国盟信息安全通报

2019 年 4 月 01 日第 189 期

国盟信息安全通报

（第 189 期）

国际信息安全学习联盟

2019 年 4 月 01 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 196 个，其中高危漏洞 54 个、中危漏洞 114 个、低危漏洞 28 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 62%），其中互联网上出现“LayerBBSQL 注入漏洞、ThinkCMF SQL 注入漏洞（CNVD-2019-07961）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1788 个，与上周（1675 个）环比增长 7%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2019 年 3 月 18 日—2019 年 4 月 1 日）.....4
➢漏洞引发的威胁（2019 年 3 月 18 日—2019 年 4 月 1 日）.....5
➢漏洞影响对象类型（2019 年 3 月 18 日—2019 年 4 月 1 日）.....5
三、安全产业动态 6
➢通向网络强国的征程上稳步前进.....6
➢大数据时代，用户不能成为“透明人”！.....11
➢历史和国际比较视角 DPO 法律制度探源.....12
➢Gartner: 2019 年七大安全与风险管理趋势.....17
四、政府之声 19
➢〔2019〕85 号文加强支付结算管理防范电信网络新型违法犯罪答记者问.....19
➢全国人力资源社会保障网络安全和信息化工作座谈会召开.....23
➢网信办发布第一批 197 个境内区块链信息服务备案编号.....23
➢2018 年全国未成年人互联网使用情况研究报告发布.....24
五、本期重要漏洞实例 25
➢Cisco IOS XE Software 信息泄露安全漏洞.....25
➢IBM Sterling B2B Integrator XML 外部实体注入安全漏洞.....25
➢WordPress social-warfare 插件跨站脚本漏洞.....26
➢Mozilla Firefox 释放后重利用漏洞.....27
六、本期网络安全事件 28
➢盗 30 万条个人信息叫价 1 比特币网偷被警方抓获.....28
➢24 岁黑客进入任天堂内部数据服务器致损失 180 万美元.....29
➢华硕回应 Live Update 软件漏洞：仅数百台受到影响.....30
➢多项腾讯服务宕机：因运营商光纤故障.....32
➢浪潮工程师监守自盗,窃取硬件网上转卖获刑三年.....33
➢饿了么等 25 款 APP 被曝收集敏感个人权限.....34

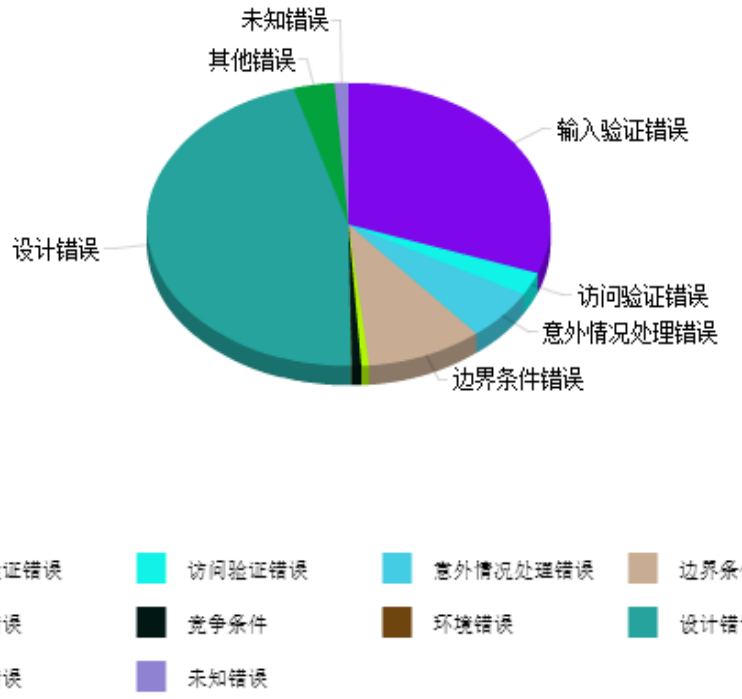
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

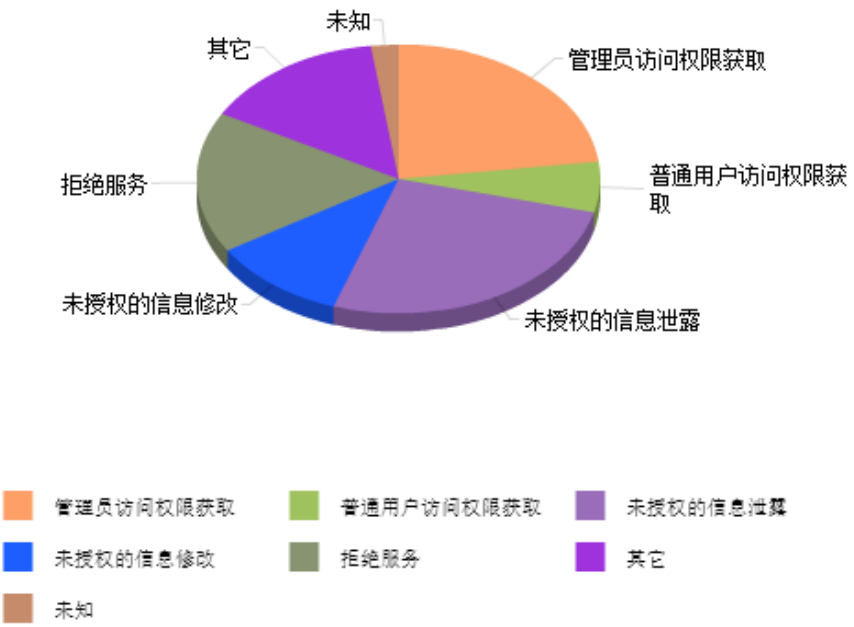
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 196 个，其中高危漏洞 54 个、中危漏洞 114 个、低危漏洞 28 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 62%），其中互联网上出现“LayerBBSQL 注入漏洞、ThinkCMF SQL 注入漏洞（CNVD-2019-07961）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1788 个，与上周（1675 个）环比增长 7%。

二、安全漏洞增长数量及种类分布情况

➢ 漏洞产生原因（2019 年 3 月 18 日—2019 年 4 月 1 日）



➢ 漏洞引发的威胁（2019 年 3 月 18 日—2019 年 4 月 1 日）



➢ 漏洞影响对象类型（2019 年 3 月 18 日—2019 年 4 月 1 日）

三、安全产业动态

➢ 通向网络强国的征程上稳步前进

——写在中央网络安全和信息化委员会成立一周年之际

为加强党中央对网信工作的集中统一领导，强化决策和统筹协调职责，2018 年 3 月，中央网络安全和信息化领导小组改为**中央网络安全和信息化委员会**，负责网信领域重大工作的顶层设计、总体布局、统筹协调、整体推进、督促落实。

去年 4 月，全国网络安全和信息化工作会议在京召开。习近平总书记出席会议并发表重要讲话。他强调，信息化为中华民族带来了千载难逢的机遇。我们必须敏锐抓住信息化发展的历史机遇，加强网上正面宣传，维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦作出新的贡献。习近平总书记关于网络强国的重要思想，深刻回答了事关网信事业发展的一系列重大理论和实践问题，为加快推进网络强国建设指明了前进方向、提供了根本遵循。

从融入日常生活的社交通信软件到电商购物平台、移动支付应用；从推动放管服、覆盖连接全国的电子政务系统到正在大力研发的 5G、大数据、物联网新兴产业技术……中央网络安全和信息化委员会成立一年来，我国网信事业快速健康发展，网络内容建设持续加强，网络安全保障能力稳步提升，信息技术和数字经济蓬勃发展，网络空间国际合作不断深化，持续为全球互联网发展治理贡献中国经验、中国智慧。

内容建设守正创新，网络空间日益清朗

2019 年 1 月，习近平总书记在主持中共中央政治局第十二次集体学习时发表重要讲话。他强调，要“深刻认识全媒体时代的挑战和机遇”“全面把握媒体融合发展的趋势和规律”“推动媒体融合向纵深发展”。习近平总书记指出：“正能量是总要求，管得住是硬道理，现在还要加一条，用得好是真本事。”

过去一年，媒体融合发展取得积极成效，网络内容建设和管理工作不断展现新气象、实现新作为。网上正面宣传守正创新，既坚持正确的政治方向、舆论导向、价值取向，又深入推进理念、内容、形式、方法、手段等创新，宣传的质量和水平进一步提升。

习近平新时代中国特色社会主义思想网上宣传不断往深里走、往实里走，党的创新理论通过互联网“飞入寻常百姓家”。网上重大主题宣传出新出彩、亮点纷呈，党的声音成为网络空间最强音。宣传思想战线主力军加速进入互联网主战场，传播力、引导力、影响力、公信力进一步提升。

一年来，依法管网治网进一步加强，网络舆论环境持续净化，网络生态日趋良好，网上正能量更加强劲、主旋律更加高昂。

联合整治炒作明星绯闻隐私和娱乐八卦、约谈自媒体平台、将违规网络主播纳入跨平台黑名单……2018 年以来，国家主管部门协同发力，对当前社交媒体及网络视频平台上存在的违法违规行为打出一系列“组合重拳”。

2018 年 11 月，《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》对社会公布，旨在督促指导具有舆论属性或社会动员能力的信息服务提供者履行法律规定的安全管理义务，维护网上信息安全、秩序稳定，防范谣言和虚假信息等违法信息传播带来的危害。

2018 年 12 月，《金融信息服务管理规定》发布，旨在加强金融信息服务内容管理，提高金融信息服务质量，促进金融信息服务健康有序发展。

2019 年 1 月，《区块链信息服务管理规定》发布，旨在明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，防范区块链信息服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。

一项项政策，剑指网络空间的不良现象与突出问题。

围绕侵犯公民个人信息的犯罪行为，公安部、工信部、网信办等部门加大与最高人民法院、最高人民检察院协作配合力度，形成治理合力。2018 年以来，公安部等部门持续开展打击整治网络侵犯公民个人信息安全的“净网”专项行动，有力筑牢公民个人信息防护墙。

