国盟信息安全通报

2020 年 5 月 10 日第 215 期

全国售后服务中心

国盟信息安全通报

（第 215 期）

国际信息安全学习联盟

2020 年 05 月 10 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 374 个，其中高危漏洞 160 个、中危漏洞 194 个、低危漏洞 20 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“PHP-FPM 远程代码执行漏洞（CNVD-2020-25851）、WordPress Catch Breadcrumb 跨站脚本漏洞”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 3232 个，与上周（5304 个）环比减少 39%。

主要内容

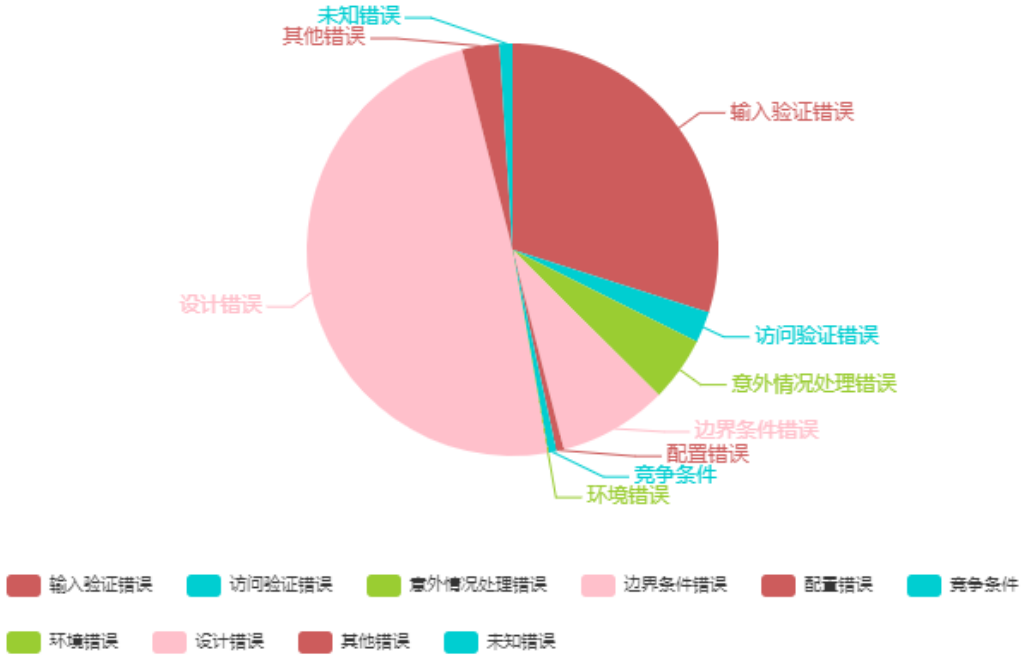
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

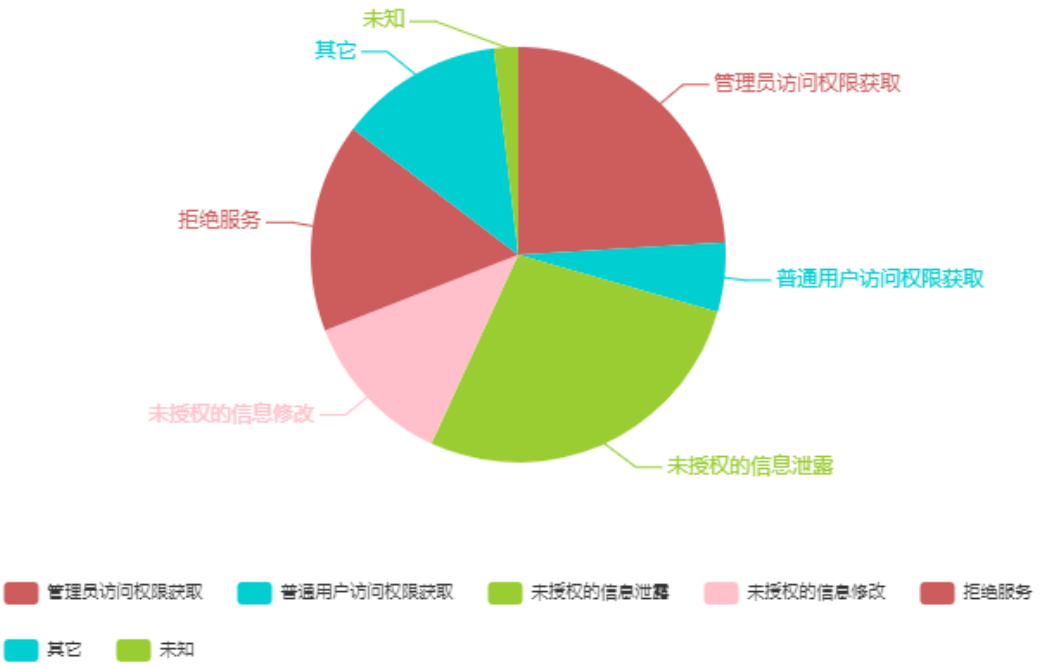
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 374 个，其中高危漏洞 160 个、中危漏洞 194 个、低危漏洞 20 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“PHP-FPM 远程代码执行漏洞（CNVD-2020-25851）、WordPress Catch Breadcrumb 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3232 个，与上周（5304 个）环比减少 39%。

二、安全漏洞增长数量及种类分布情况

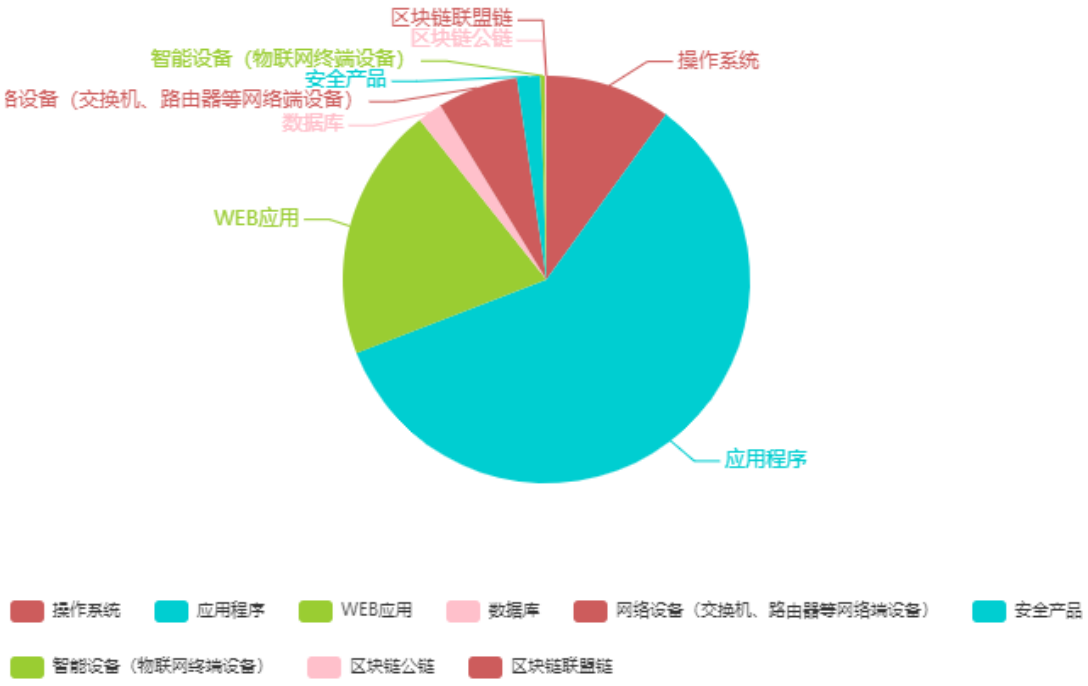
➢ 漏洞产生原因（2020 年 04 月 26 日—2020 年 05 月 10）



➢ 漏洞引发的威胁（2020 年 04 月 26 日—2020 年 05 月 10）



➢ 漏洞影响对象类型（2020 年 04 月 26 日—2020 年 05 月 10）



三、安全产业动态

➢ 深入学习贯彻习近平总书记关于网络强国的重要思想

——为全面夺取疫情防控和实现经济社会发展目标双胜利提供有力保障

党的十八大以来，习近平总书记着眼时代发展大势和国际国内大局，就网络安全和信息化工作提出了一系列新理念新思想新战略，深刻回答了事关网信事业发展的一系列方向性、根本性、全局性、战略性重大问题，形成了习近平总书记关于网络强国的重要思想。习近平总书记关于网络强国的重要思想，是我们党管网治网实践经验的理论总结，是运用马克思主义立场观点方法分析解决我国互联网发展治理问题的重大成果，是引领我国网信事业发展的行动指南，为做好新时代网络安全和信息化工作指明了前进方向、提供了根本遵循。今年是全面建成小康社会目标实现之年，是全面打赢脱贫攻坚战收官之年。当前，全国疫情防控阶段性成效进一步巩固，复工复产取得重要进展，经济社会运行秩序加快恢复。我们要深入学习贯彻习近平总书记关于网络强国的重要思想，自觉从党和国家工作大局中找准定位、履行使命、发挥作用，为全面夺取疫情防控和实现经济社会发展目标双胜利提供有力服务、支撑和保障，为实现“两个一百年”奋斗目标和中华民族伟大复兴的中国梦作出应有贡献。

深入学习宣传贯彻习近平新时代中国特色社会主义思想，凝聚全党全国人民团结奋斗的强大精神力量

习近平新时代中国特色社会主义思想是当代中国马克思主义、21 世纪马克思主义。做好习近平新时代中国特色社会主义思想网上学习宣传贯彻工作是网信工作的首要政治任务。必须用党的创新理论凝聚亿万网民，巩固全党全国人民团结奋斗的共同思想基础。聚焦强基铸魂，坚持以习近平新时代中国特色社会主义思想为统领，精心做好习近平新时代中国特色社会主义思想网上宣传阐释，引导干部群众努力掌握贯穿其中的马克思主义立场观点方法，增强“四个意识”、坚定“四个自信”、做到“两个维护”，切实在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致。聚焦入脑入心，阐释好习近平新时代中国特色社会主义思想蕴含的深刻道理学理哲理，充分展现总书记真挚深厚的为民情怀和深受爱戴的领袖形象，把彻底的理论讲彻底，把鲜活的思想讲鲜活，引导广大网民深刻领悟其中蕴含的丰富内涵、核心要义和实践要求，让党的创新理论通过互联网“飞入寻常百姓家”。聚焦守正创新，运用大数据、人工智能、算法推荐等互联网新技术新应用，开展分众化传播、差异化传播、个性化传播，推动全媒体宣传、全业态传播、全平台覆盖，做到春风化雨、润物无声。

