大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 71 期 2021 年第 47 期

（2021.12.13-2021.12.19）

大数据协同安全技术国家工程实验室

目录

政策形势

1、国家工程实验室发出首批注册数据安全官证书

为落实国家层面法律法规的相关要求，为我国培养更多优秀的数据安全管理层人才，作为我国大数据安全领域唯一的一家国家工程实验室，大数据协同安全技术国家工程实验室推出注册数据安全官（Certified Data Security Officer，简称：CDSO）人才培训。

经过严格的考试评价，共有 23 人通过了首批注册数据安全官培训考核，获得注册数据安全官证书。

数据安全官是一个“抓总”的数据安全岗位，以提升组织的数据安全整体能力，并以达到最终保障数据安全效果为最终目标，负责整体统筹规划数据安全战略目标与实施策略，协调各部门共同协作进行体系化建设。原则上，任何一个企业或者机构组织，都需要有这样的岗位。

https://mp.weixin.qq.com/s/bMMMibhVFCElWDHQSp68EQ

2、工信部组织开展工业领域数据安全管理试点工作

工业和信息化部近日印发通知，组织开展工业领域数据安全管理试点工作。将贯彻落实《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规，指导省级

工业和信息化主管部门组织开展数据安全管理试点，督促企业落实数据安全主体责任，加强数据分类分级管理、安全防护、安全评估、安全监测等工作，提升数据安全防护能力。加强试点成果转化应用，完善工业领域数据安全制度规范和工作机制，遴选一批示范企业、优秀产品和典型解决方案，形成可复制可推广的管理模式，促进提升行业数据安全保护水平。

https://www.secrss.com/articles/37152

3、多省市网信办开展 2021 年度汽车数据安全管理情况收集工作

根据国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布的《汽车数据安全管理若干规定（试行）》要求，汽车数据处理者开展重要数据处理活动的，需要向各省市互联网信息办公室和有关部门报送 2021 年度汽车数据安全管理情况。近日，天津市，广东省，河北省等多省市网信办开展年度汽车数据安全管理情况收集工作。

https://mp.weixin.qq.com/s/g8KR1Cf8FP6bB9UHYpuZrQ

4、全国信安标委征求国家标准《信息安全技术 网络安全信息共享指南》（征求意见稿）意见

12 月 17 日，全国信息安全标准化技术委员会归口的国家标准《信息安全技术 网络安全信息共享指南》现已形成标准征求意见稿。根据《全国信息安全标准化技术委员会标准制修订工作程序》要求，现将该标准征求意见稿面向社会公开征求意见，截止时间 2022 年 2 月 15 日。

https://www.wangan.com/p/7fy747c322569f41

5、美澳签署 CLOUD 法案双边协议，将跨境获取数据

2021 年 12 月 15 日，澳大利亚和美国签署了一项具有里程碑意义的 CLOUD 法案协议，该协议是第二个在《澄清境外合法使用数据法案》(CLOUD Act) 框架下达成的双边协议，此前 2019 年 10 月，美国与英国签订了第一份 CLOUD 法案协议。

该法案协议将有助于澳大利亚和美国执法机构及时访问电子数据，以预防、检测、调查和起诉严重犯罪，包括儿童性虐待、勒索软件攻击、恐怖主义和互联网上对关键基础设施的破坏。同时，将使两国的执法机构能够在法律规定的法律权限和保障措施下相互共享重要的数字信息和数据，为美国和澳大利亚之间更有效的跨境数据传输铺平了道路。

https://www.secrss.com/articles/37216

业界观点

1、姚期智院士：数据、算法、算力为何是数字经济核心技术？

数字化转型的最大挑战之一是“数据孤岛”问题。围绕央企数字化转型，要打造“数据中台”，在数据安全、数据隐私合规的前提下进行全面整合；同时建设央企间的合作联盟，打造行业级的隐私计算平台，形成企业间的数据要素流通市场。

数字经济的核心技术涉及数据、算法与算力三个方面。数据正在成为经济关键生产要素，我们需要研究推进数据确权和分类分级管理，畅通数据交易流动，实现数据要素市场化配置，合理分配数据要素收益。

https://mp.weixin.qq.com/s/jjIGE0sh3vjIx_MkrSyOgg

2、360 发布全网数据资产风险监测预警解决方案，助力提升数据安全监管效能

12 月 17 日，360 政企安全集团重磅发布基于测绘的全网数据资产风险监测预警解决方案，旨在帮助网络安全监管单位有效解决互联网侧数据安全监管问题，助力应对数字化