一年来，网络社会组织“同心圆”工程在各地深入开展，各级各类网络社会组织积极发

挥作用，有力推动互联网行业自律。

2019 年初，一批学习类 App 企业共同发布行业自律倡议，倡导建设高效、健康、有价值的“互联网+教育”行业，加强审核，杜绝色情暴力、网络游戏、商业广告及违背教育教学规律等内容。

从出台《互联网新闻信息服务管理规定》《互联网用户公众账号信息服务管理规定》等规范性文件，为依法治网、办网、用网提供基本依据；到开展“净网”“剑网”“清源”“护苗”等系列专项治理行动，网络谣言、网络色情等网络乱象得到有效整治；再到“全国网络诚信宣传日”“中国好网民工程”等一批活动成功实施，公民网络素养大幅提升。

信息技术高速发展，数字经济势头强劲

习近平总书记强调，网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步。

“刷脸”入住的民宿、招手即停的无人驾驶车、在家就能看名医的智慧医疗、不用带钱包走遍全镇的移动支付……已经连续举办五届世界互联网大会的乌镇，既是白墙黛瓦、桨声欸乃的千年水乡，又处处闪耀着互联网和数字经济的因子。

手机扫一扫二维码，共享单车上的锁应声打开；一句语音指令，灯光为你点亮家的温暖，窗帘也缓缓拉上；一觉醒来，智能穿戴设备已将你一夜的睡眠质量向手机“报告”……物联网技术应用已悄然进入人们的日常生活。

基于 5G 技术，医生通过屏幕就可以实时、全景看到远在千里之外的救护车上的情景，并通过遥感、遥控、遥测等技术直接进行心电图和 B 超检测。

“相当于把医院急救前移到了上救护车的那一刻，将来还可以实现远程手术等更为高端的医疗应用。”浙江大学医学院附属第二医院急诊科副主任医师李强说。

新时代蕴育新业态，新征程召唤新使命。

一年来，互联网与实体经济融合发展的趋势日趋明显。云计算、工业互联网成为驱动企业数字化转型的重要动力，大型互联网平台企业持续通过互联网、大数据、云计算、人工智能等技术赋能实体经济，形成一批行业领先的工业互联网平台。

一年来，我国在大数据、人工智能、5G 等领域科研能力不断增强。根据第 43 次《中国互联网络发展状况统计报告》，我国多项 5G 技术方案进入国际核心标准规范，推进速度、质量均位居世界前列；截至 2018 年 11 月，我国人工智能相关专利申请量已超过 14.4 万件，占全球申请总量的 43.4%，居全球首位。通过数字基础设施、数字消费者、数字产业生态、数字公共服务、数字科研五方面综合评价数字经济的水平、结构与发展路径，我国全球排名第二。

一年来，网络安全保障能力和水平显著提升，有效应对和化解新形势下的网络安全威胁。一批基于大数据、人工智能、区块链的网络安全技术逐渐成熟，网络安全产业规模再创新高，网络安全产品和服务的国际竞争力进一步增强。

一串串数据、一项项成果，折射出我国网信科技事业发展的一系列历史性成就、历史性变革。

更好顺应人民期待，大力提升百姓福祉

常年网购的杭州白领陈粟今年感受到一个显著变化：“过去在一些网络平台上购买机票，总是一不留神就买了默认搭售的酒店券、打车券，让人头疼。这些天我买机票时发现默认搭售的项目已经取消了，真是大快人心。”

购买“水军”刷好评、擅自删除评价、暗中搭售、利用大数据“杀熟”……部分电商利用信息不对称，严重损害消费者的知情权、选择权等合法权益。针对这些问题，今年 1 月 1 日起正式实施的电子商务法，进一步营造了公平竞争的网络市场秩序，堪称一剂“对症良药”。

习近平总书记指出，网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。

人脸识别、无人超市、VR 在线教育、无人驾驶舱、人工智能主播……数字技术正在将人们想象中的智能新生活变为现实。

上课用的电子白板换成了触摸屏、名师课程可“点单式”播放……今年全国两会期间，全

国人大代表、山东省临沂北城小学校长张淑琴展示了当地教育信息化成果。“信息技术与教育教学深度融合，让很多乡村学校享受到优质教育资源，学生的学习效果明显提升。”

一年来，各级政府部门积极推进政务服务和民生领域的信息化应用，与公众生活息息相关的应用持续拓展和延伸，更好地满足人民日益增长的美好生活需要。

随着“互联网+政务服务”深化发展，各级政府依托网上政务服务平台，推动线上线下集成融合，全国统一、多级互联的数据共享交换平台加强建设，通过“数据多跑路”，实现“群众少跑腿”。从“最多跑一次”到“不见面审批”，从“粤省事”再到“秒批”，政务服务创新层出不穷……

2018 年 6 月，中央网信办等四部门联合发布《2018 年网络扶贫工作要点》，推进网络覆盖、农村电商、网络扶智、信息服务、网络公益五大工程向纵深发展。

山西省隰县果农王平曾是村里的建档立卡贫困户，2017 年靠发展农村电商摘掉了贫困户的“帽子”，2018 年在网上卖水果，年收入超过 10 万元。依靠农村电商发展，2018 年山西省贫困地区农产品网络销售金额达 33.2 亿元，带动 27.4 万贫困人口增收。

随着乡村振兴战略推进，农村电子商务综合示范基地建设不断深入，数字经济与乡村振兴得以密切结合，成为推动全面小康社会建设的重要措施。

四川省眉山市民王凯去年底在移动营业厅办理套餐时发现，每个月只需 58 元，除了通话分钟数和流量外，还可获赠宽带和电视收视服务，家庭成员间通话全免费。

网络覆盖越来越好，网速越来越快，资费逐步降低，流量套餐包越来越实惠，全国乃至海外漫游压力不再……2018 年，包括全面取消手机流量漫游费等多项提速降费措施，让百姓得到了实实在在的优惠。

从 1997 年到 2018 年，我国网民数量从 62 万增长到 8.29 亿，互联网普及率从 0.03%增长至 59.6%，网络零售交易额规模已居世界第一。未来 5 到 10 年，我国还计划建成全球最大规模的 IPv6 商业应用网络，实现下一代互联网在经济社会各领域深度融合应用。

电子政务、农村电商、在线教育、分享经济、智慧出行、移动支付、远程诊疗……互联网新产品新业态竞相涌现，推动全社会创新创业热潮的同时，有力促进了基本公共服务均等化。互联网新动能推动民生水平再上台阶，网信事业发展成果正越来越好造福人民。（来源：新华社）

➢ 大数据时代，用户不能成为“透明人”！

移动互联网时代，智能手机如同人的体外器官，而手机上安装的 APP 就像组成细胞。可以说，过好移动生活，首先从用好智能手机的 APP 开始。**然而，现实不如理想中那样美好。**

近日，上海市消保委发布了一项评测结果，针对的是 39 款网购、旅游、生活类常用手机 APP 涉及个人信息权限问题。评测发现，有超过 6 成的 APP“不老实”，在用户安装时申请了很多敏感权限，却不提供实际功能。这其中包括读取通讯录、电话权限、短信权限、定位权限等隐私信息，成为不少消费者的“新痛点”。

新痛点从何而来？如，当一些 APP 读取个人通讯录后，会给上面的联系人推送垃圾信息，让人不胜其扰；又如，当一些 APP 获取麦克风权限后，只要捕捉到一些关键词，就会推荐相关产品；再如，当一些 APP 读取摄像头信息后，会在后台被“悄悄”打开，进行拍照。诸如此类，当人们使用 APP 时，却在被 APP“利用”，个人隐私信息、数据权限被一一调取。可以说，这既非移动生活的应有模样，更不是智能算法的应有功能，而是以精准、服务之名，让用户穿上了“皇帝的新装”——自我感觉良好，却是在信息裸露中奔跑。

用户之所以不能掌控自己的 APP 权限，既有利益因素，又是技术霸权。从利益看，不少 APP 开发者争夺用户数据资源，不同 APP 之间也存在竞争关系，只要有获取隐私信息的应用存在，就会引致各家一哄而上，“你要我也要”。从技术看，用户处于技术弱势地位，无论获取隐私权限是否被告知，只要想使用这一应用工具，除了“同意”，别无选择，更甚者是在毫不知情时就被索取了权限，连信息在哪、被谁用了，都一无所知。足见，作为用户，在 APP 权限上几无话语权，多数情况是“任人宰割”，这样的局面应该改变了。

这局面应该改变，是因为数据时代需要数据安全。越是大数据时代，用户越不能成为“透明人”。可以想见，通过不正当渠道获取的数据资源，很难被妥善保存，更谈不上有效利用、合理利用、合法利用。信息泄露、信息贩卖、“大数据杀熟”等事件时有发生，让用户的数据焦虑越来越重，一旦失去起码的数据安全保障，就难以建立数据信任，最终受损害的，不仅是用户，更是一个应用、一个行业乃至一个领域的数据体系。如此，数据时代这个大厦不免建在脆弱的地基上，怎能牢靠稳固？

这局面应该改变，是因为数据时代需要数据权利。安全是第一位，权利更要优先。数据来自于用户，但不能无条件地让渡数据权利。很显然，一些 APP 就是漠视了用户的数据权利，才会如此肆无忌惮地滥用平台的数据权力。关键问题不是 APP 能否获取用户的个人信息权限，而是如何获取、是否告知、怎么使用。用户数据权利与平台数据权力之间存在巨大张力，倘若处理不好，就像双手拉扯的皮筋，突然断裂，伤及双方。这就需要，平台不能任性索权，要事先说得明明白白；用户不能随意授权，要做到认可放心；监管方不能放任发展，要在法律与治理层面逐步“加压”，把选择权还给用户、把安全感还给用户。

大数据时代是美好时代，改变了生活，但不能左右生活。面对数据焦虑，真正需要改变的是人们对技术的驾驭方式，以及工具化的心态。惟其如此，手机才不会成为“手雷”。（来源：人民网）