加强和改进网络宣传引导工作，为打赢疫情防控阻击战、夺取全面建成小康社会新胜利营造良好舆论氛围

今年，我国将实现现行标准下农村贫困人口全部脱贫、贫困县全部摘帽，实现全面建成小康社会目标。新冠肺炎疫情给实现全年奋斗目标增添了新的挑战和工作难度。我们必须加强网络内容建设，建立健全网络综合治理体系，为打赢疫情防控阻击战、全面建成小康社会营造良好网上舆论氛围。丰富内容供给，充分利用新技术加强和改进网上正面宣传，建设网上“正能量稿池”，打造“现象级”内容产品，调动各类媒体和广大网民的积极性，大力宣传各地区各部门统筹推进疫情防控和脱贫攻坚工作的新举措新成效，提高网上正能量传播的精准性和有效性。创新舆论引导，坚持辨证施治、疏堵结合，主动设置议题，策划推送更多优质的网上视频、图片、文章，及时回应社会关切特别是群众的集中诉求，做好疫情权威信息网上发布，畅通密切联系群众的网络渠道，把网上舆情引导到正确方向。强化综合治理，加大依法管网、技术治网力度，推动落实主体责任、主管责任、监管责任，健全网上重大舆情和突发事件舆论引导机制，有效辨别不同性质问题、精准采取分门别类措施，及时处置各种谣言信息，深化网络生态治理，维护网络意识形态安全，营造清朗网络空间。

充分发挥信息化驱动引领作用，为经济社会高质量发展提供新动能

习近平总书记指出，世界正在进入以信息产业为主导的经济发展时期。我们要把握数字化、网络化、智能化融合发展的契机，以信息化、智能化为杠杆培育新动能，为推动经济社会高质量发展提供有力支撑。着力突破关键核心技术，发挥新型举国体制优势，依托广阔市

场滋养，坚定不移走自主创新之路；加强产业协同和技术合作攻关，加快补齐短板、攻克关键核心技术、突破前瞻性技术，加快建立现代信息技术和产业生态体系。着力建强新一代信息基础设施，加强总体规划引领，统筹推进 5G 发展，加快制造、能源、交通、智慧城市等重点领域应用；加快卫星互联网、北斗卫星导航系统建设应用，推进基于 IPv6 的下一代互联网规模部署，推动 5G、人工智能、工业互联网、物联网、数据中心等新型基础设施建设，抢占发展的主动权。着力发挥数字经济引擎作用，积极发展云计算、大数据、人工智能等，广泛开展应用和模式创新，扩大电子商务、电子政务、网络娱乐等方面消费，加快制造业、农业、服务业数字化、网络化、智能化，推进数字经济与实体经济深度融合。着力推动信息惠民为民便民，深入实施网络扶贫、“互联网+教育” “互联网+医疗”等，加快新型智慧城市、数字乡村建设，让互联网更好造福人民群众。着力服务疫情防控工作，充分利用大数据、人工智能等信息化手段做好疫情防控工作，动态反映疫情态势、追踪疫病传播路径、助力社区疫情防控部署、服务复工复产，助力医疗物资、生活物资有效对接，积极开展远程授课、在线办公、线上诊疗等“互联网+”便民服务，服务疫苗技术科研攻关，并做好疫情防控中的个人信息保护工作。

切实提升网络安全防护能力，筑牢国家网络安全屏障

习近平总书记指出，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。我们要树立正确的网络安全观，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，统筹推进网络安全工作，构筑起坚实的网络空间安全屏障。着力提升网络防护力，严格落实《网络安全法》、网络安全工作责任制要求，加强网络安全检查，强化关键信息基础设施安全保护，完善网络安全监测预警和应急响应机制，协同应对重大网络安全事件。着力提升数据保护力，加快制定数据安全管理办法，加强个人信息和重要数据出境安全评估，督促企业加强数据安全风险评估，加强对大数据企业的管理，依法坚决打击网络违法犯罪活动。着力提升发展支撑力，加强网络安全产业的统筹规划和整体布局，完善相关支持政策措施，增加网络安全投入，加强政府、企业、行业、技术机构等的合作，促进资源共享、优势互补，共同推动网络安全产业发展壮大。着力提升人才供给力，加快推进国家网络安全人才与创新基地建设，积极开展一流网络安全学院建设示范项目，深入开展网络安全知识技能宣传普及，办好国家网络安全宣传周，不断提高广大人民群众网络安全意识和防护技能，共筑网络安全防线。

加强对习近平总书记关于构建网络空间命运共同体理念主张的理论研究、宣介阐释和国

际传播，继续办好世界互联网大会，深度参与网络空间国际治理多边活动，加强同“一带一路”相关国家、新兴市场国家网信领域务实合作，深化互联网企业、智库等沟通互动，拓展网信合作内涵，打造覆盖全球、深度融合、互利共赢的合作新格局，持续提升我国在网络空间的国际话语权和影响力。

加强党对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进

习近平总书记强调，我们党过不了互联网这一关，就过不了长期执政这一关。要旗帜鲜明、毫不动摇坚持党管互联网，不断改革完善党对网信工作的领导方式、体制机制，加强网信领域党的建设，为网络强国建设提供有力保障。教育引导广大党员干部从我们党经受执政考验、巩固执政地位、提高执政能力的战略高度来认识互联网、运用互联网、发展互联网，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。健全网信工作体系，坚持党管互联网与全面深化改革有机结合，努力建立与网络强国战略相适应的体制机制，同时充分发挥网信部门的统筹协调作用和各部门的职能作用，各司其职、密切配合，切实形成推进网信工作的整体合力。加快健全中央、省、市三级网信工作体系，积极推动工作任务重、有条件的地方延伸到四级，完善工作体系，加强工作力量。加强网信人才和干部队伍建设，加快建立适应网信工作特点的人事、薪酬、职称等制度，为推动网络强国建设提供更加坚实的人才保障。围绕加强对干部“育选管用”综合施策，进一步树立正确的选人用人导向，激励干部担当作为。加强网信领域党的建设，贯彻落实《中共中央关于加强党的政治建设的意见》，深入实施党建高质量发展行动计划，突出全面从严治党这个关键，持之以恒正风肃纪，建设让党中央放心、让人民群众满意的模范机关，切实打造忠诚干净担当的网信铁军。（来源：本文系中共中央宣传部副部长，中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文在《旗帜》2020 年第 4 期刊发的署名文章））

➢ 强化数据分类分级安全管理，推进完善数据要素市场化配置

在当前信息技术变革浪潮中，数据资源正在朝着生产要素的形态不断演进。近期，《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》（以下简称“《意见》”）正式发布，《意见》将数据列为五大要素领域之一，明确了完善要素市场化配置的具体举措。为实现数据要素价格市场决定、流动自主有序、配置高效公平的目标，尚需要解决数据确权、数据安全、隐私保护等诸多问题，在此过程中数据分类分级管理体系的构建能够发挥重要支

撑推动作用。

一、数据要素已经成为经济发展新动能

近年来，国家高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用。2015 年 9 月国务院印发的《促进大数据发展行动纲要》已经明确指出，“数据已成为国家基础性战略资源，大数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。”2016 年，习近平总书记在网络安全和信息化工作座谈会上的讲话再一次强调，“以信息流带动技术流、资金流、人才流、物资流，促进资源配置优化，促进全要素生产率提升，为推动创新发展、转变经济发展方式、调整经济结构发挥积极作用。”由此观之，数据作为一种新型生产要素，对其他要素分配效率具有倍增作用，加快培育数据要素市场，将对推动我国经济高质量转型、数字经济创新发展注入新动能。

《意见》在数据要素部分，明确提出推进政府数据开放共享、提升社会数据资源价值，通过制定出台新一批数据共享责任清单、支持构建多领域数据开放利用场景、探索建立统一的数据管理制度，全面提升数据要素价值。同时，在“稳中求进，循序渐进”基本原则指引下，坚持安全可控，制定数据隐私保护制度和安全审查制度，完善适用于大数据环境下的数据分类分级安全保护制度。

二、实施数据分类分级安全管理的重要意义

（一） 数据分类分级安全管理是推进政务信息共享开放的重要保障

依托政务数据共享开放推进政府数字化转型、提升政府公共服务水平、促进大数据产业发展，已经成为全球共识。2016 年开始，我国颁布了《政务信息资源共享管理暂行办法》、《公共信息资源开放试点工作方案》等一系列文件，开启了政务数据共享开放进程。由于政

务数据自身特性，在开放和流通过程面临着各种不确定安全风险，出于维护国家安全、社会公共利益的考虑，目前我国政务数据向公众开放的程度相对有限。为促进政务数据进一步融入要素市场，释放政府数据可开发、可利用的潜能，需要在已建立的政务信息资源目录基础上，制定更加细化的数据分类分级规则，通过配套差异化的安全控制措施，保障政务数据在共享开放过程中的可监测、可追溯。

（二） 数据分类分级安全管理是培育数字经济新业态新模式的助推利器

运用 5G、物联网、人工智能等信息技术，创新农业、工业、交通、教育、安防、城市管理、公共资源交易等领域的数据开发利用场景，是培育数字经济新产业、新业态、新模式的重要引擎。而数据开发利用活动越活跃，数据泄露、滥用的安全风险越高，特别是对个人信息安全的影响越大。为数据开发利用活动配备高水平安全措施，又必然增加市场参与主体的经营成本。因此，健全完善社会数据资源分类分级管理制度，鼓励掌握数据资源的市场参与主体构建数据分类分级安全管理体系，以风险防控为工作导向，对高安全等级数据的开发利用活动，配套相应的安全风险控制措施，是能够充分释放数据资源价值潜能，又能够有效控制成本投入的最佳路径。

