国家工程研究中心和天枢智库联合出品

数字安全观察

DIGITAL SECURITY INSIGHT

数据安全专刊 No. 005(总第 191 期)

责编：钟力 zhongli1@360.cn

导 读

第五期《数字安全观察 数据安全专刊》旨在呈现 2022 年第三季度的全球数据安全态势。本期分为政策形势、技术趋势、行业趋势、安全事件、大咖观点五个板块，主要内容如下：

政策形势方面，本期选取了 2022 年第三季度数据安全领域备受关注的十条政策消息，并进行点评分析。国内方面，7 月份，国家互联网信息办公室制定的《数据出境安全评估办法》一经发布便备受瞩目，可谓我国数据出境制度的重要里程碑事件；9 月份，网信办发布《网络安全法》修订的征求意见稿，现行生效稿施行已逾五年，后续的修订将围绕罚则展开并提高处罚力度，相信能更好地与《数据安全法》、《个人信息保护法》相衔接。国外方面，法规监管依旧严格，欧洲议会通过了《数字服务法》和《数字市场法》、俄罗斯修订《联邦个人数据法》等，科技巨头将面临更严苛的监管。

技术趋势方面，量子加密和隐私计算技术取得重大突破，成为关注热点。一方面，NIST 发布四种新的抗量子攻击算法，其中有三种都是基于格的算法，但同时也有研究表明，仅 1 小时就可以破解一种后量子加密候选算法，可见后量子密码算法研究还需持续推进。另一方面，Gartner 发布 2022 年新兴技术成熟度曲线，前沿热门技术共 25 项，其中隐私计算相关技术高达 6 项，占比 24%，堪称当前兼具潜力价值和讨论热度的前沿技术领域。

行业趋势方面，本期重点关注市场趋势、产品、解决方案动态以及数据安全投融资动态。值得推荐的是，由贵州大数据安全工程研究中心推出的全国首款“数据安全自评估”APP 于 7 月 31 日重磅上线，该 APP 依据“数据安全能力成熟度模型”国家标准，以免费的形式向社会公众开放，能够在评估结束后，通过图表形式，直观展示该企业当前的数据安全能力建设现状，并给出提升建议。投融资方面，受疫情影响，全球经济形势不容乐观，但 2022 年上半年数据安全领域的投融资依旧不断，其中过亿元的融资厂商越来越多，可见数据安全备受资本青睐、细分赛道趋势明显。

安全事件方面，本期主要选取了 2022 年第三季度内泄露数据量较大、攻击手段代表性强、关注度较高的热点事件进行点评，主要类型集中在数据泄露、勒索攻击以及合规挑战方面。其中，比较吸引眼球的是几起因存在数据违规行为而受到行政处罚或诉讼的事件，例如“滴滴事件”、“GDPR 跨境合规事件”等，各企业及组织的网络安全及数据保护合规显然成为了相关机构的重点监管内容。另外还值得关注的是，勒索软件团伙本季度活跃依旧，攻击目标覆盖医疗卫生、电信、能源等多个关键基础设施行业，呈现出定向化、持续化、组织化的趋势。

大咖观点方面，本期收录了知名院士、业界专家、行业大咖的精彩演讲和代表性观点。从学术界、产业界、政府侧、企业侧的不同立场出发，围绕数据流通与数字经济、关基保护、数据要素开发与数据

安全、数据分类分级、数据出境安全管理等方向，共同探讨数据安全领域当下面临的问题及发展趋势、对未来进行前瞻展望并提供可行性建议。

目 录

第一部分 政策形势

第二部分 技术趋势

第三部分 行业趋势

第四部分 安全事件

第五部分 大咖观点

一、政策形势

（一）国家互联网信息办公室公布《数据出境安全评估办法》

关键词：数据出境　安全评估

7月7日，国家互联网信息办公室公布《数据出境安全评估办法》，自2022年9月1日起施行。该办法旨在规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，切实以安全保发展、以发展促安全。办法中规定了评估触发条件、评估内容、具体流程、评估主体等相关要求，对于评估活动不同阶段的重点事项、关注内容进行了明确，并提出了评估结果复评、评估结果有效期、重新申报评估等要求。

（来源：中国网信网）

【点评】：全球化背景下，数据的流动必然无法避免出境情形，但只有安全有序的流动，才能正向赋能数字经济。近年来全球多个国

家、地区先后对数据出境的规则、要求进行探索，我国也历时 5 年，正式出台了针对数据出境的安全评估管理制度，明确了数据出境安全评估的相关要求，针对性提供了可操作、可落实的法律依据，是我国数据出境制度的重要里程碑。

（二）市场监管总局发布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》

关键词：网络安全服务　认证资质

7 月 21 日，市场监管总局公布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》。《实施意见》提出，将确定并适时调整网络安全服务认证目录，组建网络安全服务认证技术委员会，从事网络安全服务认证活动的认证机构应当依法设立，具备从事网络安全服务认证活动的专业能力，并经市场监管总局征求中央网信办、公安部意见后批准取得资质等 9 项意见。

（来源：国家市场监督管理总局）

【点评】：据调查，全球网络安全支出规模中，网络安全服务占比最大，且随着政策形势、技术市场、业务需求等多种因素的发展变化，将持续提升。可见网络安全服务对网络安全的建设推动、行业发展等起着至关重要的作用，此次意见的发布表明监管侧对网络安全服务标准化、规范化监管时代的来临，将推动网络安全服务的专业化水平和服务质量的优化与提升。

（三）《中华人民共和国反电信网络诈骗法》发布

关键词：电信诈骗　个人信息

9 月 2 日，第十三届全国人民代表大会常务委员会第三十六次会议通过《中华人民共和国反电信网络诈骗法》（简称“《反电信网络诈骗法》”），自 2022 年 12 月 1 日起施行。《反电信网络诈骗法》共七章 50 条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任、附则等，坚持以人民为中心，统筹发展和安全，立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑。


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China
RSS订阅
统一搜索
看新闻 找文件 查办事 提意见 查数据 要投诉
工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏
首页 > 工业和信息化部 > 机关司局 > 产业政策与法规司 > 法律
中华人民共和国反电信网络诈骗法
发布时间：2022-09-08 08:35 来源：产业政策与法规司
（2022年9月2日第十三届全国人民代表大会常务委员会第三十六次会议通过）
目 录
第一章 总 则
第二章 电信治理

（来源：中华人民共和国工业和信息化部）

【点评】：近年来，电信网络诈骗案的发生愈发频繁，据报道超过7成的电信网络诈骗与个人信息泄漏或被窃取有关，且该比例呈现持续提升趋势。因此，《反电信网络诈骗法》衔接了《个人信息保护法》相关要求，推动个人信息处理者加强反诈建设，并通过“一案双查”追究相关方责任，力争在源头上杜绝违法“出售、提供个人信息”，防患于未然。

（四）国家网信办发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

关键词：网络安全法 法律责任

9月14日，国家互联网信息办公室发布了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，旨在适应新形势，与《中华人民共和国行政处罚法》、《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》等法律做好衔接协调，完善责任

制度，进一步保障网络安全。本次修改主要涉及四个方面：完善违反网络运行安全一般规定的法律责任制度、是修改关键信息基础设施安全保护的法律责任制度、调整网络信息安全法律责任制度、修改个人信息保护法律责任制度。

（来源：中国网信网）

【点评】：随着全球数字安全攻防态势、政治环境等多方因素的演化，此次《网络安全法》的修订正是时势的需要，是监管侧与时偕行的反应。本次修订主要涉及增加处罚款项、处罚形式或提升处罚力度，积极回应了当下数字安全风险种类不断增加，且影响愈发深刻的形势，强化法律威慑力的同时，以灵活的处罚模式深化落实法律面对不同场景、不同对象的实施效力，为数字经济发展筑牢数字安全坚实基础。

（五）上海通管局启动网络和数据安全检查工作

关键词：数据安全检查　合规性评估　个人信息保护

7 月 7 日，上海市通信管理局发布通知，决定组织开展 2022 年上海市电信和互联网行业网络和数据安全检查工作。检查内容明确了检查企业落实《数据安全法》《电信和互联网企业数据安全合规性评估要点》的要求，以及检查企业按照《个人信息保护法》《电信和互联网用户个人信息保护规定》《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》《关于开展信息通信服务感知提升行动的通知》要求，落实电信和互联网行业个人信息保护和用户权益保护专项治理工作情况。

（来源：上海市通信管理局）

【点评】：自今年年初起，各省市通信管理局陆续启动电信和互联网行业网络和数据安全检查工作，“以查促建、以查促管、以查促防、以查促改”的形式有助于尽早发现松懈点、问题项和隐患处，及时加固相关企业识别与应对数字安全风险的能力，并保持相关角色在意识、技能等方面的警觉性和抗压性。

（六）广东省工业和信息化厅关于印发《广东省企业首席数据官建设指南》

关键词：首席数据官

为建设数据管理高端人才队伍，充分挖掘数据资源价值，促进企业数字化转型，推动广东省数字经济高质量发展，广东省工业和信息化厅于 8 月 24 日印发《广东省企业首席数据官建设指南》，对数据官的建设原则、建设内容、保障措施、等内容进行规范化指导，并对数据官的岗位设置、岗位能力素质要求、岗位职责等事项进行明确。

（来源：广东省工业和信息化厅）

【点评】：近两年，首席数据官制度的概念在国内频繁出现，多个省市先后提出了对首席数据官、数据保护官等政策鼓励，广东省更是先行选取了 6 个省级部门、10 个地级以上市开展首席数据官制度试点。可以预见，针对数据治理、数据安全等方面的人才要求会不断明确，相关责任也将逐步强化，从业人员亟需从工作思维、专业技能等方面完善和提升相关能力水平，应对新形势下数据能力需求。

（七）苏州大数据交易所正式揭牌：数字苏州建设进入新阶段

关键词：数据交易　数据开放

9 月 16 日，苏州大数据交易所正式揭牌，标志着数字苏州建设进入新阶段。苏州大数据交易所以建设全国一流的数据流通交易基础设施为目标，打造基于统一的可信计算能力底座，依托苏州市公共数据开放平台、苏州大数据交易平台两大平台，支持数字金融、数字制造、数字文旅等 N 个应用创新的“1+2+N”运营模式，不断整合公共数据、社会数据、算法算力等多方资源，打造具有苏州特色的数据资源化、资产化、价值化商业模式，推进数字经济与实体经济有机融合。

（来源：苏州市人民政府）

【点评】：自 2015 年我国首家大数据交易所——贵阳大数据交易所挂牌成立至今，国内已先后设立了近 20 个数据交易平台，立足于本地数据开放共享需求，根据地方特色建立合适的运营模式。在各方的探索研究和实践验证下，相信能推动形成成熟的数据交易商业模

式，促进法律法规、标准规范、配套制度等顶层政策的明确，促进数据高效且合规的流通、全面且深入的挖掘和释放数据价值。

（八）欧洲议会通过了《数字服务法》和《数字市场法》

关键词：数字服务　数字市场　看门人

7 月 5 日，欧洲议会通过了《数字服务法》和《数字市场法》。这意味着欧美间的数字博弈正式迈入新阶段，而把控市场的美国科技巨头们即将迎来新的监管挑战。《数字服务法》将引入一些重要的保护措施，尽管它没有全面禁止广告定向推送，但该法将禁止任何针对未成年人的定向广告等。在打击非法内容方面，该法案强调各大在线平台需要承担一定的社会义务；《数字市场法》则是要求被称为“看门人”的大型平台公司不能滥用市场支配地位打压其他竞争企业，不能未经用户许可强行推送广告或安装应用软件。

EUROPEAN
COMMISSION

Brussels, 15.12.2020
COM(2020) 842 final

2020/0374 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on contestable and fair markets in the digital sector (Digital Markets Act)

(Text with EEA relevance)