➢ 历史和国际比较视角 DPO 法律制度探源

2018 年 5 月 25 日正式实施的欧盟《通用数据保护条例》（GDPR）给全球隐私实践带来巨大震动。GDPR 规定的诸多制度都对各国企业产生了不同程度的影响，其中，值得关注的一项是数据保护官（Data Protection Officer，DPO）制度。GDPR 强制要求欧盟的所有公共机关以及核心工作，包括系统性地监控大规模数据主体或处理大规模特殊类别数据的私营组织，必须任命 DPO 以确保 GDPR 合规。第 29 条工作组（Article 29 Working Party，WP29）也在其《数据保护官指引》（Guidelines on Data Protection Officers, WP243）中建议，无论是否有法律要求，“最好”都要任命 DPO。简言之，DPO 制度是 GDPR 基于问责制合规框架的重要基石。除了确保组织 GDPR 合规之外，DPO 也充当各利益相关人之间的中间人角色（包括监督机构、数据主体和组织内的业务部门等）。实际上，GDPR 中的 DPO 制度并非首家，也并非独此一家。正是由于这一要求，全球范围的 DPO 岗位需求指数性增长，相关人才储备

呈现巨大缺口。

一、DPO 法律制度的历史演进

诚如 WP29 发布的《数据保护官指引》中所言，DPO 并非是一个全新的概念，实则颇有历史渊源。

在 GDPR 出台之前，于 1978 年发布的《德国联邦数据保护法案》（BDSG）中就已经出现了关于 DPO 的强制性要求。德国 BDSG 要求雇佣不少于 9 名员工长期从事自动化数据处理或雇佣不少于 20 名员工从事非自动化数据处理的公司必须任命数据保护官（DSB）。根据 BDSG，DSB 必须具备适当的资格，除严重违反职责外，不得予以解雇；DSB 应当在业务开始后的 1 个月内以书面形式任命；若 DSB 还想担任其他职务，则不应与其应履行的 DSB 职责发生冲突；DSB 岗位应直接位于管理层之下；不遵守 DSB 强制性规定可能导致巨额罚款。事实上，德国 BDSG 提出的这一强制性制度在现实中受到许多公司的欢迎，因为这是一个“自我监督”的机制，客观上大大减轻了履行数据相关行政手续的负担。

欧洲 1995 年的《数据保护指令》（Directive 95/46/EC，95 指令）中也引入了 DPO 概念。根据 95 指令，当数据控制者根据所在国法律规定任命个人数据保护官，以确保内部合规、数据处理活动登记、数据主体的权利与自由受到保护等，成员国可以简化或免除数据控制者的通知和登记的义务；在数据处理活动开始前，应当由监督机关或数据保护官进行先期检查。然而，由于 95 指令的法律效力问题，需经由欧盟成员国转化为国内法之后方可实施，其关于 DPO 的制度并不是强制性的。2011 年，欧洲委员会重新审视了 95 指令的相关条款，并提

出考虑施行强制性的数据保护官制度，要求所有数据处理组织都任命数据保护官。这一想法引起了广泛争论，有人认为，强制性的 DPO 制度目的在于减轻企业的行政负担，但是，对能否实现存疑；95 指令的规定已经放宽了任命 DPO 实体的通知和登记的义务，也只有包括德国、法国在内的少数几个欧盟成员国采用这一模式。也有人认为，这样的强制性要求会给中小型企业带来沉重负担。还有人认为，这有可能有助于企业提升 DPO 的重视程度，毕竟 DPO 在欧洲仍是中低阶层的管理岗位，与美国的首席隐私官（Chief Privacy Officer）的中心战略地位大有不同；公司管理者关于数据治理的意识觉醒确实是个挑战，DPO 的角色应当向美式首席隐私官的方向发展。

2001 年发布的第 45/2001 号条例（Regulation No. 45/2001，2001 条例）要求所有的欧洲共同体机构（European Community Institutions and Bodies）都必须任命 DPO。2001 条例要求，DPO 确保共同体机构正确执行条例的规定，并确保数据主体以及数据控制者均了解他们的权利和义务；DPO 还应负责响应并配合欧洲数据保护监督员（European Data Protection Supervisor，EDPS）的要求；对 DPO 履行职责的独立性作出规定，并要求确保向 DPO 提供必需的人力和资源；在数据处理活动开始前应当通知 DPO，而 DPO 应当将收到通知的处理活动做好登记。

多年来，任命 DPO 的实践已在许多国家得到发展，助力公司管理者对于数据管理的意识觉醒，帮助各实体更好地履行法律法规规定的义务，而 2001 条例下的 DPO 与 EDPS 协同机制也颇具成效。虽然在 GDPR 出台之前，私人部门尚未普及 DPO 岗位设置，但是，对于所有欧洲共同体机构而言，无论大小几何，无论核心业务为何，任命 DPO 作为一项强制性的法律规定，已经超过 15 年的时间。2018 年 5 月正式施行的 GDPR，将强制性的 DPO 制度推及所有的公共机关和众多的私营组织，成为实现 GDPR 问责制、促进企业合规的重要工具，也成为企业的商业竞争优势。

二、DPO 法律制度的国际比较

GDPR 下的 DPO 制度有可能是目前全球范围内最系统化的 DPO 制度，而 GDPR 也允许各成员国在 GDPR 的规定之上提出更为详细或更为严格的要求，因此，各欧盟成员国的 DPO 制度也存在差异。此外，除了 GDPR 下 DPO 制度之外，亦有欧盟以外的其他国家/地区规定了或相似或不同的 DPO 制定或负责人制度。

根据 GDPR，若数据控制者或处理者为公共机关，核心活动需要定期地、系统化地、大规模地对数据主体进行监控，或核心活动包括大规模的敏感个人数据的处理，则其必须任命 DPO。GDPR 允许企业集团任命一名 DPO 负责多个法律实体，条件是各机构可以轻松接触该

DPO。GDPR 要求 DPO 具有数据保护法律和实践方面的专业知识，因而也允许将 DPO 职务外包给外部服务提供商。数据控制者和数据处理者应当确保 DPO 及时介入与数据保护有关的所有问题；DPO 应当向最高管理层负责，且在履行职务时不应被领导，也不应因履行职务而被解雇或处罚。GDPR 规定的 DPO 职责包括：就遵守 GDPR 和其他欧盟或成员国法律提供咨询意见；监督组织的法律、内部制度的合规，包括分派职责、提高认识、员工培训等；在有需要时对数据保护影响评估提出建议、进行监督；作为联系人并与监督机关合作等。

GDPR 下的 DPO 制度实际上是“开放式条款”，允许各成员国作出进一步规定，其中，最具代表性的是德国的新 BDSG。德国新 BDSG 与 GDPR 在同一天正式实施，旨在配合 GDPR 的施行。德国新 BDSG 要求必须任命 DPO 的“准入门槛”比 GDPR 低许多——若公司长期雇佣至少 10 名员工进行自动化数据处理，若公司进行的数据处理需要经过数据保护影响评估，若公司商业上处理数据的目的是为了转让（即便是匿名化的转让）或为了市场或舆论调研，则公司都必须任命 DPO。除德国之外，比利时法律也对应当任命 DPO 的场景作出规定；奥地利法律则规定了 DPO 及其下属负担保持特定数据主体身份秘密的义务，同时享有一定的沉默权。

在亚太地区，菲律宾、新加坡、印度有较为成型的 DPO 制度。菲律宾 2012 年的《数据隐私法》要求个人信息控制者（personal information controllers，PICs）和处理者（personal information processors，PIPs）任命 DPO，负责确保 PIC 或 PIP 的行为符合《数据隐私法》的规定。菲律宾隐私委员会（National Privacy Commission of Philippines，NPC）指出，DPO 必须是 PIC 或 PIP 的雇员，但是，也允许法律另有规定或 NPC 许可的例外情况。例如，相关公司可以任命或指定特定成员公司的 DPO 主要负责整个集团的数据保护合规，但是，这需要经过 NPC 的许可，而其他成员公司则应当有隐私合规专员（compliance officer for privacy，COP）作为 DPO 的助手。DPO 或 COP 的职责允许外包，但是，DPO 或 COP 应当在可行范围内监督第三方服务提供商职责履行的情况，且 DPO 或 COP 仍然应作为 PIC 或 PIP 与菲律宾 NPC 的联络人。与 GDPR 类似，菲律宾的 DPO 制度要求，若 DPO 任有其他职位，不应与 DPO 的职责存在冲突，DPO 不应决定个人数据处理的目的和方式；DPO 应当具备数据隐私方面的专业知识，且充分了解 PIC 或 PIP 的数据处理活动；PIC 或 PIP 应确保 DPO“相当程度的自治”以确保其履行职务的独立性。

新加坡 2012 年《个人数据保护法》要求每个组织必须任命一名或多名 DPO，负责确保组织遵守个人数据保护法。一旦任命，DPO 可以对外授权特定的职责，包括向非雇员授权。DPO 的联络方式应当公开，但是，没有要求 DPO 必须是新加坡公民或居民。若组织没有任

命 DPO，个人数据保护委员会将展开调查，不配合调查的组织或自然人将构成犯罪，自然人可能被处以罚款或监禁，组织可能被处以罚款。

印度则要求所有收集敏感个人信息的公司任命投诉专员（Grievance Officer）处理相关投诉，响应数据主体的访问、修正等请求。印度对 DPO 是否是公民或居民并无要求，对未依法任命 DPO 的公司也未有强制措施或处罚。

在美国，虽然大型企业任命首席隐私官和 IT 安全官是行业内的最佳实践，除了美国健康保险流通与责任法案（Health Insurance Portability and Accountability Act，HIPPA）规制的实体外，并没有要求任命 DPO 的有关规定，这与欧盟 GDPR 的体例大不相同。

三、结语

通过以上时间和空间维度的比较分析，不难发现，DPO 制度从形成至今，背后的立法主旨都是将个人信息的部分监管职能和相应责任由监管部门转移至企业内部，这种安排有显而易见的合理性：一方面，个人信息使用情况一般都能够揭示核心商业逻辑和价值创造机制，因此，企业是最不愿意将相关信息对外披露的；另一方面，相较于日益普遍的个人信息使用行为，监管部门的行政资源极其有限，仅靠政府规制这些行为，不可避免地会出现选择执法等问题。正是因为 DPO 制度来源于现实的需要，才使其在美国以外被广泛采用。