（三） 数据分类分级安全管理是促进大数据流动与交易的基础前提

相对于其他工业产品，数据要素与传统生产要素在本质上有巨大差异，数据产品具有可复制性、生产门槛低、时间敏感性等特点。市场各方在推动大数据流动与交易的同时，需要解决数据确权、数据安全、隐私保护等诸多问题。引入数据分类分级这一基础性数据安全管理方法，综合考虑数据属性、特点、数量、质量、格式、重要性、敏感程度等因素，对数据资源进行分类分级，梳理出非敏感、低风险等级、权属相对明确的数据资源，以要素形式优先进入数据交易市场，同时明确在市场交易过程中应配备的安全保护措施，可以在最大限度释放数据价值的同时，又兼顾数据安全和对个人隐私的保护。

（四） 数据分类分级安全管理是新一代数据资产管理理念的核心思想

数字经济的发展以数据资产作为核心生产要素，目前以网络和系统为中心的安全防护模式下，安全措施与防护目标不能精确匹配，无法达成预期的防护效果。新一代数据资产管理理念从组织的高层业务风险分析出发，以数据资产分类分级为核心，对组织业务中的各个数据集进行识别、分类和分级安全管理，针对数据集的数据流和数据分析库的机密性、完整性、可用性、可控性需求创建安全策略，根据策略落实安全管理措施和部署安全技术产品，同时对业务风险进行优先级排列，采取适当的安全措施对业务风险进行控制。从而实现数据资产安全管理从以网络和系统为中心向以数据资产为中心的安全保护模式转变。

三、推进数据分类分级安全管理工作的建议

一是健全数据分类分级安全管理制度。健全完善适应于大数据环境下的数据分类分级安全管理制度，需要涵盖参与要素市场的各方主体，包括但不限于政府部门、掌握数据资源的企业及组织、第三方专业数据服务机构，明确各方数据分类分级安全管理主体责任。同时，需要根据各行业各领域数据资源属性特点，分业施策，制定适应于本行业本领域数据资源开发利用及流通需求的数据分类分级安全管理规则。

二是加快制定数据分类分级标准。研究 5G、物联网、人工智能等新技术背景下新业务的数据形态、特点、流通场景、重要性、敏感程度等关键因素，深入调研行业、企业数据安全管理现状，鼓励企业参加标准的编制工作，明确标准应解决的实际问题，编制适合数字经济新产业、新业态、新应用模式的数据分类分级标准，为企业数据安全管理和安全资源配置提供指导。

三是提高数据分类分级优质产品供给。扶持技术实力强的数据安全产品与服务企业加大数据分类分级产品研发投入，同时引导数据交易各方积极参与数据分类分级产品的应用创新，通过引领和示范作用带动数据分类分级产品的落地实施，加速数据安全产品和技术的成熟和更新迭代，为参与要素市场的各方主体赋能，提升其数据分类分级安全管理能力，为数据要素市场的活跃与发展提供安全保障。（来源：中国信通院）

➢ 落实网络安全审查制度 保障关键信息基础设施供应链安全

对涉及国家安全的网络产品和服务进行网络安全审查已成为国际通行做法，也是国际社会所普遍接受的保障国家网络安全的正当措施。作为网络空间法治化的重要一环，网络安全审查制度对维护我国国家安全，推进国家治理体系和治理能力现代化可谓意义深远。实践证明，网络安全审查是保障关键信息基础设施供应链安全、捍卫我国网络空间主权、保障国家安全与核心利益的基础性制度。在建设网络强国、数字中国和智慧社会的过程中，网络安全审查制度必将发挥其重要作用。

一、我国网络安全审查制度的发展历程

2014 年 5 月，我国正式宣布将推出网络安全审查制度。2015 年 7 月通过的《国家安全法》第五十九条规定的国家安全审查制度，成为网络安全审查的上位制度。2016 年 7 月，《国家信息化发展战略纲要》明确我国要建立实施网络安全审查制度。2016 年 11 月通过的

《网络安全法》第三十五条规定，“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”，正式开启了网络安全审查制度法治化的历程。

为贯彻落实《网络安全法》规定的网络安全审查制度，2017 年 5 月 22 日，国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》（以下简称“试行办法”）。试行办法规定了网络安全审查的内容、审查机构和审查程序等核心制度，确保了网络安全审查的标准公开、程序透明、结论公正。

通过试行办法的实施，国家对构建网络安全审查制度进行了大量有益的探索。同时，随着物联网、区块链、人工智能、量子计算等新技术和新应用的出现，网络空间的大国博弈日趋激烈，网络安全形势发生了重大变化。为应对新的网络安全威胁和风险，同时修正试行办法的不足之处，国家互联网信息办公室等 12 个部门 2020 年 4 月 13 日印发《网络安全审查办法》（以下简称审查办法），开启了我国网络安全审查制度的新时代。

二、我国网络安全审查制度的基本定位

网络产品和服务，不能存在危及网民合法权益、公共安全的缺陷，更不能存在危及国家安全的隐患，这是对网络产品和服务的基本要求。为了应对日益严峻、复杂的网络安全威胁，有必要通过网络安全审查制度，评估和审核网络产品或者服务是否存在危害关键信息基础设施安全和国家安全的可能或者风险。网络安全审查不同于测评、认证，也不同于通用性审查、

外商投资国家安全审查，重点审查网络产品或者服务是否存在影响关键信息基础设施安全和国家安全的威胁或者风险。

我国的网络安全审查制度，是在准确理解网络安全的本质，深刻认识所面临的国内外网络安全形势的基础上，坚持总体国家安全观以及整体、动态、开放、相对、共同网络安全观，正确处理安全与发展关系的前提下，确立的在开放环境下应对网络安全威胁与风险的基础性制度，是维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益的“底层”制度，是我国掌握网络空间防御主动权的重要利器。

三、我国网络安全审查制度的四大特色

作为保障国家安全的重要制度设计，网络安全审查是我国和平利用网络空间、坚定维护网络空间安全战略理念的体现。以法律的形式确立网络安全审查制度，通过法制手段保障国家安全，是减少网络空间技术对抗与冲突的有益尝试，这是我国网络安全审查制度最大的亮点。作为防范网络空间新型国家安全风险的重要手段，我国网络安全审查制度在广泛借鉴国际通行做法的基础上，重点考虑了我国网络安全所面临的一般风险和特殊风险，制度设计具有以下特色：

（一）将关键信息基础设施供应链安全作为关注重点

美国的网络安全审查具体覆盖国家安全系统、国防系统、联邦政府系统。英国网络安全审查的重点是外国公司在英国关键基础设施的投资是否会影响国家安全。我国的审查办法聚焦于关键信息基础设施供应链安全，旨在避免可能对关键信息基础设施的保密性、完整性和可用性构成威胁而引发国家安全风险。

（二）对国内外供应商一视同仁

美国 2013 年颁布的《综合持续拨款法案》中针对特定国家的产品和服务进行网络安全审查的规定，严重违背国际贸易的“非歧视性”原则，引发了各方激烈的抨击。2010 年印度电信部以安全为由禁止本国运营商在敏感区域购买中国电信设备，但允许向欧美厂商采购，并向运营商发出通知明确在采购信息产品时，印度本地人控股或者所有的企业免于网络安全审查。反观我国网络安全审查制度的设计，对国内供应商和国外供应商一视同仁。只要符合网络安全基线的产品或者服务，都可以在关键信息基础设施中使用，而不论供应商国籍和产品来源地，这为全球网络产品和服务市场创造了一个公平竞争的场所和环境。

（三）坚持公开透明的原则

与美国、印度等国家的网络安全审查相比，我国网络安全审查做到了最大限度的公开透明。我国的审查办法明确了审查主要考虑的五方面因素，能够最大限度保证审查活动的公正

性和透明度，有利于消除各方将网络安全审查制度作为“政策工具”的顾虑。审查标准公开透明，使供应商能够依照审查标准准确判断自身产品或者服务的安全状况，为供应商提供了明确的行为指引和预期。同时，为审查机构提供明确的工作指引和依据，避免了审查权的滥用，有利于实现风险控制的目的。

（四）持续进行风险监督

审查办法要求运营者督促供应商履行网络安全审查中作出的承诺，同时，网络安全审查办公室通过接受举报等形式加强事前事中事后监督。这一规定使网络安全审查由“节点控制”转变为“过程控制”，网络安全审查源于采购阶段，但监督拓展至网络产品和服务的整个生命周期。风险的持续性监控，有利于全面提升关键信息基础设施的安全保障能力。（来源：网信中国）

➢ 顺势而为发展个人信息保护专业人员（CISP-PIP）资质测评体系

一、个人信息保护的形势

当前，数据已成为国家基础性战略资源。在为社会创造巨大价值的同时，也有越来越多的个人信息和重要数据遭到非法收集、泄露、滥用。为此，各国纷纷加强数据安全保护，欧盟《通用数据保护条例》在全球产生重大影响，数据跨境流动政策引领世界贸易规则重构。我国出台了《网络安全法》《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等法律法规，《数据安全管理办法》《个人信息出境安全评估办法》等政策文件正在加快起草，大批国家标准陆续发布实施，多个网络安全主管部门开展数据安全专项行动，全国人大已将《数据安全法》《个人信息保护法》列入本届立法规划。随着数据的基础资源作用和创新引擎作用日益显现，数据安全特别是个人信息保护的合规性成为各行业共同面临的急迫问题。

2019 年 9 月，习近平总书记对国家网络安全宣传周作出重要指示强调，保障个人信息安全，维护公民在网络空间的合法权益，提升广大人民群众在网络空间的获得感、幸福感、安全感。落实总书记的重要指示，就必须将个人信息保护作为当前一项十分重要且迫切的工作抓紧抓好。

