全球数据安全观察

总第 107 期 2022 年第 35 期

(2022.09.19-2022.09.25)

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、国内首家数字资产保险创新中心在西安成立

9 月 17 日，由西安市碑林环大学创新产业带管委会、人保西安分公司、因问科技共同发起并成立的“数字资产保险创新中心”签约仪式在 2022 年全球硬科技创新大会成功举行。

数字资产保险创新中心通过隐私计算、人工智能和区块链技术等技术识别和保护企业的数字资产，促进数据资产的创造和流通，充分应用保险对科技发展的助推作用，搭建保险与科技创新之间的交流平台和融合机制。数字科技加保险科技双轮驱动，推动企业无形资产价值的全面释放，提升企业的市场竞争力，推动科技成果转化与流通，提升社会的创新能力。

https://mp.weixin.qq.com/s/jJV2Y_JaknYm9s702yHHlA

2、中国气象局印发实施细则，推进气象数据安全合规有序开放共享

9 月 19 日，中国气象局印发《气象数据开放共享实施细则（试行）》（以下简称《实施细则》），进一步规范气象数据开放共享工作，推进气象数据安全、合规、有序开放共享，提升气象数据资源价值和应用效益。

《实施细则》指出，气象数据开放共享应当遵循依法依规原则，以确保国家安全和数据安全为前提，保护数据提供者的合法权益，充分考虑用户实际需求，注重数据服务效益，分类分级开放共享。

http://www.cma.gov.cn/2011xwzx/2011xqxxw/2011xqxyw/202209/t20220919_5092677.html

3、河南省人民政府办公厅发布《河南省大数据产业发展行动计划（2022—2025 年）》

9 月 15 日，为深入贯彻国家大数据战略，认真落实省委、省政府实施数字化转型战略部署，加快推进我省大数据产业高质量发展，河南省人民政府办公厅发布《河南省大数据产业发展行动计划（2022—2025 年）》。

计划中明确要完善数据安全保障体系，包括实施数据安全“铸盾”行动，开展数据资源分类分级管理试点工作，加强数据应用、数据流转、数据共享、数据隐私、数据交易等环节监管等。并明确加强隐私计算、数据脱敏、密码、区块链等技术和产品的研发应用。

https://www.henan.gov.cn/2022/09-21/2610744.html

4、《海南省省级共享数据目录清单(第一批)》印发

海南省政府大数据推进工作领导小组办公室近日印发了《海南省省级共享数据目录清单(第一批)》，共编录了 50 家省级政府单位的 29431 项数据项。

清单包括数据目录名称、数据项名称、共享属性、数据提供方式、更新周期、目录申请量等。从信息内容来看，涉及的数据目录主要有海南健康码信息、人口信息、法人信息等 1307 条数据目录 29431 项数据项。从共享方式来看，有条件共享 20852 项数据项，无条件共享 8392 项数据项，不予共享 187 项数据项。从接口方式来看，有条件共享的数据可通过接口、库表、文件被申请使用，其中以接口方式提供的数据有 10948 项，库表方式提供的数据有 18176 项，文件方式提供的数据有 120 项。

https://hainan.newshainan.com/20220915/3590.htm

5、印尼数据保护法获通过: 非法收集个人信息面临最高五年监禁

9 月 20 日，根据印度尼西亚（以下简称“印尼”）众议院官网消息，印尼通过了一项个人数据保护法法案（PDP）。该法案规定，非法收集或使用他人个人资料的数据处理者，可能面临最高五年的监禁；发生数据泄露的情况下，公司可能

被处以多达年收入 2%的行政罚款。PDP 共 16 章 76 条，分别从个人数据主体权利、行政处罚、国际合作、刑事规定等方面展开。

https://mp.weixin.qq.com/s/dp5t6ka0OLisJWH1zLQnYg

技术、产品与市场

1、五分之二的美国消费者遭受个人数据盗窃

根据身份盗窃资源中心（ITRC）的数据显示，在过去一年中，大约 40% 的美国消费者的个人信息被盗、泄露或滥用。

研究显示，尽管遭受重复身份犯罪的受害者人数同比下降，但仍有一半人证实他们不止一次受害。此外，针对受害者的复杂网络攻击数量也在逐年上升，比例从 2020 年的 35% 猛增到 2021 年的 55%。

