全球数据安全观察

总第 111 期 2022 年第 39 期

(2022.10.24-2022.10.30)

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、国务院印发《全国一体化政务大数据体系建设指南》

10 月 28 日，《全国一体化政务大数据体系建设指南》印发，明确指出“政务数据安全保障能力亟需强化”是当前存在的主要问题之一，并提出健全数据安全制度规范、提升平台技术防护能力、强化数据安全运行管理以实现安全保障一体化。

http://www.gov.cn/zhengce/content/2022-10/28/content_5722322.htm

2、海南省、山东省互联网信息办公室开通数据出境安全评估申报通道

10 月 26、27 日，紧随天津市、贵州省、福建省等地的步伐，海南省、山东省互联网信息办公室先后开通数据出境安全评估申报通道，以指导所辖范围内开展数据处理活动的组织和个人规范、有序申报数据出境安全评估。

https://mp.weixin.qq.com/s/uZHQHb6ytfTIcTW3lOoW4g

3、上海市智能网联汽车高精度地图管理试点规定（草案）》公开征询意见

10 月 26 日，上海市规划和自然资源局发布《上海市智能网联汽车高精度地图管理试点规定（草案）》并公开征询社会公众意见。其中，通过“存储高精度地图相关数据的服务器应当设在中华人民共和国境内”、“应当建立健全全流程数据安全管理制度”等内容提出对数据安全的要求。

http://www.dsac.cn/News/Detail/30240

4、《浙江省推进产业数据价值化改革试点方案》印发

10 月 19 日，《浙江省推进产业数据价值化改革试点方案》印发，提出实施产业数据分类分级安全防护、推进工业领域数据安全管理试点工作、加强数据产品流通交易合规监管以提升产业数据安全化能力。

https://mp.weixin.qq.com/s/Zje-8Gl_NMAtk1LbJjwZrA

5、《JR/T 0258—2022 金融领域科技伦理指引》发布

10 月 9 日，中国人民银行正式发布了《金融领域科技伦理指引》（JR/T 0258—2022）标准，其中关于数据安全方面，从充分获取用户授权、最小必要采集数据、专事专用使用数据、严格采取防护措施、依法合规共享数据、主动清理留存

数据几个方面提出要求。

http://www.czifi.org/newsinfo/4509335.html

技术、产品与市场

1、日本个人信息保护委员会推出数据映射工具包

今年 10 月，日本的数据保护机构个人信息保护委员会（PIPC）专门发布了数据映射工具包，以帮助企业等私营部门“处理整个组织业务的数据，并将处理情况可视化”。

这一监管机构表示，随着 IT 社会的发展，数字化增加了每个运营商拥有的数据，企业需要面对“日益增加的正确管理数据的需求”，而数据映射工具包可以帮助组织合规地处理增加的数据。数据映射工具包内容包含了一个映射工具包文件和三个附件，三个附件分别为：（1）数据映射表中的项目示例；（2）向外国第三方提供个人数据的检查表；（3）在外国处理个人数据的检查表。

近年来，日本、新加坡等一些国家的数据保护部门纷纷推出企业隐私合规/数据合规的评估工具包，帮助本地企业达到隐私合规的标准，按法律规定保护数据。这些措施往往是通过鼓励企业的“自愿努力”来达到合规要求，具有很强的可操作性。虽然这些评估工具是非强制性的，但是也表明了这些国家对隐私保护的高度重视和贯彻执行的决心。日本 PIPC

今年的一系列操作，更是对企业在业务设计和组织处理数据（包括跨境处理数据）时考虑隐私保护的提醒和帮助，值得参考和借鉴。

https://www.secrss.com/articles/48367

2、2022 年第三季度全球数据泄露增加 70%

媒体 10 月 25 日报道，Surfshark 发布了关于 2022 年 Q3 全球数据泄露事件的报告。报告指出，2022 年第三季度共有 1.089 亿个账户被盗，比上一季度高出 70%；Q3 受数据泄露影响最大的 5 个国家和地区是俄罗斯、法国、印度尼西亚、美国和西班牙；虽然俄罗斯的泄露总数最多（2230 万），但法国的数据泄露密度最高，平均每 1000 人就有 212 个泄露账户；在过去十年中，美国仍然是被攻击最多的国家。

https://www.infosecurity-magazine.com/news/data-breaches-rise-by-70-q3-2022/

3、“数据自主保护”技术的未来

数据泄露防护（DLP）技术是目前数据安全防护领域的事实标准之一，在远程工作模式和云计算应用大量普及之前，DLP 在组织数据泄露防护中发挥了巨大作用。但有研究人员认为，由于组织现在需要更多共享数据，企业的数据分布开