但是，要实现 DPO 制度的初衷，在制度设计上仍需着力解决两个难题，这也是各国 DPO 制度差异的根源所在：

第一，DPO 的独立性与内部性之间的矛盾。DPO 是设置在企业内部的一个岗位，其作用是对企业的数据处理行为进行相对独立的监督，在一定程度上扮演监管部门的角色。如何在岗位设计上确保 DPO 可以不受层级领导的影响作出独立判断和决策，同时又能与企业保持一般意义上的内部关系，从而使其能够深入到企业的业务中去，是各国在制度设计中都着力解决的一个难题。

第二，DPO 制度所节约的合规成本和 DPO 制度本身所带来的合规成本之间的矛盾。如前所述，DPO 制度设立的初衷绝不是为企业增负，而是通过将外部合规转化为内部合规降低企业的合规负担。但是，DPO 制度本身也是有成本的，这种成本的大小取决于 DPO 适用范围、DPO 选任的资质要求等重要因素，而这些因素也决定了 DPO 制度是否可以在何种程度上实现相应的监管目的。换言之，各国在制定 DPO 制度时，需要权衡制度给企业带来的用人成本与其帮助企业节约的合规成本之间的关系，过重的成本将阻碍企业的发展，这有违 DPO 制度的初衷。（来源:《中国信息安全》杂志 2019 年第 2 期）

➢ Gartner:2019 年七大安全与风险管理趋势

2019 年 3 月 28 日，全球领先的信息技术研究和顾问公司 Gartner 近日发布了将在更长时期内影响安全、隐私与风险领导者的七个安全与风险管理新兴趋势。Gartner 将“大”趋势定义为安全生态系统中尚未得到广泛认可、但有望产生广泛的行业影响并有可能带来重大颠覆的持续战略性转变。Gartner 研究副总裁 Peter Firstbrook 表示：“外部因素与安全领域特定威胁正在共同影响着整体安全与风险态势，因此该领域的领导者必须做好提高弹性并支持业务目标的充分准备。”

趋势一：风险偏好声明（Risk Appetite Statements）正在与业务成果挂钩

随着 IT 战略与业务目标更加紧密地结合在一起，安全与风险管理（SRM）领导者向主要业务决策者有效提出安全事务的能力变得愈发重要。Firstbrook 先生表示：“为了避免只关注与 IT 决策相关的问题，请创建可以与业务目标以及董事会级别决策相关联的简单、实际且实用的风险偏好声明。业务领导者必须明白为何安全领导者要平等地参加战略性会议。”

趋势二：正在重点围绕威胁检测与响应而部署安全运营中心

随着安全警报的复杂性与频率不断增加，安全投资在从威胁防御向威胁检测的转变过程中，需要对安全运营中心（SOC）进行投资。根据 Gartner 提供的信息，到 2022 年，50%的安全运营中心将转变为具备综合事件响应、威胁情报和威胁搜索能力的现代化安全运营中心，而在 2015 年这一比例还不到 10%。Firstbrook 先生表示：“安全与风险管理领导者需要建立或外包能够集成威胁情报、整合安全警报并自动响应的安全运营中心，这一需求怎么强调都不过分。”

趋势三：数据安全治理框架应该优先考虑数据安全投资

数据安全是一个复杂的问题，如果没有对数据本身、数据的创建与使用环境及其受监管

程度的深入理解，就无法解决该问题。一些领先的企业机构正在开始通过数据安全治理框架（DSGF）解决数据安全问题，而非获取数据保护产品并尝试对其进行修改以满足业务需求。Firstbrook 先生表示："数据安全治理框架提供了一个以数据为中心的蓝图，用于识别与归类数据资产并定义数据安全策略。随后，这用于选择相关技术，借以将风险降至最低限度。解决数据安全问题的关键，在于从其所解决的业务风险入手，而不是像多数公司那样首先考虑获取技术。"

趋势四：无密码认证正在引领市场

无密码身份验证（例如智能手机上的 Touch ID）开始真正引领市场。由于供需充足，该技术正在被越来越多地部署到针对消费者与员工的企业应用之中。Firstbrook 先生表示："为了打击以密码为目标来访问云端应用的黑客，将用户与其设备关联起来的无密码方法提供了更高的安全性和可用性，这是一种难得的安全双赢。"

趋势五：安全产品厂商正在逐渐提供高级技能与培训服务

Gartner 的研究显示，网络安全岗位空缺将从 2018 年的 100 万增至 2020 年底的 150 万。虽然人工智能和自动化的进步确实减少了人类分析标准安全警报的需求，但敏感、复杂的警报仍然需要人的参与。Firstbrook 先生表示："我们开始看到一些厂商在提供融合产品与运维服务的解决方案以加速产品采用。从全面管理到部分支持等一系列服务均旨在提高管理员的技能水平，并减少日常工作量。"

趋势六：投资云安全能力并将其作为主流计算平台

由于可能无法获得人才且企业机构完全未为此做好准备，向云端迁移意味着安全团队的力量有所减弱。Gartner 估计，到 2023 年，大部分云安全故障都将是由客户的过错而引发的。Firstbrook 先生表示："对于许多企业机构而言，公有云是一种安全可行的选择，但保证安全性是双方共同的责任。各企业机构必须投资于用来构建知识库的安全技能与治理工具，以跟上云开发与创新的快速步伐。"

趋势七：Gartner 的持续自适应风险与信任评估将更多地出现于传统安全市场

Gartner 的持续自适应风险与信任评估（CARTA）是一种处理数字商业信任评估模糊性的策略。Firstbrook 先生表示："尽管是一个多年过程，但 CARTA 背后的构思是一种应对安全的战略性方法，其平衡了安全摩擦与交易风险。持续自适应风险与信任评估的一个关键组成部分，是即使在访问得到展期之后也要持续评估风险与信任。随着解决方案日益关注检测异常行为——即使用户与设备通过了认证，电子邮件与网络安全成为迈向持续自适应风险与信任评估方法的两个安全领域示例。"（来源：至顶网）

四、政府之声

➢ 〔2019〕85 号文加强支付结算管理防范电信网络新型违法犯罪答记者问

2019 年 3 月 28 日，中国人民银行发布了《关于进一步加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85 号，以下简称《通知》），中国人民银行有关负责人就《通知》有关问题回答了记者提问。

一、《通知》出台的背景是什么？

答：电信网络新型违法犯罪严重危害人民群众财产安全和合法权益，损害社会诚信和社会秩序，是影响群众安全和社会和谐稳定的一大公害。对此，党中央、国务院高度重视，中央领导同志多次作出重要指示批示。为贯彻落实中央领导的重要指示批示精神、国务院工作部署要求，近年来各相关部门加强协作，密切配合，加大打击防范电信网络新型违法犯罪工作力度，取得了阶段性成效。人民银行于 2016 年 9 月印发《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号，以下简称 261 号文），切实加强支付结算管理，构筑金融业支付结算安全防线，在打击治理电信网络新型违法犯罪中发挥了重要作用。

尽管经过各部门共同努力，打击治理电信网络新型违法犯罪工作取得了阶段性成效，但是当前电信网络新型违法犯罪案件高发的势头还没有从根本上得到有效遏制，电信网络新型违法犯罪的诈骗手法、资金转移等出现了新的情况和问题。2018 年 11 月 29 日，国务院召开全国打击治理电信网络新型违法犯罪工作电视电话会议，就打击治理电信网络新型违法犯罪工作再次作出部署，要求进一步加大打击治理电信网络新型违法犯罪工作力度。为落实此

次会议精神，人民银行研究制定了《通知》，针对当前打击治理电信网络新型违法犯罪面临的新形势、新要求和新情况，从健全紧急止付和快速冻结机制、加强账户实名制管理、加强转账管理、强化特约商户与受理终端管理、广泛宣传教育、落实责任追究机制等方面提出 21 项措施，进一步筑牢金融业支付结算安全防线。

二、《通知》为什么要加强单位支付账户管理？

答：大量电信网络新型违法犯罪案件反映出，当前不法分子转移诈骗资金使用的账户有从银行账户向支付账户，特别是单位支付账户转移的趋势。而部分非银行支付机构也存在单位支付账户实名审核不到位、使用不规范等问题，易被不法分子利用。为此，《通知》从三方面进一步加强单位支付账户管理。一是支付机构为单位开立支付账户应当严格审核单位开户证明文件的真实性、完整性和合规性，开户申请人与开户证明文件所属人的一致性，并向单位法定代表人或负责人核实开户意愿，留存相关工作记录。支付机构可采取面对面、视频等方式向单位法定代表人或负责人核实开户意愿，具体方式由支付机构根据客户风险评级选择。二是要求支付机构于 2019 年 6 月 30 日前按上述要求完成存量单位支付账户实名制落实情况核实工作。三是要求支付机构根据单位客户风险评级，合理设置并动态调整同一单位所有支付账户余额付款总限额。对同一单位所有支付账户余额付款总金额进行限制。

三、《通知》对买卖账户行为采取哪些强化管理措施？

答：目前，一些单位和个人仍不了解非法买卖、出租、出借账户法律责任及其危害性，违规向不法分子出租、出借、出售银行账户和支付账户牟利。利用买卖的账户转移诈骗资金成为当前电信网络新型违法犯罪中的突出问题。为使社会公众清楚认识非法买卖、出租、出借账户的法律责任，加大对买卖账户等违规行为的惩戒力度，《通知》要求：一是建立合法开立和使用账户承诺机制。银行和支付机构为客户开立账户时，应当在开户申请书、服务协议或开户申请信息填写界面醒目告知客户出租、出借、出售、购买账户的相关法律责任和惩戒措施，并载明以下语句：“本人（单位）充分了解并清楚知晓出租、出借、出售、购买账户的相关法律责任和惩戒措施，承诺依法依规开立和使用本人（单位）账户”，由客户确认。二是加大对买卖账户等违规行为惩戒力度。261 号文已规定，“银行和支付机构对公安机关认定的出租、出借、出售、购买银行账户（含银行卡，下同）或支付账户的单位和个人，组织购买、出租、出借、出售银行账户或支付账户的单位和个人，假冒他人身份或者虚构代理关系开立银行账户或支付账户的单位和个人，5 年内停止其银行账户非柜面业务、支付账户所有业务，3 年内不得为其新开立账户”。为进一步加大对买卖账户等违规行为惩戒力度，提高违规成本，对违规行为形成强有力的震慑，《通知》将惩戒措施调整为“5 年内暂停其银

