维护国家安全、公共利益和个人合法权益；**强调重点保护关键信息基础设施，支持建立数据治理和合规运营制度，加强个人信息安全保护**；建立健全互联网平台管理制度规则，督促平台企业规范运营；督促市、区人民政府及有关部门强化数字经济安全风险防范的职责，促进数字经济均衡、有序发展。

https://mp.weixin.qq.com/s/1srwOcYG4R7AqzDdotlJ-w

2、北京经信局：数字经济全产业链开放

为贯彻落实市委市政府关于加快建设全球数字经济标杆城市的战略部署，进一步推动数字经济高水平开放，按照全市“两区”建设全产业链、全环节改革工作要求，北京市经济和信息化局制定了《北京市数字经济全产业链开放行动方案(征求意见稿)》。《行动方案》力求解决数字经济发展中遇到的政策、机制、标准等全产业链开放方面的突出问题，主要把握以下五点：

一是突出数据要素，以数据链贯穿“数字经济”全链条。以激活数据要素潜能为引擎，以全方位数字化转型为主线，采用数据链、产业链并行方式梳理数字经济发展的共性与垂直领域的个性问题。其中，数据链涵盖数据“聚、通、用、管”全生命周期，包括数据采集、加工、共享、开放、登记、评估、交易等环节；二是坚持问题导向，力求解决企业发展主要诉求。按照“小切口、快落地、先易后难”的原则，针对数据规模扩容和质量有待提升、数据共享和开发利用缺乏制度保障、数据交易制度规则尚不完善、重点领域创新发展和要素支撑不足等问题，提出两到三年内可落地，且有针对性的措施对策，形成激活数字经济全产业链的实施路径。三

是注重衔接互补，与其他规划共筑“一盘棋”形成合力。《方案》聚焦数字经济全链条发展的关键议题，注重与全球数字经济标杆城市实施方案等，做好与数字贸易示范区和国家服务贸易创新发展示范区实施方案的错位协同，同时为即将出台的《北京市数字经济促进条例》进行政策性探索。四是体现多维开放，力争形成数字经济领域改革创新的北京标杆。对标国际国内先进规则，以数字经济产业链的关键环节开放带动改革创新，以“对内为主”，重点呼应国家“十四五”期间决策部署和重点任务，力求在北京先行先试。五是统筹发展与安全，牢牢守住安全底线。《方案》以数字安全为前提推动数字经济发展，**构建保障数据安全的系统能力，落实数据全生命周期安全保护**，加强新业务、新业态风险防范，以科技手段赋能监管创新，探索包容审慎的新型监管机制。

https://mp.weixin.qq.com/s/5UM8sJXvGtxAqlPl0in6KA

3、上海将研制“生物特征及用户习惯采集、数据跨境流通安全评估”等标准

4 月 20 日晚间，上海市人民政府官网发布《上海城市数字化转型标准化建设实施方案》（以下简称“《实施方案》”）全文，围绕“经济、生活、治理”全面数字化转型要求，通过研制实施一批能用、管用、好用的数字化转型标准，构建具

有系统性、协调性、开放性的城市数字化转型标准体系。

《实施方案》指出，到 2023 年底，上海将新增发布 100 项以上城市数字化转型地方标准及团体标准，主导或参与制定 50 项以上国际标准和国家标准，形成 15 项以上“上海标准”，推动 50 项以上城市数字化转型标准化试点，有效支撑上海城市数字化转型。

在数字安全方面，将聚焦信息安全、链路安全、**数据安全防护，研制实施数据资源全流程监测、生物特征及用户习惯采集和应用管理、数据跨境流通安全评估**等标准，以标准化支撑构建城市数字化转型的大安全格局。

https://mp.weixin.qq.com/s/tf7XjuORCBYaa1jyFw3wUw

4、广西发布《广西壮族自治区大数据发展条例（征求意见稿）》

4 月 24 日消息，广西壮族自治区大数据发展局发布关于征求《广西壮族自治区大数据发展条例（征求意见稿）》修改意见的函。

征求意见稿分为总则、基础设施、数据资源、数据要素市场、产业发展、数据安全、促进措施、法律责任和附则 9 个章节，围绕**规范数据处理活动，保障数据安全，促进数据开发利用**，保护自然人、法人、非法人组织的合法权益，加快培育统一的技术和数据市场，推进数字广西建设，推动数