在泄露的数据中，社交媒体账户信息占据了很大一部分，因此近几年被攻击者“接管”的社交媒体账户数量同比飙升了 1000%，其中一半（51%）的受害者在被入侵后损失了个人资金。最常见的是 Instagram 帐户被劫持 (85%)，四分之一 (25%) 用户指出 Facebook 遭受入侵。虽然受害者的总体损失较少，其中大多数属于“500 美元以下”类别，但损失超过 10,000 美元的受害者占总数的近三分之一（30%），高于 2020 年的 9%。

https://www.infosecurity-magazine.com/news/two-fifths-consumers-personal-data/?&web_view=true

2、服务先行，《IDC Perspective：中国数据安全服务市场洞察，2022》报告正式启动

从安全技术上来讲，数据安全相关产品技术已发展多年，并不是一个新话题，数据加密、脱敏、防泄漏等产品经过了多年的打磨已经成为了相对成熟的产品市场。然而，由于数据的强业务属性，其呈现分散性、多样性、复杂性等诸多特性，仅产品部署难以解决企业的**全局数据安全建设问题**，数据安全服务由此受到了越来越多最终用户的青睐。

IDC 定义下的数据安全服务即以保护数据安全为核心而开展的一系列专业服务，其中包括数据安全咨询服务、数据安全集成服务、数据安全教育与培训服务以及数据安全托管服务。对于最终用户来说，数据安全服务可以切实帮助其解决数据安全“是什么”、“建什么”、“怎么建”的问题，运用“同步规划、同步建设、同步使用”的原则，站在业务之上规划数据安全建设蓝图，了解数据安全风险状况，从而进行数据安全建设与运营。**“服务先行”**已逐步成为了企业数据安全体系建设的第一步。

https://mp.weixin.qq.com/s/NUnEtRRhr5_VQUJU_eEYyw

3、研究：量子计算已经将数据置于风险之中

根据德勤的一项新研究，超过一半的组织认为当前的数

据集已经受到未来量子计算进步的威胁。

在对 400 多名网络安全专业人士的调查中，50.2% 的受访者表示，他们的组织面临“现在收获，以后解密”攻击的风险，网络犯罪分子在预期量子计算机能够破解现有密码的时候提取加密数据算法。

这种现象被称为“Q Day”，专家认为这将在未来 5-10 年内发生。如果不开发量子安全加密，这可能会使所有数字信息容易受到威胁行为者的攻击。

https://www.infosecurity-magazine.com/news/quantum-computing-data-risk-cyber/?&web_view=true

4、[调查]从 2009 年到 2022 年，美国医疗事故占 3.42 亿条泄露记录

自 2009 年以来，美国的医疗机构遭受了近 5,000 起数据泄露事件，影响了超过 3.42 亿条医疗记录。研究人员团队分析了 2009 年至 2022 年 6 月的数据并深入研究了 2021 年 1 月至 2022 年 6 月的数据泄露事件，得出如下结论:

- 从 2009 年到 2022 年 6 月，记录了 4,746 起医疗事故
- 342,017,215 条个人记录因这些违规行为而受到影响
- 2020 年是医疗事故最多的一年，报告了 803 起（第二高的是 2021 年，有 711 起）

- 2015 年受影响的记录数量最多，总计超过 1.12 亿条
- 在 2021 年和 2022 年（到目前为止），专科诊所（专门从事某一医学领域的诊所，例如心脏病学或放射学等）占数据泄露最多（15%），共有 130 个被泄露实体，但医院网络占被泄露记录最多的记录，共有 880 万条记录受到影响（占受影响记录总数的 16%）
- 在 2021 年和 2022 年（到目前为止），黑客攻击是最常见的违规类型，占违规行为的 40%(862 起中的 353 起)

https://mp.weixin.qq.com/s/xizAa9JOvRIyGRQ5myJfQQ

业界观点

1、陈秋玲：高校如何构建数据安全防护体系

针对近年来，高校数据安全面临“孕灾环境复杂、风险因子庞杂、承灾主体脆弱、风险类型多元”的挑战，上海大学发展规划处大数据中心主任、教授陈秋玲提出共同谱写数据安全“五线谱”：