转型进程中的数据安全风险。该解决方案，基于事前大网数据资产测绘威胁情报及漏洞数据汇总、事中数据资产风险监测预警以及事后数据安全事件响应通报的全生命周期设计思路，成为监管单位监管其管辖区域内企事业单位在互联网上数据的重要抓手。

在事前大网数据资产测绘威胁情报及漏洞数据汇总阶段，该方案将基于 360 大网测绘收集的多维数据，360 威胁情报平台、360 漏洞云收集到的威胁情报与漏洞数据，客户提供的数据及根据客户需求定制化采集的其他数据，可形成全网基础数据的汇总。**在事中数据资产风险监测预警阶段，**该方案通过构建全网数据资产风险监测预警平台，实现监管单位对管辖区域内企事业单位的全网数据资产开展威胁监测预警，监测出有安全风险隐患的数据（诸如关基数据库重大漏洞、暴露在互联网上的重要数据/个人隐私数据等），并发出预警信息或事件。**而在事后数据安全事件响应通报阶段，**监管单位可通过公文\邮件\电话方式，将全网数据资产风险监测预警平台提供的预警信息或事件提供给存在数据安全风险与隐患的企事业单位，并限期进行整改，监督检查其整改效果，此外还提供数据安全应急通报监管预案。

https://mp.weixin.qq.com/s/II2MRu1tOtPLaOcNSvo4vw

3、2021 年度中国数字安全能力图谱

基于三元论的三大支点——信息技术、业务应用和网络攻防，能力图谱分为八大方向：**信息基础设施保护、信息计算环境保护；行业环境安全、应用场景安全；基础与通用技术、体系框架、安全运营和数据安全**。

1）信息基础设施是指数字空间中最为基础与关键的计算实体，它们是电子信息进行计算、处理、传输、存储的载体。

2）信息计算环境是指以现象级新兴信息技术为主要特征的各类计算实体的集合，进而形成的信息计算环境。

3）行业环境安全是指自身行业属性非常突出的安全需求，能力图谱将其划分为个 4 个一级领域，即公共安全、工业互联网安全、车联网安全、信创安全。

4）应用场景是指机构或组织较为典型的通用业务场景。

5）基础与通用是指网络安全体系中的必备能力和普适能力，如密码、网络空间资产测绘、身份安全等等。

6）体系框架是指多种安全技术、产品的整合，并体现出一个相对完善的安全理念，能力图谱将其划分为 3 个一级领域，即态势感知、威胁检测与响应、零信任。

7）安全运营是指安全体系的评估、规划、设计、建设、运行、维护、保障等一系列以人员服务为主驱动的安全工作。

8）数据安全可以从三个视角来看待，资产视角（注重静态保护）、访问视角（注重访问控制）和共享视角（注重流动应用）。

https://mp.weixin.qq.com/s/2TzInNe2YNwiGZRBGvp-Pg

4、维度、力度和限度：中国数字经济发展观察报告

数字经济时代，我国宏观经济增长逻辑、产业组织形式、企业组织形态、政府治理模式等多个维度均产生了革命性变化。

从宏观经济层面看，高技术产业投资、新基建、云服务、电子商务、电子信息产品出口及数字服务贸易等持续高速增长，培育了经济增长的新动能。

从产业组织形式看，数字技术将产业链上下游贯通达成规模效应，以产业链数字化锻造产业发展新势能。

从企业组织形态看，随着企业数字化转型的深入推进，企业组织架构日益扁平化、网络化，特别是虚拟组织打破了传统组织的边界，要素的共享化、生产的柔性化、产供销的一体化逐步成为现实。

从政府治理模式看，一网通办、一网统管、以网管网等数字时代的治理新要求加速了政府数字化转型进程，数据共享开放压力、数据技术业务融合的新逻辑对府际关系和政策

创新提出了新要求。

https://mp.weixin.qq.com/s/iV7b2x1UeOnedvPScdBeZA

5、Gartner：谁是政府数字化转型的真正负责人？

政府数字化转型乃至优化的真正驱动力始于通过强有力的规划和战略改变整个企业机构中孤立的业务政策、流程和规则。

在规划数字化转型时，政府领导人想当然地认为应由 IT 领导人负责这项工作。如果 IT 部门无法实现这一目标，他们往往会找来首席数字官（CDO）或首席公民体验官（CCXO）。