人才是第一资源。由于个人信息保护和数据安全形势变化迅速、技术更新快等原因，仅依靠知识体系较为固定的学历教育难以满足实际工作需求，具有较强时效性、针对性、灵活性的专业人员认证已成为个人信息保护工作的重要抓手。从全球看，此类认证制度方兴未艾，

目前各国都在积极推进。

二、国外个人信息保护专业人员认证情况

目前，国际影响力较大的个人信息保护认证项目为“国际隐私专业人员协会”（IAPP）认证。IAPP 成立于 2000 年，是一个非盈利性组织，也是全球最大的隐私信息保护社区和资源库，致力于提升隐私保护从业人员职业技能，帮助不同组织提高管理和保护隐私数据的能力。

IAPP 认证作为目前全球顶级的隐私保护认证，包括隐私保护专业人员认证（CIPP）、隐私保护经理认证（CIPM）和隐私保护技术专家认证（CIPT）3 个项目。其中，CIPP 认证主要适用于隐私保护法律法规、合规性审查、信息管理、数据治理、人力资源等领域的从业人员。因各国（地区）数据安全政策不同，CIPP 认证又分为 CIPP/A（Asia）、CIPP/US（U.S. private-sector）、CIPP/G（U.S. Government）、CIPP/C（Canada）和 CIPP/E（Europe）等 5 个子类。CIPM 则主要满足隐私项目生命周期内风险管理、隐私运行、审计与追责、隐私分析等方面的需求。CIPT 面向 IT 从业者开展隐私保护认证，可证明专业人员在 IT 产品和服务的开发、工程、部署与审计方面，对于隐私和数据保护实践的理解程度，以及管理和建立隐私保护要求和控制措施的能力。

获得 IAPP 认证的过程包括申请、准备、考试、发证、认证维持等环节。IAPP 在全球各地设置了 800 多个机考考试点，也可在美国全球隐私峰会、美国隐私安全风险、欧洲数据保护会议三个国际会议期间进行笔考。IAPP 所有考试均采用英语，对于 CIPP/E 也可采用法语和德语。机考和笔考的考试内容相同，不同种类认证的考试要求有所不同。IAPP 采用持续隐私教育（CPE）政策维持认证证书的有效性。证书有效期内（一般为 2 年），为了维持认证资格，所有证书持有人必须至少满足两个要求：一是每年缴纳证书维持费；二是以 2 年为周期，每种证书持有人应完成规定课时的 CPE。IAPP 为获得 CPE 课时提供了多种方式，如参加

隐私保护相关国际会议、学术演讲、学习资料、参加 IAP 的培训等。

三、我国个人信息保护专业人员认证实践——CISP-PIP 项目

适应我国个人信息保护和数据安全工作需要，2019 年，中国信息安全测评中心依据中编办批准开展“信息安全人员培训与资质认证”的职能，推出了对个人信息保护专业人员能力认定的 CISP-PIP（注册信息安全专业人员-个人信息保护）项目，并授权设立了 CISP-PIP 运营中心。该项目面向我国数据保护、信息审计、组织合规与风险管理等领域的信息安全专业人员，紧密围绕《网络安全法》及其他数据安全管理政策法规的要求，以加强个人信息保护为目标，同时兼顾国家重要数据保护需求以及医疗健康、金融等领域的行业大数据应用及安全需求，突出了对重要政策法规、重要标准的合规性培训，旨在为我国个人信息安全保护工作培养一支强有力的专业人才队伍。

CISP-PIP 知识体系以个人信息安全保护为主线，以落实政策、衔接国际、注重实效为基本原则，全面覆盖基础、标准、法规、技术、管理和工程等领域，并与典型案例和全球最新实践紧密结合。一方面，该项目与 CISP 形成进阶关系，适度保留注册信息安全专业人员应掌握的三类通用知识：国家网络安全顶层设计、网络安全体系结构以及网络安全管理与工程。另一方面，参考 IAPP 等知识体系，基于《网络安全法》《个人信息安全规范》等主要法规标准要求，设计专业培训与考试内容。专业知识包含五个方面：数据安全基础、GB/T 35273《个人信息安全规范》、个人信息安全标准体系、个人信息保护实践、行业个人信息保护。如图 1 所示。

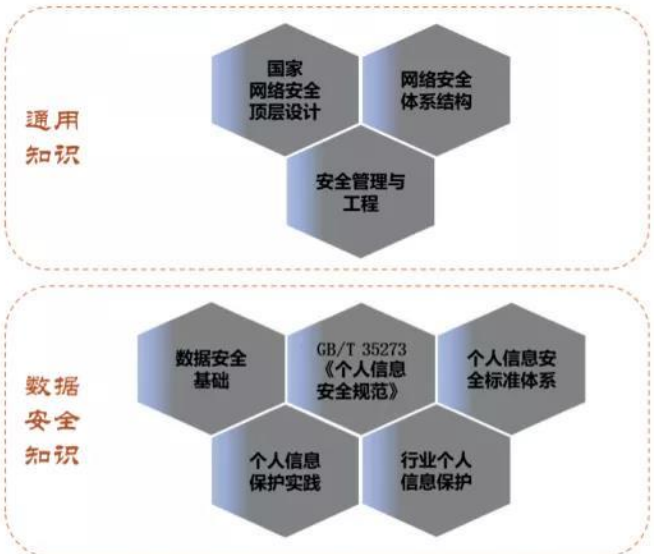


图 1：CISP-PIP 知识体系结构框架

CISP-PIP 项目认证过程与 CISP 一致，认证过程主要包括注册申请、资格审核、参加考试、证书发放、证后监督等环节。

四、下一步推进工作的建议

通过对国外 IAPP 认证制度的分析和我国 CISP-PIP 项目实践，关于我国个人信息保护专业人员资质测评体系的建设，提出以下建议。

一是进一步细化 CISP-PIP 项目。

可在先期成功探索的基础上，借鉴 IAPP，择机将 CISP-PIP 扩展至 3 类资质认定项目：个人信息保护专业人士，主要适用于个人信息保护法律法规、合规审查、信息管理、数据治理、人力资源等领域的从业人员；个人信息保护项目经理，主要面向来自政府、监管部门以及企事业单位等从事个人信息保护项目管理人员；个人信息保护技术专家，主要面向 IT 产品和服务开发、工程、部署、运维和审计专业人士。必要时，还可针对医疗健康、金融、交通、教育、能源等数据安全影响较为突出的行业设立定制化培训内容，开展更细粒度的人员资质测评。

二是逐步建立我国个人信息保护专业人员认证持续教育政策。

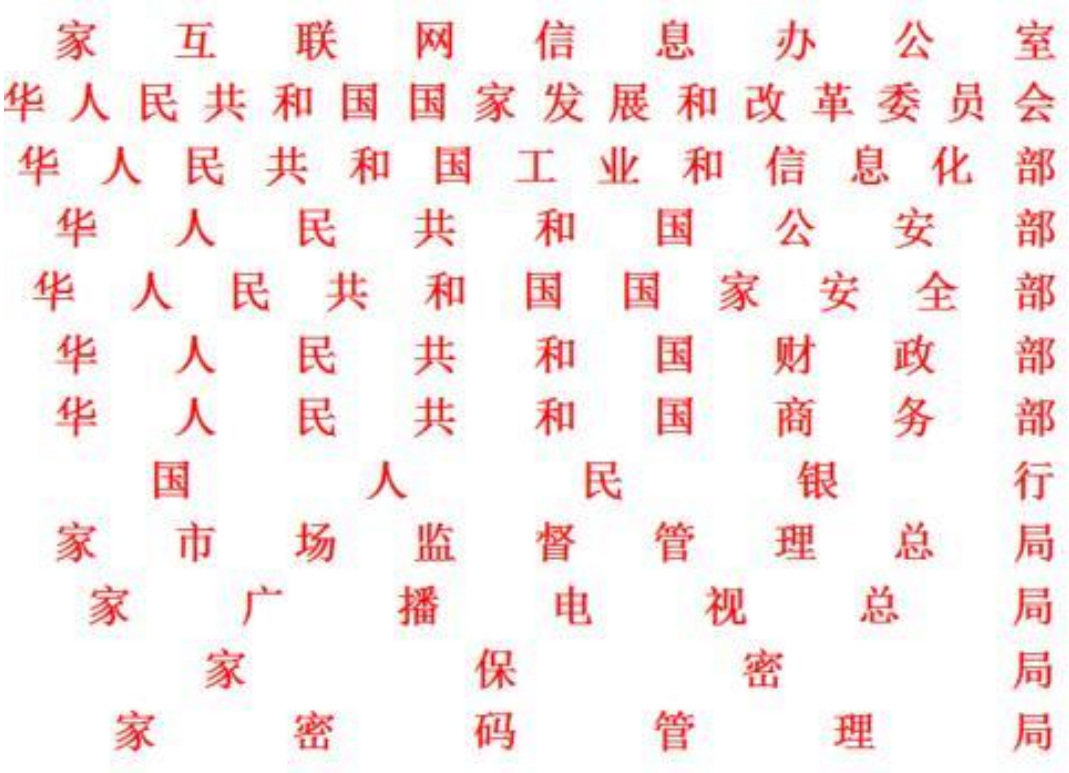
持续教育主要服务于人员认证制度，用于支撑认证证书有效期的维持；也可以服务于国内个人信息保护相关教育、培训等需求。一个可行的举措是，将我国多个主管部门牵头开展的个人信息保护专项行动、标准制定等与持续教育相衔接，鼓励获证人员积极参与。

三是以网站、公众号等形式建立一个以个人信息保护专业人员认证为主题的交流平台，并借此在国内推广个人信息保护文化。（来源:《中国信息安全》杂志 2020 年第 4 期）

四、政府之声

➢ 《网络安全审查办法》发布附答记者问

2020 年 4 月 27 日，国家互联网信息办公室、国家发改委等 12 个部门联合发布了《网络安全审查办法》（以下简称《办法》）。国家互联网信息办公室有关负责人就《办法》相关问题回答了记者的提问。