{SEC(2020) 437 final} - {SWD(2020) 363 final} - {SWD(2020) 364 final}

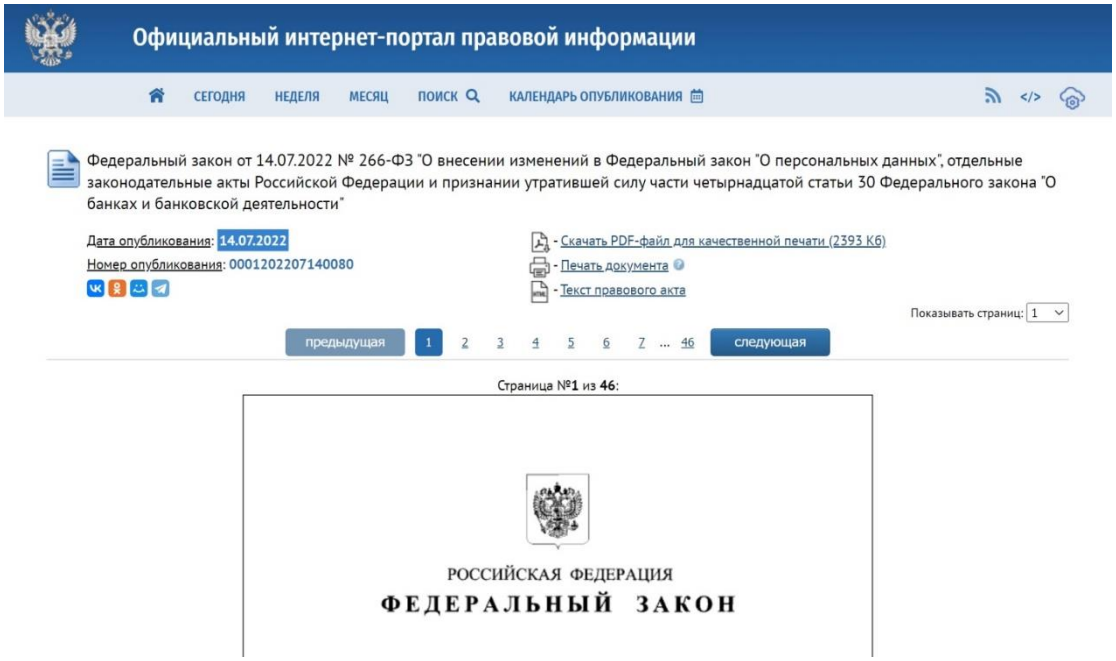
（来源：中国服务贸易指南网）

【点评】：内容偏好、操作行为、运动轨迹等个人信息的分析和应用，有助于推动为用户提供更具针对性和定制化的服务，降低用户决策成本。但大量个人信息的收集加剧了数据被滥用、泄露的风险，也易导致算法歧视、信息茧房等反向效应。我国通过去年颁布的《个人信息保护法》赋予了用户拒绝个性化推荐的权利，美国于今年 8 月就探索打击有害的商业监控和松懈的数据安全规则向社会公开征集意见。可见，各互联网平台致力于“千人千面”的定制化服务时，务必重视其合规性并采取有效措施保障用户数据安全。

（九）俄罗斯修订《联邦个人数据法》，强化运营商数据安全责任

关键词：用户信息泄露　跨境数据传输　运营商

8 月 11 日，俄罗斯联邦通信、信息技术和大众传媒监督局（Roskomnadzor）领导的公共委员会举行了例行会议，会上讨论了最



近通过的《联邦个人数据法》的变化以及在数字服务发展的背景下保护其主体的权利，部分修正案将于将于 9 月 1 日生效。此次修订将加强对用户的保护以及数据运营商的泄密责任，包括运营商将被要求将用户信息泄露事件通知 Roskomnadzor、运营商必须在开始跨境数据传输之前通知 Roskomnadzor 等。

（来源：“安全内参”公众号）

【点评】：数据作为重要战略资源和生产要素，对经济发展、社会稳定、国家安全等方面的价值越来越显著，各国都加紧了对数据的法律法规建设，保障本国数据有序利用、降低数据泄露影响，同时加强数据跨境流动的管控，均已成为主要国家的共识。据报道，全球已有近 150 个要求数据存储在特定国家的法律法规和政府政策，进而更好的争取数据资源优势以推动自身数字经济发展。

（十）拜登签署新行政令：涉及芯片、AI、量子计算等领域

关键词：外国投资　审查　敏感数据

9 月 15 日，美国总统拜登签署一项行政命令，要求美国外国投资委员会（CFIUS）确保美国对不断变化的国家安全风险进行强有力的审查。其中两个法定因素包括：特定交易可能对事关美国国家安全的供应链产生影响，包括在国防产业之外的交易；特定交易会影响到美国国家安全领域的技术领先地位。另外三个因素包括：特定交易可

能影响事关美国国家安全的行业投资趋势；威胁事关国家安全的网络安全风险；事关美国人敏感数据的相关风险。

（来源：“数据法盟”公众号）

【点评】：近年来，随着经济全球化进程的受阻，世界主要国家的外资安全审查制度呈收紧趋势，通过扩大审查范围、增加审查程序、强化审查力度等形式，向“投资保护主义”倾向发展。数据的关键性使其不仅成为跨境流动中重要监管对象，现在也成为外资安全审查的重要因素，势必会制约数据价值的充分挖掘与释放。

二、技术趋势

（一）NIST发布新算法应对量子攻击，可支持下一代加密标准

关键词：量子攻击　加密算法　NIST

7月5日，美国国家标准与技术研究所（NIST）正式发布四种新的加密算法，用于保护联邦政府计算机和应用系统应对新型量子计算的网络攻击。据了解，这四种新加密算法包括一种用于通用加密用途

的算法：CRYSTALS-Kyber，以及另外三种用于数字签名和身份验证的算法：CRYSTALS-Dilithium、Falcon 和 Sphincs+，它们将在 2024 年之前支持 NIST 未来的加密标准。

NIST 算法项目负责人 Dustin Moody 表示：“我的项目团队一直在评估审核新的加密算法，安全性是我们进行评价的第一标准。所有进入到评审阶段的算法都达到了这一基准标准，最后的取舍在于速度和易用性等方面细微但又可衡量的差异，比如密钥大小、签名大小、实施时需要多少内存、参照衡量基准，以及在各平台上实施应用的便捷性等。”

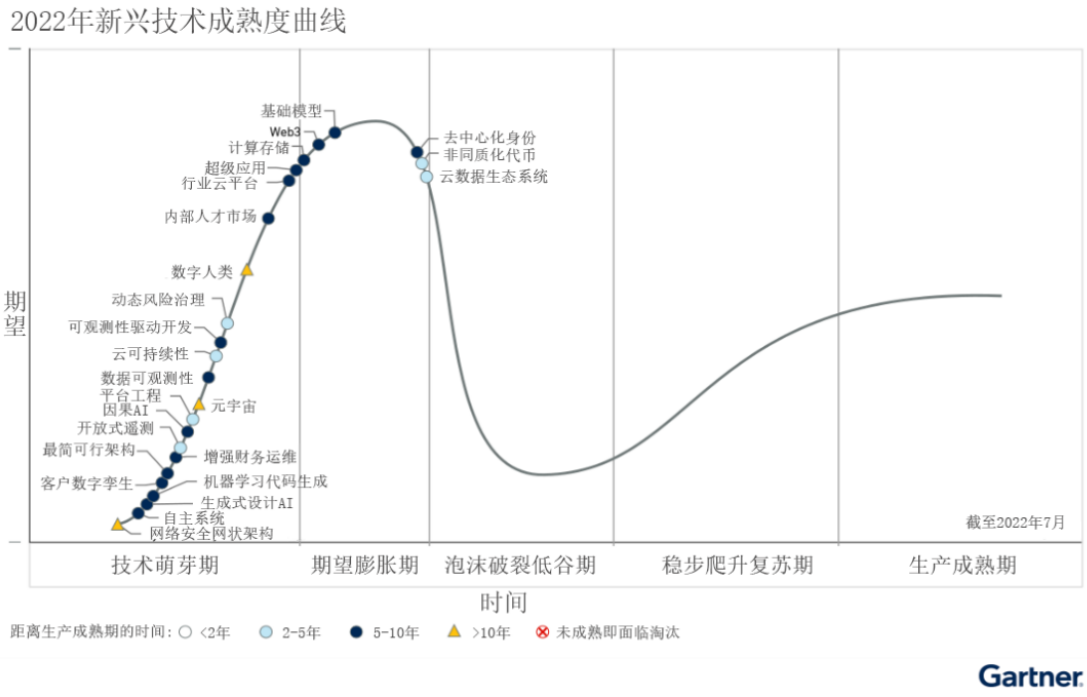
值得注意的是，本次推出的四种算法中，有三种算法 CRYSTALS-Kyber、Crystals-Dilithium 和 Falcon 是基于格（lattice）的算法。NIST 预计在后续应用中，大多数企业组织会使用 Crystals-Dilithium，原因是它性能良好、文档完备，而且更易于实施。不过，尽管 Falcon 算法需要相对复杂的实施过程，也无法适用于所有设备上，但它更小巧，会在使用较小数字签名的应用场合发挥作用。

（来源：“安全内参”公众号）

（二）Gartner发布2022年新兴技术成熟度曲线

关键词：隐私计算

Gartner 2022 年新兴技术成熟度曲线列出了 25 项值得关注的新兴技术，这些技术正在推动沉浸式体验的发展和扩展、加速人工智能（AI）自动化并优化技术人员交付。新兴技术趋势的三个主题：**沉浸式体验不断发展和扩展、AI 自动化提速、技术人员交付得到优化。**



今年的前沿热门技术共25项，其中隐私计算相关技术高达6项，占比24%，绝对称得上当前兼具潜力价值和讨论热度的前沿技术领域。25 项新兴技术中与隐私计算相关的有：**去中心化身份、元宇宙、非同质化代币、Web3、网络安全网格架构、数据可观察性。**

去中心化身份：允许实体（通常是用户）利用区块链或其他分布式账本技术以及数字钱包来控制自己的数字身份。去中心化身份的过程涉及到身份匿名、加密存储等，这些都是隐私计算的基础技术架构。有了去中心化身份，用户才能在诸如元宇宙、Web3 体系中构建信任机制。

非同质化代币：是一种独特的基于区块链的可编程数字项目，可公开证明数字资产（如数字艺术或音乐）或标记化的物理资产（如房屋，汽车或文档）的所有权。这是和去中心化身份对应的“去中心化资产”，资产管理不再由统一的权威机构控制，而是交给区块链等信任机制，同时在资产确权、资产交易中保护用户隐私。

元宇宙：是一个集体虚拟 3D 共享空间，由虚拟增强的物理和数字现实的融合创建。元宇宙具备持久性，提供增强的沉浸式体验。元宇宙的核心在于数字映射，如何将现实场景数字化、虚拟化，这涉及到隐私保护交易、隐私保护应用、隐私保护建模、隐私计算网络、隐私边缘计算等许多隐私计算相关技术体系。

Web3：是一个新的技术栈，用于开发分布式的 Web 应用程序，使用户能够控制自己的身份和数据。数据的归属和使用都属于数据生产者用户本身，有效地缓解了隐私泄露等数据安全问题，隐私计算在其中发挥了举足轻重的作用，如何在保障数据安全的同时充分发挥数据的价值，这是 Web3 依靠隐私计算的关键应用。

网络安全网格架构：是一种新兴的方法用来构建可组合的分布式安全控制，从而提高整体安全有效性。整个网络体系的安全是个庞大的课题，隐私计算在其中的角色可以理解为技术骨架，从网络节点的组建、网络通信的加密、网络数据的安全存储，都需要隐私计算保驾护航。

数据可观察性：是通过持续监控、跟踪、警报、分析和故障排除处理来了解组织数据环境、数据管道和数据基础架构运行状况的能力。数据的全生命周期管理，这恰是隐私计算目前主流的定义，数据从产生、存储、共享、利用、销毁，到潜在的泄露、结构破坏风险，都需要数据组织的管控，隐私计算是强有力的技术工具。

数据是当下全球范围内各个组织机构的关键生产要素，不难发现，许多新兴技术都是在对数据进行创新利用和管理，或者构建一个数据安全的保障机制。随着相关法律法规的持续跟进，越来越多的关键技术注入，隐私计算技术体系将愈发完善，成为数据利用、数据安全、数据治理的中流砥柱。