字经济发展提出实施规划。

https://mp.weixin.qq.com/s/3JZL4Bc37sA2ot7R7HktsQ

5、武汉颁布支持数字经济加快发展若干政策，推进数据开放共享

5 月 6 日，武汉市人民政府印发《武汉市支持数字经济加快若干政策的通知》，涉及推进数字新型基础设施建设、推动数字产业化升级、促进产业数字化转型、提升数字化治理能力、强化数字经济要素支撑等五大方面，共计 23 条具体政策保障措施，为全面加快数字经济发展提供坚实支撑。

其中提到：“推进数据开放共享。深化城市大脑建设，建立数据共享责任清单机制，促进数据资源互通共享。依法依规推动信用、医疗、教育等重点领域数据资源开放共享。促进公共服务、互联网应用服务、重点行业和大型企业云计算数据中心高效利用，探索建立跨区域数据资源共享机制。对具有经济和社会价值、允许加工利用的政务数据和公共数据，通过数据开放、特许开发、授权应用等方式，鼓励更多社会力量进行增值开发利用。要推进数据资源管理科学化。探索建立统一规范的数据管理制度，提高数据质量和规范性。制定**数据隐私保护制度和安全审查制度**。推动完善适用于大数据环境下的数据分类分级安全保护制度，加大对政务数据、

企业商业秘密和个人数据的保护力度。”

https://mp.weixin.qq.com/s/aT9fshtHCYA4yBsT0YboUg

6、新国标《App 收集个人信息基本要求》：无单独同意，不应分析相册中生物识别信息

4 月 24 日，全国信息安全标准化技术委员会归口的 10 项国家标准正式发布，并于 2022 年 11 月 1 日正式实施，其中包括一项个人信息保护方面的重点标准：《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求（GB/T 41391-2022）》（以下简称“《App 收集个人信息基本要求》”）。该标准旨在落实《常见类型移动互联网应用程序必要个人信息范围规定》和《App 违法违规收集使用个人信息行为认定方法》两项部门工作文件，沿袭了两项部门工作文件的重要概念，并进一步细化了 App 收集个人信息的要求，具有很强的实践参考价值。

App 运营者规范其个人信息收集活动，也适用于监管部门、第三方评估机构等对 App 个人信息收集活动进行监督、管理和评估。其中，App 包括移动智能终端预置、下载安装的应用程序和小程序。小程序指基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

《App 收集个人信息基本要求》以 App 类型划分为基础，

区分不同类型以要求和附录相结合的形式**明确了 App 收集个人信息中如何贯彻最小必要原则、如何确定必要个人信息范围、特定类型个人信息的收集处理方式、告知同意的具体要求、系统权限和第三方的管理方式**。

https://mp.weixin.qq.com/s/LYA6ptlXy4kaVN1SZRK0WQ

7、加拿大发布联邦隐私法的最新修改建议

加拿大隐私专员办公室（OPC）已经为新的联邦隐私法出台了一些修改建议，以取代目前的《个人信息保护和电子文件法》（PIPEDA）。

这些建议考虑到了政府关于 C-11 法案，即《2020 年数字宪章实施法》的建议。C-11 法案随着 2021 年联邦选举的号召而在秩序文件上夭折。政府已表示，它计划提出一个新的法案。这些建议旨在支持制定一部新的法律，在承认隐私是基本人权的法律框架内，实现负责任的数字创新。OPC 关于 C-11 的意见书提供了关于每个建议的进一步细节。建议提出实现负责任的创新、采用基于权利的框架、加强公司的问责制、确保国际和国内法律的互操作性等，提出通过设计保护隐私和对高风险活动进行隐私影响评估的义务等内容