问：请您介绍一下《办法》出台的背景？

答：关键信息基础设施对国家安全、经济安全、社会稳定、公众健康和安全至关重要。我国建立网络安全审查制度，目的是通过网络安全审查这一举措，及早发现并避免采购产品和服务给关键信息基础设施运行带来风险和危害，保障关键信息基础设施供应链安全，维护国家安全。《办法》的出台，为我国开展网络安全审查工作提供了重要的制度保障。

问：网络安全审查的法律依据是什么？

答：网络安全审查是依据《国家安全法》《网络安全法》开展的一项工作。《国家安全法》第五十九条规定，国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的网络信息技术产品和服务，以及其他重大事项和活动，进行国家安全审查。《网络安全法》第三十五条规定，“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安

全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”。

问：网络安全审查主要审查哪些内容？

答：网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险，包括：产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；其他可能危害关键信息基础设施安全和国家安全的因素。

问：哪些网络运营者采购产品和服务需要考虑申报网络安全审查？

答：关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照《办法》进行网络安全审查。

根据中央网络安全和信息化委员会《关于关键信息基础设施安全保护工作有关事项的通知》精神，电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照《办法》要求考虑申报网络安全审查。

问：何时申报网络安全审查？

答：通常情况下，关键信息基础设施运营者应当在与产品和服务提供方正式签署合同前申报网络安全审查。如果在签署合同后申报网络安全审查，建议在合同中注明此合同须在产品和服务采购通过网络安全审查后方可生效，以避免因为没有通过网络安全审查而造成损失。

问：网络安全审查有无时限要求？

答：通常情况下，网络安全审查在 45 个工作日内完成，情况复杂的会延长 15 个工作日。进入特别审查程序的审查项目，可能还需要 45 个工作日或者更长。根据《办法》要求，补充提供材料的时间不计入审查时限。

问：审查过程中如何保证关键信息基础设施运营者及产品和服务提供者的商业秘密和知识产权？

答：网络安全审查充分尊重和严格保护企业的知识产权。《办法》规定，参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对关键信息基础设施运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。关键信息基础设施运

营者或产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或有关部门举报。

问：网络安全审查是否会限制或歧视国外产品和服务？

答：《办法》明确规定了要审查的内容，从中可以看出，网络安全审查的目的是维护国家网络安全，不是要限制或歧视国外产品和服务。

对外开放是我们的基本国策，我们欢迎国外产品和服务进入中国市场的政策没有改变。

问：违反《办法》规定应承担哪些法律责任？

答：根据《网络安全法》第六十五条规定，应当申报网络安全审查而没有申报的，或者使用网络安全审查未通过的产品和服务，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

问：网络安全审查向谁申报？

答：根据《办法》，网络安全审查办公室设在国家互联网信息办公室。具体工作委托中国网络安全审查技术与认证中心承担。

中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接收申报材料、对申报材料进行形式审查、具体组织审查工作等任务。（来源：国家网信办）

- **《网络安全审查办法》**
- **全文：**http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

➢ CNNIC：第 45 次《中国互联网络发展状况统计报告》发布

2020 年 4 月 28 日，中国互联网络信息中心（CNNIC）发布第 45 次《中国互联网络发展状况统计报告》（以下简称:《报告》）。《报告》围绕互联网基础建设、网民规模及结构、互联网应用发展、互联网政务发展、产业与技术发展和互联网安全等六个方面，力求通过多角度、全方位的数据展现，综合反映 2019 年及 2020 年初我国互联网发展状况。

网民规模突破 9 亿 为数字经济发展打下坚实用户基础

《报告》显示，截至 2020 年 3 月，我国网民规模为 9.04 亿，互联网普及率达 64.5%，庞大的网民构成了中国蓬勃发展的消费市场，也为数字经济发展打下了坚实的用户基础。

CNNIC 主任曾宇指出，当前，数字经济已成为经济增长的新动能，新业态、新模式层出不穷。在此次疫情中，数字经济在保障消费和就业、推动复工复产等方面发挥了重要作用，展现出了强大的增长潜力。曾宇表示，本次报告主要呈现三个特点：

一是基础设施建设持续完善，“新基建”助力产业结构升级。2019 年，我国已建成全球最大规模光纤和移动通信网络，行政村通光纤和 4G 比例均超过 98%，固定互联网宽带用户接入超过 4.5 亿户。同时，围绕高技术产业、科研创新、智慧城市等相关的新型基础设施建设不断加快，进一步加速新技术的产业应用，并催生新的产业形态，扩大了新供给，推动形成新的经济模式，将有力推动区域经济发展质量提升和产业结构优化升级。

二是数字经济蓬勃发展，成为经济发展的新增长点。网络购物持续助力消费市场蓬勃发展。截至 2020 年 3 月，我国网络购物用户规模达 7.10 亿，2019 年交易规模达 10.63 万亿元，同比增长 16.5%。数字贸易不断开辟外贸发展的新空间。2019 年，通过海关跨境电子商务管理平台零售进出口商品总额达 1862.1 亿元，增长了 38.3%。数字企业加速赋能产业发展。数字企业通过商业模式创新、加快数字技术应用不断提升供应链数字化水平，为产业转型升级提供了重要支撑。

三是互联网应用提升群众获得感，网络扶贫助力脱贫攻坚。互联网应用与群众生活结合

日趋紧密，微信、短视频、直播等应用降低了互联网使用门槛，不断丰富群众的文化娱乐生活；在线政务应用以民为本，着力解决群众日常办事的堵点、痛点和难点；网络购物、网络公益等互联网服务在实现农民增收、带动广大网民参与脱贫攻坚行动中发挥了日趋重要的作用。

疫情期间部分互联网应用呈现快速增长态势

CNNIC 副主任张晓表示，2020 年初，受新冠肺炎疫情影响，大部分网络应用的用户规模呈现较大幅度增长。其中，在线教育、在线政务、网络支付、网络视频、网络购物、即时通信、网络音乐、搜索引擎等应用的用户规模较 2018 年底增长迅速，增幅均在 10%以上。

在线教育呈现爆发式增长。截至 2020 年 3 月，我国在线教育用户规模达 4.23 亿，较 2018 年底增长 110.2%，占网民整体的 46.8%。2020 年初，全国大中小学校推迟开学，2.65 亿在校生普遍转向线上课程，用户需求得到充分释放，在线教育应用呈现爆发式增长态势。

网络零售成为消费增长重要动力。截至 2020 年 3 月，我国网络购物用户规模达 7.10 亿，较 2018 年底增长 16.4%，占网民整体的 78.6%。2020 年 1-2 月份，全国实物商品网上零售额同比增长 3.0%，实现逆势增长，占社会消费品零售总额的比重为 21.5%，比上年同期提高 5 个百分点。

全国一体化政务服务平台在疫情防控中发挥有力支撑。截至 2020 年 3 月，我国在线政务服务用户规模达 6.94 亿，较 2018 年底增长 76.3%，占网民整体的 76.8%。疫情期间，国家及各地区一体化政务服务平台提供疫情信息服务，推行线上办理，协助推进精准防疫，应用成效越来越大，已经成为创新政府管理和优化政务服务的新渠道。

抗击疫情加速互联网产业发展 带来新机遇与挑战

此次报告记录了新冠肺炎疫情特殊背景下的互联网发展情况，国家信息化专家咨询委员会委员、中央党校（国家行政学院）教授汪玉凯认为，我国互联网产业拥有庞大的消费市场、企业和技术基础，在后疫情时代将迎来新一轮快速发展的历史机遇，互联网产业将呈现全新的蓬勃发展态势。一是新基建将迎来大发展，成为经济社会的重要底层支撑；二是在线服务、网络消费等互联网业态将进一步繁荣发展，成为驱动经济增长的新动能；三是消费互联网向产业互联网加速升级，产业数字化转型进程将不断加快；四是万物互联将形成大连接，进一步推动互联网红利共享；五是数据要素将形成大流动，数字产业的价值和潜力进一步得到发挥；六是平台经济大生态将更加丰富，对实体产业转型的赋能作用将持续凸显。

我国技术创新能力持续增强 产业互联网加速推进

中国互联网协会原副秘书长孙永革表示，此次报告体现了区块链、IPV6、5G、人工智能、

大数据等核心技术领域的快速发展，其深度融合形成的产业互联网将成为推动数字经济发展的新动能和构建智慧型社会的新支柱。首先，区块链技术受到我国政府和企业的高度重视。在政府与企业的共同推动下，我国区块链发明专利数量实现连续两年位居全球第一，区块链技术已经在很多传统产业的数字化转型升级过程中发挥作用。其次，5G 商业化的全面启动将有力推动科技产业创新升级。截至 2019 年 12 月，我国已经建成 5G 基站超过 13 万个，5G 产业链推动人工智能与物联网结合发展到智联网。最后，人工智能技术在我国实现快速发展，将成为赢得全球科技竞争主动权的重要战略抓手。2019 年，我国人工智能企业数量超过 4000 家，位列全球第二，在智能制造和车联网等应用领域优势明显。实现基于人工智能的智能制造将是个长期过程，我们需要将管理创新和技术创新并重，来应对发展中的挑战，推动数字经济发展。

2020 年是全面建成小康社会和“十三五”规划收官之年，是网信事业全面提升的新起点。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。作为网络强国建设历程的忠实记录者，CNNIC 将持续跟进我国互联网发展进程，不断扩大研究范围，深化研究领域，与全社会一起推动网络安全和信息化工作再上新台阶。（来源：中国互联网络信息中心）

- **第 45 次《中国互联网络发展状况统计报告》全文**
- http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202004/P020200428596599037028.pdf

➢ 国家市场监管总局（标准委）发布《个人健康信息码》系列国家标准

2020 年 4 月 29 日，市场监管总局（标准委）印发公告，发布《个人健康信息码》系列国家标准。该系列标准采用了国家标准快速程序，从立项到发布仅用了 14 天时间。