（来源：“开放隐私计算”公众号）

（三）单核CPU破解后量子加密候选算法只需一小时

关键词：抗量子密码算法 密钥恢复

鲁汶大学研究人员提出一种针对 SIDH 协议的高效密钥恢复攻击方法，使用普通单核 CPU，一小时即可攻破 SIKE 抗量子密码算法。

密钥封装机制是一种使用非对称密码学技术安全交换对称密钥的协议。SIKE (Supersingular Isogeny Key Encapsulation，超奇异同源密钥封装)是一种广泛应用的密钥封装机制，2022 年 7 月入选 NIST 后量子密码学算法第 4 轮。有多个工业实现和部署实验。相比对称密钥算法，目前使用的密钥封装易被量子计算机攻击。使用复杂数学构建的超奇异同源图被认为可以对抗量子计算机的攻击。

SIKE 协议的正确性和安全性依赖于 SIDH（Supersingular Isogeny Diffie-Hellman，超奇异同源 Diffie-Hellman），即计算超奇异椭圆曲线间同源的困难性问题。SIDH 的安全性与寻找两条具有相同点数的超奇异椭圆曲线之间的同源映射问题密切相关。

研究人员对攻击算法进行了实现——Magma，Magma 成功破解了 SIKEp434。Magma 分别在 4 分钟和 6 分钟内成功解决了微软 SIKE 挑战赛$IKEp182 和$IKEp217 问题。研究人员将 Magma 部署在 Intel Xeon CPU E5-2630v2（2.60GHz）单核 CPU 上，运行约 62 分钟即成功恢复 SIKEp434 参数（满足 NIST 后量子安全等级 level 1）。对于具有更高安全级别的 SIKEp503 (安全等级 level 2)、SIKEp610 (安全等级 level 3)和 SIKEp751 (安全等级 level 5)，分别在 2 小时 19 分钟、8 小时 15 分钟和 21 小时 37 分钟内恢复密钥。

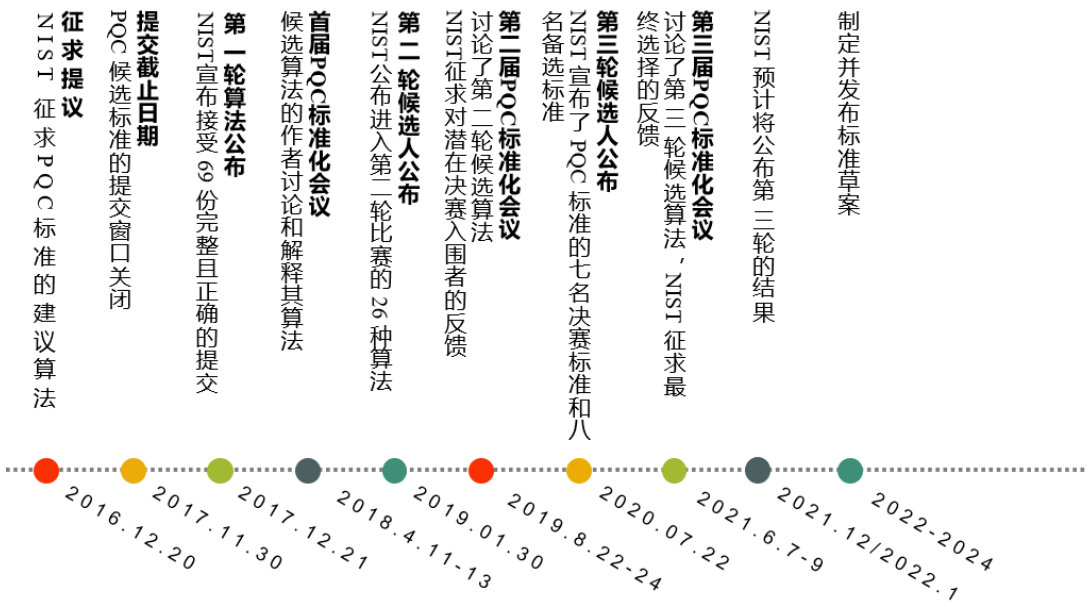
（来源：安全内参）

（四）2022年密码学的全球新兴趋势

关键词：后量子密码学

经济时代，组织依靠公钥基础设施 (PKI)和加密技术在其企业 IT 基础设施和互联产品解决方案中建立所需的数字信任。致力于为汽车、金融、医疗保健和零售等垂直领域提供自动化数字安全管理的 Keyfactor 发布的一份产业报告指出，**2022 年密码学的新兴趋势包括：PKI 的治理兴起、后量子密码学（PQC）研究更为活跃、eIDAS 得到扩展、供应链安全的需求凸显、数字机器身份成为制造业的未来、加密敏捷成为主流。**上述六大趋势的预测有助于分析和研判对公司业务的影响和加密需求的变化。

量子计算对经典的非对称加密算法构成了重大威胁。为了应对这一威胁，各国持续关注并推进对后量子加密（PQC）算法的研究开发。在此方面，美国 NIST 一直在进行为期多年的公开竞赛，以评估各种 PQC 算法，并选择确定将被认可为 PQC 标准的算法。NIST 举办了为期五年的竞赛，旨在为未来的 PQC 标准选择候选算法。



这意味着从 2022 年开始，相关的标准草案将陆续出台，最终标准预计将于 2024 年出台。IETF 和 NIST 的官方标准制定发布，将标志着 PQC 时代的到来。新的标准将为针对广泛的政府和工业部门的解决方案所应涵盖的内容提供合理预期。

（来源：安全内参）

（五）Gartner发布当前至2024年的五大隐私趋势

关键词：Gartner 隐私增强计算技术

频发的安全事件对数字经济发展带来巨大挑战，全行业从危机管理现实需求出发，正促进灾备体系向全行业广泛延伸应用。威胁加剧、灾备云化、云化应用是灾备向全行业延伸应用的关键。

根据 Gartner 的研究，随着全球隐私法规数量的不断增加，企业机构应关注五项重大隐私趋势，以应对保护个人数据和遵守监管要求

方面的挑战。五大隐私趋势分别是：**数据本地化、隐私增强计算技术、AI 治理、集中式隐私用户体验和远程模式进化为“万物皆混合”**。

Gartner 研究副总裁 Nader Henein 表示：“根据 Gartner 的预测，**到 2024 年末，全球 75%人口的个人数据将得到现代隐私法规的保护**。这一监管方面的进步已成为推动企业机构加强隐私保护的主要动力。由于多数企业机构尚未形成专门的隐私保护实践，隐私保护责任落到了技术人员身上，更确切地说，落到了首席信息安全官所领导的安全团队身上。”

未来两年，几十个司法管辖区将陆续实施隐私法规，因此许多企业机构认为有必要马上启动隐私工作计划。**根据 Gartner 的预测，到 2024 年，大型企业机构的年均隐私预算将超过 250 万美元**。

（来源：“开放隐私计算”公众号）

（六）《2022十大风控技术趋势指南》重磅发布，隐私计算在列

关键词：隐私计算

近日，在“2022 IDC 中国数字金融论坛”上，国际权威咨询机构 IDC 联合蚂蚁集团正式发布了《十大风控技术趋势指南》白皮书。这是风控行业技术创新的一次风向标，也意味着和黑灰产对抗中技术升级迫在眉睫。白皮书指出多方风控主要由区块链及隐私计算技术支撑，比如可信执行环境（TEE），多方安全计算和联邦学习，能使得不同的机构能够在数据隐私得到极好保护的前提下进行风险数据共享，甚

至联合建模。因此，为应对连通性风险，各商家、银行和第三方支付机构之间的“互联互通”十分必要，同时，还须保证这种“互联互通”的安全性。

（来源：“开放隐私计算”公众号）

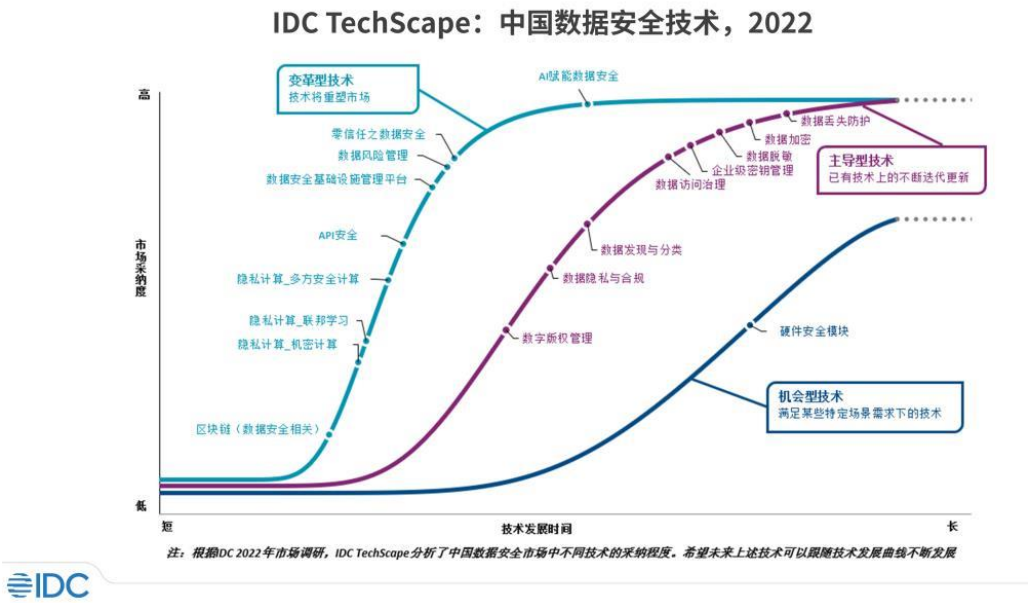
（七）《IDC TechScape：中国数据安全发展路线图，2022》首发

关键词：IDC　数据安全

2022 CSO 全球网络安全峰会于 8 月 31 日在上海召开。IDC 在会上首次发布了《IDC Tachyscope:中国数据安全发展路线图，2022》，通过对中国数据安全市场的系统评估和分析，选取了 18 项新兴且重要的数据安全技术进行详细分析，并针对每项技术给出了三家推荐厂商，以期为最终用户的数据安全体系建设和产品选择提供技术参考。

IDC 分析师观点表示，未来，数据安全市场将在国家政策和市场需求的共同驱动下保持快速发展态势，并呈现出数据安全合规变成刚需，数据安全领域多技术融合，新兴科技赋能数据安全和聚焦场景应用等市场和技术趋势。面向合规、面向需求，以解决数据全生命周期安全为核心，帮助用户构建全方位数据安全治理体系将成为大趋势，各项数据安全和密码技术将在治理体系中作为重点能力模块帮助用