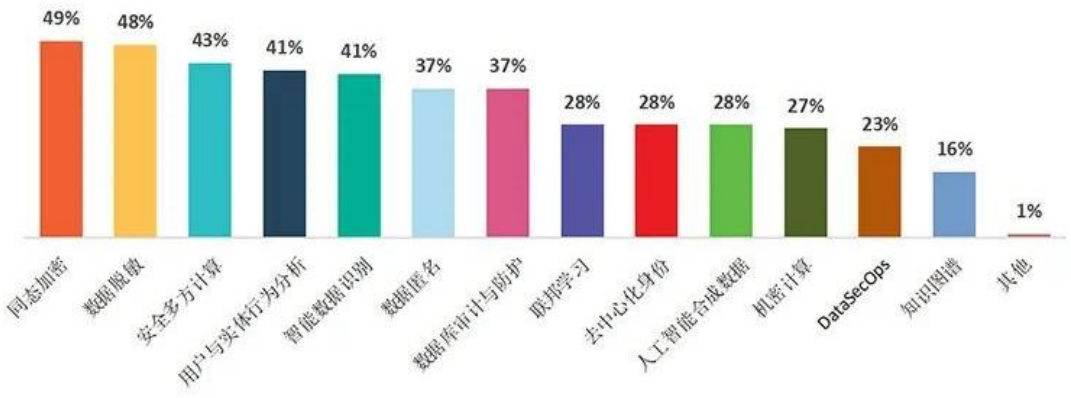
https://mp.weixin.qq.com/s/U7EcNgSaEE1EG2r_93ueXQ

技术、产品与市场

1、《2022 年中国企业数据安全现状调查报告》发布

为了帮助广大中国企业提高数据安全“能见度”，推动安全主管的跨行业交流，在“枪炮、病毒与数据安全”的高不确定性年代制订有效的数据安全战略，GoUpSec 联合承制科技发起《2022 年中国企业数据安全现状调查报告》，对大型行业企业和关键基础设施用户安全主管进行多维度调研。

在热门数据安全技术的调研中，隐私增强和隐私保护相关的数据安全技术受到了企业安全主管的重点关注，这包括同态加密（第一名）、数据脱敏（第二名）、安全多方计算（第三名）、智能数据识别（第五名）、数据匿名（第六名）和联邦学习（第八名）。



同态加密作为目前市场上最强大的隐私增强保护技术之一，可以让企业在云环境中安全存储、使用和管理数据，

而无需向云服务商提供对加密密钥的访问权限，同态加密可广泛应用于在数据隐私、法规合规、反洗钱、金融欺诈和数据货币化等领域，从本次调研结果来看已经成为企业数字化转型中最热门的隐私增强技术。

https://www.secrss.com/articles/41929

2、GitHub：2023 年底前所有用户账户需启用双因素身份验证

5 月 4 日，代码托管平台 GitHub 宣布了一项新的账户保护机制，**所有上传代码的开发者及用户账户必须在 2023 年底前启用一种或多种形式的双因素身份验证 (2FA)**。

GitHub 给定的 2FA 提供了多种选项，包括物理安全密钥、内置于手机和笔记本电脑等设备中的虚拟安全密钥、或基于时间的一次性密码 (TOTP) 身份验证器应用程序。尽管基于短信验证的 2FA 在一些国家和地区已经得到广泛应用，但 GitHub 仍希望用户启用安全密钥或 TOTP，在既往的攻击事件中，黑客已能够绕过或窃取短信验证信息。

根据 GitHub 此前的内部统计显示，只有约 16.5%的活跃用户在账户上启用了增强的安全措施，鉴于该平台的用户群应该意识到仅有密码保护的风险，这个数字低得令人惊讶。但根据新的规定，如果用户账户没有在规定的最后期限内启

