国盟信息安全通报

2019 年 5 月 13 日第 192 期

国盟信息安全通报

（第 192 期）

国际信息安全学习联盟

2019 年 5 月 13 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 288 个，其中高危漏洞 104 个、中危漏洞 153 个、低危漏洞 31 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 106 个（占 37%），其中互联网上出现“LaravelSQL 注入漏洞、NagiosXI 提权漏洞”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 2245 与上周（1994 个）环比增长 13%。

主要内容

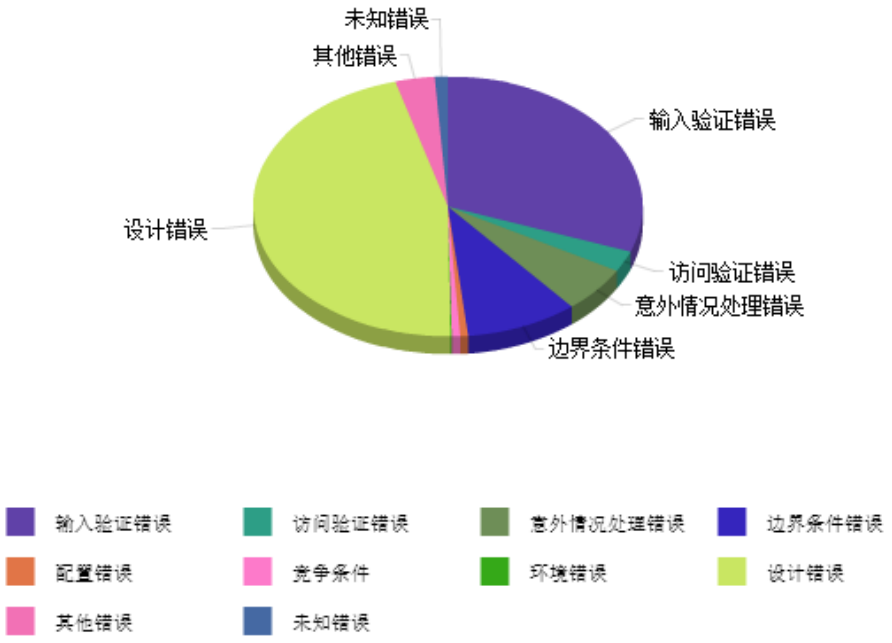
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

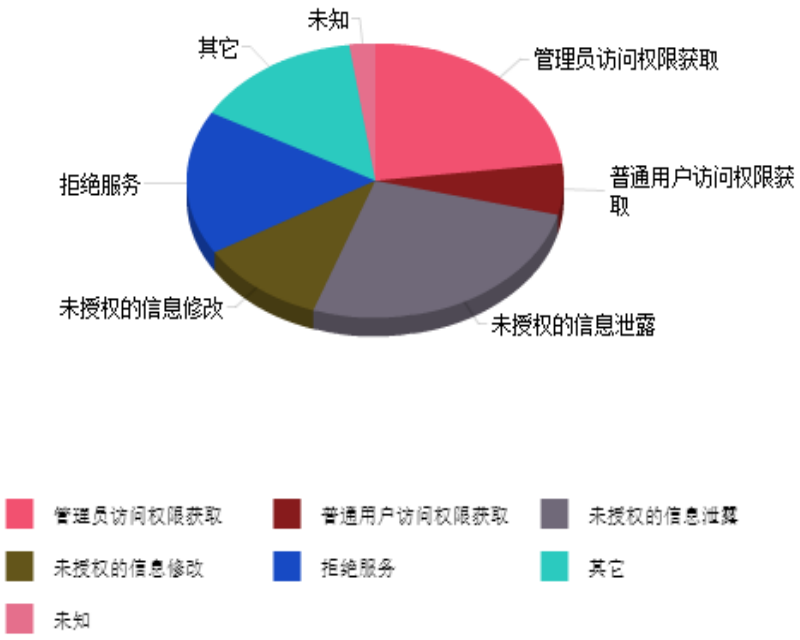
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 288 个，其中高危漏洞 104 个、中危漏洞 153 个、低危漏洞 31 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 106 个（占 37%），其中互联网上出现“LaravelSQL 注入漏洞、NagiosXI 提权漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2245 与上周（1994 个）环比增长 13%。