一是在全校范围内宣传高校数据安全的重要性和紧迫感，形塑“数据安全是高校生命线”的价值观；二是定期向全体用户宣讲数据安全的法律法规和规范性文件，划定学校数据安全的标准线；三是引导师生自觉遵守有关数据安全的法律法规和规范，避免触碰数据安全的高压线；四是引导数据用户培养规范的数据运用行为，不越过数据安全事件发生的警戒线；五是提高师生数据风险的防范意识，共同守护大数据时代数据作为“石油资产”的安全线。

同时，她提出强化全生命周期的数据安全管理技能精准赋能。针对数据安全风险具有快速、隐蔽、破坏大的特点，要提高管理精准度，实行智能化管理。一是利用人工智能、大数据等技术对高校数据安全进行自动化、智能化分析，缩短响应时间，降低管理成本，减少对数据安全管理人员的技术、知识、经验的依赖，以其精准度实现管理的高效性。二

是对高校数据生命周期全过程进行监测监控，密切关注高校数据安全重点领域、重点群体、重点时空节点的动态，对风险生命周期各阶段的警源、警兆、警情进行预测预警预报，并根据风险等级启动应急响应预案，从而达到最大限度地降低数据破坏给高校带来的损失。

https://www.163.com/dy/article/HHKU62J705506BEH.html

2、专家：对数字政府安全技术合规分析的建议

今年，国务院颁布了《关于加强数字政府建设的指导意见》，提出要“构建数字政府全方位安全保障体系”“促进数据有序开发利用”。显然，保障政务数据的安全合规，是推进数字政府建设的重要工作。

根据《个人信息保护法》相关要求，履行个人信息安全处理义务的技术建议包括引入并应用有效的技术手段进行个人信息保护的响应和保障，如：建立政务体系下统一的个人信息安全风险评估标准（国家标准或政府行业标准），引入身份认证技术、访问控制技术，引入加密技术、去标识化技术，引入数据备份技术，引入电子签名技术、哈希技术，引入行为审计分析技术，引入数据资产识别、自动化分类分级、细粒度权限管理（标签化）等技术。

同时，还需涵盖对合规审计、影响评估、补救措施等事

务，如：引入日志审计技术，引入数据流转审计技术，引入个人信息处理风险评估技术，引入脱敏评估技术，引入区块链存证技术，引入个人信息风险评估技术，引入安全事件分析技术。

此外，还可以通过以安全多方计算、联邦学习、可信执行环境（TEE）三大技术为基础实现数据“可用不可见”的隐私计算技术，或以身份认证、数据加密、访问控制、日志审计等技术为基础实现的传统数据安全管理技术，两条不同的技术路线进行个人信息保护。

https://it.ynnu.edu.cn/info/1055/2648.htm

3、赵闻飙：释放安全科技生产力，构建数实融合下的新安全体系

9 月 23 日，“2022 年度 21 世纪科技峰会”在线上召开，蚂蚁集团副总裁、大安全事业群总裁赵闻飙表示，数实融合趋势下，安全需要具备四大特点：安全一定是以“合规”为根本的；满足未来需求，安全一定是“大规模智能化”的；满足未来需求，安全一定是“强化人文关怀和责任担当”的；满足未来需求，安全一定是“生态协同”的。

对此，蚂蚁提出了以 IMAGE 命名的下一代风控体系：

首先，IMAGE 的“I”即交互式主动安全技术，其关键在

于“主动”和“交互“二词，安全必须从静态的被动防守，转变为动态的主动对抗。

IMAGE 的“M”即“多方安全技术”，以多方安全计算等技术代表，通过结合区块链、应用密码学等，在保护合作伙伴用户隐私和商业秘密的前提下，在平台之间实现 1+1>2 的价值效果。