用 2FA，账户将会被 GitHub 注销。

https://mp.weixin.qq.com/s/xuXGEabXjzy2uMgmaiSV8g

3、中国信息协会信息安全专业委员会发布《数据防泄露（DLP）技术指南》

作为一个比较成熟的技术，数据防泄露（DataLoss Prevention，简称 DLP）是国内外广泛应用的数据安全防护手段，衍生技术也多种多样，但国内市场对数据防泄露还没有建立统一的标准。近日，中国信息协会信息安全专业委员会于近日联合 DLP 厂商天空卫士发布《数据防泄露（DLP）技术指南》，从 DLP 与数字安全治理的关系，DLP 的定义、应用、核心技术、扩展等方面进行了详细介绍和深入探讨，旨在帮助使用者更好地使用数据防泄露技术来提升数据安全管理能力，促进企业的数据合理、合法、合规使用和流通，发挥数据价值和创新活力。

在 Gartner 的数据安全治理体系中，明确把 DLP 作为技术支撑体系中一个非常重要的技术。其次，数据分级分类是做好数据安全工作的前提，而 DLP 技术天生具有数据分类分级的能力，对数据的识别和保护能力贯穿于数据生命周期的全过程。最后，根据 IDC 的预测，2018 年到 2025 年，全球产生的数据量会增长到 175ZB，其中超过 80%的数据都是非

结构化数据，而对非结构化数据的分析、识别、保护正是 DLP 技术所擅长的，可谓直达数据安全技术的痛点所在。

https://mp.weixin.qq.com/s/-51zPn3tfITKIEhhuEHtsA

4、新华三预测：未来十年，将会有 95%的企业采用隐私计算技术

近日，新华三集团发布了《面向未来的数字社会——2022 新华三 十大技术趋势白皮书》(以下简称“白皮书”)，将隐私计算列为十大技术趋势之一，**并认为未来十年将会有 95%的企业将采用一种或者多种隐私计算技术**。

《白皮书》提到，数字经济时代，数据被视作关键生产要素，比肩石油，其价值释放需通过跨领 域、跨行业、跨地域的机构间数据融通共享实现。当前主流数据集中共享方案面临很多问题，数据资产权益得不到有效的保护、安全性得不到保证、数据泄露风险高；国际国内的隐私和数据保护法律不断成熟完善，也从合规监管层面大大增加了数据融合共享难度。

《白皮书》介绍，隐私计算是多种技术的统称，目的是为了让多个数据拥有者在不暴露数据本身的前提下，实现数据汇聚、共享、建模与分析，最终产生超出自身数据的价值，同时保证数据不泄露给其他参与方。新华三认为，未来十年

将会有 95%的企业采用一种或多种隐私计算技术。

https://mp.weixin.qq.com/s/JSIMd-K5yOxwqyxD3lHLhg

5、印度将引入六小时数据泄露通知规则

在该国计算机应急响应团队 CERT-In 引入新规则后，印度的组织面临 6 小时的数据泄露报告截止日期。

新规则将适用于印度网络和 IT 基础设施的关键部分，包括服务提供商、数据中心、政府组织和企业。

报告窗口比其他大型经济体短得多：在欧盟，GDPR 要求在 72 小时内报告违规行为。事件可以通过电话、传真或电子邮件报告。

该规则涵盖的组织必须在事件发生后保留日志 180 天。

https://portswigger.net/daily-swig/india-to-introduce-six-hour-data-breach-notification-rule

业界观点

1、左晓栋：对重要数据识别问题应更多强调国家安全属性

围绕数据防泄露、数据分级分类等当前我国数据安全工作热点问题，中国科学技术大学教授左晓栋在采访中发表了自己的观点。

关于如何建立重要数据的目录，左晓栋认为，一是国家会对重要数据的识别给出统一规定，即重要数据识别规则。但这是原则性规定，不同行业要根据国家标准的原则性规定，制定反映自己行业特色的重要数据识别细则；二是数据的分级按照一般数据、重要数据、核心数据划分，但国家不会对数据进行统一分类，即国家层面只分级不分类，到了行业和地方层面则可以自行根据实际情况来确定分类方法。