户构建能力生态，最终赋能用户实现数据安全治理目标。

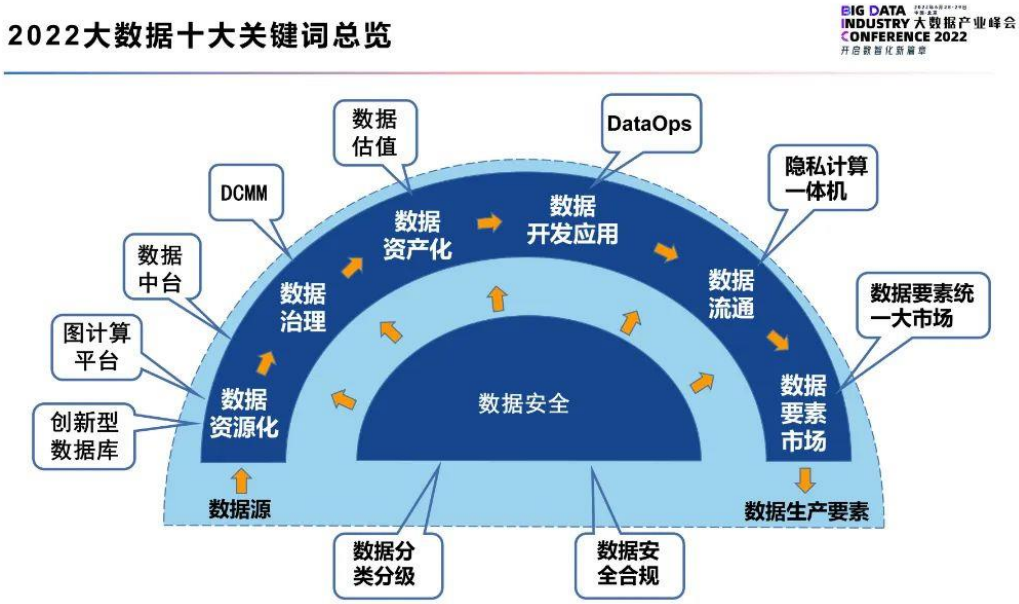


（来源：潇湘晨报）

（八）信通院发布2022年大数据十大关键词

关键词：大数据　十大关键词

2022 大数据产业峰会，信通院基于长期对于产业的研究观察，以及与一线专家的研讨交流发布了《2022 大数据十大关键词》。



如图所示，本年度十大关键词涉及数据从计算机语言到成为生产要素的全生命周期，包括（1）【数据资源化】，即数据从计算机语言到成为可被人类识别的信息（2）【数据治理】，即将散乱的、庞杂的数据进行归类、整理、管理（3）【数据资产化】，即将数据与货币进行对应挂钩，（4）【数据开发应用】，即加工数据使其为业务赋能，（5）【数据流通】，即完成数据在部门与部门间、机构与机构间进行点对点的合规交换共享，（6）【数据要素市场】，即促进全社会按照统一规范的制度、体系完成数据的合规流通利用，（7）【数据安全】，即保障数据流转的全生命周期符合相关法律法规。

（来源：网易科技）

三、行业趋势

（一）行业动态

1、IDC：2021 年中国大数据平台公有云服务市场规模达 33.7 亿元

关键词：IDC　大数据平台公有云服务

IDC 于近日发布了《中国大数据平台公有云服务市场份额，2021》，报告数据显示，**2021 年中国大数据平台公有云服务市场规模达 33.7 亿元人民币，相比 2020 年实现 53.8%的快速增长**。市场增长驱动力主要来自于电商行业、互联网音视频业务、政府行业政策驱动上云、抗疫公共服务、交通行业、媒体行业，其次来自金融、制造、零售和教育行业。随着数据量明显增长以及厂商对业务实时性要求提高，从数据管理到数据应用，企业对数据分析的重视程度日益提高。

IDC 认为，在大数据领域，公有云服务相比私有化部署方案可以提供更好的扩展性、更低的开发运维门槛，更能够适应今天行业用户对于大数据存储计算的需求。随着数据平台、数据湖、数据仓库的建设，组织的数据可能分散在不同的位置，在选择云服务厂商时需要关注其多云数据管理能力、数据迁移的便捷性、数据存储与使用的安全合规、计算存储资源的整体性价比。

（来源：安全内参）

2、IDC：2021 年中国数字政府大数据管理平台市场规模达 49.6 亿元

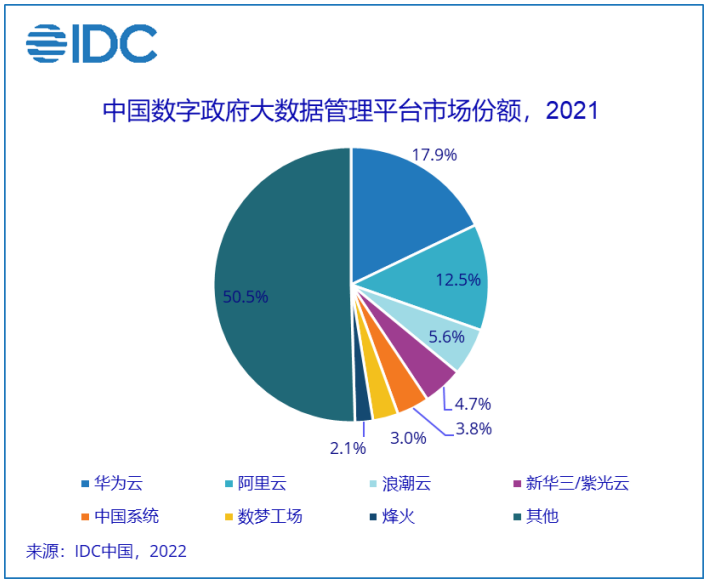
关键词：IDC　大数据管理平台

近日，IDC 发布了《中国数字政府大数据管理平台市场份额，2021》报告，报告显示，2021 年中国数字政府大数据管理平台整体规模达 49.6 亿元人民币，年复合增长率 25.3%，处于稳步增长阶段。

大数据管理平台支撑了城市运行管理指挥中心、城市治理一网统管、政务服务一网通办、城管网格化管理、智慧交通、智慧水务、智慧应急等典型场景。尤其是在疫情期间，健康码的频繁使用对大数据管理平台的稳定性、实时性、大容量提出了更高的要求。随着政务服务质量提升及安平方面的需求，对数据实时性、智能化、安全性要求越来越高。同时，大数据平台技术领域也在持续迭代演讲，如大数据 AI 一体化、跨域协同计算、可信联邦计算、轻量化部署等，这些技术在数据加工、数据共享、业务支撑等不同层面促进政务领域的数据开发利用。

2021 年中国数字政府大数据管理平台整体规模达 49.6 亿元人民币，年复合增长率 25.3%，处于稳步增长阶段。从竞争格局来看，华为云、阿里云和浪潮云在 2021 年中国数字政府大数据管理平台市场排名前三，新华三/紫光云、中国系统、数梦工场和烽火分列第四到第七位。同时，联通数科、软通智慧、星环科技和中兴等企业都是此领域重要的参与者。

建议相关技术提供商在大数据平台建设时覆盖省市县三级，支持大数据平台的集约化建设。



（来源：安全内参）

3、机密计算在国际市场高速发展，以可信执行环境为核心的机密计算成为隐私计算赋能领域重要的解决方案

关键词：机密计算 可信执行环境

大数据时代，数据流通、安全等问题接踵而至，基于 CPU 可信执行环境的机密计算技术可以在保证数据“可用而不可见”的前提下进行数据运算，成为解决数据流通安全问题的热点技术。根据国外著名信息调查机构 Everest Group 最近的一项市场研究表明，**机密计算市场预计将在 5 年内增长到 54 亿美元。**

Everest Group 的市场调研中显示，2021 年，机密计算的可触达市场空间（TAM）为 19-20 亿美元。预计到 2026 年，机密计算市场

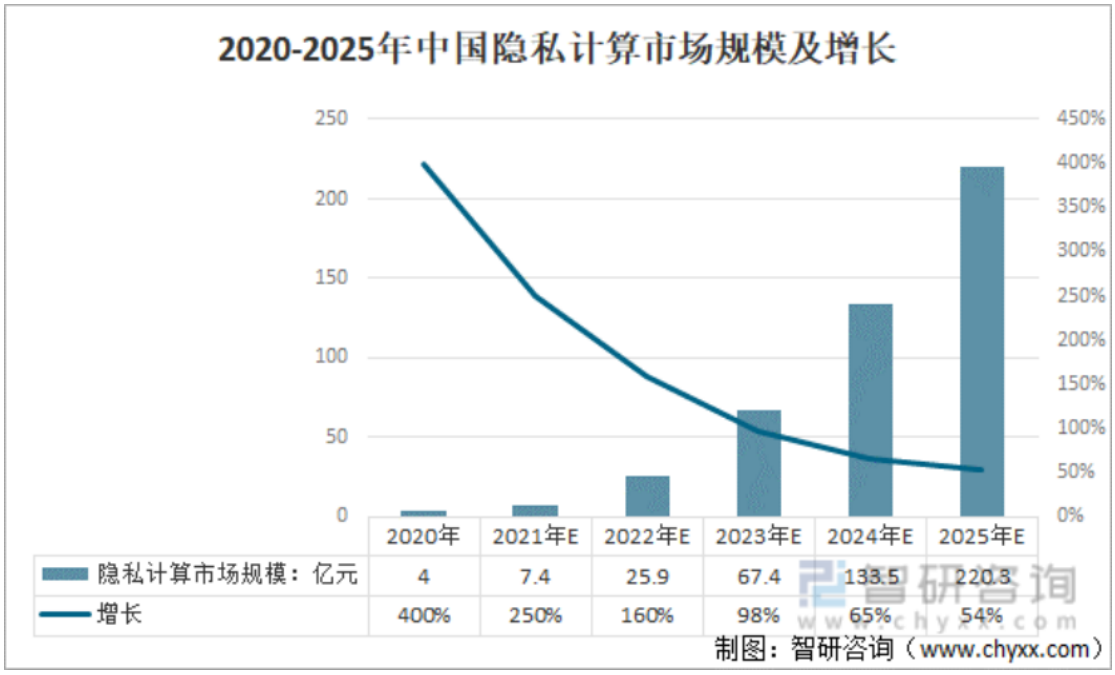
在理想的情况下将以 90-95%的年复合增长率增长，在不理想的情况下至少以 40-45%的年复合增长率增长。其中在 2021 年超过 75%的需求受到银行、金融和医疗保健等受监管行业的推动。

（来源：“隐私计算联盟”公众号）

4、2022 年中国隐私计算市场规模

关键词：隐私计算　市场规模

随着中国大数据产业发展以及隐私计算技术不断实现商业化，隐私计算技术产品蓬勃发展，形成一定优势，市场规模将持续增长。目前数据使用方支出主要为产品及服务费，预计到 2025 年该领域市场将超过 200 亿，2021 年至 2025 年年均复合增长率达 133.4%。



资料来源：甲子光年、智研咨询整理

从中国隐私计算各行业市场规模占比来看，金融领域占 39%；政务领域占 28%；医疗领域占 22%；其他领域占 11%。通过对金融、政务、医疗领域隐私计算市场规模进行测算，2021 年至 2025 年，年均复合增长率均在 130-150%左右，呈现高速增长态势。预计到 2025 年隐私计算金融领域市场规模 116.2 亿元，政务领域市场规模 61.6 亿元，医疗领域市场规模 59.5 亿元。

（来源：“开放隐私计算”公众号）

5、身份访问管理 (IAM) 将迎来爆发式增长

关键词：身份访问管理（IAM）

根据瞻博网络上周发布的一项研究报告，**未来五年，全球在身份和访问管理（IAM）解决方案上的支出将增长 62%**，从今年预计的 160 亿美元增加到 2027 年的 265 亿美元。新增的 IAM 市场将主要基于 SaaS 模式（云 IAM），分析师认为 SaaS 正在迅速成为购买 IAM 解决方案的主要模式——预计到 2027 年，云 IAM 将占据 IAM 市场的绝大部分。

随着 SaaS 模式在 IAM 市场的激增，越来越多的小公司发现 IAM 已经触手可及，研究表明，这一趋势将以滚雪球的方式持续增长。虽然云 IAM 现在仅占市场的 60%，但研究人员预测五年后云 IAM 将占据 IAM 总体市场的 94%。

（来源：安全内参）

6、全国首款“数据安全自评估”APP 重磅上线

关键词：DSMM　数据安全自评估

7 月 31 日，在 ISC2022“护航数字山河 数据安全协同创新”峰会上，贵州大数据安全工程中心和大数据协同安全技术国家工程研究中心联合推出全国首款“数据安全自评估”App，向各行各业免费提供数据安全自评估服务，帮助提升数据安全能力水位。

为贯彻落实国家相关法律法规和标准规范，让企业能够“零成本”了解自身数据安全能力，鼓励大家共同提升数据安全水位。“数据安全自评估”APP 依据“数据安全能力成熟度模型”国家标准，以“免费”的形式向社会公众开放，企业可通过实名注册后，开启“免费”的数据安全自评估，依据企业提供真实的、有效的信息，APP 能够在评估结束后，通过图表形式，直观展示该企业当前的数据安全现状，并给出提升建议。