始从内部环境转向多种类型的云存储平台，这使得 DLP 的应用价值正在发生变化。

数据自主保护的核心是**在数据生产和运营体系中嵌入数据安全属性，以解决数据应用过程中的数据安全问题，其主要特点是能够根据应用程序和用户操作所处的上下文中的时间、位置、数据敏感性等因素，做出精确、智能的安全决策**。数据自主保护需要能够持续监测网络流量、应用程序活动、用户行为、端点状态及其他相关数据集，获得尽可能全面的上下文信息，并依据获取的数据分析结果采取管控行动，而不是依赖死板的规则阻断。

在数据自主保护模式中，任何解决方案（包括基于人工智能的解决方案）必须全面集成。它必须能够连接到每个系统和数据存储位置，包括原有的旧系统、云存储和共享驱动器等。它还必须支持结构化数据和非结构化数据，比如 PDF、文档和电子表格。这种方法可以向基于目的的控制不断演进，支持全面的数据访问治理。它生成满足最小特权原则所需的内容观察，还可以根据不断变化的用户角色及其他情况（比如监管框架的变化），动态调整访问权限。

https://mp.weixin.qq.com/s/6rDn1ZVfXpxm3aJOJwOXcA

4、主动安全策略有效应用的 8 个关键条件

随着企业数字化发展需求不断升级、网络接入方式更加多元，以“被动防御”为主要特征的传统网络安全防护模式面临着巨大挑战，业界对主动安全防护策略应用的期望也不断增长。

目前，主动安全策略应用的主要问题是误报率高、实施难度大、可管理性差，导致主动安全技术需求旺盛，但真正成功应用的项目还很有限。尽管被动安全任务的需求会长期存在，但企业应该从现在开始积极尝试采取更积极的措施，实现更智能、更主动的安全防护策略，从而更好地保护组织的数字资产。研究人员认为，企业在应用主动安全防护策略时，应该重点关注是否具备以下 8 个前提条件：①做好资产梳理和发现；②拥有强大的身份安全措施；③提升快速应变能力；④持续性的安全监测；⑤主动搜寻威胁；⑥高效的漏洞管理计划；⑦实战化的攻防演练；⑧发现并掌握应用新兴的安全技术、产品和标准，高瞻远瞩、洞察未来，防患于未然。

https://mp.weixin.qq.com/s/l8OFZeg21n9QFS7J03lRWw

业界观点

1、杨继东：党的二十大报告指明数字经济发展方向

党的二十大报告进一步凸显了中国高质量发展的要求和趋势。经济高质量发展的一个重要方面是建立现代化经济体系,现代化经济体系建立离不开实体经济发展。二十大报告提出,坚持把发展经济的着力点放在实体经济上。**数字经济主要包括数字产业化和产业数字化。**发展数字经济,能够推动5G网络、工业互联网、人工智能、大数据、基础软件等数字产业发展。数字技术发展又能进一步推动数实融合,通过运用数字技术对传统产业进行全方位、全链条改造,可以有效提高全要素生产率,促进传统产业数字化、网络化、智能化发展。发展数字经济,促进数字经济和实体经济深度融合,打造具有国际竞争力的数字产业集群,将是未来数字经济发展的着力点。

未来数字经济发展需要进一步坚持发展与安全并重。面对复杂的国内外经济和社会发展的风险和挑战,中国经济发展需要行稳才能致远。党的二十大报告非常强调中国发展的安全问题。**报告提出要强化经济、重大基础设施、网络、数据等安全保障体系建设。**这再次表明,数字经济发展离不开数字安全的保驾护航。**首先是关键生产技术的安全**,需要把发展