行账户非柜面业务、支付账户所有业务，并不得为其新开立账户”。

四、《通知》为什么要调整自助柜员机转账管理政策？

答：261 号文规定，除向本人同行账户转账外，个人通过自助柜员机转账（ATM，含其他具有存取款功能自助设备，下同）的，发卡行在受理 24 小时后办理资金转账。该文件出台时，电信网络新型违法犯罪中近一半受害人是在不法分子的诱骗下，通过自助柜员机具向诈骗账户转账，而其中又有很大一部分受害人是在不知情的情况下被不法分子引导在自助柜员机具的英文界面中进行转账操作。针对这一情况，为保护人民群众财产安全，为挽回资金争取时间，261 号文采取了个人自助柜员机具转账资金在 24 小时后到账的临时性措施。该规定有效阻断了不法分子诱骗受害人通过自助柜员机具将资金转入诈骗账户的犯罪行为。与此同时，该措施也一定程度上影响了客户正常使用自助柜员机转账的客户体验。

目前，不法分子转移诈骗资金的渠道发生了很大变化，通过自助柜员机具诱骗诈骗数量已很少。同时，银行自助柜员机具均已基本完成改造，在办理转账业务中增加了汉语语音提示，通过文字、标识、弹窗等设置了防诈骗提醒，非汉语提示界面能对资金转出等核心关键字段提供汉语提示，防诈骗功能大幅提升。在此背景下，许多银行呼吁适当调整自助柜员机具转账管理政策，以满足正常客户实时转账需求。在兼顾安全性与便捷性的基础上，经商公安部门，《通知》对自助柜员机转账管理政策作了适当调整，即通过自助柜员机具为个人办理业务时，可在转账受理界面（含外文界面）以中文显示收款人姓名、账号和转账金额等信息（姓名应当脱敏处理），并以中文明确提示该业务实时到账，由客户确认。符合上述要求的，可不再执行自助柜员机具转账 24 小时后到账的规定。

五、《通知》针对特约商户与受理终端提出了哪些管理措施？

答：许多电信网络新型违法犯罪案件反映出，部分银行和支付机构存在特约商户资质审核不严、注册信息不真实，机具安装地址与实际经营地址不符等问题，部分机具甚至被移机境外使用，为不法分子利用银行、支付机构的支付服务从事违法犯罪活动提供可乘之机，也增加公安机关的办案难度。

对此，《通知》规范了特约商户与受理终端管理要求：

一是严格特约商户审核。要求收单机构严格按规定审核特约商户申请资料，采取有效措施核实其经营活动的真实性和合法性，不得仅凭特约商户主要负责人身份证件为其提供收单服务。同时，通过中国支付清算协会或银行卡清算机构的特约商户信息管理系统查询其签约、更换收单机构情况和黑名单信息。对于同一特约商户频繁更换收单机构等异常情形的，谨慎将其拓展为特约商户。对于黑名单中的单位以及相关个人担任法定代表人或负责人的单位，

不得将其拓展为特约商户；已经拓展为特约商户的，自其被列入黑名单之日起 10 日内予以清退。

二是严格受理终端管理。要求收单机构为特约商户安装可移动的银行卡、条码支付受理终端（以下简称移动受理终端）时，结合商户经营地址限定受理终端的使用地域范围。对移动受理终端所处位置持续开展实时监测，并逐笔记录交易位置信息，对于无法监测位置或与商户经营地址不符的交易，暂停办理资金结算并立即核实；确认存在移机等违规行为的，停止收单服务并收回受理机具。对于连续 3 个月内未发生交易的受理终端或收款码，要求收单机构重新核实特约商户身份，对无法核实的停止为其提供收款服务。对于连续 12 个月内未发生交易的受理终端或收款码，停止提供收款服务。

三是强化收单业务风险监测。要求收单机构、清算机构持续监测和分析交易金额、笔数、类型、时间、频率和收付款方等特征，完善可疑交易监测模型。发现异常情形的，对特约商户采取延迟资金结算、设置收款限额、暂停银行卡交易、收回受理终端（关闭网络支付接口）等措施；发现涉嫌电信网络新型违法犯罪的，立即向公安机关报告。

四是健全特约商户分类巡检机制。对于具备固定经营场所的实体特约商户，要求收单机构每年独立开展至少一次现场巡检；对于不具备固定经营场所的实体特约商户，要求定期采集其经营影像或照片、开展受理终端定位监测；对于网络特约商户，要求定期登录其经营网页查看经营内容、开展网络支付接口技术监测和大数据分析。同时，要求 2019 年 6 月底前对存量特约商户开展一次全面巡检。

六、社会公众需要配合做好哪些工作？

答：《通知》主要针对电信网络新型违法犯罪新形势和新问题，采取针对性管理措施，以保护人民群众财产安全和合法权益，对社会公众日常支付体验的影响较小。同时，《通知》实施过程中一些工作要求，如单位支付账户开户审核、存量单位支付账户重新核实，实施合法开立和使用账户承诺机制等，需要相关单位和个人给予配合。

另外，为了保障自身资金安全，希望广大公众能掌握电信网络新型违法犯罪典型手法及应对措施、转账汇款注意事项，认识买卖账户社会危害，强化个人金融信息保护意识。日常生活中，要注意保管好自己的身份证、银行账户和支付账户，妥善保护个人身份信息、账户信息、金融交易信息等，确保自己的个人金融信息等隐私信息不受侵害。（来源：）

- **银发〔2019〕85 号《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》全文：**
- https://mp.weixin.qq.com/s/owNv4UBus7XhUiQcayyIeg

➢ 全国人力资源社会保障网络安全和信息化工作座谈会召开

2019 年 3 月 28 日至 29 日，全国人力资源社会保障网络安全和信息化工作座谈会在广东珠海召开。会议总结交流“互联网+人社”实践经验，研究今后一个时期的工作思路，部署 2019 年重点任务。人社部副部长游钧出席会议并讲话。

会议指出，“互联网＋人社”取得积极进展，有力促进了人社部门的管理服务创新。第三代社保卡、电子社保卡在各地同步发行，全国持卡人数达到 12.41 亿，社保卡被更多政府部门作为惠民惠农资金和民生服务的唯一载体；人社大数据进入加速发展期，以数据为支撑的应用创新取得成效；人社一体化在线政务服务体系启动建设，进一步提升人社领域信息服务能力。

会议强调，要准确把握人社事业发展的阶段特征和信息技术发展趋势，坚持以人民为中心的发展思想，围绕中央决策部署和人社系统行风建设要求，以信息化为支点，打造群众满意的人社服务。要按照“国家平台引领、标准体系先行、打通两大系统、创新四类服务”的工作思路，着力构建全国一体化的信息化服务平台，提升信息化便民服务效能，使信息化在提升人社服务能力和水平方面发挥更大作用。

会议要求，2019 年要在习近平新时代中国特色社会主义思想指引下，围绕打造人民满意的人社服务目标，全力做好社保卡和电子社保卡发行及应用；加快推进全国统一的社会保险公共服务平台建设，全力做好人社扶贫、社会保险省级统筹等改革任务的信息化保障工作；通过信息化建设防范风险，提升网络和信息安全保障能力，努力开创网络安全和信息化建设新局面。（来源：人力资源社会保障部网站）

➢ 网信办发布第一批 197 个境内区块链信息服务备案编号

2018 年 3 月 30 日国家互联网信息办公室关于发布第一批境内区块链信息服务备案编号的公告：2019 年 2 月 15 日《区块链信息服务管理规定》（以下简称《管理规定》）正式实施以来，国家互联网信息办公室依法依规组织开展备案审核工作。现公开发布第一批共 197 个区块链信息服务名称及备案编号。任何单位或个人如有疑议，请于即日起 10 个工作日内将相关意见通过电子邮件发送至 bc_beian@cert.org.cn，或邮寄至北京市朝阳区裕民路甲 3 号

国家互联网应急中心，邮编：100029（信封上注明“备案公告反馈”）。提出疑议应以事实为依据，并提供相关证据材料。

根据《管理规定》要求，区块链信息服务提供者应当在其对外提供服务的互联网站、应用程序等显著位置标明其备案编号。备案仅是对主体区块链信息服务相关情况的登记，不代表对其机构、产品和服务的认可，任何机构和个人不得用于任何商业目的。网信部门后续将会同各有关部门，依据《管理规定》对备案主体进行监督检查，并督促未备案主体尽快履行备案义务。请尚未履行备案手续的相关机构和个人尽快申请备案。（来源：国家互联网信息办公室）

- **通知全文：**http://www.cac.gov.cn/2019-03/30/c_1124305122.htm

➢ 2018 年全国未成年人互联网使用情况研究报告发布

2019 年 3 月 26 日，共青团中央维护青少年权益部、中国互联网络信息中心（CNNIC）邀请专家学者、知名网络作家等走进“团团直播间”，围绕“互联网空间中的未成年人”主题与网友进行互动交流，并现场发布《2018 年全国未成年人互联网使用情况研究报告》（以下简称《报告》）。

《报告》基于对全国 31 个省（自治区、直辖市）的小学、初中、高中和中职院校 31158 学生抽样调查，从未成年人互联网普及情况、网络接入环境、应用使用情况和利用网络自我保护能力等多个方面，展示了当前未成年人互联网使用现状和行为特点。