《个人健康信息码》系列国家标准包括《个人健康信息码 参考模型》（GB/T 38961-2020）、《个人健康信息码 数据格式》（GB/T 38962-2020）和《个人健康信息码 应用接口》（GB/T 38963-2020）3 项内容，由国务院办公厅电子政务办公室会同卫生健康委及国务院相关部门研究提出，全国信息技术标准化技术委员会负责技术归口。

其中，《个人健康信息码 参考模型》规定了健康码的组成和展现形式，提出了健康码应用系统的参考模型和跨地区互认的技术机制。《个人健康信息码 数据格式》规定了疫情防控

所需个人健康信息的数据结构、数据元属性和数据管理要求。《个人健康信息码 应用接口》规定了个人健康信息服务的接口，各类应用可通过统一接口对接不同的个人健康信息服务，为打通个人健康证明属地管理限制提供了技术支持，也为各地出行人员跨地区流动提供了便利。

该系列国家标准实施后，可实现个人健康信息码的码制统一、展现方式统一、数据内容统一，统筹兼顾个人信息保护和信息共享利用，适用于指导健康码相关信息系统的设计、开发和系统集成。（来源：国家市场监管总局）

➢ 工业和信息化部办公厅发布《关于深入推进移动物联网全面发展的通知》

2020 年 5 月 7 日，工业和信息化部近日发文部署深入推进移动物联网全面发展，提出建立 NB-IoT（窄带物联网）、4G（含 LTE-Cat1，即速率类别 1 的 4G 网络）和 5G 协同发展的移动物联网综合生态体系，在深化 4G 网络覆盖、加快 5G 网络建设的基础上，以 NB-IoT 满足大部分低速率场景需求，以 LTE-Cat1（以下简称 Cat1）满足中等速率物联需求和话音需求，以 5G 技术满足更高速率、低时延联网需求。

到 2020 年底，NB-IoT 网络实现县级以上城市主城区普遍覆盖，重点区域深度覆盖；移动物联网连接数达到 12 亿；推动 NB-IoT 模组价格与 2G 模组趋同，引导新增物联网终端向 NB-IoT 和 Cat1 迁移；打造一批 NB-IoT 应用标杆工程和 NB-IoT 百万级连接规模应用场景。同时明确，要着力完成加快移动物联网网络建设、加强移动物联网标准和技术研究、提升移动物联网应用广度和深度、构建高质量产业发展体系、建立健全移动物联网安全保障体系等五项重点任务。（来源：工业和信息化部）

- **《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》全文**
- **全文：**http://www.miit.gov.cn/n1146290/n1146402/c7901537/content.html

五、本期重要漏洞实例

➢ Adobe Bridge 越界写入漏洞

发布日期：2020-04-29
更新日期：2020-04-29
受影响系统：
Adobe Bridge 10.0.4
描述：

CVE(CAN) ID: CVE-2020-9560
Adobe Bridge 是 Adobe 公司推出的一款免费数字资产管理应用程序。
Adobe Bridge 存在安全漏洞。攻击者可利用漏洞执行任意。
*>
建议：

厂商补丁：
Adobe
用户可参考如下供应商提供的安全公告获得补丁信息：
https://helpx.adobe.com/security/products/bridge/apsb20-19.html

➢ Microsoft Windows 和 Windows Server 提权漏洞

发布日期：2020-04-29
更新日期：2020-04-29
受影响系统：
Microsoft Windows Server 1803
Microsoft Windows Server 2019
Microsoft Windows Server 1903
Microsoft Windows 10 1803
Microsoft Windows 10 1809
Microsoft Windows 10 1903
Microsoft Windows Server 1909
Microsoft Windows 10 1909
描述：

CVE(CAN) ID: CVE-2020-0996
Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft

Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Microsoft Windows 和 Windows Server 中存在提权漏洞，攻击者可通过登录到系统并运行特制的应用程序利用该漏洞在内核模式下运行任意代码。

*>

建议：

厂商补丁：

Microsoft

目前厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0996

➢ IBM Spectrum Protect 代码执行漏洞

发布日期：2020-4-29

更新日期：2020-4-29

受影响系统：

IBM Spectrum Protect >=8.1.0.0，<=8.1.9.200

IBM Spectrum Protect >=7.1.0.0，<=7.1.10.0

描述：

CVE(CAN) ID: CVE-2020-4415

IBM Spectrum Protect（前称 Tivoli Storage Manager）是美国 IBM 公司的一套数据保护平台。

IBM Spectrum Protect 8.1.0.0 版本至 8.1.9.200 版本和 7.1.0.0 版本至 7.1.10.0 版本中存在代码执行漏洞。该漏洞源于用户输入构造执行命令过程中，网络系统或产品未能正确过滤其中的特殊字符、命令等。远程攻击者可利用该漏洞执行任意代码或造成 Spectrum Protect 服务器崩溃。

*>

建议：

厂商补丁：

IBM

目前厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：

https://www.ibm.com/blogs/psirt/security-bulletin-stack-based-buffer-overflow-vulnerability-in-ibm-spectrum-protect-server/

➢ 多款 NETGEAR 产品缓冲区溢出漏洞

发布日期：2020-04-30
更新日期：2020-04-30
受影响系统：
NETGEAR D6200 <1.1.00.24
NETGEAR R6700v2 <1.1.0.42
NETGEAR R6800 <1.1.0.42
NETGEAR R6900v2 <1.1.0.42
NETGEAR R6020 <1.0.0.30
NETGEAR R6080 <1.0.0.30
NETGEAR R6120 <1.0.0.36
描述：

CVE(CAN) ID: CVE-2017-18730
NETGEAR R6700 等都是美国网件（NETGEAR）公司的产品。NETGEAR R6700 是一款无线路由器。NETGEAR D6200 是一款无线调制解调器。NETGEAR R6800 是一款无线路由器。
多款 NETGEAR 产品中存在缓冲区溢出漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。
*>
建议：

厂商补丁：
NETGEAR
目前厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：
https://kb.netgear.com/000051525/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-Some-Routers-and-Gateways-PSV-2017-2134

六、本期网络安全事件

➢ B 站 500 万粉 up 主被勒索 律师:黑客难罚除非涉商业机密

2020 年 4 月 28 日，视频红利时代，一位网红 up 主在 B 站积累了数百万粉丝，却也因此被盯上而遭遇了勒索病毒攻击。昨晚，B 站 500 多万粉丝的 up 主“机智的党妹”（下称“党妹”）发视频称，自己被勒索病毒攻击了，导致正在制作的数百个 GB 的视频素材文件，全都被病毒加密绑架，黑客留下一封勒索信，要求党妹“交出赎金，赎回人质”。

像这种黑客攻击，一般都不会受到处罚，除非你能证明他侵犯了你的商业秘密。”一位网络安全与数据合规领域的律师告诉新浪财经，遇到这样的事情，暂时无解，只能依靠“预防”。她建议，互动平台的 up 主们要注意提高自己的安全能力，必要的情况下，up 主们可以引入第三方的技术公司来做专门的安全测评，加固公司 IT 系统的安全性。

但实际上，党妹已经为素材备份做了一些准备，却并幸免。党妹介绍，为了方便存储使

用数百个 GB 的的视频素材，她的公司花了十几万在内部搭建了一个 NAS 系统，相当于一个公司内部人人可以访问公共硬盘，或者说私有云。

不幸的是，NAS 搭建好测试一段时间后，投入使用的第一天，也就是昨天，便遭到黑客攻击。NAS 里的所有文件都被改成了奇怪的格式，无法打开使用，而且黑客还在文件夹里留下了一封．txt 格式的勒索信。

据其介绍，信中说，这个 NAS 所有的文档、照片、数据等均已被加密，不要试图自己解密，恢复文件的唯一办法是购买一个独一无二的密匙，只有这个密匙才能解密这些文件。如果被攻击者想要验证黑客说的是不是真的，那就要给黑客发邮件，免费解开一个文件来证明。党妹称，黑客给被攻击者留下了一串 ID，需要给两个特定的邮箱发邮件联系，并通过这串 ID 来表明身份，与黑客谈判才能解开文件。

随后，党妹报警并抵达公安局，民警迅速受理，联系了网安部门进行速查评估，但警方最终给出的反馈是无法立案。警方建议党妹联系数据恢复公司，但由于黑客在勒索信中提醒，不要重命名这些文件，也不要用第三方软件解密，不仅可能让文件丢失，并且还会因为成本增加而让黑客收更高的解密费用，甚至遇到第三方可能是个骗子。

党妹介绍，据公司 IT 人员排查后发现，黑客用的是一种叫做 Buran 的勒索病毒，它专门攻击 Windows 系统。“它会运行自身，对硬盘里的其他文件进行加密，之后留下邮箱的 TXT 文档，再将自己删除。最可怕的是此次攻击技术难度几乎为 0：只需要知道 IP 地址，通过穷举法破译密码，获取一系列的权限。”党妹在视频中解释道。

党妹的遭遇，引发了一波网友对网络安全问题的讨论。近年来，像党妹这样的视频 up 主愈发受到网友的关注和喜爱，而视频的制作也从过去的极小成本逐渐向着复杂化专业化的方向发展。党妹曾在视频里透露过自己目前年收入在百万以上，而赚的钱一半以上都花在视频制作上。她表示自己曾为拍一支舞蹈视频花了 21 万，包括搭建场景、服化道等，因此丢失素材就意味着前期投入的人力物力所有的成本都付之一炬，而可量化计算的成本还不包括精力和创意。

一位网络安全与数据合规领域的律师称：党妹这起事件就是典型的网络安全事件。“像这种黑客攻击，一般都不会受到处罚，除非你能证明他侵犯了你的商业秘密。而对于尚未发布的视频素材，还没有盈利，很难去解释它的商业价值。一般的数据泄露就是因为公司的安全能力不够，不仅对方不会受到惩罚，而且如果是一个体量比较大的公司的话，还有可能会遭到那个监管机构对这个公司的处罚。”