数字经济的关键技术掌握在中国人自己手中。**其次是数字经济发展涉及信息安全,这不仅涉及个人信息保护,还包括在对外开放发展过程中的数据安全等问题**。最后,也要防止数字经济发展产生的泡沫,防止数字经济过度金融化和虚拟化,严重脱离经济发展的现实情况和内在规律,进而损害整体经济的健康发展。

http://www.ciia.org.cn/news/19474.cshtml

2、李凯：数智商务的基座——企业数据安全治理

近年来，众多企业将数智化升级视为发展的重点，产业的数智化变革已经成为当前时代最大的确定性和机遇，李凯指出，企业数智化升级背后是海量的数据，因此企业数据安全治理已经成为未来数智化时代企业发展的一个重要的基础性命题。

他认为在我国，企业数据安全治理问题可以从以下几个方面研究：

第一、企业数据安全治理的标准体系、制度结构与基础理论。从理论研究层面对我国企业的数据安全治理实践进行体系化的总结归纳，实现中国特色企业数据安全治理的基础理论创新，并基于相关理论基础提出系统性的标准规范、制度结构对企业数据安全治理实践具有重大指导意义。

第二、企业数字安全治理的风险识别与防护问题。企业风险识别就是保证其快速感知内外部环境所蕴藏的各类风险，并为企业及时应对风险做好铺垫的一种科学机制，也是企业走内涵式发展模式的必然之路。

第三、企业数据安全治理监管问题。基于社会共治视角对平台企业数据安全监管进行研究，探讨如何利用新兴技术保障国家和企业数据安全，并构建平台企业数据安全监管社会共治机制意义重大。

第四、企业数据安全治理应急机制。如何构建一个统一指挥、反应灵敏、上下联动、平战结合的数据安全治理应急机制，科学有效的提高数据安全应急管理能力，维护国家安全、公共安全和社会秩序等一系列问题都迫切需要相关理论研究的指导。

第五、企业数据安全治理参与主体的协同问题。企业数据安全的保护是一个动态、多主体、长期的协作过程。因此，探究安全链上各关键主体之间的协作机制是必要且迫切的。

https://bs.nankai.edu.cn/2022/1025/c9014a488159/page.htm

3、张雷：智慧医院数据接口安全治理的思考

随着智慧医疗快速发展，网上挂号、在线问诊、电子病历、AI 影像等移动医疗为我们带来了诸多便利，沉淀了大量

敏感数据的同时，也加剧了医疗数据泄漏风险。

河北医科大学第一医院元氏院区院长张雷认为，当前智慧医院呈现勒索病毒攻击日渐频繁、个人信息泄漏频发不止的趋势，在数据安全治理方面具有数据接口资产理不清、数据接口安全业务状况不明确、数据接口安全暴露面广，被攻击风险大、传统安全防御部分失效的痛点。

对此，他提出以下解决思路提升数据安全管理、技术、合规能力，加强医护数据安全意识，实现健康医疗数据安全运营的可视、可控、可持续:

一、数据资产梳理。医院信息系统中数据量巨大，数据关系复杂，需要与众多机构进行数据交换，跨科室业务数据对接共享，跨单位数据对接共享以及开放给互联网平台等。

二、数据分类分级。在数据资产梳理的基础上还需要对医院信息系统中的数据进行合理的分类分级，在数据接口安全治理实践过程中利用数据识别探测引擎，构造了医疗行业数据分类分级规范以及目录。

三、数据安全评估。建立安全特征库与业务规则库，对应用接口进行安全态势监测，同时对在线业务与即将上线业务进行风险评估。

四、数据安全防护。在数据防护方面可考虑采取以下措施：(1)实时监测流量中的威胁攻击;(2)用旁路流量分析技术，

不影响正常业务运行;(3)对敏感数据访问行为管控,防止非授权人员的数据滥用行为。

https://chima.org.cn/Html/News/Articles/15866.html

4、翟云：准确把握数据流动和安全发展的平衡点

随着数字政府建设号角全面吹响并逐步驶入快车道，数据流动和安全发展的矛盾逐渐显现：在开放共享过程中，数据泄露、数据贩卖、数据滥用事件频发，为个人隐私、商业秘密、国家重要数据存储与使用带来了严重的安全隐患。

科学把握数据流动和安全发展的平衡之策。找准数据流动和安全发展的平衡点，既应立足当下消解数据流动中的安全隐患，更需着眼未来科学建构安全有序的发展环境。一是建立数据要流动、流动促发展、发展要安全的总体目标。二是营造良好的数据流动法治生态。法治是数据平稳有序流动的“金钥匙”。