《报告》显示，截至 2018 年 7 月 31 日，我国未成年网民规模达 1.69 亿，未成年人的互联网普及率达到 93.7%，明显高于同期全国人口的互联网普及率（57.7%）。这是近年来我国互联网覆盖范围扩大、移动流量资费下降的直接表现，也与未成年人对互联网的兴趣浓、学习能力强、应用需求大密切相关。从各学历段情况看，小学、初中、高中和中职学生上网比例分别达到 89.5%、99.4%、96.3%和 99.0%。从城乡分布看，城镇未成年人上网比例为 95.1%，农村未成年人上网比例为 89.7%。我国通过持续改善农村学校信息化基础设施环境，互联网为农村学校输送了丰富的数字教育资源，城乡未成年人的上网比例差异逐渐缩小。（来源：共青团中央维护青少年权益部）

五、本期重要漏洞实例

➢ Cisco IOS XE Software 信息泄露安全漏洞

发布日期：2019-03-27
更新日期：2019-03-29
受影响系统：
Cisco IOS XE
描述：

BUGTRAQ ID: 107600
CVE(CAN) ID: CVE-2019-1742
Cisco IOS 和 IOS XE 都是一套为其网络设备开发的操作系统。
Cisco IOS XE Software 由于没有对 Web UI 中的文件执行正确的访问控制，在实现中存在配置错误漏洞，当设备启用了 Web 服务器功能时，远程攻击者可通过发送恶意的请求，利用该漏洞访问敏感的配置信息。

<*来源：vendor
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-xeid
*>

建议：

厂商补丁：

Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190327-xeid）以及相应补丁：
cisco-sa-20190327-xeid：Cisco IOS XE Software Information Disclosure Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-xeid

➢ IBM Sterling B2B Integrator XML 外部实体注入安全漏洞

发布日期：2019-03-26
更新日期：2019-03-28
受影响系统：
IBM Sterling B2B Integrator 6.0.0.0
描述：

CVE(CAN) ID: CVE-2019-4043

IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM Sterling B2B Integrator 6.0.0.0 版本，在解析 XML 数据中存在 XML 外部实体注入漏洞。远程攻击者可利用该漏洞泄露敏感信息或消耗内存资源。

<*来源：vendor
*>

建议：

厂商补丁：
IBM

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://www-01.ibm.com/support/docview.wss?uid=ibm10874238

➢ WordPress social-warfare 插件跨站脚本漏洞

发布日期：2019-03-24
更新日期：2019-03-26
受影响系统：
WordPress social-warfare < 3.5.3
描述：

CVE(CAN) ID: CVE-2019-9978
WordPress 是一套使用 PHP 语言开发的博客平台。
WordPress social-warfare 插件 3.5.3 之前版本，在 wp-admin/admin-post.php?swp_debug=load_options swp_ur 参数中存在跨站脚本漏洞。远程攻击者利用该漏洞注入恶意的 JavaScript 脚本。

<*来源：vendor
*>

建议：

厂商补丁：
WordPress

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://wordpress.org/plugins/social-warfare/#developers
参考：

https://blog.sucuri.net/2019/03/zero-day-stored-xss-in-social-warfare.html
https://twitter.com/warfareplugins/status/1108852747099652099
https://wordpress.org/plugins/social-warfare/#developers
https://wpvulndb.com/vulnerabilities/9238
https://www.cybersecurity-help.cz/vdb/SB2019032105
https://www.pluginvulnerabilities.com/2019/03/21/full-disclosure-of-settings-change-persistent-cross-site-scripting-xss-vulnerability-in-social-warfare/
https://www.wordfence.com/blog/2019/03/unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild/

➢ Mozilla Firefox 释放后重利用漏洞

发布日期：2019-03-19
更新日期：2019-03-22
受影响系统：
Mozilla Firefox < 66
描述：

CVE(CAN) ID: CVE-2019-9790

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox 的一个延长支持版本。Mozilla Firefox 66 之前版本在实现中存在释放后重用漏洞。远程攻击者可利用该漏洞造成拒绝服务。

<*来源：Mozilla
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/
*>

建议：

厂商补丁：
Mozilla

Mozilla 已经为此发布了一个安全公告（mfsa2019-07）以及相应补丁：
mfsa2019-07：Security vulnerabilities fixed in Firefox 66
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/

六、本期网络安全事件

➢ 盗 30 万条个人信息叫价 1 比特币网偷被警方抓获

2019 年 3 月 25 日，暴力破解汽车金融服务平台后台管理权限，盗取大量数据放至“暗网叫卖”；篡改短视频软件，破坏系统安全防护机制，还在网上“炫技”，24 日，武汉警方通报上述两起案例，嫌疑人均被收入法网。

30 余万条个人信息叫价 1 比特币

去年 11 月，一篇微信公众号信息引起人们关注，“‘暗网’上有人挂售某网站 30 余万条用户资料信息，叫价 1 个比特币。”这个涉事网站负责人获此消息，焦急万分，匆匆到江汉区公安分局报警。

在互联网上，暗网犹如沉入水中的冰山，追查暗网信息的幕后黑手，相比一般的网上追踪困难得多。这名作案的黑客还声称，他不仅攻克了数据库，还拿到了包括服务器在内的全部权限，并晒出网站管理后台信息。

武汉市公安局网安支队迅速介入调查。经查，这家网站后台管理权限已被盗取，被偷走的客户信息包括身份证、手机号、银行卡、家庭住址、工作单位、贷款情况等，在暗网上的售价是 1 个比特币（时值 3.5 万元）。网安支队会同江汉区分局组织专案组立案侦查。专案组民警最终查明这只幕后黑手，指向四川省成都市双流区华阳镇的一个青年男子吴某。今年 1 月 22 日，专案组在成都警方的配合下，将吴某抓获归案。

年仅 22 岁的吴某交代，他利用一个软件以暴力破解手段入侵受侵网站后台。他找到服务器的用户注册信息，盗取这家网站大批量、多维度的用户数据，共计 30 余万条。因为不了解“暗网”相关技术，他还曾向一网友交 180 元学费。

他没有想到，两个月时间，武汉警方就追查并抓捕了他。目前，武汉警方正进一步围绕吴某贩卖的公民个人信息流向，深挖案件线索，追查犯罪链条、犯罪团伙。

恶意篡改短视频 App 还在网上“炫技”

去年 11 月，武汉网警在网上公开巡查时发现，有人恶意篡改短视频 App 软件，并在网络论坛传播。网警当即将此消息反馈给开发这款软件的科技公司。该公司技术人员分析发现，这种篡改会导致核心数据丢失，尤其严重的是，篡改后的软件极易被不法分子利用，将境外一些暴力、色情等视频传入境内。

网安支队迅速会同武昌区公安分局成立专班展开侦查工作。他们通过分析篡改软件，比对相关信息，查明篡改软件的犯罪嫌疑人竟是不到 20 岁的辽宁青年郭某某。郭某某通过修软件代码并重新打包，使普通用户可突破安全机制随意浏览不良信息。根据该公司后台数据显示，已有 40 余万人次使用了该篡改软件，在使公司利益受损的同时，也形成很大的网络安全隐患。今年 3 月 8 日，工作专班赶赴辽宁本溪，将郭某某抓获归案。

经审查，郭某某交代了全部作案过程。他是一所大专学校就读的在校生，所学并非计算机专业。自高二起就对计算机编程产生浓厚兴趣的他，由于家里没有经济条件买电脑，竟用手机编代码 10 万条。他篡改这款短视频的初衷并非为谋利，只为“炫技”。

他将篡改后的“版本”连同篡改的技术细节在网络论坛上分享给网友们，一时间数万粉丝称之为“大神”。大受“鼓舞”的他又进一步篡改软件，并将其分为“免费版”“收费版”两个版本，并获利 3000 余元。办案民警介绍，社交能力较差，还有点结巴的郭某某，兼职写代码、送外卖补贴家用。今年 1 月初，他发现经过篡改的软件的扩散已经不受控制，有些害怕，遂停止了更新。（来源：武汉晚报）

➢ 24 岁黑客进入任天堂内部数据服务器致损失 180 万美元

2019 年 3 月 29 日，2018 年 3 月至 5 月期间，任天堂用于保存游戏开发资料的内部服务器被黑客攻陷，目前尚不清楚到底有多少开发中的游戏资料被泄露，不过预计任天堂从这次攻击中损失大概在 180 万美元。攻陷任天堂内部服务器的是一名 24 岁的安全研究员，名叫扎米斯克拉克(Zammis Clark)。