该律师表示，体量较大的公司发生的安全事件，可能涉及到向当地的通信主管部门汇报，

对此，网信办有相应的法条《国家网络安全事件应急预案》，工信部也有《公共互联网网络安全突发事件应急预案》，但小公司通常不会涉及到。

上述律师建议，up 主们要注意提高自己的安全能力，采取一些比较好的安全措施。此外，她还提示道，必要的情况下，up 主们可以引入第三方的技术公司来做专门的安全测评，加固公司 IT 系统的安全性。一位粉丝量级较小的 up 主表示，从没考虑过关于网络安全以及素材被盗的隐患，因为粉丝较少，不会被盯上。

那么一些安全意识薄弱的小型企业及个人如何提升自身的勒索病毒防范能力？

建议如下：一、及时修复系统漏洞，做好日常安全运维；二、采用高强度密码，杜绝弱口令，增加勒索病毒入侵难度；三定期备份重要资料，建议使用单独的文件服务器对备份文件进行隔离存储；四、加强安全配置提高安全基线，例如关闭不必要的文件共享，关闭 3389、445、139、135 等不用的高危端口等；五、提高员工安全意识，不要点击来源不明的邮件，不要从不明网站下载软件；六、选择技术能力强的杀毒软件，以便在勒索病毒攻击愈演愈烈的情况下免受伤害。（来源：新浪）

➢ 四名辅警出售公民个人信息被判刑

2020 年 4 月 27 日，江苏淮安清江浦区人民法院公布一份侵犯公民个人信息刑事判决书。四位辅警利用职务便利，违规查询、出售公民个人车辆档案信息被判刑。

层层倒卖一条信息卖至 80 元

近年来，公安机关持续重拳打击侵犯公民个人信息的违法犯罪活动。据隐私护卫队了解，有些个人信息是从运营商、银行、政府部门等掌握大量个人信息的机构泄露的，违法出售信息者为内部员工。

在江苏淮安清江浦人民法院公布的这起案件中，泄露公民个人信息的源头正是四名辅警。2019 年 4 月至 6 月，浙江省乐清市白石交警中队辅警葛某某、赵某某利用职务之便，查询下载公民个人车辆档案信息（包括车辆牌照、车主信息、抵押情况等）330 余条，并出售给下线潘某某，每条价格为 30 元。

不仅如此，葛某某还让同事毛某某、徐某帮忙下载个人车辆档案信息，并以每条 20 元的价格购买。其中，毛某某下载个人车辆档案信息 140 余条，徐某下载 70 余条。

值得注意的是，信息经过层层倒卖，价格升至原来的四倍。潘某某购买信息后，转手卖给了雷某，每条售价为 80 元。此外雷某还从其他地方购买 1023 条信息。

最终，上述倒卖、侵犯公民个人信息的违法分子均被判刑。其中，雷某被判处有期徒刑三年四个月，罚款两万元；吴某被判处有期徒刑三年，缓刑五年；四位辅警被判处拘役四个月到有期徒刑三年、缓刑四年不等的处罚。

员工购买个人信息公司负责报销

近日湖南省衡阳市蒸湘区人民法院公布两份侵犯公民个人信息的判决书，其中个人信息的泄露源头也与公司内部员工有关。

2016 年 5 月至 2018 年 2 月，衡阳某装饰有限公司董事长周某某购买楼盘业主信息三万多条，花费 16000 余元。随后，他将这些信息分发给员工，用于拨打推销电话。为提升业绩，董事长、总裁等上级领导还鼓励店长、市场经理等员工购买楼盘业主信息，公司负责报销。

2017 年 10 月，该装饰公司员工李女士购买楼盘业主信息 845 条，花费 2000 元，后经公司报销 1600 元。2018 年 3 月，该公司市场二部经理阳某某购买楼盘业主信息 1499 条，并经公司报销，随后分发给部门员工拨打推销电话。

在这起案件中，出售个人信息者大都为“内鬼”，有的是房地产公司员工，有的则是物业工作人员。判决书中，法院认为该案系单位犯罪，装饰公司被判处罚金五万元；董事长周某某被判处有期徒刑三年，并处罚金四万元；其他员工被判处有期徒刑九个月至一年不等的处罚。

据了解，“内鬼”利用职务便利，非法获取并出售公民个人信息的案件频发。在“净网 2018”、“净网 2019”、“净网 2020”专项行动中，公安机关在侵犯公民个人信息案件中抓获

各行业“内鬼”3000 余名。（来源：南方都市报）

➢ 黑客入侵印尼最大在线商店 1500 万用户信息遭泄露

2020 年 5 月 8 日，据外媒 ZDNet 消息，黑客从印度尼西亚最大的在线商店 Tokopedia 窃取了 1500 万用户的详细信息，并在一个著名的黑客论坛上发布。

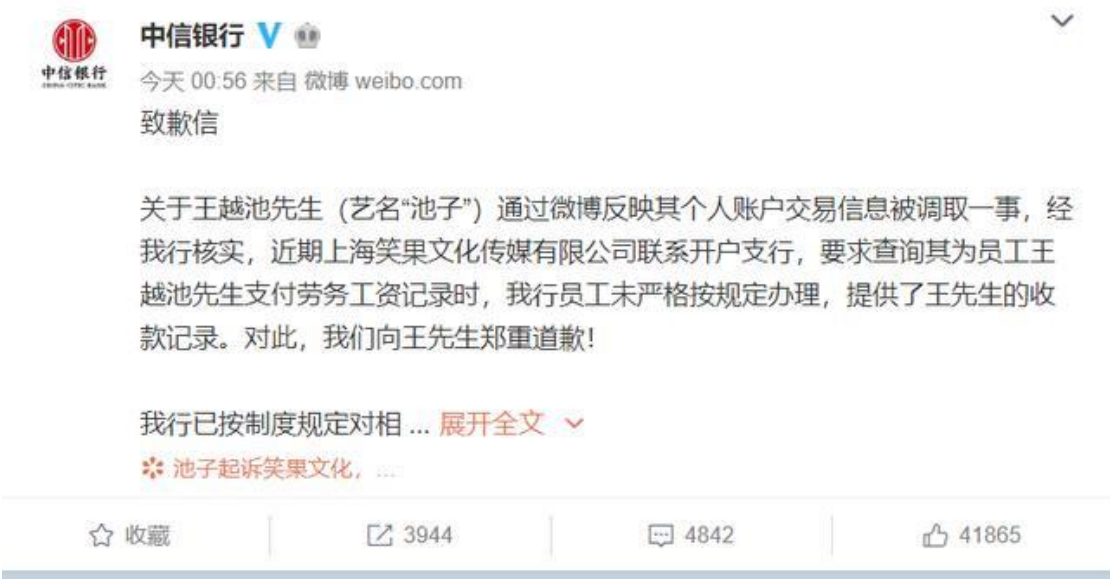
黑客声称数据是在 2020 年 3 月的一次入侵中获得的，这些数据只是黑客在该网站中获得的整个用户数据库的一小部分。黑客表示他正在分享 1500 万用户样本，希望有人可以帮助破解用户密码，以便访问其用户帐户。

据悉，ZDNet 已在数据泄露监视服务 Under Breach 的帮助下获得了该泄露文件的副本。该文件是 PostgreSQL 数据库转储文件，包含用户信息如全名、电子邮件、电话号码、哈希密码、生日和与 Tokopedia 个人资料相关的详细信息（帐户创建日期、登录名、电子邮件激活码、密码重置代码、位置详细信息、Messenger ID、爱好、教育等）。

Tokopedia 在九轮融资中总共筹集了 24 亿美元的资金，目前是印度尼西亚最大的科技独角兽之一。该网站类似于亚马逊，允许用户从该网站购买产品或开设商店并自行销售产品。该网站声称每月有 9000 万活跃用户和 700 万注册商家。（来源：ZDNet）

➢ 中信银行就艺人池子交易流水泄露深夜致歉

2020 年 5 月 7 日，凌晨 00：56 分中信银行发布微博公开致歉信：关于王越池先生(艺名“池子”)通过微博反映其个人账户交易信息被调取一事，经我行核实，近期上海笑果文化传媒有限公司联系开户支行，要求查询其为员工王越池先生支付劳务工资记录时，我行员工未严格按规定办理，提供了王先生的收款记录。对此，我们向王先生郑重道歉!



我行已按制度规定对相关员工予以处分，并对支行行长予以撤职。

保护客户信息安全是我行秉持的服务宗旨，也是银行的生命线。在客户信息保护方面，我行建立了一整套制度及流程，但个别员工未严格按照制度操作，反映出我行个别机构在制度执行上不到位。我行将举一反三，全面检查，加大培训，强抓制度执行，坚决避免此类问题再次发生，切实保护金融消费者合法权益。真诚欢迎社会各界继续对我行进行监督，感谢大家的关心与支持!