与此同时，需立足找准二者的平衡点，多措并举打出系列“组合拳”，无缝隙拉起数据流动的安全绳：

一是筑牢技术防线。如可以利用区块链分布式、透明性、可追溯性和不可篡改性等特征，促进数据治理主体权益公开化、流动过程透明化，不断增强数据流动的时效性和安全性。

二是筑牢权责防线。聚焦数据确权这个核心利益问题，

加快数据清权确权，建立数据权责清单，让各使用主体在数据全生命周期流动过程中以规治数、按权用数、决策循数。

三是筑牢应用防线。随着数据流动逐渐呈现出应用场景复杂化、服务要求实时化、终端渠道在线化的发展态势，推进数字政府建设必须进一步加强网络安全、数据安全和应用安全意识，将安全理念、安全技术、安全机制与数字政府同步规划、同步建设、同步使用，真正给数据流动戴上“安全帽”。

http://www.echinagov.com/viewpoint/331500.htm

5、田力：数据治理助推隐私保护生态构建

10 月 10 日，由上海华瑞银行与中国人民大学国际货币研究所、金融科技研究所联合主办的“华瑞金融科技系列沙龙”第 3 期线上研讨会成功举办。中国国际经济咨询高级研究员、北大光华博士后田力作题为《数据治理助推隐私保护生态构建》的主题报告。

其中，田力在“以数据治理强化个人信息保护”部分从数据治理视角出发探讨当前企业、机构或组织数字化转型发展中的“致命”问题，也就是数据安全、隐私保护的问题。他提出了数据安全管理的步骤：

第一步，识别敏感数据资产和分级分类管理，分级分类管理也是非常重要的数据安全、数据保护关键工作，例如某

些数据是个人敏感数据，包括个人身份信息、医疗信息、金融信息等，应当给予较高级别的保护。

第二步，在企业中查找敏感数据，这取决于数据存储的位置，安全要求有所不同。大量敏感数据若存于同一位置，如果这个数据遭到破坏会带来极高风险。

第三步，确定保护每项资产的方法，选择相应的保护技术或安全措施。

第四步，识别数据和业务流程如何交互，业务如何融合。

同时认为个人信息保护的数据治理路径包含四步走：

第一步，数据确权，数据权利归属于平台、个体或者政府的初始配置将影响数 据市场的发展和社会福利水平，数据的界权和交易需要平衡数据市场发展和个人权利保护。

第二步，数据分级分类管理。

第三步，制定隐私保护制度。

第四步，选择或开发隐私技术。

https://mp.weixin.qq.com/s/ZSXL3zXqmFB-VJtwyK9D6A

数据安全事件

1、英国一公司因暴露员工数据被监管机构罚款 440 万英镑

10 月 24 日，据外媒报道，英国数据监管机构对一家设施管理外包和建筑公司处以 440 万英镑的罚款，原因是该公司因勒索软件攻击暴露了员工数据。

黑客于 2020 年 3 月下旬侵入了 Interserve Group Limited，破坏了包含 113,000 名员工个人数据的四个人力资源数据库的机密性。暴露的数据涵盖联系方式和识别信息，包括出生日期、婚姻状况、受抚养人和工资金额等。

英国信息专员办公室表示，该公司未能采取适当的安全措施来防止入侵，包括运行不受支持的 Windows 服务器操作系统版本和使用过时版本的 McAfee 防病毒软件。

https://www.bankinfosecurity.com/uk-firm-fined-for-poor-security-prior-to-ransomware-attack-a-20317?&web_view=true

2、美国 FTC 因数据安全问题处罚优步旗下电商平台及其 CEO

10 月 24 日，美国联邦贸易委员会（FTC）发布公告称，拟对优步旗下酒类电商平台 Drizly 及其首席执行官（CEO）James Cory Rellas 采取执法行动，以解决该公司的数据安全

问题。

FTC 认为，由于 Drizly 及其 CEO 未能尽到数据安全义务，约 250 万消费者的个人信息被泄漏。具体而言，FTC 提出了以下四项指控:（1）Drizly 和 Rellas 未能采取合理的保护措施来保护其收集和存储的个人信息，例如设置双重身份验证和访问限制、制定数据安全政策或进行相关员工培训；（2）将关键数据库信息存储在不安全的软件开发和托管平台上；（3）Drizly 没有任命高级管理人员专门负责数据安全事务，也没有进行网络监控以防止未经授权的访问或个人数据删除；（4）个人信息的泄露导致黑客和信息窃贼可以对消费者实施欺诈性行为。

