全球数据安全观察

总第 94 期 2022 年第 22 期

（2022.06.20-2022.06.26）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、国务院印发《关于加强数字政府建设的指导意见》

6 月 23 日，国务院印发了《关于加强数字政府建设的指导意见》，就全面开创数字政府建设新局面作出部署，提出 2025 年和 2035 年两阶段的工作目标，六项基本原则，七方面重点任务。

其中，《指导意见》要求落实安全制度要求。建立健全**数据分类分级保护、风险评估、检测认证**等制度，加强**数据全生命周期安全管理和技术防护**。加大对涉及**国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据**的保护力度，完善相应问责机制，依法加强**重要数据出境安全管理**。加强**关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密码应用安全性评估的机制**，定期开展网络安全、保密和密码应用检查，提升数字政府领域关键信息基础设施保护水平。

https://mp.weixin.qq.com/s/Jf0AaWf7H5Uy2YY62GH8bA

2、习近平主持召开深改会，强调加快构建数据基础制度

据新华社 2022 年 6 月 22 日报道，中共中央总书记、国家主席、中央军委主席、中央全面深化改革委员会主任习近

平 6 月 22 日下午主持召开中央全面深化改革委员会第二十六次会议，审议通过了《关于构建数据基础制度更好发挥数据要素作用的意见》、《关于加强和改进行政区划工作的意见》、《关于开展科技人才评价改革试点的工作方案》、《强化大型支付平台企业监管促进支付和金融科技规范健康发展工作方案》。

习近平在主持会议时强调，数据基础制度建设事关国家发展和安全大局，要**维护国家数据安全，保护个人信息和商业秘密**，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

会议指出，数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。我国具有数据规模和数据应用优势，我们推动出台数据安全法、个人信息保护法等法律法规，积极探索推进数据要素市场化，加快构建以数据为关键要素的数字经济，取得了积极进展。**要建立数据产权制度**，推进公共数据、企业数据、个人数据分类分级确权授权使用，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，健全数据要素权益保护制度。**要建立合规高效的数据**

要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。**要完善数据要素市场化配置机制，**更好发挥政府在数据要素收益分配中的引导调节作用，建立体现效率、促进公平的数据要素收益分配制度。**要把安全贯穿数据治理全过程**，守住安全底线，明确监管红线，加强重点领域执法司法，把必须管住的坚决管到位。要构建政府、企业、社会多方协同治理模式，强化分行业监管和跨行业协同监管，压实企业数据安全责任。

https://mp.weixin.qq.com/s/eBfNBGyMbM1S7pHryxldEA

3、最高检：严厉打击行业“内鬼”泄露公民个人信息违法犯罪

近日，最高人民检察院印发《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》（下称《通知》）。要求各地检察机关积极推动促进个人信息保护法等法律法规的统一正确实施，参与网络空间治理，强化刑事检察和公益诉讼检察职能衔接协作，实现全链条打击、一体化网络治理。

《通知》要求，深入开展依法打击行业“内鬼”泄露公民个人信息违法犯罪工作，积极配合“清朗”系列专项行动，探索积累常态化监督办案的典型经验。聚焦重点行业、重点领域、重点群体开展监督办案，包括处理大规模个人信息特别

是个人敏感信息，容易产生个人信息泄露风险的重点行业；金融、电信、互联网、就业招聘行业中容易产生电信网络诈骗违法犯罪风险的重点领域；容易受到电信网络诈骗违法犯罪侵害的老年人、在校学生、未成年人等重点群体。在严厉打击刑事犯罪的同时，充分发挥公益诉讼检察职能，依法追究违法主体的民事责任，督促行政机关履职尽责，增强惩治预防效能。

https://mp.weixin.qq.com/s/5PGsnLNWRZDs1M6CF3FaJw

4、深圳发布《深圳市数字政府和智慧城市“十四五”发展规划》

近日，深圳市政务服务数据管理局联合市发展改革委发布了《深圳市数字政府和智慧城市“十四五”发展规划》（下称《规划》）。《规划》提出，到 2025 年，打造国际新型智慧城市标杆和“数字中国”城市典范，成为全球数字先锋城市；到 2035 年，数字化转型驱动生产方式、生活方式和治理方式变革成效更加显著，实现数字化到智能化的飞跃，全面支撑城市治理体系和治理能力现代化，成为更具竞争力、创新力、影响力的全球数字先锋城市。