IMAGE 的“A”即对抗智能，是实现安全“大规模智能化”的一个较为有效的手段。

IMAGE 的“G”即“全图安全技术”，指以“图”的形态，实现对风险变化趋势的预测，提前遏制风险的发生。

IMAGE 的“E”是“端云协同安全技术”，是“大规模智能化”趋势下，兼顾风险防控与隐私保护发展的实践探索。

https://m.21jingji.com/article/20220923/herald/a974977161be8efecc4c22686594671b.html

4、专家：汽车行业亟需构建数据管理制度

汽车数据出境领域，国家信息技术安全研究中心副主任兼总工程师、中国信息协会信息安全专委会副主任李京春曾公开做出过风险提示。在他看来，目前汽车数据出境领域的问题依然比较突出，一是个别企业未按国家有关法律法规和部门规章，采集位置数据和周边环境数据，数据违法违规出

境；二是数据交易不规范，数据跨境合同不符合国家法规要求，数据跨境未评估、未认证、未备案、未目录申报等问题。

针对上述问题以及相关法规出台后给汽车行业带来的挑战，产业界认为应该从监管层、机制层以及企业层逐一攻克。

首先是监管层面，张永伟认为目前最迫切的是需要进一步完善智能网联汽车发展所需要的汽车数据管理制度，特别是在进度数据爆炸的时代，对数据的监管应该有明确的职能分工；陈文昊认为对数据出境的监管不仅要覆盖得广，还要有深度，建议监管层多与行业组织及头部企业交流，以破解不同行业的特点存在差异，商业模式也有很大区别的困难；

其次是机制方面，多位业内人士表示，汽车数据出境需要率先对数据进行明确的分级、分类，这样可提升数据出境合规的效率。希望行业主管部门或机构制定企业数据分类分级盘点表，并以其指导数据出境安全评估中的数据梳理与识别工作；

最后是企业层面，赵剑建议，发展车联网相关业务的企业，有必要对数据进行分类工作，并按照国家法律规定建立数据资产台账，以此来保障对重要数据和个人信息的精准识别。

https://www.jwview.com/jingwei/html/09-22/504797.shtml

5、梅冠群：积极融入和重塑全球数字治理格局

数字经济是大国竞争的重要领域,主要大国不仅对先进数字技术激烈争夺,在国际数字治理方面也在相互博弈。目前全球尚未形成统一协调的数字治理体系,国际数字治理碎片化、分裂化。美国和欧盟主导了最主要的两大数字治理体系,即“美式模板”和“欧式模板”。两套模板治理重点各有不同,但均致力于升级成为国际规则模板。其他国家在数字治理话语权方面尚不能与美欧抗衡,在国际数字规则制定中扮演参与者和跟随者角色。

数字经济十分依赖市场规模,如果我国数字企业仅局限在国内市场,不能在更大规模的国际市场发展壮大,未来我国数字企业将在企业规模、技术水平、国际市场占有率方面居于劣势。为应对这一变局,中国应做好三件事。

第一,加强国内数字治理。当前我国应先把自己的事做好,加快完善国内数字治理制度框架,形成兼顾发展与安全的治理体系,提升数字治理能力,为与美欧开展数字治理博弈夯实基础。可以在自贸区(港)基础上,建立数字自贸区(港),允许地方就上述领域先行先试,开展制度创新,为全国摸索新鲜经验。

第二,立足我国优势领域探索建立数字治理的“中式模板”。我国数字经济规模位居世界第二,仅次于美,在跨境电商、

电子支付等领域甚至远超美国。应积极探索在这些优势领域率先形成国际规则和范本,形成具有中国特色的“中式模板”,并通过双多边经贸安排的方式,优先向东南亚、中亚、中东欧、非洲等地区推广,共建“数字丝绸之路”,逐步形成由我国主导和影响的“数字流通圈”,增强与美欧“数字流通圈”的博弈能力。