对此，FTC 拟发布命令要求 Drizly:（1）销毁其收集的所有对于向消费者提供产品或服务来说非必要的个人数据，并向委员会报告相关情况；（2）避免未来对此类非必要个人数据的收集和保存，并在网站上公开说明其数据收集清单及理由；（3）进行全面的信息安全合规并建立安全保障措施，以防止数据安全事件再度发生。

https://mp.weixin.qq.com/s/4Suk8n1C4uu22qKujf9sLA

3、印度塔塔电力公司数据被勒索团伙公开泄露

勒索软件组织 Hive 上周二在其数据泄露网站上公布了

塔塔电力公司（Tata Power）的数据。作为跨国企业集团塔塔集团的子公司，塔塔电力是印度最大的综合电力公司，总部位于孟买。本月初，该公司遭遇攻击发生数据泄露，勒索软件组织 Hive 宣称对此次攻击负责。

一位安全研究人员 Rakesh Krishnan 分享了被盗数据的屏幕截图（上图），其中似乎包括塔塔电力员工的个人身份信息(PII)、国民身份证号、PAN（税号）、工资信息等。此外，泄露数据还包含工程图纸、财务和银行记录以及客户信息。

https://www.secrss.com/articles/48314

4、澳洲物业公司 SSKB 遭网络攻击 黑客勒索 46 万澳元

10 月 30 日，据报道，澳大利亚物业管理公司 SSKB 遭网络攻击。黑客称，已经盗取该公司 200GB 的数据，并欲勒索赎金 46 万澳元。这是澳洲近期发生的又一起网络安全事件。

黑客已经在暗网公布了进行网络攻击的“证据”，并要求 8 天内付款赎金，否则将把数据公布。黑客称，被盗内容包括建设项目、金融文件、高管邮件、合同以及协议等。SSKB 尚未对该报道做出回应。

https://new.qq.com/rain/a/20221030A05GCR00

5、伊朗原子能组织遭黑客攻击，大量敏感数据泄露

10 月 25 日，据外媒报道，Black Reward 组织声称已经侵入伊朗政府，并渗出了与他们的核计划有关的敏感数据。

伊朗原子能组织在官网（aeoi.org.ir）发表声明称布什尔核电站的电子邮件服务器遭到黑客攻击。该组织将责任归咎于某国政府，但一个名为 Black Reward 的伊朗黑客组织声称对此次攻击行为负责。该组织在帖子中声称，该黑客攻击是为了支持全国范围内的一场持续的抗议活动（起因是一名伊朗年轻女子 Mahsa Amini 因未能正确佩戴头巾遭拘留并在警方拘留期间死亡）。

该组织发布了一个指向其 Telegram 频道的信息下载链接并表示，这些信息包括大约 8.5 万封电子邮件的“经过清理的、可用浏览器查看的版本”。泄露的信息包括布什尔发电厂各部门的管理和运营时间表，以及在那里工作的伊朗和俄罗斯核专家的签证和护照信息、财务收据以及与当地和外国组织的协议。

https://www.secrss.com/articles/48251

6、汤森路透 3 个数据库处于公开访问状态，至少包含 3TB 敏感数据

据 Cybernews 10 月 27 日报道，**跨国传媒集团汤森路透**

公司至少有三个数据库处于开放状态，访客无需验证即可访问，里面包含敏感客户和企业数据以及明文格式储存的第三方服务器密码。攻击者可以利用这些细节进行供应链攻击。

Cybernews 研究小组发现，汤森路透至少保留了三个任何人都可访问的数据库。其中一个是面向公众的 ElasticSearch 数据库，**3TB 大小**，包含该公司各个平台的最新和最敏感信息。汤森路透已经发现该问题，目前已修复。