在打造数字生态方面，《规划》提出，加快推动《深圳经济特区数据条例》实施，逐步完善数据产权、数据交易等法规、制度和标准体系。加强粤港澳大湾区智慧城市群合作，

推进标准互认、规则衔接。探索建立数据跨境流动、共享等机制。构建全市统一网络安全体系架构，打造全天候、全场景的网络安全保障体系。

到2025年，推进《深圳经济特区数据条例》相关配套制度建设，完成数据要素市场化配置改革试点，培育数据要素市场，实现数据交易活跃度和数据服务业规模全国领先。公共数据服务体系逐步健全，公共数据资源社会开放数据集不少于5000个，“一数一源”覆盖率达85%。网络安全建设、运营、管理和标准规范体系进一步健全。对外合作不断深化，打造数字化领域合作新范式。

《规划》创新工作推进机制，探索建立数字政府和智慧城市建设绩效评估体系和评估指标，以年度为周期对数字政府和智慧城市发展水平，以及各区各部门应用系统建设情况和使用效果进行评估。同时，设立首席数据官（CDO），明确首席数据官职责范围和评价机制，促进公共数据开发利用，优化数据要素资源配置。

https://mp.weixin.qq.com/s/gMozIi-ummxwrs4NtriACg

5、《江西省“十四五”数字经济发展规划》发布！加快数据要素市场化流通、创新数据要素开发利用机制

近日，江西省政府印发《江西省“十四五”数字经济发展

规划》，聚焦深耕产业赛道、加快产业数字化转型、优化区域布局等重点领域，对江西数字经济发展作出系统谋划和总体部署。

其中关于提升数字经济治理能力，强化数字经济安全体系指出以下要点:

统筹发展与安全，坚持发展和监管两手抓，探索建立与数字经济发展相适应的治理方式，进一步推动数字经济规范健康持续发展。

关于健全网络安全保障体系——贯彻《中华人民共和国网络安全法》《中华人民共和国密码法》，落实等级保护、安全测评、电子认证、应急管理、国产密码应用等制度。强化落实网络安全技术措施同步规划、同步建设、同步使用的要求，确保重要系统和设施安全有序运行。加强网络安全基础设施建设，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力。健全网络安全保障工作体系，落实网络安全等级保护 2.0、涉密网络分级保护、商用密码应用安全评估等工作。加快建设省网络安全应急指挥平台，提升网络安全监测预警、应急处置能力。加快发展网络安全产业，促进拟态防御、数据加密等网络安全技术应用。加强防范、严厉打击各类新型网络违法犯罪。关于**强化数据安全保护**——全面贯彻落实《中华人民共和国

数据安全法》《中华人民共和国个人信息保护法》，建立健全数据安全相关管理制度。制定重要数据具体目录，加强数据分类分级保护。依法依规做好网络安全审查、云计算服务安全评估等，有效防范国家安全风险。建立健全政务数据安全管理制度，落实数据安全保护责任，保障政务数据安全。落实个人信息保护制度规范，引导互联网平台加强内部管理和安全保障，加强个人信息安全管理。建立数据安全风险评估、报告、信息共享、监测预警和应急处置机制，加强数据安全风险信息的获取、分析、研判、预警和处置。

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

6、《厦门市全面提升营商环境数字化便利化水平培育和激发市场主体活力行动方案》发布！深化公共数据共享、加强数据归集应用

经厦门市政府研究同意，《厦门市全面提升营商环境数字化便利化水平培育和激发市场主体活力行动方案》（以下简称《方案》）于近日印发实施。

方案提出要持续优化公共数据应用场景共享授权，推动需求清单快速获批。推动省、市间政务数据共享。建立完善全市公共数据分层采集体系，各区开展基层业务数据、视频数据和物联数据的统一规范采集和结构化处理，各市级部门