（来源：“大数据安全工程研究中心”公众号）

7、原语隐私计算服务平台 SaaS 版正式发布

关键词：原语科技　隐私计算平台

7 月 9 日，原语科技正式对外发布 SaaS 版隐私计算服务平台，旨在让企业方便快速使用隐私计算产品。原语科技自主研发的隐私计算平台 Primihub 及管理平台 Primihub-Platform 均已在 GitHub 上开源。

SaaS 版 Primihub 隐私计算服务平台涵盖匿踪查询、隐私求交、联合建模、联合统计、审核授权、数据资源管理等主要应用服务功能。企业既能保障数据安全，又能安全合规地发挥数据最大价值，可以很好地解决业界的数据孤岛难题。

（来源：“原语科技”公众号）

8、隐私浏览器 Brave 推出隐私保护数据收集系统 STAR

关键词：Brav **隐私保护**

7 月 20 日消息，隐私浏览器 Brave 宣布推出隐私保护数据收集系统 STAR，该系统使用 k-anonymity 匿名算法，可在用户贡献数据且共享的情况下保护用户隐私。

STAR 可提供与现有系统相似或更高的隐私，使用现有的加密工具而非加密原语因此可更易理解，部署不需特殊硬件因此降低了成本，可提供小用户群的准确结果。

STAR 系统将在洛杉矶举行的 2022 年 ACM 计算机和通信安全会议上推出，并正在讨论 IETF（国际互联网工程任务组）可能的标准化。

（来源：博链财经）

（二）投融资动态

1、「Wire」获 2400 万欧元 C 轮融资，致力于数据安全领域

关键词：端到端信息加密

欧洲数据安全技术开发商 Wire 完成 2400 万欧元的 C 轮融资，由成长型股权投资公司 Cipio Partners 和 Skype 联合创始人 Janus Friis 名下的基金 Iconical 领投，现有投资者 UVC Partners 和一批回归投资者跟投。Wire 提供一款端到端信息加密 App，目前主要针对企业客户，客户主要为政府、军队等安全级别较高的机构，以及金融和医疗行业等有着严格合规要求的、受到高度监管的企业。但 Wire 同时也向消费者提供免费的软件版本，但主要“聚焦 B2B 使命”，提供了一套广泛的员工协作、合规和用户管理工具，允许客户将加密后的数据存储在本地。

（来源：创业邦）

2、数据安全平台 Flow Security 获 1000 万美元种子轮融资

关键词：Flow Security

Flow Security 是一个数据安全平台，通过持续映射和检测所有与数据相关的风险来发现和保护静态和动态数据，从而改善数据安全状况。Flow Security 宣布完成 1000 万美元种子轮融资。本轮融资由 Amiti 牵头，GFC、Amdocs Ventures 以及 CyberArk 首席执行官 Udi

Mokady 和 Demisto 首席执行官兼联合创始人 Slavik Markovich 等行业领导者参与。

（来源：猎云网）

3、数据安全公司 Fortanix 完成 C 轮融资

关键词：机密计算

近日，数据安全公司 Fortanix 宣布完成 9000 万美元 C 轮融资，由高盛资产管理公司（Goldman Sachs）旗下的成长股权业务领投。Fortanix 由 Ambuj Kumar 和 Anand Kashyap 于 2016 年创立，它提供一种数据优先的方法来帮助各种规模的企业在本地、云端以及介于两者之间的任何地方实现其安全解决方案的现代化。

Fortanix 认为，传统的数据安全模型无法跟上云优先的世界。“我们意识到机密计算不仅仅是一种奇特的技术，一种寻找问题的解决方案，而且是数据保护和安全计算的颠覆性推动者。”随着越来越多的公司依赖公共和混合云服务，云中的数据隐私势在必行。机密计算的主要目标是为用户提供更强大的安全保证，确保他们的云数据是受保护的和机密的，并鼓励他们将更多的敏感数据和计算工作负载转移到公共云服务。

（来源:机器之能）

4、数据安全厂商瑞数信息获 3 亿元 C2 轮融资

关键词：数据风险管理　动态安全

9 月 9 日，瑞数信息宣布完成人民币 3 亿元的 C2 轮融资。本轮融资由钟鼎资本领投、厦门建发新兴投资、三奕资本联合参投，君联资本和德宁资本等老股东超额跟投。跃为资本担任本轮融资独家财务顾问。本轮融资将用于发展现有业务及应用安全产品线，加大数据安全领域的研发投入、人才引进和市场拓展，以及全面加速三大细分安全领域的市场版图。同时，瑞数信息重磅推出了全新数据安全产品——瑞数智能数据安全检测与应急响应系统（Data Detection and Response，简称 River DDR），采用了基于创新 AI 人工智能的快速数据检测与响应技术，以数据安全底座为支撑，提供数据风险管理、实时智能检测、威胁验证和快速恢复等功能。

瑞数信息（River Security）是中国动态安全技术的创新者和 Bots 自动化攻击防护领域的专业厂商。该公司提供涵盖 Web、App 和 API 的全渠道应用安全、业务安全、数据安全、云安全等在内的专业网络安全产品及服务。

（来源：金融界网）

5、 薮猫科技完成 A 轮融资 成立 1 年累计融资上亿元

关键词：创新型企业

数据安全领域的创新型企业薮猫科技正式宣布完成 A 轮融资。本轮融资由源码资本领投，红华繁星网安天使基金及老股东云九资本跟投。至此，加上三一集团、深涧资本等老股东在内，公司已累计获得上亿元融资。本轮融资将用于加大公司在研发创新、人才建设和市场拓展的投入，持续深耕数据安全领域的技术与实践，为企业提供下一代数据安全解决方案。

（来源：IPO 早知道）

6、观源科技完成数千万元 A 轮融资

关键词：密码技术

以密码技术为核心的数据安全产品及解决方案提供商观源（上海）科技有限公司（以下简称“观源科技”）正式宣布完成数千万元的 A 轮融资，此次融资后，观源科技估值达到数亿元。

观源科技是一家数据安全产品及解决方案提供商，专注于密码产品研究、开发、生产和销售，为用户提供相关安全咨询、安全集成和行业应用开发等服务。以观源研究院为技术基石，和上海交通大学密码与计算机安全实验室（LoCCS）联合打造了密码前沿研究基地。

观源科技官网显示，公司始于 2014 年，重组于 2020 年。在主营业务上，观源科技以密码技术作为核心，聚焦商用密码、隐私计算、区块链等技术在芯片安全、移动安全、应用安全、数据安全、云安全、安全管理等方面的应用。在技术积累上，其表示，自身以观源研究院

为技术基石，在密码算法、安全协议、软硬件安全、程序代码分析、移动智能终端安全、加密通信协议分析、嵌入式设备分析、云安全方面具备较深的研究基础。

（来源：36 氪）

7、数据安全、工控安全和隐私计算为近一年半投资 TOP 3 方向

关键词：数据安全　工控安全　隐私计算

2022 年上半年我国网络安全领域投融资受疫情影响相对较小，其中数据安全、工控安全和隐私计算为近一年半投资 TOP 3 方向。根据嘶吼安全产品研究院收集公开数据显示，数据安全方向的融资事件数量 32 起，以创投为主资方，阿里、腾讯、奇安信等均有布局；融资轮次呈现两极化趋势：A 轮前的早期融资占比达 39%，D 轮及以上、战略并购占比达 35%。

（来源：嘶吼 RoarTalk）

四、安全事件

（一）AMD被黑客窃取450GB机密数据原因曝光：用123456当密码

关键词：勒索攻击　数据泄露　弱口令

2022 年 7 月 5 日报道，上月底 RansomHouse 表示，黑客从 AMD 服务器上盗取了 450GB 的数据。RansomHouse 自称是一个专业调解社区，旨在帮助黑客和被勒索的公司之间进行谈判付款。

早在 2022 年 1 月 5 日，AMD 服务器就被黑客组织入侵。RansomHouse 目前公布了被窃取的部分数据作为证据，其中包括一些 AMD 员工的密码和一些系统文件。据 RansomHouse 称，AMD 几乎没有安全系统，许多员工使用简单的密码，如“password”、“123456”或“amd123”。AMD 的安全部门也使用了这些密码，正是因为这个原因黑客才窃取了上述大量数据。

（来源：IT 之家）

【点评】：根据 Verizon 发布的《2022 年数据泄露调查报告》显示，82%的数据泄露都是人为因素导致，包括社会工程学攻击、弱口令、配置错误等。其中，使用弱口令对网络发起攻击以获取访问权限是黑客的常用攻击手段，但讽刺的是，像 AMD 这样的科技巨头也只是使用“password”、“123456”这样一些简单密码来保护其网络，足以见其安全管理薄弱、员工安全意识不足。弱口令安全风险不容忽视，任何企业都应该要求对所有登录进行多因素认证，或者使用复杂的密码，以降低弱口令的危害。

（二）云配置错误暴露了Amazon S3存储桶中的3TB敏感机场数据

关键词：配置错误　亚马逊云存储　数据泄露

2022 年 7 月 7 日，据外媒报道，错误配置的 Amazon S3 存储桶导致 3TB 的机场数据（超过 150 万个文件）可开且无需身份验证的访问，凸显了旅游行业中不安全的云础设施所带来的危险。

Skyhigh Security 发现的泄露信息包括员工个人身份信息（PII）和其他敏感的公司数据，影响哥伦比亚和秘鲁的至少四个机场。PII 的范围从航空公司员工、身份证的照片（如果被恐怖组织或犯罪组织利用可能会造成严重威胁）到有关飞机、燃料管线和 GPS 地图坐标

的信息。报告称，该存储桶（现已安全）包含可追溯到 2018 年的信息。

（来源：DARKReading）

【点评】：因数据库或服务器配置不当，导致企业或组织的大量敏感数据被暴露在互联网上的事件频繁发生。网络安全服务商 McAfee 公司在一份调查报告中发现，近年来，将近 70%泄露的数据（总计 54 亿条）是由于云服务配置错误所导致的。而大多数错误配置是人为操作失误造成的，主要是由于基础设施策略过于复杂或对安全实践了解不足等因素。可以看出，人在数据泄露事件中始终扮演着非常重要的角色。

（三）PFC承认遭勒索软件攻击，191万患者信息被泄露

关键词：勒索攻击　医疗卫生　第三方供应商　数据泄露

2022 年 7 月 14 日报道，PFC（Professional Finance Company,Inc.）是一家总部位于美国科罗拉多州的债务催收公司，其承认过去数月持

续遭到勒索软件攻击。由于该公司服务于数百家美国医院和医疗机构，因此本次勒索攻击可能成为今年美国历史上最大规模的私人和健康信息泄露事件。

PFC 表示本次数据泄漏将影响 650 家医疗提供商，黑客获取了患者名称、家庭住址、尚未偿还的结算金额和其他金融信息。PFC 表示部分数据还涉及患者的出生日期、身份证号码、医疗保险、药物救治等信息。在提交给美国卫生与公众服务部的文件中，PFC 确认本次勒索软件攻击至少影响了 191 万患者。

（来源：cnBeta）

【点评】: 医疗卫生行业关系国计民生，涉及大量个人隐私信息，其数据蕴含着巨大价值，加之在全球新冠疫情背景下，领域信息化、智能化进程加速，导致医疗行业成为勒索病毒、数据泄露的重灾区。值得我们注意的是，本次事件是由第三方供应商造成的数据泄露，因医疗行业中的大多数业务系统及安全运维都依赖于外部供应商进行维护，这导致安全风险不断外延，而太多医院都未能对供应商合作伙伴进行充分的安全风险评估。随着能够接触到敏感数据的供应商和服

务提供商的数量不断增多，外部供应链所引发的安全威胁需要得到足够重视。

（四）因传送居民IP地址等数据到美国，欧委会被诉违反GDPR

关键词：数据跨境　GDPR　个人信息

2022 年 7 月 19 日，据欧洲媒体 EURACTIV 报道，因 IP 地址等个人信息被转移到美国，一位德国公民起诉欧盟委员会违反《通用数据保护条例》（GDPR）。