https://www.freebuf.com/news/348202.html

7、黑客使用 PoS 恶意软件窃取超过 16 万张信用卡的信息

媒体 10 月 25 日称，Group-IB 发现了两个 PoS 恶意软件，用于从 PoS 支付终端窃取 167000 多张信用卡的数据。据悉，被盗的数据转储可以通过在黑客论坛上出售给运营团伙带来高达 334 万美元的净收入。Group-IB 确认了与两个 PoS 恶意软件相关的 C2 服务器，称在 2022 年 2 月至 9 月期间，MajikPOS 和 Treasure Hunter 分别窃取了 77428 和 900024 条支付记录。大部分被盗信用卡是由美国、波多黎各、秘鲁、巴拿马、英国、加拿大、法国、波兰、挪威和哥斯达黎加的银行发行的。目前，尚不清楚攻击者身份，以及数据是否已被出售。

https://thehackernews.com/2022/10/cybercriminals-used-two-

pos-malware-to.html

8、台湾全岛个人信息被放在网上兜售，经调查至少 20 万条真实信息

10 月 30 日，据台媒报道，台湾地区户政系统传出遭黑客入侵，有网友在海外论坛 BreachForums 上贩售 20 万笔台湾民众户籍资料，并宣称手上有全台 2300 万民众资料。台湾“调查局”本月 25 日获报后即展开追查，初步调查确认目前释出的 20 万笔集中在宜兰地区，且资料都吻合，宜兰县长林姿妙、民进党“立委”陈欧珀等人的个人资料都在其中。

调查人员追查后发现，20 万笔台湾人的户籍资料，内容非常详细，包括婚姻状况、居住地址、学历等。据了解，目前在“Breach Forums”论坛公开的 20 万笔资料均为真实信息，黑客将 2300 余万笔资料“包裹”出售，一包售价五千美金，相当于十六万元新台币。

https://www.secrss.com/articles/48453

9、票务巨头 See Tickets 数据泄露两年半未察觉

10 月 27 日报道，法国媒体巨头维旺迪旗下的 See Tickets 是全球领先的国际票务服务提供商之一，在欧洲和北美市场零售和分销音乐、节日、戏剧、体育、喜剧、展览等各种娱

乐活动的门票，与全球 5000 多家客户合作。

近日，See Tickets 因数据泄露事件曝光登上媒体头条，并在美国多个州发布通知披露了违规消息，但尚未发布任何官方声明。

根据 See Tickets 发给客户的个人和财务数据暴露通知，该数据泄露事件已经持续了两年半多，攻击者可能通过在 See Tickets 网站上注入的 Skimmer 脚本窃取了敏感的支付卡数据。此后，See Tickets 花了八个月的时间确定泄露的支付卡数据，包括以下内容：全名、邮政编码、CVV 编号、支付卡号、卡有效期、实际地址。

https://www.secrss.com/articles/48363

10、黑客瞄上了中国游戏产品《原神》，米哈游或遭大规模数据泄露

10 月 29 日报道，全球火热的二次元开放世界游戏《原神》(Genshin Impact)的开发商米哈游(海外公司名 HoYoverse) 遭遇了大规模数据泄露。

上周末，大量的信息在网上被分享，揭示了从 3.3 到 3.8 版本的新角色、任务和事件的细节。据 GamesRadar 报道，这是一个几乎前所未有的非法转储信息量，相当于这款免费在线服务游戏大约 36 周的开发内容。媒体已联系 HoYoverse

了解最新情况。

http://cn-sec.com/archives/1378601.html

11、Medibank 客户数据遭受网络攻击泄露，市值单日蒸发 17.5 亿澳元

10 月 28 日报道，Medibank 隐私部门已经证实，黑客从拥有约 100 万客户记录的系统中窃取了敏感的健康信息，同时不法分子威胁要传播这些信息，除非公司支付赎金。近日 Medibank 又表示他们已经从黑客那里收到了 100 名客户的数据样本，并被警告预计未来几天受影响的客户数量将大幅增长。

Medibank 首席执行官大卫·科奇卡尔（David Koczkar）表示，该样本包括指定客户在哪里接受治疗以及治疗哪些情况的代码。数据范围可以从扭伤手腕到吸毒、酗酒。样本数据涉及的业务总共有大约 100 万客户，数据包括姓名、地址、出生日期、医疗保险号码和联系信息。

Medibank 公司表示，预计此次网络攻击造成的数据泄露事件将给公司带来 2500 万澳元至 3500 万澳元的损失，对客户的赔偿金额目前仍无法预估。

https://mp.weixin.qq.com/s/zVVnkDrWVZ9_56QKfxwCwg

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/