依法依规实现数据全量归集和整合，对于无法实现数据全量归集和整合的，则通过接口调用等方式实现数据的按需共享。

市发改委表示，营商环境是企业生存和发展的土壤，事关城市核心竞争力。根据《方案》，厦门市将聚焦营商环境数字化便利化建设的难点、堵点，启动新一轮“数字政府”强基工程，强化系统整合、标准统一、数据共享、跨域联动，倒逼政务服务方式、路径、规则、机制等重塑，大幅提升我市营商环境数字化便利化水平。

https://mp.weixin.qq.com/s/aGQAgUB61fALmy8bTUCCog

7、《西安市政务数据开放管理办法（征求意见稿）》发布

近日西安市大数据资源管理局公开征求《西安市政务数据开放管理办法（征求意见稿）》，本办法从2022年6月25日至2022年7月25日公开向社会征求意见。征求意见稿提到：

关于数据开放——第十九条 **政务数据开放属性分为无条件开放类、有条件开放类和不予开放类3类**。对法律、法规和规章禁止开放，开放后可能危及国家安全、公共安全、经济安全、社会稳定的，或者涉及商业秘密、个人隐私等开放后会对第三方合法利益造成损害的政务数据，列入不予开放类；对数据安全和处理能力要求较高或者需要按照特定条

件提供给数据使用主体的政务数据列入有条件开放类；其他政务数据列入无条件开放类。

不予开放类政务数据依法进行脱密、脱敏处理后可列入有条件开放类或者无条件开放类；第三方同意开放或数据开放主体认为不开放会对公共利益造成重大影响的，列入有条件开放类或者无条件开放类。

关于数据使用——第二十七条　数据使用主体应严格按照数据开放使用协议的约定使用有条件开放类数据。如发现数据使用主体违规、超范围使用等情况或使用过程中存在安全风险，政务数据主管部门和数据开放主体有权暂停或终止数据开放服务。违反相关法律的，依法追究数据使用主体法律责任。

第二十八条　鼓励高等院校、科研机构和市场主体开展政务数据分析挖掘、数据可视化、数据安全与隐私保护等关键技术研究，提高数据开发使用和安全管理水平。

鼓励数据使用主体使用开放数据开展科技研究、咨询服务、产品开发、数据加工等活动，充分挖掘数据价值。所获得的合法收益，受法律保护。

https://mp.weixin.qq.com/s/QMjg9scVKX3OiLMCZQsxqw

8、信安标委《个人信息跨境处理活动安全认证规范》发布

为落实《个人信息保护法》关于建立个人信息保护认证制度的相关要求，指导个人信息处理者规范开展个人信息跨境处理活动，信安标委秘书处组织编制了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》。

实践指南依据有关政策法规要求，为落实《个人信息保护法》建立个人信息保护认证制度提供认证依据。申请个人信息保护认证的个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求；对于开展跨境处理活动的个人信息处理者，还必须符合本实践指南的要求。

实践指南从基本原则、个人信息处理者和境外接收方在跨境处理活动中应遵循的要求、个人信息主体权益保障等方面提出了要求，为认证机构实施个人信息保护认证提供跨境处理活动认证依据，也为个人信息处理者规范个人信息跨境处理活动提供参考。

https://mp.weixin.qq.com/s/G5K4QzgytQvOckGjl-fhQw

技术、产品与市场

1、全球首个 IEEE 隐私计算互联互通国际标准正式启动

6 月 21 日，IEEE SA 隐私计算互联互通标准 P3117《Standard for Interworking Framework for Privacy-Preserving Computation》（以下简称 IEEE P3117）第一次工作启动会成功召开，标志着全球首个隐私计算互联互通国际标准工作组正式成立并启动标准制定工作。

隐私计算互联互通是指异构闭源隐私计算平台间，在不暴露平台内部设计细节且不受平台自身更新、升级、扩容影响的情况下，通过统一标准化的接口和协议，实现跨平台交互协作，共同完成相同的隐私计算任务。IEEE P3117 标准将建立基于隐私计算互联互通的技术框架规范，定义实现异构隐私计算平台之间互通所需的节点、资源、算法组件以及其他必要部分的功能，为不同技术路径下隐私计算平台跨平台协作的设计、开发、测试和维护提供互联互通标准参考。