支持原告方的欧洲数据协会（EuGD）指出，该诉讼涉及欧洲未来会议（Conference of The Future of Europe）网站。该网站为欧盟委员会牵头成立，旨在让欧盟公民参与决定欧盟及其成员国的未来。亚马逊网络服务（Amazon Web Services）托管此网站，这也意味着，用户在此网站进行注册时，IP 地址等个人数据都将被转移到位于美国的亚马逊服务器。

根据 GDPR 规定，在欧盟委员会未作出充分性认定的情况下，控制者或处理者只有在提供了适当的保障措施，并为数据主体提供了可执行的权利和有效的法律救济措施的条件下，才可将个人数据转移到第三国。

（来源：安全内参）

【点评】："充分性认定"是欧盟核心的个人数据出境管控制度，由欧盟委员会负责对欧盟以外国家或地区的数据保护立法实施、执法能力、监管机构设置和国际条约等因素进行综合评估，最终确定数据自由流动的"白名单"国家。这一机制促使其他国家按照 GDPR 的要求进行数据保护，以便本国企业能够与欧盟企业正常进行数据流动，进而有助于欧盟引领全球的数据合作。因此，了解 GDPR 下的数据跨境转移机制对于跨国企业而言尤为重要。

（五）国家网信办对滴滴作出网络安全审查相关行政处罚

关键词：网络安全审查　关键信息基础设施

根据网络安全审查结论及发现的问题和线索，国家互联网信息办公室依法对滴滴全球股份有限公司涉嫌违法行为进行立案调查。经查实，滴滴全球股份有限公司违反《网络安全法》《数据安全法》《个人信息保护法》的违法违规行为事实清楚、证据确凿、情节严重、性质恶劣。

7 月 21 日，国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对滴滴全球股份有限公司处人民币 80.26 亿元罚款，对滴滴全球股份有限公司董事长兼 CEO 程维、总裁柳青各处人民币 100 万元罚款。

（来源：网信中国）

【点评】：从滴滴事件可以看出，对于存在严重影响国家安全的数据处理活动的行为，国家绝不会坐视不管，中央网信办这一举动也是在告诫中国的互联网企业要把合规当做运营发展的前提。滴滴事件可谓是我国网络安全、数据安全领域的标志性案例，也给企业敲醒了警钟，强监管时代已经来临！

（六）广东首例！广州一公司未履行数据安全保护义务被警方处罚

关键词：数据安全法　数据安全保护　个人信息

2022 年 7 月 26 日，广州警方公布了广东省公安机关**首例适用《中华人民共和国数据安全法》的案件**：广州一公司未履行数据安全保护义务被警方处罚 5 万元。

都市新闻 11

广州警方全链条打击整治网络突出犯罪 破案160余起

一公司未履行数据安全保护义务，罚！

“内鬼”偷卖快递单信息，包裹给境外诈骗分子

存学员信息的“驾培平台”存严重数据安全隐患，罚5万元！

广州警方检查发现，某公司开发的“驾培平台”存储了驾校培训学员的姓名、身份证号、手机号、个人照片等信息 1070 万余条，但该公司**没有建立数据安全管理制度和操作规程**，对于日常经营活动采集到的驾校学员个人信息**未采取去标识化和加密措施**，系统存在未授权访问漏洞等严重数据安全隐患。系统平台一旦被不法分子突破窃取，将导致大量驾校学员个人信息泄露，给广大人民群众个人利益造成重大影响。

（来源：广州日报）

【点评】：该公司因未履行数据安全保护义务，成为了广东首例适用于《数据安全法》的执法案件，这也意味着不少信息技术企业将需进一步重视安全问题。自《数据安全法》2021 年 9 月 1 日实施以来，数据安全已步入法治化轨道，未来企业的数据安全防护将逐步常

态化，企业作为数据处理者，需要在平衡业务发展的前提下，保障数据合法合规应用。

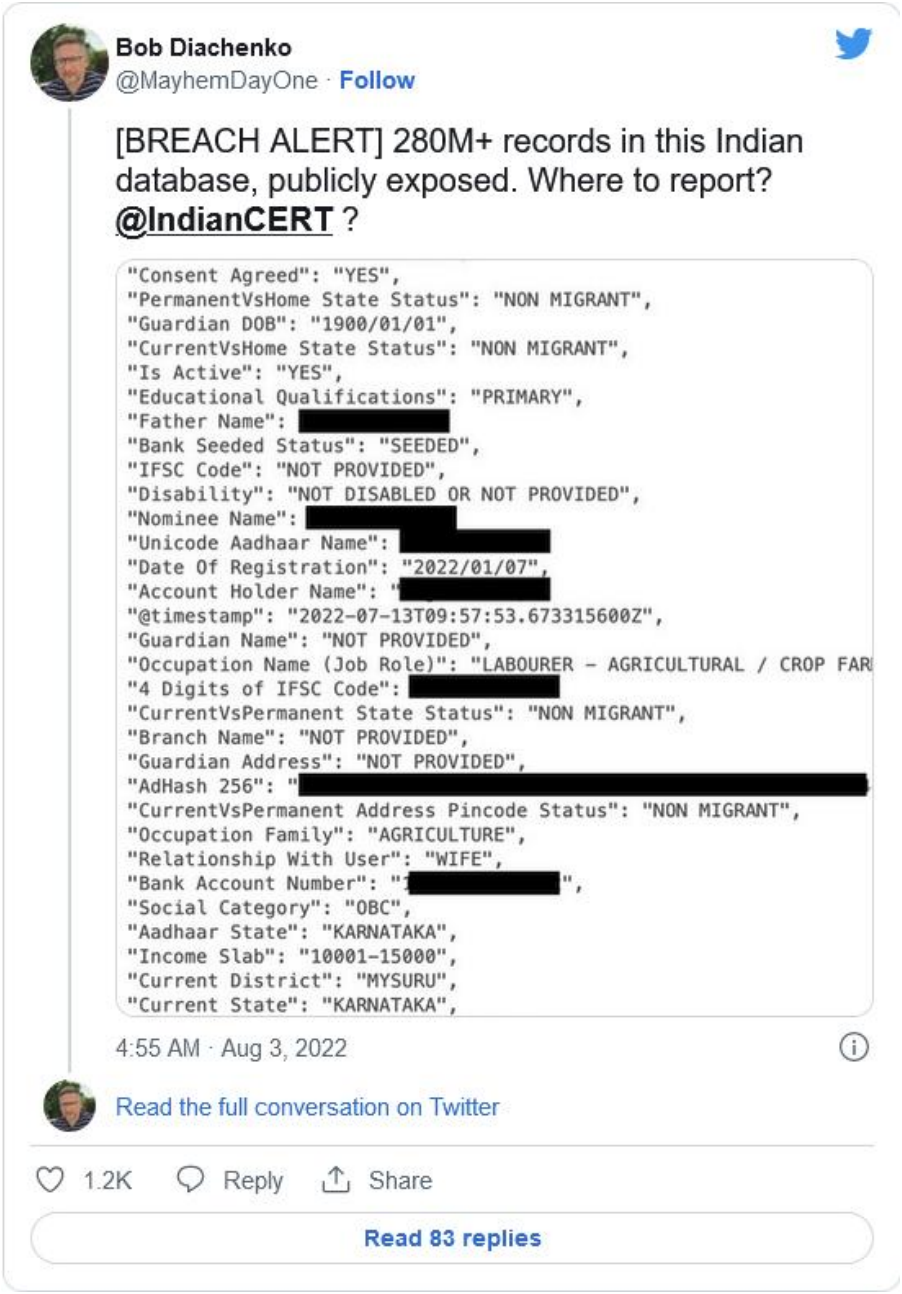
（七）2.88亿条印度养老基金持有人的身份数据被暴露在互联网

关键词：数据库暴露　个人信息　数据泄露

2022 年 8 月 3 日报道，一个包含印度养老基金持有人全名、银行账户号码等信息的巨大数据缓存已在网上浮出水面。安全研究员 Bob Diachenko 发现两个独立的 IP 地址存储了超过 2.88 亿条记录——其中一个 IP 地址下有约 2.8 亿条记录，约 840 万条是第二个 IP 地址的一部分。该研究人员说，这两个 IP 地址都公开向互联网暴露数据，但没有密码保护。

这些记录是名为“UAN”的集群指数的一部分，这显然是指该国国有雇员公积金组织（EPFO）分配给养老基金持有人的通用账户号码。Diachenko 表示：“据我所知，数据库中的信息可能被用来拼凑出一个印度公民的完整档案，使他们成为网络钓鱼或诈骗攻击的目标。”

每条记录都包括详细的个人信息，包括他们的婚姻状况、性别和出生日期。还有一些细节主要与他们的养老基金账户有关，包括 UAN、银行账户号码和就业状况。除了泄露持有养老基金账户的个人身份信息（PII）外，这些记录还暴露了其办理人的详细信息。



（来源：cnBeta）

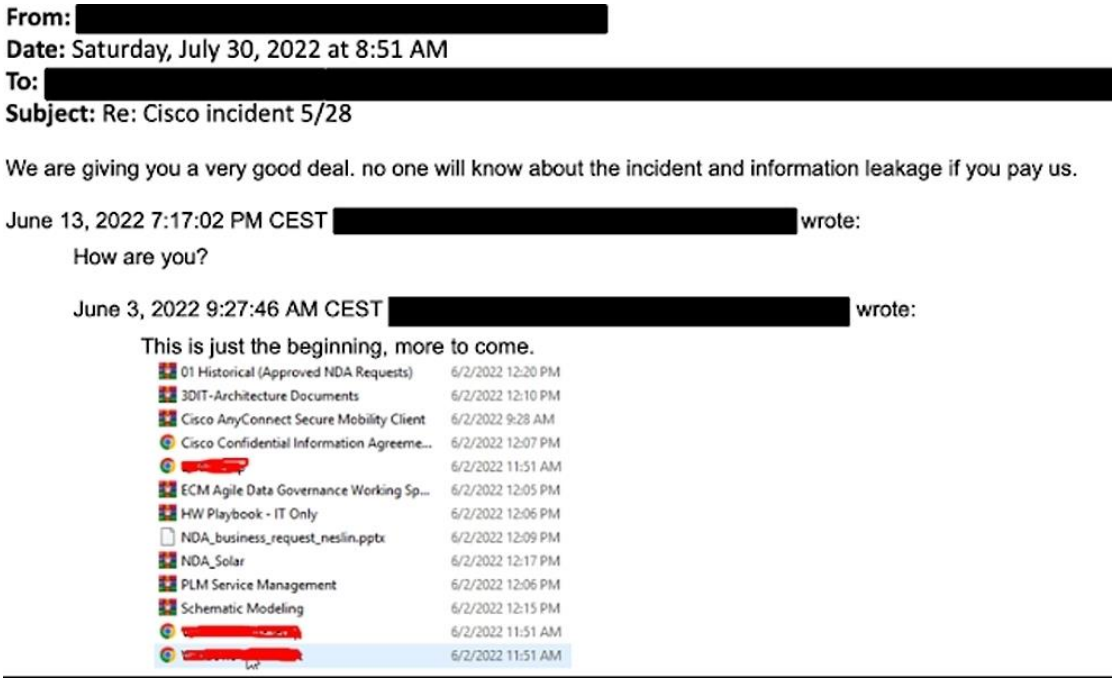
【点评】：不受保护的数据库存储相当于是将数据裸奔在互联网上，是最危险的安全威胁。此次印度养老基金持有人的身份数据因无密码保护而导致 2.88 亿条数据被泄露，影响重大。事实上，类似事件众多，因未加密数据或安全措施不当引起的数据泄露事件在如今依旧

层出不穷，强烈呼吁数据持有方注重数据的加密存储，以防出现数据安全问题。

（八）思科证实遭阎罗王勒索软件组织入侵，2.8GB数据泄露

关键词：勒索攻击　凭证窃取　数据泄露

思科公司于 2022 年 8 月 10 日证实，“阎罗王”（音译，原名 Yanluowang）勒索软件团伙在今年 5 月下旬入侵了其企业网络，攻击者还试图公布被盗文件以要挟索取赎金。