当被问到分类分级方面的关注点时，左晓栋表示，国家正在制定两个标准，一个是数据分类分级指南，另一个是重要数据识别规则。由于形势变化和国家需求，现在对数据分类分级特别是对重要数据识别问题上，应该更多强调数据的国家安全和公共利益属性。

关于如何判定一个数据是不是属于重要数据，左晓栋提出要重点突出它对国家安全的影响。比如说，算法推荐、定向推荐是一种舆论动员能力。此时，这些用户地址、用户特

征、用户画像等，都是用来进行信息推送、舆论引导、社会动员的必备条件，这些就应当属于重要数据。

https://www.secrss.com/articles/42022

2、杨强：数据安全时代，可信联邦学习正在改变人工智能的发展逻辑

针对近两年来隐私计算和联邦学习发展和应用中面临的安全、效率等挑战，“可信联邦学习”被提出，这一范式将隐私保护、模型性能、算法效率作为核心，共同构成了更加安全可信的联邦学习。

针对可信联邦学习这一新范式，香港科技大学计算机与工程系讲席教授、FATE 开源社区技术指导委员会主席，可信联邦学习提出者杨强院士在接受采访时表示：“现在越来越多的公司主动要求引入隐私计算的解决方案，所以可信联邦学习的商业前景的大门是开的，只不过技术的人要更加聪敏地设计平衡的方案。”

“可信联邦学习的核心命题是结合分布式机器学习和人工智能算法，找到联合建模可信、可行及可控的解决方案，极大降低隐私计算的成本，提升隐私计算应用质量，进而推动隐私计算的加速发展。”杨强介绍。

同时，杨强认为，目前开源已成为大势所趋，成为隐私计算产业生态核心组成部分。以国内首个联邦学习开源社区 FATE 为例，作为向隐私计算、联邦学习开源生态中的开发者、贡献者、用户及生态伙伴建立的学习与交流平台，帮助开发人员快速实现联邦学习应用开发与部署，可通过可信联邦学习中模型的“版权保护”(FedIPR)，实现数据版权的保护和结果可溯源、可审计、可解释；通过开源、开放和共享，实现普惠。

https://www.sohu.com/a/544262854_114778

3、全球数据勒索攻击威胁新特点及对策建议

目前，全球数据勒索攻击呈现以下新特点：

（1）攻击目的：由单纯经济牟利转向实施数据破坏、窃取战略机密、谋取政治诉求等多重企图，勒索意图愈加复杂化。

（2）攻击对象：由无差别的个人设备转向政府及公共部门、大型企业等具有关键信息基础设施属性的定向机构，且勒索策略日趋精准化。

（3）攻击主体：由个人或单个黑客团伙攻击转向层级分明、分工明确的黑色产业活动，勒索行为日益专业化。

（4）攻击模式：由单一加密勒索转向多重勒索获利，勒

索手段趋于多样化。

对此，国外通过四个方面的建设应对数据勒索攻击威胁：一是建立强制性勒索攻击事件报告机制。二是规范勒索赎金支付，防止缴纳大额勒索赎金引发的重复攻击。三是赋予执法人员“数据中断”权利，以帮助勒索攻击受害者在不支付赎金的情况下防止潜在的数据泄露风险。四是对勒索攻击者实施更严厉的惩罚，增强勒索犯罪活动威慑力。

对于我国数据勒索攻击威胁应对措施，专家提出了以下建议：

（1）探索反勒索立法，积极推进勒索攻击治理法治化建设。

（2）强化关键信息基础设施网络安全保护，增强勒索攻击防护能力和抵御弹性。一是推进标准化勒索攻击应急响应机制建设与落实。二是加强反勒索攻击技术的研发与应用。三是提供反勒索专业培训、工具等安全方案支持。