这就是问题所在。数字化转型的确需要技术，但技术只起到助推作用。转型乃至优化的真正驱动力始于通过强有力的规划和战略改变整个企业机构中孤立的业务政策、流程和规则。数字化转型的首要负责人必须是**首席执行官（或同等职位的人员）**，而不是首席信息官。

https://www.secrss.com/articles/37133

安全事件

1、擅自采集上传 43 万张人脸照片，小鹏汽车被罚 10 万元

2021 年 12 月 14 日，从上海市市场监管局获悉，近日，上海小鹏汽车销售服务有限公司被上海市徐汇区市场监督管理局罚款 10 万元。

据行政处罚决定书显示，上海小鹏汽车销售服务有限公司购买了具有人脸识别功能的摄像设备 22 台，全部安装在旗下门店，2021 年 1 月至 6 月期间，共计采集上传人脸照片 431623 张。通过算法对面部数据进行识别计算，以此进行门店的客流统计和客流分析，包括进店人数统计、男女比例、年龄分析等。然而，采集消费者面部识别数据，并未经得消费者同意，也无明示、告知消费者收集、使用目的。

https://www.secrss.com/articles/37159

2、未经明确同意出售用户数据，交友应用 Grindr 被罚 650 万欧元

2021 年 12 月 15 日，著名约会交友应用 Grindr 被挪威数据保护局（DPA）**罚款 650 万欧元**（约合人民币 4963 万），原因是 Grindr “严重”违反 GDPR 规则，**未经用户明确同意向广告商出售位置、IP、年龄等用户个人数据。**

挪威 DPA 国际部负责人 Tobias Judin 解释，“我们认为，

Grindr 在没有法律依据的情况下向第三方披露了用户数据并用于广告。这与 GDPR 的‘有效同意’要求相违背。”

https://www.freebuf.com/news/312469.html

3、辛集两千余群众个人信息遭泄露: 警示基层政府须提高法治意识

据新华报业网 2021 年 12 月 13 日报道，日前，河北省辛集市政府官网公布的一份城乡特困人员公示名单引发社会广泛关注。该名单中不仅详细列出了两千多名城乡特困人员所属街道（乡镇）、社区、姓名、性别、特困类别和金额，还公布了完整身份证号码等隐私。

这凸显出有关部门把关审核程序存在缺失和纰漏，部分执法人员法治意识淡薄。辛集市两千多名群众个人身份证号码信息遭泄露，再次警示基层政府须提高法治意识，在法治轨道上统筹推进各项工作。

https://mp.weixin.qq.com/s/4o111qQN7-pPU1CX7rZbIA

4、51 人因在欧盟和美国出售 3 亿人的数据而于乌克兰被捕

2021 年 12 月 13 日，据外媒报道，乌克兰警方在一份新闻稿中透露，他们逮捕了一个 51 人的团体，据称他们在美国、欧洲和乌克兰境内散布并出售属于大约 3 亿人的被盗

个人信息，包括公民的个人数据、个人和法人实体金融和经济活动的机密信息、银行和商业机构客户的信息等等。警方表示，已从互联网上删除了大约 90,000 GB 的数据。

https://tech.co/news/51-arrested-in-ukraine-for-selling-data-of-300m-people-in-eu-us?web_view=true

5、德国耳机巨头森海塞尔泄露 55GB 客户数据

2021 年 12 月 19 日，据报道，德国专业话筒和耳机制造巨头森海塞尔 (Sennheiser) 将超过 28000 名客户的个人数据暴露在配置错误的 Amazon Web Services (AWS) 服务器上。

根据针对德国音频设备制造商森海塞尔的一份报告表述，森海塞尔在网上留下了一个不安全的亚马逊网络服务 (AWS) 服务器。该服务器存储了大约 55GB 的超过 28000 名森海塞尔客户的信息。泄露的数据库包括：全名、电子邮件 ID、家庭地址、电话号码、员工姓名、公司名称等。

https://www.wangan.com/p/7fy747b8840d7905

6、四个运动装备网站的 180 万客户受到信用卡泄露的影响

2021 年 12 月 19 日，据报道，威胁行为者窃取了属于四个附属在线体育装备网站的 1，813，224 名客户的信用卡。

2021 年 11 月 29 日，该公司证实其客户的个人和财务数据被盗，包括全名、财务帐号、信用卡号码（带 CVV）、借记卡号码（带 CVV）、网站账号密码等。2021 年 12 月 16 日，这四个网站通知了受影响的客户。目前，这些网站尚未披露安全漏洞的原因。

https://www.wangan.com/p/7fy747f2f91270c3