第三,择机与美欧围绕数字规则开展对话和谈判。我国已正式提出加入 CPTPP 和 DEPA(数字伙伴关系协定),应该积极寻求与这些高标准国际数字规则的衔接。同时美欧等数字企业十分希望扩大其在中国市场规模,我国应以国内大市场和以我主导的“数字流通圈”为筹码,以数字治理“中式模板”为蓝本,围绕数字市场准入、数字安全、数据跨境流动、数据本地化存储、隐私数据保护、执法跨境数据调取等重点议题,在多边和双边场合,择机与美欧等开展对话沟通和平等谈判,推动全球数字治理协调,在参与国际数字规则塑造中维护我国数字领域的国家利益。

http://www.ciia.org.cn/news/18259.cshtml

数据安全事件

1、摩根士丹利因泄露数百万客户信息支付 3500 万美元罚款

2022 年 9 月 21 日报道，美国证券交易委员会(SEC)宣布，摩根士丹利（Morgan Stanley）已同意支付 3500 万美元的罚款。SEC 称，这家金融服务公司未能保护大约 1500 万客户的个人信息。从 2015 年开始，该公司多次聘请一家公司来处理数千台报废设备。然而，这家公司在数据销毁方面没有经验，甚至将数千台设备出售给第三方，其中包含了客户信息的设备，然后这些设备在拍卖网站上被转售。该公司试图取回这些设备，但其中绝大多数无法恢复。

https://www.securityweek.com/morgan-stanley-pay-35m-fine-exposing-information-millions-customers

2、黑客 Data 在暗网出售约 3.5 亿条 Ask.FM 用户的记录

据媒体 9 月 20 日报道，名为 Data 的黑客在暗网出售社交网站 Ask.FM(ASKfm)的用户数据。Data 表示，买家可以获得 607 个存储库以及他们的 Gitlab、Jira、Confluence 数据库，数据库中有约 3.5 亿条记录，其中约 4500 万条使用单点登录进行登录。据悉，攻击者在 2019 年首次访问服务器，在 2020 年 3 月 14 日获取了数据库。Data 还提供了攻击的技术细节，

并表示 Ask.FM 仍然很脆弱。

https://www.databreaches.net/ask-fm-user-database-with-350m-user-records-has-shown-up-for-sale/

3、加密货币公司 Wintermute 遭到攻击损失约 1.6 亿美元

9 月 20 日报道称，加密货币公司 Wintermute 已被黑客入侵，并在 DeFi 业务中损失了 1.622 亿美元。该公司并未提供窃取资金的详细信息，但研究人员认为，攻击者可能利用了 Profanity 中的漏洞。Wintermute 是加密货币平台的“做市商”，仍然有偿付能力，持有两倍于被盗数额的股权。不过，预计接下来的几天服务会中断，因为该平台仍在努力恢复业务。公司 CEO Gaevoy 表示，愿意将此事视为白帽事件，这意味着他们愿意提供赏金且没有任何法律后果，但不知道攻击者是否会将被盗资金返还给 Wintermute。

https://therecord.media/cryptocurrency-company-wintermute-says-hackers-stole-160-million/

4、Guacamaya 公开智利等多个国家的军事机构约 10 GB 数据

据 9 月 19 日报道，自称 Guacamaya 的黑客团伙发布了来自智利和墨西哥等多个国家的军事和警察机构约 10 GB 的

电子邮件等材料。该团伙主要针对中美洲地区的组织，这是其自 2022 年 3 月以来第四次公开数据，这些数据都被发布到了 Enlace Hacktivista。据悉，此次事件主要涉及了智利武装部队参谋长联席会议、墨西哥国防部、萨尔瓦多国家民警和萨尔瓦多武装部队、哥伦比亚武装部队总司令部、秘鲁武装部队联合司令部和秘鲁军队。

https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

5、一黑客兜售印尼 13 亿手机卡用户数据，公开嘲讽多名高官

2022 年 9 月 20 日消息，印度尼西亚近期成立的数据保护工作组正在追捕一名黑客。此人据称涉嫌窃取了 13 亿注册手机用户与 1.05 亿选民数据，甚至掌握了总统通信日志。

这位化名 Bjorka、声称居住在波兰华沙的黑客，过去几周来一直在黑客论坛 BreachForums 上兜售被盗数据，受害者包括印尼多家国有企业、手机运营商及大选委员会。Bjorka 还掌握一份机密文件日志，其中记录着印尼总统佐科·维多多（Joko Widodo）与国家情报局之间的往来信息。