https://mp.weixin.qq.com/s/B3W6OReHKOrwoK11ufk3mA

2、首个元宇宙国际标准联盟成立

据外媒报道，首个元宇宙国际标准联盟近日正式宣告成立。这个组织名为“元宇宙标准论坛”（Metaverse Standards

Forum），由全球数十家科技行业巨头组成。根据元宇宙标准论坛发布的声明，该组织成立的目的是，就构建开放元宇宙所需的互操作性标准进行全行业合作，以及探讨如何加速标准开发组织定义并推动元宇宙标准制定相关的工作。

https://mp.weixin.qq.com/s/xx7xNCQ4-OeWAWVGcmrI5w

3、2021 年 80%的公司遭遇身份相关数据泄露

6 月 22 日，Dimensional Research 发布了一项针对 IT 和身份专业人员的调查，结果显示，在不断增加的云采用、第三方合作伙伴和机器身份的推动下，几乎每家企业（98%）需要管理的身份数量都在快速增长。而且，须管理身份数量的暴增还导致了数据泄露事件的增长，84%的公司在过去一年里经历了身份相关的数据泄露，而此前一项覆盖两年时间的调查研究中这一比例还只是 79%。

根据此项调查数据编撰的《2022 年数字身份保护趋势》白皮书中显示，在大多数情况下，企业关注员工身份，其中 70%的受访企业认为员工身份最有可能遭到泄露，58%认为员工身份泄露的影响最大。但是，第三方合作伙伴和企业客户也是重大风险来源，分别有 35%和 25%的受访者认为二者是主要的数据泄露源头。

https://mp.weixin.qq.com/s/G1hGrpZG2nNGcnr3Te5D5Q

4、2021 年针对美国教育机构的勒索软件攻击共造成 35.6 亿美元损失

在过去的几年里，勒索软件攻击已经成为全世界学校和学院越来越关注的问题。它们使关键系统瘫痪，使学校连续数日关闭，并使教师无法访问教案和学生数据。据 Comparitech 研究团队报告显示，2021 年，67 次单独的勒索软件攻击影响了 954 所美国教育机构（包含学校和学院），影响到 950129 名学生。估计这些攻击仅在停机时间方面就使教育机构损失了 35.6 亿美元。大多数学校还将面临天文数字般的恢复成本，因为他们试图恢复计算机，恢复数据并加固系统以防止未来的攻击。虽然这些数字可能看起来很高，但它们都标志着比 2020 年的水平下降了两位数的百分比，包括受影响的学生人数下降了近 50%。

https://www.cnbeta.com/articles/tech/1285049.htm

5、国内首个个人信息保护、确权服务平台“人民数保”正式上线

2022 年 6 月 20 日，由人民日报、人民网旗下“党管数据”理论和实践平台—人民数据和世纪互联倾力打造的“人民数保”平台正式上线。这是我国首个个人信息保护与确权服务平台，旨在保护个人数据不被非法乱用的同时，实现数

据精准确权、授权、流转及二次开发，将个人数据权利还归个人，让数据真正取用于民、造福于民，让广大人民群众共享数字化红利。

据介绍，人民数保基于数据权限管理和资源调度机制，利用区块链技术，既防止数据滥用、盗用、泄露，又提供了数据共享的酬劳分配机制，确保了数据消费者在请求、授权和行权过程中的责权清晰，从而促进数据消费者对所授权数据的利用和价值挖掘，实现了从数据资源到数据资产乃至数据资本的发展。

https://mp.weixin.qq.com/s/PqAByhoIC6ht_CT-kRsvgw

业界观点

1、盘和林：产权是数据交易的基础，以需求推动数据供给

浙江大学国际联合商学院数字经济与金融创新研究中心联席主任、研究员盘和林认为，数据要素和其他要素的差异主要包括：一、数据要素流通有安全性的要求；二、数据要素权属界限并不清晰，并且数据要素的权属是一种权益，而不是一种所有权，这也和其他要素不同，权益是可以分割的，是要进行利益分配的，但事实上数据的权益分配依然是个难题；三、数据的需求是多元且复杂的，数据的价值链条更为复杂。

盘和林表示，数据确权是数据市场交易的前提，他认为可以从以下几个方面完善确权体系：

一、划定个人信息隐私和公共数据之间的边界。

二、多从需求方来倒推数据权属。“谁投入，谁贡献”是从供给侧，而谁受益是从需求侧，由于数据需求很多都是定制的，同样数据在使用的时候，目的不同，其权益分配规则和数据责任也不同。