思科声称，攻击者窃取到的只是与受感染员工账户关联的 Box 文件夹中的非敏感数据。据披露，攻击者窃取了一名员工的谷歌账号，通过浏览器同步的凭证获得了思科内网 VPN 账号，利用多因素身份验证（MFA）疲劳攻击和一系列复杂语音钓鱼电话获得了该员工的二次验证码，从而进入内网实施窃密。

恶意黑客声称窃取到 2.75GB 数据，约 3100 个文件，其中不少文件为保密协议、数据转储和工程图纸。

（来源：安全内参）

【点评】：MFA 被认为是一种能有效降低账户失窃风险的身份验证方法，但攻击者开始采用一种名为 MFA 疲劳攻击的方法来绕过 MFA。所谓 MFA 疲劳攻击，指的是攻击者向用户无休止地发送多因素身份验证请求，利用“疲劳轰炸”摧垮目标的安全意识，直至用户被诱骗确认其中一个 MFA 授权通知。在社会工程学攻击如此泛滥的今天，为更好地应对勒索攻击，大中小企业都应加强安全教育培训并引入更多的策略对接入设备进行多维度检测。不能因为低级安全问题就放松警惕，很可能这是某些大规模攻击的开始。

（九）微软员工在GitHub上意外泄露内部敏感登录凭据

关键词：内部威胁　凭证泄露

2022 年 8 月 18 日报道，微软的员工已暴露了公司在线基础设施的敏感登录凭据。该漏洞首先由网络安全研究公司 SpiderSilk 报告，随后由微软证实。文章称，暴露的数据来自 GitHub 上的员工。

SpiderSilk 首席安全官 Mossab Hussein 表示，源代码和凭证泄露导致的事故变得越来越多，提前识别越来越困难。他说：“我们继续观察到意外的源代码和凭证泄露是公司攻击面的一部分，并且越来越难以及时准确地识别出来。这对当今大多数公司来说都是非常具有挑战性的问题。”

据获悉，Azure 是微软云计算机服务，类似于亚马逊 AWS 服务。泄露的凭据与微软官方 tenant ID 有关。tenant ID 是链接到一组特定 Azure 用户的唯一标识符。此次泄漏并未访问任何敏感数据，该公司已采取更安全措施来防止凭证共享。

（来源：IT 之家）

【点评】：登录凭证泄露是最常见的数据安全漏洞之一，据报告显示，80%的安全漏洞与泄露的凭证有关。凭证一旦泄露，就有可能为攻击者提供进入公司内部系统的途径，是一项严重的安全威胁。而在今年 3 月份，就有黑客在网络攻击中获得了 Azure DevOps 账户的访问权，然后窃取了约 40GB 的微软源代码，其中包括 Bing 和微软

的 Cortana 助手的相关代码。企业可使用无密码登录服务或多重身份验证等技术尽可能降低该类事件发生的频率。

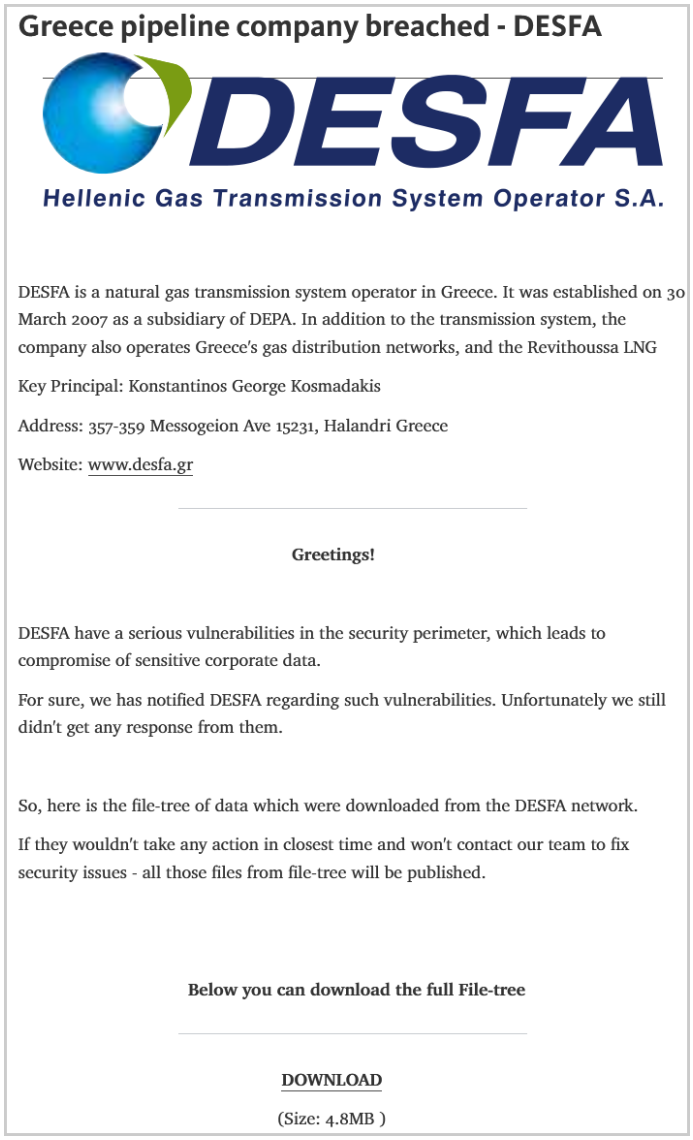
（十）希腊最大天然气运营商遭勒索软件攻击，多项在线服务被迫中断

关键词：勒索攻击　关键基础设施　电力能源　数据泄露

2022 年 8 月 22 日消息，欧洲国家希腊最大的天然气分销商 DESFA 在 8 月 20 日证实，由于遭受网络攻击，该公司出现了一定程度的数据泄露与 IT 系统中断。

在向当地新闻媒体发布的公开声明中，DESFA 称有黑客试图渗透其网络，但因为 IT 团队快速反应而被阻断。然而，对方仍在有限范围内实施了入侵，导致部分文件和数据被访问并可能“外泄”，DESFA 为此**停用了多项在线服务**，希望保护客户数据。而且随着专家们努力进行恢复，各项服务已经逐渐恢复运行。

Ragnar Locker 勒索软件团伙在窃取数据后确认了此次攻击。该恶意黑客团伙还在其数据泄露与勒索门户上发布了所谓被盗数据清单，展示了一小部分似乎不涉及机密信息的被盗文件。如果受害组织不满足赎金要求，该恶意黑客团伙威胁将发布整个文件树内对应的所有文件。



（来源：安全内参）

【点评】：Ragnar Locker 勒索软件于 2019 年首次被发现，并在近两年间频繁攻击全球知名组织，其攻击手法具有高度针对性。勒索攻击引起的数据泄露已成为近年来数据安全事件发生的主要原因之一。如今，全球越来越多的勒索软件组织将攻击目标转向工业、能源、医疗等重要行业的运营者以索取高额赎金，可见，关键信息基础设施安全保护刻不容缓。

五、大咖观点

（一）姚期智：只有数据要素流通起来才能产生大规模的经济价值

世界著名计算机学家、2000 年图灵奖得主、中国科学院院士 姚期智

“数据正在成为数字经济的关键生产要素，充分释放数据要素价值，迫切需要加快推进数据要素市场化建设。”图灵奖获得者、中科院院士、清华大学交叉信息研究院院长姚期智近日接受记者专访时表示，数字经济的发展需要核心技术为基础，应该进一步增加数据交易类技术、数据流通审计技术、数据建模与模型治理等底层技术的投入，并以这些底层技术“新基建”为引领，加快实现数据要素市场化配置、合理分配数据要素收益等。

在姚期智看来，数据产权、流通交易、收益分配、安全治理等都与数据要素市场化建设密切相关，需要四大类关键技术的支撑。

第一，数据交易类技术，包括高效实现数据撮合、数据价值分配的技术，以及记录数据交易过程的技术。

第二，数据流通过程中的安全审计、合规审计类技术。

第三，数据加工分析的技术，包括辅助数据科学家建模，或自动化建模的技术。

第四，数据模型治理的技术。

（来源：“开放隐私计算”公众号）

（二）邬贺铨：数据要素的开发与利用离不开数据安全

中国工程院院士 邬贺铨

在 2022 北京网络安全大会上，中国工程院院士邬贺铨详细介绍了数据要素的九大基本特征，并阐述了这九大特征与网络安全之间的内在关联。

第一大特征是**数据的可见性**。通常情况下，安全检测会使用数据可视化来发现异常，大量政企机构希望将云化的可视化工具下载到本地终端进行部署，在增加数据可见性的同时，确保数据的安全性。

第二大特征是**数据的易理解性**。邬贺铨表示，为了让计算机能更好的理解数据，工程师们会对数据进行前期的预处理，目前标注依然需要人工处理，甚至需要外包、众包的参与，这就带来了极大的用户隐私泄漏风险。

第三个特征是**数据的可链接性**。大数据技术能够将海量异构分布数据结合在一起，实现数据深度地挖掘。邬贺铨认为，跨多个应用程序和云服务存储的数据共享需要明确可共享的原则、范围、层次和内容，规定共享程序与审计。

第四是**数据互操作性**。数据要流动、要使用才能产生价值，尤其是跨境数据流动。邬贺铨认为，数据流动的管理首先需明确并确

定数据类型，以便在出境口拦截未经批准的敏感数据。其次还需还原数据路径，实施数据处理流程的全链路监控，便于事后追溯。

第五是**数据的可信性**。深度神经网络是个分类器，当事件和图像处于 AI 模型辨识分界线或被干扰时会使 AI 误判，可通过区域截图、放大缩小等预处理发现数据被投毒；在整个供应链中，数据也极易受到污染而出现失真现象，可采用区块链+隐私计算方法，整合订单、发票、物流和资金流等数据，来发现有无造假。

第六是**数据的安全性**。数据是生产要素，因此要使用加密手段防止数据被窃取或者滥用，但也需要实时对数据进行审计与版本核对，防止被恶意再加密而被控或被勒索；另一方面，可以利用多方计算技术，允许各参与方只提交密文分片的前提下，通过既定逻辑共同计算出结果，但不透露各自数据。

第七是**数据的资产性**。数据是生产要素，需要从数据采集、数据开发利用、数据鉴权、数据应用等全生命周期去保证数据资产的安全性。邬贺铨强调，在所有环节中，特别注意元数据的管理、开发过程的管理、流通过程的管理和运维过程的管理，这些过程需要采用相应的安全技术支持资产安全管理。

第八是**数据的归属性**。毋庸置疑的是，数据本身是有归属权的，包括持有权、使用权、经营权，关系到数据使用的安全性和合法性。不同于传统资产的是，数据是可复制的，数据使用也基本上可以不留痕迹，这为数据的归属确权带来了很大的困难。

第九是**数据的开放性**。邬贺铨认为，原则上不涉及国家安全、企业秘密和个人隐私的政务数据，都应该向社会开放，才能发挥更大的价值。但政务数据开放要特别注意个人身份识别和地理位置等隐私保护，在大数据技术日益发达的今天，通过混合不同数据集进行关联分析，可以间接地追踪到个人工作生活等隐私，因此需要进行匿名化等脱敏处理。

（来源：cww.net）

（三）冯登国：关键信息基础设施安全保护三大关键能力

中国科学院院士 冯登国

《关键信息基础设施安全保护条例》自 2021 年 9 月 1 日起施行，即将实施一周年，值此之际，冯登国院士发表三点建议。

大力提升关键信息基础设施的弹性安全能力。要真正使得弹性安全技术落地生效，充分发挥其在关键信息基础设施安全保护中的重要作用，不能仅仅停留在口头上，要有检验弹性安全技术发挥效果的手段和方法，从而引导关键信息基础设施安全保护体系向着正确的方向发展。

要确实加强关键信息基础设施的数据安全治理能力。不仅要重视数据的存储和传输安全，也要重视数据的使用安全，更要重视数据的全生命周期安全。我们要重点围绕关键信息基础设施敏感数据的窃取、破解、篡改等攻击活动，确实加强数据安全防护和治理能力。

要高度重视新技术应用对关键信息基础设施带来的安全威胁风险评估能力，积极采取有效的应对措施，提升关键信息基础设施的对抗能力和防护水平。

（来源：安全内参）

（四）樊友山：筑牢数字安全屏障应做到三个“新”