（3）加强组织或国际间合作，联合打击勒索攻击网络犯罪行为。

https://www.secrss.com/articles/42105

4、“四步”推动 5G 数据安全保护发展

日前，中国移动通信集团有限公司、中国信息通信研究

院、中国通信学会和华为技术有限公司联合发布《5G 数据安全防护白皮书》（简称《白皮书》）。

《白皮书》指出，国内数据安全技术产业发展方兴未艾，数据安全产品、解决方案、服务体系尚未成熟，存在数据安全保障基础薄弱、数据安全产品类型与解决方案单一等问题，针对 5G 应用的数据安全技术产品防护水平有待提升。

为了进一步推动 5G 数据安全的发展，《白皮书》提出了四点发展建议与展望:

（1）明晰 5G 数据安全与发展并重的防护思路。一是统一思想提高认识，坚持鼓励与规范并举的发展思路。二是将数据安全贯穿网络规划建设和应用发展全过程。

（2）完善 5G 数据安全法律法规和监管手段。一是《数据安全法》的出台标志着数据安全建设及监管工作进入有法可循、有法可依的新时代，但 5G 数据安全相关法规制度仍不完善。二是建立差异化的数据安全保护机制。三是开展 5G 融合应用数据安全检测认证。

（3）推进 5G 数据安全标准研制和技术攻关。一是加强 5G 数据安全国际标准体系布局。二是推进 5G 融合应用数据安全标准研制。三是加强 5G 数据安全技术攻关。

（4）加速 5G 数据安全生态共建和国际协同。一是打造 5G 数据安全产品供给支撑体系。二是在《全球数据安全倡议》

的基础上，加强同东盟、二十国集团（G20）、金砖国家、亚太经合组织及一带一路等相关国家地区 5G 数据安全沟通交流，充分重视各方对 5G 数据安全问题的正当关切，秉承共商共建共享理念，协调更多有着相近立场主张的国家共同推进 5G 数据安全治理体系建设。三是基于我国 5G 数据规模和发展优势，组织企业、高校、研究机构等深入研究 5G 技术应用场景以及 5G 产业生态数据安全防护，开展数据安全和个人信息保护及相关规则、标准的国际交流合作，推动符合《联合国宪章》宗旨的个人信息保护规则国际互认，通过规则外溢效应，提升数据空间国际影响力。

https://www.c114.com.cn/news/16/a1195184.html

5、元宇宙时代，我们的隐私何处安放？

据 360 公司的一项调查结果显示，超八成参与调查者认为，元宇宙会让数字世界的安全问题日益突出，如数据安全、信息安全、新型网络骗局等，其中个人信息泄露问题让人最为担心。

在元宇宙空间里，要实现随心而动、深度沉浸的体验，个人数据的交付需要全面升级，种类、维度、深度要求都将出现前所未有的提升。除了身份属性、行为习惯、人际关系、场景位置等数据的全方位交付之外，元宇宙索取数据的边界

还向人类身体内部更进一步拓展——人脸、指纹、声纹、眼球运动、肌电信号、脑电波等等。

由于元宇宙个人信息收集的海量性、集中性、隐私性，导致一旦被泄露，个人隐私的损失将是全方位的，将对公众人身安全、财产安全带来巨大威胁。例如借助深度伪造技术，利用个人信息制作色情视频、实施财产诈骗、煽动社会舆论等。

对于元宇宙的隐私风险，专家认为必须要从一开始就前瞻性地规划设计，“防病于未然,而非已发时刻”。

首先要树立基本的原则导向，将增进人类福祉、促进公平公正、保护隐私安全、确保可控可信、强化责任担当等作为基本的伦理要求。

第二要设置前置性的规则，比如把避免上瘾作为重要的技术指标，数据收集应坚守合法、目的正当、最小化、公开原则。

第三是要前瞻性地进行法律完善，中国的《数据安全法》《个人信息保护法》等法律法主要是面向移动互联网行业生态。在元宇宙时代，立法应当提出更高的数据保护标准，着眼于新风险新问题，强化平台要求，清晰责任界定，以切实保障用户的个人信息权益。

https://mp.weixin.qq.com/s/iKwlPe0aP2NTOKkldrDV7Q

数据安全事件

1、宜家加拿大公司承认数据泄露涉及约 95000 名客户信息

2022 年 5 月 6 日，当地时间宜家(IKEA)加拿大公司表示已经将该公司大约 9.5 万名客户的个人信息数据泄露事件通报给加拿大的隐私监管机构。宜家(IKEA)加拿大公司在致受影响客户的一封信中表示，可能已被泄露的数据包括客户姓名、电子邮件地址、电话号码和邮政编码。