三、以案例来确权。应对复杂情况的最好办法是案例说明，能够为数据产权裁量提供更多参考，实践才是检验真理的唯一标准，案例积累能够为数据交易带来更有参考价值的

权属认定标准。

此外，盘和林对数据集中、数据定价、数据应用促创新等也提出了相应的解决方案。

https://weyt.p5w.net/article/5557808

2、王新锐：建立数据产权制度的新思路

6 月 22 日中央召开专门会议，审议通过了《关于构建数据基础制度更好发挥数据要素作用的意见》(简称《意见》)。《意见》为数据产权制度提供新的思路，即数据产权并不等于数据所有权。而且，赋予数据持有权、加工使用权、经营权等也是更为现实和灵活的做法。

实际上，数据权属也不应单纯地被理解为数据所有权，持有权、加工使用权、经营权都可以被认定为数据权属，而且数据权属也不应只包括上述三种类型。当今多数国家和地区在立法上都没有承认主体对数据享有所有权，英国法院的一些判例就直接表明了数据不是财产的观点。数据流通的关键问题不在于谁享有所有权，而在于如何激励主体之间主动进行数据共享。欧盟为了激励企业主体共享自身数据，专门设计了由数据接收者合理补偿数据持有者共享数据产生的费用。欧盟还尝试通过立法建立公共数据空间，确立非个人数据访问权等制度来促进数据流通。特别是今年 2 月 23 日

欧盟委员会通过的《数据法案》提案，针对个人、企业及公共部门数据共享建立了全新的制度框架，确保数据权益者能够自由访问数据，并通过推动跨部门数据共享和开发利用激发数据要素。

在促进我国数字经济高速发展的背景下，《意见》无疑提供了数据产权制度的新的思路，摆脱数据产权等于数据所有权的窠臼。同时，《意见》也为参与数据活动的数据持有者、加工使用者、经营者提供制度保障，有利于促进数据的利用和发展。

https://m.21jingji.com/article/20220626/herald/55b4b636852ef4743806d4f201638e2b.html

3、韩言妮：加快数字安全先进技术落地 构建安全发展新格局

在 6 月 21 日召开的 2022 年科技周暨移动信息产业创新大会上的大数据分论坛上，中国科学院信息工程研究所网络与系统安全实验室副研究员韩言妮指出，随着数字经济在全球范围内的蓬勃发展，人们对数据主权和安全保护的需求也日益增加。数据安全首次被提到国家层面的新高度，成为战略布局的要点。因此，一定要提升数据安全保障能力。

数据安全、数据基础设施的建设、数据的存储、数据的

跨境流通和数据新兴技术，将会成为战略部署的重点和要点。同时数据安全也给全新的产业带来了千载难逢的发展机遇，加快数字安全的先进技术落地，将有助于构建安全发展的新格局。

韩言妮认为，数据安全法的法治法规仍然需要细化，才能成为监管的有力抓手。因此，下一步相配套的重要的规范标准体系，也成为未来重点的工作。

https://www.c114.com.cn/4app/3542/a1199767.html

4、人民日报：把个人信息“安全堤”筑得更牢

置身移动互联时代，人们在享受智能设备带来便利的同时，也在一些场景中面临个人信息泄露风险。随着技术的演进、网络应用的迭代，无论从硬件还是软件的角度来看，人们正面临着比以往更加复杂多样的信息使用场景。与之相应，非法采集、盗取个人信息的行为和手段也更具欺骗性、迷惑性。这些都给监管和治理增加了难度，带来了挑战。

仔细推究，造成信息泄露的主要原因往往在于：前期未经同意擅自收集用户信息，或者过度索权、超限收集；后期对信息处理不当，甚至为了牟利出售信息。这启示我们，守护个人信息安全要有整体思维、系统思维，必须紧盯信息采集、储存、共享、披露等各环节，进行全链条管理。