全国工商联党组副书记、副主席 樊友山

数字经济在突破传统生产要素的流动限制，促进市场效率的同时，也带来了不容忽视的信息安全问题，这就要求我们必须筑牢数字安全屏障。应积极推动数字安全技术新发展，发挥市场主体新作用，完善新规则，助力构筑数字经济安全新长城。

当前，我国正进入数字化转型、智能化升级的关键时期。数字安全形势较过往发生了重大变化，防御理念、防御体系、防御技术都亟待变革。对此，樊友山提出网络安全企业助力数字安全建设的三个关键点。网络安全龙头企业要发挥自身技术、人才优势和技术创新主体作用，开展数字安全基础理论创新、重大问题研究和核心技术攻关，助力数字安全技术创新发展。广大网络安全企业要提高政治站位，牢固树立总体国家安全观，加强与政府部门、产业链上下游企业协同，共同维护国家网络空间主权、兼顾安全和发展。各网络安全企业作为护网主力，要加强对网络安全产业发展规律的认识，积极推动网信领域法律法规不断完善，积极参与网络空间国际标准规则制定，助力形

成良性的数据安全治理体系。

（来源：中华网）

（五）周鸿祎：在数字安全时代，“看见”是安全的分水岭

360 集团创始人、董事长 周鸿祎

7 月 30 日，第十届互联网安全大会（ISC2022）在北京国家会议中心开幕，本届大会以“护航数字文明、开创数字安全新时代”为主题，三六零公司创始人周鸿祎发表主题演讲时表示，在数字安全时代，“看见”是安全的分水岭，回避“看见”谈安全都是假把式，只是隔靴搔痒。正因为“看见”，我们才知道，网络攻击时时刻刻都在发生，并且所及之处一片狼藉，比如城市断水断电，企业受到勒索，损失动辄上百万。

周鸿祎表示，针对数字化过程中的安全挑战，数字化的内在脆弱性导致安全风险更大，同时外部威胁也在不断升级，在内外部双重安全挑战之下，风险遍布数字化的所有场景，倒逼网络安全升级为数字安全。

目前，外部威胁不断升级。“过去的‘小毛贼’已经鸟枪换炮，升级为专业化的网络犯罪组织，技术能力不亚于安全公司。”周鸿祎指出，勒索攻击、挖矿攻击、供应链攻击、DDoS 攻击、网站攻击等新攻击手段层出不穷，国家背景的 APT 攻击已经成为大国对抗的主流，网络攻击目标、手法、产生的破坏都突破常规。

数字安全时代的最大痛点就是“看不见”。为解决这一“卡脖子”难题，近 20 年间，360 投入了 200 亿，聚集了 2000 名安全专家，积累了 2000PB 的安全大数据，建立了一套以“看见”为核心的数字安全大脑框架，帮助国家感知风险、看见威胁、抵御攻击，并将服务国家的能力服务于政企客户、中小微企业，守护数字经济发展。

（来源：新华网）

（六）杜跃进：保护“东数西算”工程数据流动安全 服务数字中国战略

360 首席安全官、大数据协同安全技术国家工程研究中心常务副主任 杜跃进

在数智时代，社会的运转方式、安全风险和对抗方式、复杂程度等，都和之前有本质不同，单点的、局部的方案无法满足深度融合的新世界的安全需求，安全需要重新定义，升级为数字安全。

“数字安全事关数字战略成败。”杜跃进认为，作为国家战略性工程，“东数西算”使数据要素大范围跨域流动，即把东部产生的巨量数据在西部进行计算和处理。在如此庞大、复杂场景下，针对“东数西算”中数据的全生命周期的安全保障势在必行。

针对东数西算需要关注的问题：第一是高级持续性威胁（APT），数据集中的地方将是更有价值的攻击目标；第二是防窃取和破坏、防滥用、防误用等；第三是保护数据的流动和计算，保证数据在流动中风险可控。因此，要从合规监管、威胁、治理、生命周期安全管理、

数据安全研究创新支撑等维度考虑“东数西算”数据安全需求，服务数字中国战略。

关于数据安全治理已经形成一套方法论，核心思想是“以数据为中心，以组织为单位，以数据安全能力成熟度为抓手”。数据安全能力成熟度模型(DSMM)国家标准已于 2019 年正式发布。目前，DSMM 和围绕 DSMM 的数据安全治理体系获得广泛认同，已有超过 200 家 DSMM 测评案例，覆盖全国 11 个省及 8 个行业。DSMM 测评师、注册数据安全官（CDSO）和注册数据安全工程师（CDSE）等专业人才培养需求增长迅速。

（来源：freebuf.com）

（七）钟力：东数西算数据安全需进行体系化布局和建设

360 集团数据安全研究院院长、大数据协同安全技术国家工程研究中心副主任
钟力

“东数西算”工程已全面启动，在全国布局了贵州、内蒙古、甘肃、宁夏、粤港澳大湾区、成渝地区、长三角地区、京津冀地区等八个国家算力枢纽节点，节点之间建立高速直联网络，从而支撑大规模算力调度，使算力资源有序向西部转移，形成以数据流为导向的新型算力网络格局。可以看到，算力调度将引发大规模数据的频繁流动和使用，而且，国家级的数据中心集群无疑将会引来国家级的、有组织的高级网络安全威胁。因此，数据安全将成为“东数西算”工程能否成功推进的关键因素，应从如下三个方面进行体系化的建设：

一是强化数据安全治理。建立数据安全能力成熟度模型（DSMM）测评认证的工作机制、组织和业务支撑平台，对“东数西算”数据相关方组织（提供方、接收方、处理方等）进行数据安全能力测评认证，从组织建设、制度流程、技术工具和人员能力四个方面系统提升组织的数据安全能力，从而有效管控数据跨组织、跨平台甚至跨境流通的安全风险。对“东数西算”网络运营者进行数据安全管理认证，以规范数据处理活动，加强数据安全保护。同时，建立和完善数据安全测评的相关机制、组织和安全检测评估手段，对出境数据进行安全评估，对数据中心的数据和数据服务进行量化风险评估。

二是建设数据安全基础设施。在加密、访问控制、数据库安全等常规数据安全手段基础上，面向数据流通共享和开发利用需求建设专门的数据安全基础设施，至少包括：数据资产安全管理平台，对枢纽节点备份数据和离线计算大数据进行安全管理，更好支撑西部枢纽节点的后台加工、离线分析、存储备份等业务；大数据安全监管审计平台，为枢纽节点运营方提供数据处理活动感知、数据安全态势感知和应急处置等能力，以全面掌握本地计算任务、数据处理情况和数据安全状况；数据安全计算与共享交换平台，为枢纽节点提供数据安全传输、数据访问与检索安全、本地数据计算安全、多源数据联合安全计算、数据交易安全等能力，来支撑不同层次的数据流通共享与融合需求。

三是建设高级安全威胁主动防御基础设施。建设安全大脑及相关附属基础设施，通过“大数据安全分析+人工智能驱动+历史安全大数据+安全专家运营”相结合，各枢纽节点的协同联动，形成强大的高级数据安全威胁主动防御能力，防范数据窃取、数据泄露和加密勒索等安全风险。建设大数据安全靶场，虚实结合提升枢纽节点应对高级数据安全威胁的能力，同时培训合格的安全运营人员。

（八）李京春：数据分类分级需要同时考虑分类安全与发展两个视角

国家信息技术安全研究中心原副主任兼总工程师 李京春

当数据确权的讨论还在学术理论界争执不下时，数据分类分级的实践早已在各行各业遍地开花。数据安全需要采用分类分级安全管理，按重要级别备份/恢复，按数据类别进行强制访问控制、身份识别等密码措施加以保护。国家信息技术安全研究中心总师组专家李京春采访时表示，**为保证数据质量和高效利用，数据本身必须治理，数据分类分级就是数据治理的重要内容，需要站在不同的视角多维度管理和利用。**比如，监管部门或数据安全企业可能会更多地关注在数据处理活动当中是否合法、正当、必要，是否合规。毕竟数据关乎国家安全和经济发展，关乎公共利益，关乎我们每个人的隐私安全，所以说**安全是数据分类分级需要考虑的重要因素。**数据分类分级需要同时考虑到安全与发展，两个视角观察世界。

（来源：“数字生产力研究”公众号）

（九）潘剑锋：真正的EDR是“看见”威胁的眼睛

360 集团副总裁兼首席科学家 潘剑锋

“真正的 EDR 是看见威胁的眼睛，需要具备看见的能力。”360 集团副总裁兼首席科学家潘剑锋在第十届互联网安全大会（ISC 2022）未来峰会上谈到。

数字时代大量设备入网、业务和数据上云背后，是终端作为数字化基础节点面临对抗加剧、安全挑战严峻的现状。

“看见是检测的基础。只有快速、完整地理解网络攻击事件发生的全部情节，跟踪攻击事件每一步，才能以有效的方式做出响应。真正的 EDR 是看见威胁的眼睛。”潘剑锋表示，想要看见高级威胁攻击、勒索攻击、供应链攻击等各类威胁事件，需要具备全球视野、海量云端大数据的存储及处理能力、高质量事件的捕获能力、AI 分析技术及实战经验丰富的安全专家团队。

终端安全往往被视为最后一道防线，面对穷凶极恶的攻击者，终端防御方案“木桶效应”明显。EDR 必须同时在全球视野、云端分析能力、高级端点能力、AI 分析技术、实战专家五个方面具备顶尖实力，才能真正解决数字时代终端高级威胁防护难题，实现安全能力从被动式单点防护到主动式纵深防御的演进。

（来源：新华网）

（十）左晓栋：对数据出境安全管理制度的几点思考

中国科学技术大学公共事务学院、网络空间安全学院教授 左晓栋

当前，我国政策并未明确强调要实施数据本地化存储。对数据出境施加一些条件要求甚至是条件限制，并不等于不让数据出境，也不等于数据必须存在境内。在数据管理方面，我国正在建立重要数据出境安全监管制度，相关政策仍处于动态调整阶段。特别是，对重要数据的定义存在不一致是该阶段的特定现象，未来将逐步达成共识。

理解我国当前的数据出境安全管理制度，主要有以下几个要点：

一是当前我国政策并未明确强调要实施数据本地化存储。对数据出境施加一些条件要求，甚至有时候是条件限制，并不等于不让数据出境，也不等于数据必须存在境内。必须看到，除了《网络安全法》外，后续出台的法律法规的确没有再强调数据本地化存储的概念。在个别场合下，可能数据还是要坚持本地化存储，但这一定是某种特定的数据，而不是针对所有的数据。

二是对数据出境安全管理政策的认定，不是所有的数据出境都按现在的数据出境条件来实施。《网络安全法》和《数据安全法》明确了重要数据的出境条件，即必须经过网信部门组织的安全评估，《个人信息保护法》与《网络安全法》也明确了个人信息出境的条件。

个人信息出境有四条不同的途径，不属于规定的情况，按照目前法律法规规定，这是可以自由出的（涉密信息或行业有特殊要求的除外）。大家的注意力都被前一阶段国家政策的数据出境安全要求吸引

过去了，误以为数据必须这么出境。实际上还有相当多的数据是不必通过以上路径就可以出境，即，既非重要数据也非个人信息。目前的法律没有规定所有的数据出境都必须经过评估、标准合同或者认证。当企业进行数据出境时，可以对数据进行梳理，将重要数据、个人信息与其他出境数据分类处理。

（来源：“信息安全与通信保密杂志社”公众号）

《数字安全观察》产品系列

- 每周动态：政策法规/行业动向/安全事件/技术趋势
- 深度分析：政策解读/行业洞察/市场预测/事件分析/技术前瞻/策略建议/国际智库精编
- 国防专刊：网空战略/力量建设/科装动态/空天态势
- 数据安全专刊：政策形势/安全事件/安全研究/大咖观点
- 公安专刊（筹备中）

总编辑：杜跃进

执行编辑：张义荣

本期编委：钟力、唐会芳、王雨薇、陈璐、翟婷婷