事件始末：2020 年 5 月 6 日，被笑果文化“移出群聊”近四个月的池子，再度“活跃”在大众视野中。“池子起诉笑果文化”“中信银行”双双登上微博热搜，原因来自池子的一篇长文。池子在个人微博号“池子池子大池子”中称：“去年(2019 年)我发现笑果文化违约，拖欠了很多应付的演艺报酬，而且没有按照合同给我账单明细，我提出异议之后，笑果基本上刻意停止了我的一切工作，我多次提出和平解约，笑果不同意，我只能提出仲裁，让他们付清我的报酬。然后笑果文化也提出仲裁，让我赔给他们 3000 多万。”在微博中，池子表明目前并没有办法开展任何工作，一直在和笑果文化打官司，但这些纠纷仅仅属于合约纠纷，也就是违约。

随后池子又称：“在笑果文化寄给我的案件材料里面，竟然发现了我在中信银行的个人账户交易明细。”直指笑果文化涉嫌在未经本人允许的情况下触犯了他的个人隐私，而中信银行给他的回复则是：“这是配合大客户要求。”对此，池子本人表示已向公安局报案，且向银保监会等政府监管机关投诉，要求相关方进行赔偿并公开道歉。

北京志霖律师事务所副主任赵占领律师向虎嗅表示，从池子公开的微博可以获取到的信息是银行方的口径是“配合大客户的要求。”**而具体如何获取目前并不明晰，但不排除以下几种情况：**

第一种可能性，由银行某个工作人员利用职务之便私下提供，这种情况虽然不属于银行主动作为，而是个别员工违规操作，但是银行没有尽到管理责任，理应对其员工的违规行为负责，只是这种情况下银行并不构成刑事犯罪，员工则有可能构成刑事犯罪。

银行与储户之间存在合同关系，银行依法应当保管包括交易流水在内的个人信息，如果存在管理漏洞或技术漏洞导致储户的个人信息泄露，则银行违反了《商业银行法》《消费者权益保护法》等法律规定的义务，需要承担相应的行政责任和民事责任。行政责任是指，监管部门也可以对其违规行为进行行政处罚，一般是责令改正，罚款等处罚。

民事责任主要是指银行未尽到个人信息安全保障义务，而应对储户承担的民事赔偿责任，其中包括赔偿因个人信息泄露给储户造成的经济损失，如果储户不能提供直接证据，通常由法院根据具体情况酌定。

第二种可能性，这种行为是银行自身所为，比如，因笑果是其大客户而应其要求，把其中某个储户的个人信息提供给对方，这种情况下银行的行为不仅构成民事侵权，还可能涉嫌刑事犯罪。

刑法第 253 条规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

不管是银行故意泄露出去，或者员工个人利用职务之便故意泄露，都可能涉嫌构成侵犯公民个人信息罪。

此外，还有一种可能性，赵占领律师称，因池子个人原因导致其银行流水泄露，比如池子因某种原因，办理买房、贷款、出国等需要，而自行打印了银行流水，而后未能妥善保管

而被笑果获取到个人流水，当然这种可能性很小。

另有一点值得注意的是，据赵占领律师介绍，如果自行去银行打印流水，身份证原件必不可少，如果委托他人办理，也需要代理人拿着委托人身份证原件。赵占领律师也称，只有权力机关，比如公安机关、法院等，经过法定程序，才能依法、依职权进行调取个人信息。（来源：互联网综合整理）

➢ 特斯拉二手车被曝隐私问题 黑客获得大量个人信息

2020 年 5 月 7 日，据外媒报道，特斯拉的车载计算机系统，可能没有大家想象的那么安全。根据某一网络安全研究员的说法，即便在完全恢复出厂设置后，黑客依旧可以从旧的特斯拉面板系统中恢复大量个人信息。

这位账号为“greentheonly”的研究员在研究了 13 块二手特斯拉媒体控制单元（MCU）后得出了上述结论，其中 12 块 MCU 是他从 eBay 上购买的，另一块从朋友手中购买。

尽管每一块控制单元都已经重置删除之前所有者的全部个人信息，但研究员还是能从系统中恢复大量数据，如密码，GPS 定位信息等。黑客可以访问控制单元原主人的完整联系人列表，通话记录，日历信息以及在控制单元上运行过的第三方应用（Spotify、Netflix(435.55, -0.98, -0.22%)、Gmail、YouTube 等）的账户 ID 和密码。

每次车辆的启动的时候，车载媒体控制单元也会保存车辆位置的屏幕快照，并且系统户保留最近的 50 个位置屏幕快照，所有这些信息也可以访问。

Greentheonly 称，他可以访问这些信息，是因为特斯拉系统使用的是 SQLite 数据库。对

于 SQLite 数据库，只有当硬盘驱动器上的特定模块被新信息覆盖重写后，原有信息才会真正删除。

恢复出厂设置仅意味着特斯拉的操作系统将释放该特定模块上的空间。但已经写入的数据仍保留在那里，直到系统重新写入数据后，原先的数据才会清除。在一次采访中，greentheonly 还表示，用过的特斯拉车载媒体控制单元在二手市场上比较容易购买。（来源：新浪科技）

➢ 5000 万条个人信息“暗网”倒卖 南通警方抓获 27 名嫌疑人

2020 年 5 月 7 日，所谓“暗网”，是利用加密传输、P2P 对等网络等，为用户提供匿名的互联网信息访问的一类技术手段。“暗网”最大特点是经过加密处理，普通浏览器和搜索引擎无法进入，且使用比特币作为交易货币，很难追查到使用者的真实身份和所处位置，受到互联网犯罪分子青睐。

5 月 7 日，南通市公安局对外公布，经过 4 个多月的缜密侦查，南通、如东两级公安机关突破层层技术难关，横跨 8 省 26 市，行程数十万公里，成功破获一起公安部督办的特大“暗网”侵犯公民个人信息案，抓获犯罪嫌疑人 27 名，查获被售卖的公民个人信息数据 5000 万余条。近日，这起案件被公安部列为 2019 年以来全国公安机关侦破的十起侵犯公

民个人信息违法犯罪典型案件之一。

网上巡查获线索大量公民个人信息被叫卖

去年 8 月，南通市公安局网安支队在日常网上巡查工作中发现，网名为“akula98”的用户在“暗网”交易平台出售公民个人信息，其中部分涉及南通如东等地市民的个人信息。“主要是些银行开户、手机注册等数据，查询属实，极易被诈骗等犯罪团伙利用，潜在危害严重。”网络安全技术专家、南通市公安局网安支队三大队副大队长许平楠介绍说。

南通市公安局网安支队会同如东县公安局立即成立专案组全力开展破案攻坚。经进一步侦查，南通警方发现，自 2019 年 5 月以来，“akula98”多次通过“暗网”交易平台出售公民个人信息，数量较大。然而，“暗网”能够提供给专案组的破案线索仅仅只有一个用户名，犯罪嫌疑人的真实身份却无从得知，案件侦办一时陷入僵局。

在许平楠的带领下，专案组自建数据模型，通过深度研判，艰难锁定“akula98”的真实身份为浙江宁波的王某城。

9 月 9 日晚，专案组民警将王某城抓获归案，并在其手机上成功提取到比特币交易 APP 以及用于储存公民个人信息数据的网盘。

据王某城交代，自己通过多种途径收集大量商家信息，并非法购买包括期货、外汇投资人等公民个人信息数据，在“暗网”交易平台上兜售。同时，他还通过“暗网”交易平台批量购买“股民”“车主”“银行”“房产”等行业的公民个人信息，转卖获利。截至案发，王某城累计贩卖公民个人信息 100 余万条，非法获利折合人民币 10 万余元。

盯案不放现源头“暗网”成非法交易集散地

为逃避公安机关打击，王某城与买家、卖家交流均使用特殊软件，且以比特币结算。专案组民警日夜追踪，硬是从大量资金流水中，研判出一条买家的线索。10 月 29 日，这名买家在苏州昆山落网。由此，专案组也查找到了这一利用“暗网”侵犯公民个人信息犯罪链条的关键一环。

经查，该买家为王某阳，长期经营期货交易平台。王某阳到案后交代，自己购买公民个人信息是为了业务推广需要。此外，王某阳不仅通过王某城购买公民个人信息，还另有渠道，购买了数百万余条涉及期货和 pos 机的公民个人信息。

“作为中间人，他还帮忙介绍，从中拿点‘好处费’。”侦办此案的如东县公安局网安大队侦查中队中队长姜光程说。根据王某阳提供的线索，专案组很快查清另一贩卖公民个人信息的渠道来源是年仅 21 岁的林某伟。11 月 12 日，林某伟在上海落网。

据林某伟交代，其经朋友介绍认识王某阳。2018 年底至案发，自己将从“暗网”等非

法渠道购得的 350 余万条银行开户、手机用户注册等数据，卖给了王某阳及其介绍的费某贵等人，非法牟利 70 余万元。

从王某阳、林某伟等人的供述中，专案组意识到他们身后还有庞大的个人数据信息倒卖网络，“暗网”俨然成为犯罪嫌疑人非法买卖公民个人信息的集散地。案情重大，南通市公安局迅速将案件逐层上报至公安部，引起高度重视，被列为公安部挂牌督办案件。

循线追查断链条买方多用于广告推广和诈骗

专案组盯案不放，紧追被贩卖的公民个人信息的数据源头，发现王某阳加入的某聊天工具群组，当群成员缴纳费用后，群主将一对一教授如何进入“暗网”进行交易。而林某伟的另一“暗网”渠道则是某网络公司的安全工程师贺某。至此，这一以暗网、私密交流软件等为交易、交流平台的侵犯公民个人信息黑产利益链完全浮出水面。

11 月 26 日，专案组赶赴湖北武汉成功抓获犯罪嫌疑人贺某。日常工作中，贺某就能收集到一些公民个人信息，很快手头上积累了一批公民个人信息数据，加之其熟知“暗网”，于是通过“暗网”或熟人介绍，对外出售牟利，买家遍布全国各地。在前期工作基础上，2019 年 12 月，专案组抽调 30 余名警力，成立 6 个抓捕组，先后赴湖北、黑龙江、上海、广东等 8 省 26 市，对购买公民个人信息的下线进行集中收网，截至今年 1 月，累计抓获犯罪嫌疑人 27 名，查获被贩卖的各类公民个人信息数据多达 5000 万余条。

今年 33 岁的费某贵，在昆山经营一家公司，主要代理各支付公司的 POS 机刷卡业务。为推销业务，经王某阳介绍，费某贵从林某伟处购得 350 万条 POS 机刷卡消费数据，并分发给业务员进行有针对性的电话推销，客户购买 POS 机并刷卡消费的，支付公司再“分红”给费某贵。

“买家有庞大需求，一定程度上刺激了这一网络黑产的发展。” 南通市公安局网安支队支队长张建说，大多数买家与费某贵的目的类似，主要将这些非法获取的公民个人信息用于各类广告的精准投放和业务推广，同时又继续通过“暗网”交易平台出售自己手中的公民个人信息。“这就容易成为其他网络犯罪的‘帮凶’。”张建说，侵犯公民个人信息案件极具社会危害性，必须严厉打击。同时，广大群众应文明绿色上网，注重提升对个人信息的保护意识，防止个人信息在不经意间泄露出去。

目前，该案仍在进一步深挖中，到案的犯罪嫌疑人已移交当地检察机关审查起诉。（来源：新华报业网）

信息安全意识产品服务

021-33663299