筑牢信息安全边界，需要凝聚众力，相关部门、行业、平台和用户应共同作为。对于违法违规现象和行为，**监管部门**应加强治理，及时予以惩处。对**企业和平台**而言，理应秉持“合法、正当、必要”“最小够用”等收集和处理用户信息的原则，加强自查自律，谨守法律红线。作为**用户**，也应增强个人信息保护意识，敢于善于维护自身合法权益。多措并举、久久为功，方能织密个人信息安全防护网，尽可能减少信息泄露带来的危害。

https://www.c114.com.cn/news/211/a1199648.html

5、人民网评：全面开创数字政府建设新局面

近年来，我国数字政府建设已进入快车道。各级政府业务信息系统建设和应用成效显著，数据共享和开发利用取得积极进展，一体化政务服务和监管效能大幅提升，“最多跑一次”“一网通办”等创新实践不断涌现。也要看到，数字政府建设仍存在顶层设计不足、创新应用能力不强、数据壁垒依然存在、网络安全保障体系存在短板、干部队伍数字意识和数字素养有待提升等问题。

破堵点、攻难点，让数字政府成色更足，是提升政府治理数字化水平的题中之义。具体包括:

一、加强数字政府建设，必须强化系统观念。政府履职

和政务运行数字化转型，不是针对具体业务的小修小补，而是着眼政府职能的全面改革。

二、加强数字政府建设，必须夯实数字基础。一方面，数字技术是数字政府建设的根基。建设智能集约的平台支撑体系，强化信息技术应用创新，有助于扩大社会治理的覆盖面、提升政务服务的精准度。另一方面，数据安全是数字政府建设的保障。需要落实安全管理制度，加快关键核心技术攻关，加强关键信息基础设施安全保障，强化安全防护技术应用，筑牢数字政府建设安全防线。

三、数字政府建设不仅是技术应用问题，更是组织管理问题。明确制度打破藩篱，以统一规则共享数据，同时倒逼政府工作人员提升网络素养。从审批事项削减，到网上自主办理，数字政府建设势必要对原有组织架构、工作方式来一场革新。

http://opinion.people.com.cn/n1/2022/0625/c223228-32456430.html

数据安全事件

1、日本汽车零件制造商 Nichirin 称其遭到勒索攻击

2022 年 6 月 23 日报道，日本汽车和摩托车软管制造商 Nichirin 的子公司 Nichirin-Flex USA 遭到了勒索攻击，导致该公司的网络中断。攻击发生在 6 月 14 日，该公司在检测到其网络上未经授权的访问后立即将操作切换到手动模式。由于网络攻击也影响了产品分销，并且订单是手动完成的，因此客户的订单应该会延迟。该公司的声明表示，恢复系统已成为恢复业务运营的优先事项，其目前正在调查未经授权的访问是如何发生的，并试图确定信息泄露的影响。

https://www.bleepingcomputer.com/news/security/automotive-hose-maker-nichirin-hit-by-ransomware-attack/

2、巴西零售商 Fast Shop 披露“勒索”网络攻击

2022 年 6 月 22 日，巴西最大的零售商之一 Fast Shop 遭受了“勒索”网络攻击，导致网络中断并暂时关闭其在线商店。该次攻击影响了 Fast Shop 主网站、移动应用程序和在线订购系统，没有影响实体店。

https://www.bleepingcomputer.com/news/security/fast-shop-brazilian-retailer-discloses-extortion-cyberattack/

3、宾夕法尼亚州 HIM 服务提供商遭到勒索软件攻击

2022 年 6 月 22 日，据称，Hive 威胁攻击者袭击了总部位于宾夕法尼亚州的公司 Diskriter，该公司提供健康信息管理服务、收入周期管理解决方案、转录服务和人员配备。Diskriter 的客户包括许多州和市政府以及医疗机构。Hive 的发言人声称，勒索软件组织能够窃取超过 160 GB 的文件，其中包括合同和其他商业文件、公司的财务记录、公司高管的个人和财务信息、员工的人事信息以及与软件源有关的文件代码。

https://www.databreaches.net/a-pennsylvania-him-services-provider-hit-with-ransomware-threat-actors-claim-they-will-leak-source-code/

4、Facebook 面临一项集体诉讼，被控私自收集数百万医疗用户信息

2022 年 6 月 21 日，据外媒报道，Facebook 正面临一项拟议的联邦集体诉讼，指控 Facebook 在患者不知情和同意的情况下，从医疗网站和患者门户网站非法收集“数百万”个人信息。

该诉讼于周五由加利福尼亚北区的一名匿名“John Doe”