Bjorka 在 9 月 10 号的一条推文中表示，他的意图是展示“在糟糕的数据保护政策之下，黑客渗透、特别是针对政

府部门的渗透，是多么易如反掌。”

https://www.secrss.com/articles/47128

6、金融科技公司 Revolut 5 万多客户的个人信息泄露

2022 年 9 月 19 日称，Revolut 遭到攻击，未经授权的第三方访问了 5 万多个客户的信息。Revolut 成立于 2015 年，是一家金融科技公司，目前为全球客户提供银行、资金管理和投资服务。攻击发生在一周前，根据初步调查结果，攻击者通过社会工程技术访问了 Revolut 的数据库，影响了该公司 0.16%的客户。此次事件泄露了客户的姓名、地址、邮件、电话号码、部分支付卡数据和账户数据等。

https://www.bleepingcomputer.com/news/security/revolut-hack-exposes-data-of-50-000-users-fuels-new-phishing-wave/

7、澳大利亚 Optus 遭受重大网络攻击，多达 900 万用户受影响

2022 年 9 月 23 日，Optus 是新加坡电信旗下的一家公司，据该运营商澳大利亚子公司透露，它受到了一次网络攻击，导致当前和以前客户的信息被非法获取，包括姓名、出生日期、机密身份证件和电子邮箱地址。在一份声明中，这家新加坡电信的澳大利亚子公司解释说，它已立即制止了侵

犯行为，并与澳大利亚网络安全中心合作以减轻客户面临的任何风险。

可能泄露的信息包括电话号码等个人详细信息，而部分客户的地址和身份证件号码也被泄露。受到影响的客户据称多达 900 万。

https://www.cnbeta.com/articles/tech/1319717.htm

8、美国航空发生数据泄露事件：部分客户和员工受影响

2022 年 9 月 21 日报道，美国航空公司上周末发出客户通知信确认遭遇黑客攻击，声称攻击者获取了数量不明的客户和员工电子邮件账户和敏感个人信息。

美国航空公司的企业传播高级经理表示，该公司员工的账户在一次网络钓鱼活动中遭到入侵，但拒绝透露有多少客户和员工受到影响，而是说这是“非常少数”。在攻击中暴露并可能被攻击者访问的个人信息可能包括：员工和客户的姓名、出生日期、邮寄地址、电话号码、电子邮件地址、驾驶执照号码、护照号码和/或某些医疗信息。

https://www.secrss.com/articles/47166

9、河南一高校学生干部协助公司做问卷致学信网信息泄露，校方通报

近日，网传河南省信阳师范学院存在”学信网信息泄露”，一些学生在三个月内不能享受购买苹果电脑、耳机等产品的优惠政策。

9 月 20 日晚，信阳师范学院发布通报称，学校有关部门已于 9 月 19 日上午向信阳市五星乡派出所报案，并立案调查。经调查，8 月 28 日，校学生会一名学生干部参加社会实践活动期间，应郑州泽梦企业管理咨询有限公司业务人员要求，协助该公司擅自组织学生参与网上《信师宿舍满意度调查问卷》活动，通过学生干部 QQ 交流群发布调查问卷，组织 2020 级和 2021 级学生参加问卷调查。该调查问卷最后一题是要求学生登录学信网并填写学信码，涉事公司事前向该生隐瞒了学信码的真实用途，该生对问卷调查的真实目的缺乏了解。经与填写问卷学生核实，确实存在部分学生学信码被盗用情况。

https://www.sohu.com/a/586829603_120914498

10、公司技术人员勾结他人倒卖平台密码 侵犯公民信息被判刑

2022 年 9 月 24 日，据合肥市瑶海区人民法院消息，某

公司技术人员，利用参与某信息资源共享项目的权限，可以帮助他人找回、重置服务平台上密码之便，勾结无业人员倒卖平台密码，非法获取公民信息，从中谋取高额利益。2022年9月15日，合肥市瑶海区人民法院对此案进行公开宣判，以侵犯公民个人信息罪，判处被告人杨某某、陶某、许某某、王某某有期徒刑三年，缓刑四年至二年八个月，缓刑三年八个月，并处罚金人民币二十五万元至二十万元不等。

https://mp.weixin.qq.com/s/Ezb9uJ-nM3SBUXPA-sFXng