在其对任天堂服务器进行攻击之前，他还攻击了微软的服务器。虽然没有公布详细的手段，不过媒体透露扎米斯使用 VPN 连接到了任天堂的内部网络，并得到了游戏开发代码。

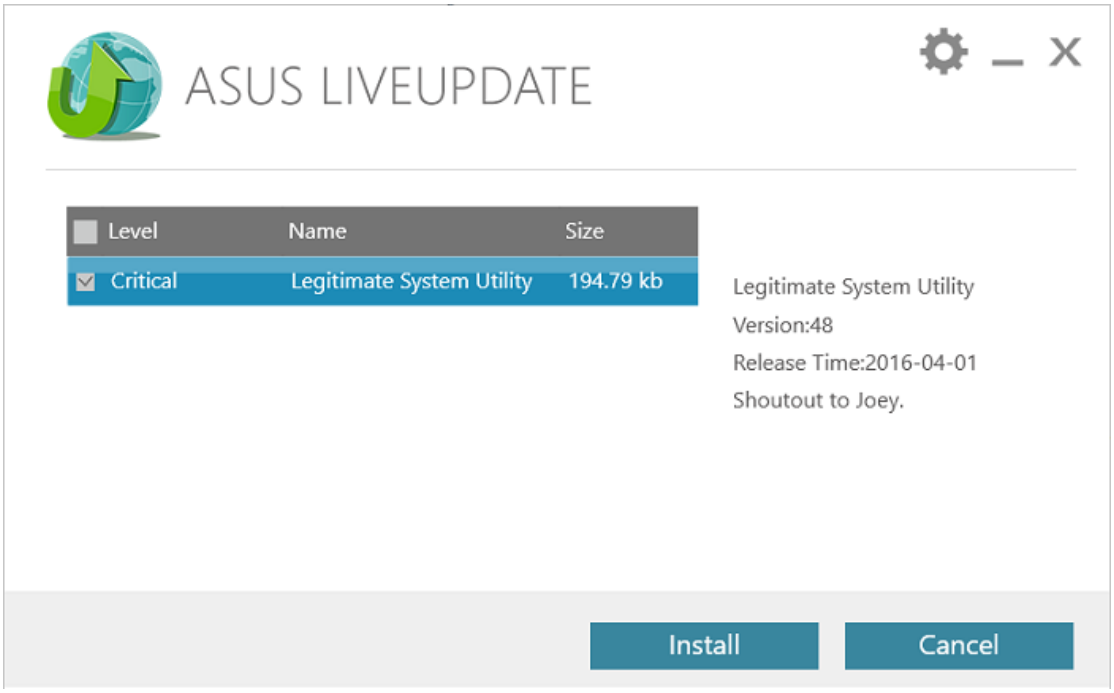
有 2365 个用户名和密码被盗。然而任天堂在去年 5 月才发现了这一问题。

任天堂估计损失在 91.3 万美元到 180 万美元之间。该公司目前尚未对此发表评论。扎米斯克拉克已被判 15 个月监禁。还将面临数额未知的罚款，如果拒交罚款，他将被判最高 5 年监禁。不过由于扎米斯克拉克患有自闭症，而且即将失去视力，法官决定对其缓刑 18 个月，如果不再继续犯罪的话，不会立刻入狱。（来源：3DMGame）

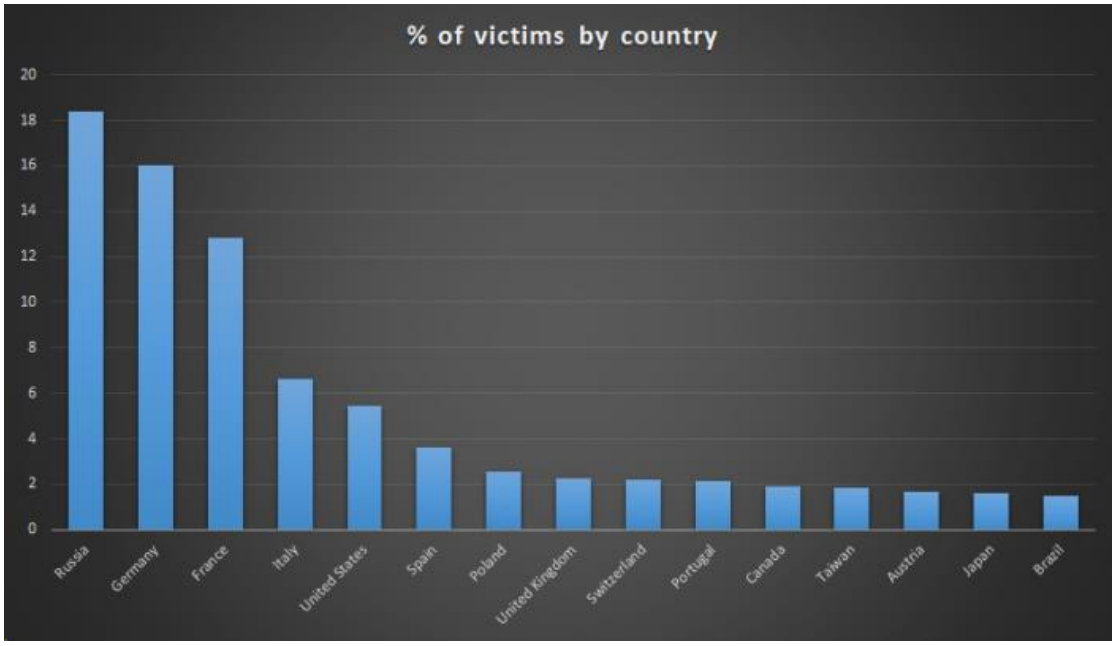
➢ 华硕回应 Live Update 软件漏洞：仅数百台受到影响

2019 年 3 月 26 日，来自卡巴斯基实验室（Kaspersky Labs）的安全研究人员周一表示，他们发现去年黑客通过华硕 Live Update 软件的漏洞入侵计算机，向 100 多万华硕电脑用户发送了恶意软件，导致这些电脑可能存在后门。据台湾地区媒体《中时电子报》报道，华硕今天下午表示，此事件已在华硕的管理及监控之中。

华硕称，媒体报道华硕 Live Update 工具程序(以下简称 Live Update)可能遭受特定 APT 集团攻击，APT 通常由第三世界国家主导，针对全世界特定机构用户进行攻击，甚少针对一般消费用户。经过华硕的调查和第三方安全顾问的验证，目前受影响的数量是数百台，大部份的消费者用户原则上并不属于 APT 集团的锁定攻击范围。



华硕表示，Live Update 为华硕笔记本电脑搭载的自动更新软件，部份机型搭载的版本遭黑客植入恶意程序后，上传至档案服务器(download server)，企图对少数特定对象发动攻击，华硕已主动联系此部份用户提供产品检测及软件更新服务，并由客服专员协助客户解决问题，并持续追踪处理，确保产品使用无虞。



针对此次攻击，华硕已对 Live Update 软体升级了全新的多重验证机制，对于软体更新及传递路径各种可能的漏洞，强化端对端的密钥加密机制，同时更新服务器端与用户端的软件架构，确保这样的入侵事件不会再发生。（来源：新浪科技）

➢ 多项腾讯服务宕机：因运营商光纤故障

2019 年 3 月 25 日上午消息，腾讯云发布公告，详细解释了 23 日下午腾讯服务器出现问题的全过程，称因上海南汇网络光纤因施工被意外挖断，导致该区不少互联网公司的业务受到不同程度的影响。

3 月 23 日下午大量用户反馈腾讯旗下诸多服务出现服务器未响应问题。受影响的腾讯服务包括腾讯微云、腾讯游戏、QQ 安全中心等服务。

根据网友描述，通过腾讯登录相关游戏界面会出现登录超时问题。另外，还有网友反馈腾讯微云网盘服务也出现异常。有用户通过 QQ 安全中心修改密码也提示失败。

腾讯方面此前公告称：2019 年 03 月 23 日 16 时左右，因上海当地网络运营商光纤线路大面积故障，腾讯多个产品业务使用受到影响。目前运营商正在紧急抢修中，我们也正在积极做容灾处理，业务陆续恢复中。后续修复进展会及时向各位公布。

腾讯云表示，当天下午，网络监控平台监测到上海到浙江电信出现小范围公网质量下降。腾讯云随即启动流量智能调度系统，将上海地区公网流量通过腾讯云内部 T 级骨干网，引导至腾讯云广州区电信出口，再由电信骨干网直达浙江电信。

腾讯云称，此次光纤故障，腾讯云从发现到恢复故障，全程只有 2 分钟(抖动时间：14:40:15-14:42:45)，并且所有流程自动化执行，在短短 150 秒之内就快速恢复了网络。（来源：新浪财经）

➢ 浪潮工程师监守自盗,窃取硬件网上转卖获刑三年

2019 年 3 月 28 日，利用自由进出实验室的便利,信息工程师孙华(化名)窃取公司 CPU、硬盘、SSD 卡等计算机硬件,并在淘宝二手交易网站咸鱼上挂卖。近日,济南市中级人民法院二审宣判,孙华犯盗窃罪,被判处有期徒刑三年三个月,并处罚金 1.3 万元。

工程师监守自盗，窃取硬件网上转卖

因犯盗窃罪，二审获刑三年三个月

本报济南3月28日讯（记者 崔岩 马云云）利用自由进出实验室的便利，信息工程师孙华（化名）窃取公司CPU、硬盘、SSD卡等计算机硬件，并在淘宝二手交易网站咸鱼上挂卖。近日，济南市中级人民法院二审宣判，孙华犯盗窃罪，被判处有期徒刑三年三个月，并处罚金1.3万元。

孙华于2016年2月24日入职浪潮，负责服务器系统测试工作，平时可自由进出实验室。原审判决认定，2017年9月至12月，孙华趁无人之际，在位于济南市高新技术产业开发区的浪潮电子信息产业股份有限公司（以下简称“浪潮公司”）S05号楼二楼实验室内，多次窃取2650V4型计算机CPU四块、2660型计算机CPU两块、2670型计算机CPU两块、2680型计算机CPU两块、8176型CPU两块，并在账户名为“f2728888”的淘宝闲鱼网站上以卖手机的名义将被盗物品销售给倪某某。

经鉴定，上述物品价值人民币13.8516万元。2018年11月29日，孙华家属交至济南高新技术产业开发区人民法院14.7203万元作为赔偿款。

然而，这起盗窃案件最终案发并非浪潮公司自己发现，而是由阿里公司发现。2018年3月31日，阿里公司从网上发现他们提供给浪潮公司的一块定制SSD卡（SN:FL170700037）在淘宝网上售卖，并将信息反馈。浪潮公司自查发现，该SSD卡确实是阿里公司提供给浪潮公司的定制卡。

浪潮公司通过阿里公司联系到了淘宝网店店主倪某某。倪某某工作之余，在家中干组装电脑服务器的活挣钱，平时需要从网上买一些二手的电脑配件如CPU、硬盘等。经核实，倪某某通过支付交易查实，该买家名叫孙华，确实是浪潮公司一名员工。2018年4月17日，孙华经公安机关依法传唤后到案，并如实供述了自己的犯罪事实。

原审法院认为，被告人孙华的行为构成盗窃罪，鉴于其系自首，认罪认罚，积极退赃，依法对其从轻处罚。孙华犯盗窃罪，判处有期徒刑3年3个月，并处罚金1.3万元。宣判后，孙华不服判决，认为其行为构成职务侵占罪，原审量刑过重，提出上诉。

2019年2月28日，济南市中级人民法院认为，孙华作为测试工程师，能够自由出入实验室，可以接触到被盗物品，孙华将不属于其管理范围的CPU秘密带出实验室并在网上售卖，其行为符合盗窃罪的构成要件，据此，该上诉理由及辩护意见不能成立，不予采纳，裁定驳回上诉，维持原判。