原告提起，指控 Facebook 在医疗中心部署旨在改进营销活动的名为 Meta Pixel 的跟踪工具时故意接收患者数据。投诉称，至少有 664 家医院或医疗服务提供者部署了跟踪技术。原告的律师声称该行为违反了多项联邦和州法律，包括电子通信隐私和窃听索赔、加利福尼亚州的《侵犯隐私法》和该州的《不公平竞争法》。

https://www.inforisktoday.com/lawsuit-facebook-collecting-patient-data-millions-a-19424

5、CafePress 因影响 2300 万用户的违规行为被罚款 50 万美元

2022 年 6 月 24 日消息，美国联邦贸易委员会 (FTC) 已责令 CafePress T 恤和商品网站的前所有者 Residual Pumpkin Entity 支付 500,000 美元的罚款，原因是其掩盖了影响超过 2300 万客户的数据泄露事件，并且未能保护他们的数据。

https://www.bleepingcomputer.com/news/security/cafepress-fined-500-000-for-breach-affecting-23-million-users/

6、美国 Flagstar 银行 150 万客户数据遭泄露

近日，Flagstar 银行向其 150 多万名客户发送了一则通知，告知他们在去年 **2021 年 12 月的一次网络攻击中，他们**

的个人数据遭到了黑客的访问。2021 年 12 月，Flagstar 银行发生了一起安全事件，攻击者入侵了银行的内部网络。此后，银行方面着手对这起事件开展了调查，并于近日发现，攻击者当时访问了许多客户的敏感信息，包括姓名和社会保障号码等。根据提交给缅因州总检察长办公室（Office of the Maine Attorney General）的信息显示，这次数据泄露事件共对 1,547,169 名美国人造成了影响。

https://www.secrss.com/articles/43828

7、英国汽车服务提供商 Halfords 因网站漏洞泄露客户详细信息

2022 年 6 月 23 日，据外媒报道，根据一名安全研究人员的调查结果，英国汽车服务和零部件销售商 Halfords 过于随意地分享了其客户的详细信息。

仅凭借电子邮件地址，安全研究人员就能够提取有关他的预订的各种信息，包括他的电话号码、汽车详细信息以及他家的确切位置。同样，还可以检索与该 ID 关联的所有客户详细信息。“通过订单 ID 似乎可以找到数十万不同的订单，每个订单都包含个人身份信息。”研究人员表示。

https://www.theregister.com/2022/06/23/halfords_data_leak_vulnerability/?&web_view=true

8、Jacuzzi SmartTub 应用程序中的漏洞可能允许访问用户数据

2022 年 6 月 24 日报道，据研究人员称，Jacuzzi SmartTub 应用程序 Web 界面中的多个漏洞可能使攻击者能够查看并可能操纵热水浴缸所有者的个人数据。

SmartTub 应用程序可用于 iOS 和 Android，允许客户远程控制按摩浴缸，例如设置水温和打开喷水器。研究人员能够轻易设法绕过 Smarttub.io 的登录页面，进入两个仅供内部使用的管理面板。“一旦进入管理面板，我被允许访问的数据量是惊人的。我可以查看每个水疗中心的详细信息、查看其所有者，甚至删除其所有权。”研究人员表示。

https://securityaffairs.co/wordpress/132559/hacking/jacuzzi-smarttub-app-flaws.html

9、印第安纳大学健康中心遭受敏感数据泄露事件

2022 年 6 月 23 日，据外媒报道，不明身份的肇事者访问了全国超过 100 万医院患者的敏感医疗保健数据和个人信息，其中包括在印第安纳大学健康中心（IU Health）接受治疗的患者。

IU Health 的供应商之一，总部位于西雅图的 MCG，已

向患者发送信函，通知他们未经授权的一方访问了患者的个人信息，包括姓名、医疗代码、邮政地址、电话号码、电子邮件地址、出生日期和社会安全号码。

据一封发给当地患者的信表明，数据泄露影响了美国至少九个州的患者。而根据缅因州总检察长办公室的说法，此次泄露泄露了大约 110 万人的数据。

https://www.heraldbulletin.com/news/iu-health-has-sensitive-data-breach/article_a0e6b638-f357-11ec-a9ce-7f6d3a931aaf.html?&web_view=true