这家来自瑞典的家具零售商说，它被告知一些顾客的个人信息泄露风险出现在"2022 年 3 月 1 日至 3 月 3 日期间，宜家加拿大公司的一名同事进行的普通搜索"的结果中。“该同事利用宜家加拿大公司的客户数据库获取了这些个人信息。我们可以确认，没有财务或银行信息被获取，”宜家加拿大公司在一份电子邮件声明中说，并补充说，“我们已经采取行动补救这种情况，包括采取措施防止数据被使用、储存或与任何第三方共享。”

https://mp.weixin.qq.com/s/PIG1RP-n5pYBWTNZvEC4JA

2、美国能源供应商 Riviera Utilities 的数据泄露暴露了客户信息

2022 年 5 月 3 日报道，为阿拉巴马州鲍德温县服务的公

用事业公司 Riviera Utilities 发生数据泄露事件，在员工电子邮件帐户被访问后暴露了客户的个人详细信息。

在 5 月 2 日发布的一份声明中，该公司证实一名不知名的黑客获得了内部数据的访问权限。暴露的细节包括“有限数量”的个人信息，例如姓名、社会安全号码、驾驶执照或州身份证号码、护照号码、医疗信息、健康保险信息、信用卡或借记卡号码、卡到期日期、和卡片 CVV。

https://portswigger.net/daily-swig/data-breach-at-us-energy-supplier-riviera-utilities-exposes-customer-information

3、美国农业机械制造商爱科（AGCO）遭受勒索软件攻击

2022 年 5 月 6 日，总部位于美国的领先农业机械生产商 AGCO 宣布受到勒索软件攻击，影响其部分生产设施。AGCO 仍在调查攻击的程度，但预计其业务运营将受到几天的不利影响，甚至可能更长的时间才能完全恢复所有服务，具体取决于公司能够修复其系统的速度。

https://www.bleepingcomputer.com/news/security/us-agricultural-machinery-maker-agco-hit-by-ransomware-attack/

4、Conti 勒索软件声称入侵了秘鲁情报总局

2022 年 5 月 8 日，Conti 勒索软件团伙将秘鲁情报总局

(DIGIMIN) 添加到其 Tor 泄漏站点上的受害者名单中。国家情报局是秘鲁首屈一指的情报机构。该机构负责国家、军事和警察情报以及反情报工作。该勒索软件团伙声称窃取了 9.41 GB 的数据。

https://securityaffairs.co/wordpress/131093/cyber-crime/conti-ransomware-peru-direccion-general-de-inteligencia.html

5、英伟达涉嫌违规披露被罚款 550 万美元

2022 年 5 月 7 日，据相关媒体报道报道，近日，美国证券交易委员会指控英伟达在加密采矿对公司显卡等销售业务的影响方面，披露的信息并不够充分。目前，英伟达已经接受停终调令，为此支付了 550 万美元（折合人民币约 3666 万元）的罚款。不过，英伟达的财报数据显示，2021-2022 全年，英伟达的总计营业收入超过了 269 亿美元（折合人民币约 1793 亿元），利润达到了 97.52 亿美元（折合人民币约 650 亿元）。所以，这次的罚款并不会对其经营造成什么影响。