山东省高级人民法院 齐鲁晚报

开栏的话

全面推进依法治国，离不开法治精神的弘扬。山东是案件大省，去年全省法院收案173.9万件，结案168.1万件，均创历史新高，数字是抽象的，但具体个案却蕴含着法治精神，彰显公平正义。为传播法治理念，传递法治好声音，即日起，齐鲁晚报联合山东省高级人民法院开办《以案说法》栏目，选取全省各级法院审判、执行的具有典型意义的案件，以案说法，以案释法，努力让人民群众在每一个司法案件中感受到公平正义。

“内鬼”犯罪不乏高学历者

“公司‘内鬼’盗窃，事实相对清楚，难点在于，要明确被告人的行为属于盗窃还是职务侵占或者污。”济南高新区法院刑庭庭长张钢分析，辨别的核心是被告人有没有“利用职务之便”，也就是在其职责范围内将财物非法占为己有。

在济南高新区法院办理涉及“内鬼”的案件中，进行一部分被认定为侵犯商业秘密罪，这类犯罪分子多是以不正当手段窃取企业的商业秘密“当主门户”，给老东家带来损失。这些犯罪分子中，不乏高学历者，例如曾有一名计算机博士在高新区一家企业盗取代码后对其扩了一层包装，法院在审理中邀请科技领专家进行鉴定分析，最终得出有力证据，依法对其作出相决。 本报记者 崔岩 马云云

减肥路上

公告声明 齐鲁晚报 24小时手机/微信：18615502833 18615502822 18615502811 全省联动 【山东各地】公告/挂失/声明/招商/供求/合作/服务/招生/酒水/中介等 0531-88778968 商业资讯

孙华于 2016 年 2 月 24 日入职浪潮,负责服务器系统测试工作,平时可自由进出实验室。原审判决认定,2017 年 9 月至 12 月,孙华趁无人之际,在位于济南市高新技术产业开发区的浪潮电子信息产业股份有限公司(以下简称“浪潮公司”)S05 号楼二楼实验室内,多次窃取 2650V4 型计算机 CPU 四块、2660 型计算机 CPU 两块、2670 型计算机 CPU 两块、2680 型计算机 CPU 两块、8176 型 CPU 两块,并在账户名为“f2728888”的淘宝闲鱼网站上以卖手机的名义将被盗物品销售给倪某某。

经鉴定,上述物品价值人民币 13.8516 万元。2018 年 11 月 29 日,孙华家属交至济南高新技术产业开发区人民法院 14.7203 万元作为赔偿款。

然而,这起盗窃案件最终案发并非浪潮公司自己发现,而是由阿里公司发现。2018 年 3 月 31 日,阿里公司从网上发现他们提供给浪潮公司的一块定制 SSD 卡(SN:FL170700037)在淘宝网上售卖,并将信息反馈。浪潮公司自查发现,该 SSD 卡确实是阿里公司提供给浪潮公司的定制卡。

浪潮公司通过阿里公司联系到了淘宝网店店主倪某某。倪某某工作之余,在家中干组装电脑服务器的活挣钱,平时需要从网上买一些二手的电脑配件如 CPU、硬盘等。经核实,倪某

某曾在闲鱼网站上和一个叫“f2728888”的卖家多次交易,该 SSD 卡也在其中。倪某某通过支付交易查实,该卖家名叫孙华,确实是浪潮公司一名员工。2018 年 4 月 17 日,孙华经公安机关依法传唤后到案,并如实供述了自己的犯罪事实。

原审法院认为,被告人孙华的行为构成盗窃罪。鉴于其系自首,认罪认罚,积极退赔,依法对其从轻处罚。孙华犯盗窃罪,判处有期徒刑 3 年 3 个月,并处罚金 1.3 万元。宣判后,孙华不服判决,认为其行为构成职务侵占罪,原审量刑过重,提出上诉。

2019 年 2 月 28 日,济南市中级人民法院认为,孙华作为测试工程师,能够自由出入实验室,可以接触到被盗物品,孙华将不属于其管理范围的 CPU 秘密带出实验室并在网上售卖,其行为符合盗窃罪的构成要件。据此,该上诉理由及辩护意见不能成立,不予采纳。裁定驳回上诉,维持原判。

“内鬼”犯罪　不乏高学历者

“公司‘内鬼’盗窃,事实相对清楚,难点在于,要明确被告人的行为属于盗窃还是职务侵占或贪污。”济南高新区法院刑庭庭长张钊分析,辨别的核心是被告人有没有“利用职务之便”,也就是在其职责范围内将财物非法占为己有。

在济南高新区法院办理涉及“内鬼”的案件中,还有一部分被认定为侵犯商业秘密罪。这些犯罪分子多是以不正当手段获取企业的商业秘密后“自立门户”,给老东家带来损失。这些犯罪分子中,不乏高学历者,例如曾有一名计算机博士在高新区一家企业盗取源代码后对其加了一层伪装,法院在审理中邀请科技部专家进行鉴定分析,最终得出有力证据,依法对其作出判决。（来源：齐鲁晚报）

➢ 饿了么等 25 款 APP 被曝收集敏感个人权限

2019 年 3 月 27 日，上海市消保委发布了针对 39 款网购平台、旅游出行、生活服务等手机 App 涉及个人信息权限的评测结果通报，发现有 25 款存在问题，其中 9 款至今未整改，而“日历”权限的过度申请和随意授权更令人担忧。

9 款 App 仍在收集敏感权限

本次主要评测四个方面，包括 App 所使用的目标 API 级别、App 敏感权限的数量、敏感权限的授权方式（即是否存在一揽子授权），及查看是否存在无实际功能对应用的权限申请。

结果发现，15 款网购平台类 App 中 10 款存在问题，13 款旅游平台类 APP 中 7 款有问题，11 款生活平台类 App 中 8 款有问题。截至 3 月 23 日，仍有 9 款 App 尚在收集敏感个人权限，包括：聚美（v7.951）、贝贝（v8.2.01）、穷游（v9.2.0）、TripAdvisor 猫途鹰（v29.4.1）、神州租车（v6.4.4）、一嗨租车（v6.2.1）、饿了么（v8.13.1）、百度糯米（v8.4.7）、格瓦拉生活（v9.5.0）等。这些 App 的主要问题在于，申请了发送短信、录音、拨打电话、读取联系人、监控外拨电话、重新设置外拨电话的路径、读取通话记录等敏感权限，却未在应用中进行使用。

饿了么涉嫌读取通话记录

涉及的 39 款 App，共有 37 家来到现场，部分企业代表做出了回应。“一嗨租车”表示，“短信权限是开发时的失误造成的，但并未去用，也没有运用的场景，在新版本中已去除”。

“饿了么”则申请了 11 个权限，包括拨打电话、日历等。在测试新版本时，专家发现旧版中的拨打电话和日历权限已删除，但又新增了“读取通话记录”权限。在现场，饿了么回应称，该权限“在不知情的情况下上线，3 月 22 日已下线”。

而“格瓦拉”申请的短信、通讯录、麦克风 3 个权限并未找到对应功能。格瓦拉回应称，在 3 月 26 日发布的新版本中，已取消了上述 3 个权限。

“聚美”申请了 12 个权限，但专家认为通讯录和日历权限并不必要。“贝贝”申请的 8 个权限中，麦克风权限在实际运用中并未发现。而“穷游”申请的电话、通讯录权限，“猫途鹰”申请的电话权限，“神州租车”申请的电话、监控外拨电话和重新设置外拨电话

的路径、麦克风等权限，也未在对应功能中发现。

“日历”让生活工作都暴露

发布会上，上海市消保委特别对“日历”权限进行了提示。调查发现，52.5%的消费者用手机日历记录重要行程。其中，27.5%会记录日常生活行程，18.5%会记录生活及工作等。虽然常用日历记录行程，但只有 0.4%的消费者关注“日历”权限有否被滥用。

“App 为何要申请日历权限？有些平台告诉我们，如果平台上有抢购，消费者点击‘关注’，就会将信息放在日历中，抢购前可以提醒。但我们咨询了技术专家，这个功能完全可以通过后台的信息推送等别的途径来实现。”上海市消保委副秘书长唐健盛说。

上海市消保委认为，日历权限与个人隐私的密切度比通讯录等权限还要高，将日历权限授权给 App，带来的风险远大于便利。消保委建议，经常用日历来记录敏感事项的消费者，在授权时要谨慎。而 App 开发者如无十分必要，建议尽可能不开发日历权限。

上海市消保委秘书长陶爱莲表示，沪消保委近年来持续关注 App 对于个人信息的获取，此次发布的调查已是第三期。但从发布情况来看，个人敏感权限的收集仍是较突出的问题，而企业并不会主动反思或下线。消费者越来越关注个人隐私的保护，拼命防守但防不胜防。政府和企业应创造放心安全的消费环境，让消费者更“敢”消费。

中消协开通 App 举报通道

3 月 28 日，中国消费者协会官方公号发表文章称，由全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立的 App 专项治理工作组，目前已经初步建成“App 个人信息举报”微信公众号，公众号受理对 App 违法违规收集使用个人信息的举报，发布对 App 隐私政策和个人信息收集情况的评估及处置结果。关注公众号，通过点击公众号举报按钮进行举报，举报后会将被举报的 App 纳入评估范围。

记者发现，“App 个人信息举报”公号显示，其受理民众对 App 违法违规收集个人信息的行为进行举报。具体来看，举报人可以选择匿名或实名举报，而举报问题包括“App 无隐私政策”、“超范围收集与业务功能无关个人信息”、“强制或频繁索要业务功能非必需权限”等 10 个选项。

消费者协会称，该公号目前收到了许多高质量的举报信息，其中被举报的最多的 App 类型有金融借贷类、社区社交类、学习教育类。而在举报问题上，“超范围收集与业务功能无关个人信息”占所有举报信息的 20%，排行首位。（来源：新京报）

信息安全意识产品免费大赠送

isa@spisec.com