https://mp.weixin.qq.com/s/QR8RrI6oRtSy0XGB7coVxA

6、2021 年 30.8 万个数据库暴露 美国和中国占大头

2022 年 5 月 8 日报道，去年 7 月，研究人员发现超过 1 万个不安全数据库暴露在网上，无需通过任何安全身份验证

即可公开访问其中 10 亿多条记录。如今，Group-IB 的 IT 安全研究人员披露令人震惊的数据，揭示数据库暴露激增情况。

Group-IB 位于新加坡，其研究人员持续扫描 IPv4 生态系统，检测面向外部的资产是否托管着易受攻击的公开数据库、网络钓鱼面板、恶意软件和 JS 嗅探器等。2021 年第一季度到 2022 年第一季度，研究人员发现了 39.92 万个公开数据库；而 2021 年全年发现的公开数据库数量为 30.8 万个，表明 2022 年暴露在公网上的数据库数量增长了 16%。其发现的公开数据库中约 9.36 万个位于美国的服务器上，美国是数据库暴露最严重的地区；其次是中国，有 5.47 万个数据库暴露在公网上。

https://mp.weixin.qq.com/s/_aT3iOycNEuyKjeUIZ_2vw

7、行车记录全暴露！高合汽车陷隐私泄露风波

2022 年 5 月 6 日，南都报道，一则“高合行车记录仪疑似泄露隐私”的话题引发关注。汽车博主@李老鼠说车爆料称，高合汽车的行车记录仪可通过车主互联功能接收其他高合汽车的信号，并读取这些汽车行车记录仪内容。次日，高合汽车对此作出回应，称该功能主要用于车队出行、车路协同，开启时需经用户同意，无隐私安全隐患。

资深律师告诉南都记者，行车记录仪收集的画面包括车

外人员的个人信息，高合汽车向其他车辆提供其采集的音视频信息是违法的，应将涉及车外人员的画面进行删除或匿名化处理。

https://www.secrss.com/articles/42165

8、Heroku 承认客户凭证在网络攻击中被盗

2022 年 5 月 5 日，Salesforce 的子公司 Heroku 透露，上个月被盗的 GitHub 集成 OAuth 令牌进一步导致了内部客户数据库的入侵。Salesforce 拥有的云平台承认，攻击者使用相同的受损令牌从“数据库”中窃取客户的散列和加盐密码。

5 月 4 日， Heroku 强制重置了所有用户的密码以应对上个月的安全事件，但是并未解释具体原因。之后，该公司在 5 月 5 日发布了最新消息，表示其被盗的 GitHub OAuth 令牌已被用于入侵数据库并泄露用户的账户和密码。GitHub 于 4 月 12 日发现了该攻击，泄露了包括 NPM 在内的数十个组织的数据。

https://www.bleepingcomputer.com/news/security/heroku-admits-that-customer-credentials-were-stolen-in-cyberattack/

9、攻击者劫持英国 NHS 电子邮件帐户以窃取 Microsoft 登录信息

2022 年 5 月 5 日报道，据调查，在近半年的时间里，英国国家卫生系统(NHS)的 100 多名员工的工作电子邮件帐户被多次用于网络钓鱼活动，其中一些活动旨在窃取 Microsoft 登录信息。在劫持合法的 NHS 电子邮件帐户后，这些攻击者于去年 10 月开始使用它们，并至少在今年 4 月之前将其继续用于网络钓鱼活动。据电子邮件安全 INKY 的研究人员称，已经从英格兰和苏格兰员工的 NHS 电子邮件帐户发送出 1000 多条网络钓鱼邮件。

https://mp.weixin.qq.com/s/VG0NJk7l0L9ZRSJajc87xQ

10、数以千计的借款人数据从 ENCollect 收债服务中暴露

2022 年 5 月 5 日，据外媒报道，一个在 Internet 上暴露且没有密码的 ElasticSearch 服务器实例包含有关印度和非洲金融服务机构贷款的敏感财务信息。由信息安全公司 UpGuard 的研究人员发现其泄漏量为 5.8GB，共有 1,686,363 条记录。“这些记录包括姓名、贷款金额、出生日期、帐号等个人信息，” UpGuard 表示。“收集中共有 48,043 个唯一的电子邮件地址，其中一些用于分配给每个案例的产品管理员、企业客户和收集代理。”

https://thehackernews.com/2022/05/thousands-of-borrowers-data-exposed.html?&web_view=true