二、安全漏洞增长数量及种类分布情况

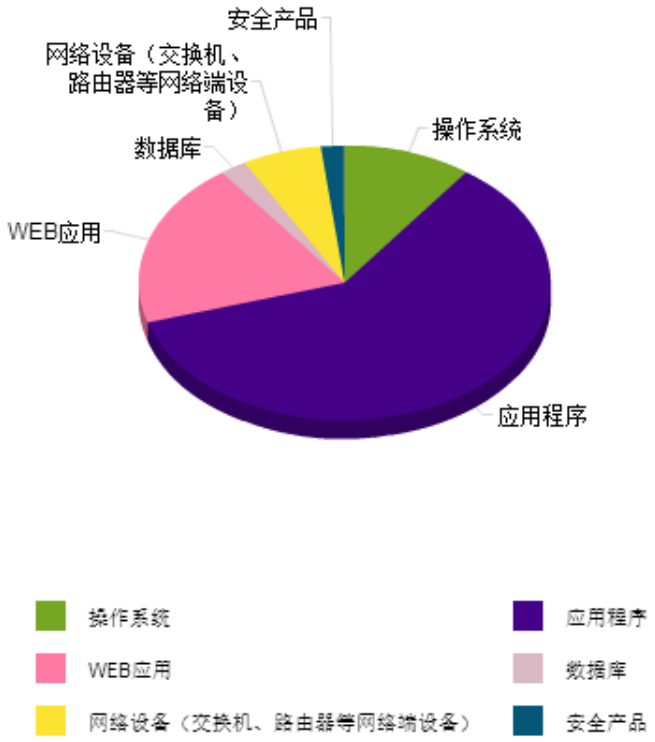
➢ 漏洞产生原因（2019 年 4 月 29 日—2019 年 5 月 13 日）



➢ 漏洞引发的威胁（2019 年 4 月 29 日—2019 年 5 月 13 日）



➢ 漏洞影响对象类型（2019 年 4 月 29 日—2019 年 5 月 13 日）



三、安全产业动态

➢ 在信息强国的道路上阔步前行

全从数字福建到数字中国，从数字中国到数字海丝，十余年间，澎湃跳动的数字世界里，中国挺立潮头，引领风骚。当数字化的影响日益广泛与深刻，生产生活随之而变的数字时代，正奇迹而来。

2000 年，习近平总书记在福建工作期间，率先提出建设“数字福建”的战略构想，拉开了中国数字化进程的大幕。2018 年 4 月，首届数字中国建设峰会在福建举办。“加快数字中国建设，就是要适应我国发展新的历史方位，全面贯彻新发展理念，以信息化培育新动能，用新动能推动新发展，以新发展创造新辉煌。”习近平总书记为首届数字中国建设峰会发来的贺信，为中国的信息化发展擘画蓝图，为办好数字中国建设峰会指引方向。

当今世界，信息化、数字化代表新的生产力和新的发展方向，已经成为引领创新、驱动转型、塑造优势的先导力量，正深刻改变着世界的竞争方式和经济格局。加快数字中国建设，已成为建设现代化强国的必经之路和重要抓手。可以说，数字中国建设峰会的举办，顺应了中国数字化进程的需要，也正成为加快推进这一澎湃进程的关键一环与发动机。一年来，中国的数字化建设者牢记嘱托，不忘使命。电子政务全面推进，数字经济异军突起，智慧生活

深入人心，丰硕成果令人瞩目。

5 月的榕城，春意盎然。第二届数字中国建设峰会举办在即。当中国数字化领域最具活力的企业以及最有影响力的人才，再次汇聚闽江之滨、有福之州，必将掀起中国数字化建设新的浪潮。

办事像网购一样方便

19 年前“数字福建”提出之时，首先聚焦的就是政府的信息化建设。实际上，电子政务正是中国数字化建设在起步阶段率先找到的一个立足点，发展至今，已成为中国数字化进程中成果显著的一个领域。

“数据多跑路，百姓少跑腿。”从探索前行到全面推进，一年来，我国电子政务的创新发展，有力促进了政府决策科学化、社会治理精准化和公共服务高效化。如今，企业和群众办事就像网购一样方便。

2018 年首届峰会期间，闽政通 App 成为电子政务明星，其全面接入福建省行政审批和公共服务事项，省内居民办理社会保险、出境入境等 21 类事项在手机上可一键完成。如今，闽政通 App 从明星升格为福建人民的伙伴，成为大家手机里的标配，已接入行政审批、公共服务事项超过 16 万项，实名注册用户约 300 万。轻点指尖，公众和企业就可随时随地获取所需服务，服务能力在全国名列前茅。

以“放管服”为目标，“互联网+政务”服务成为数字中国建设的一抹亮色。湖北打造电子政务升级版，提出今年底与国家平台全面对接，200 个高频事项办理最多跑一次。云南省采取政银合作模式，开发出“一部手机办事通”App，让许多到窗口才能办理的事项实现“指尖办”。上线仅 3 个月，注册人数即达 136.74 万，业务办理 359.75 万件。山西加快建设一体化在线政务服务平台，全面推进“三晋通办”模式。截至目前，全国已建成 25 个省级移动政务服务平台，越来越多的群众和企业办事实现“一趟不用跑”“最多跑一趟”。

为人民服务，永远在路上。有专家指出，电子政务发展的高级阶段是数字政府。“它是指以新一代信息技术为支撑、以制度改革为前提，实现效率提升、监管公正、服务便捷的信息化政府，是国家治理体系和治理能力现代化的重要组成部分。”中国互联网协会副理事长、国家信息化专家咨询委员会委员高新民这样表示。

打造数字政府，在更加便民的同时，还将促进政府决策更科学。福建“生态云”平台是全国首个省级生态环境大数据平台，汇聚了来自省、市、县三级环保系统及部分相关厅局的业务数据，构建起环境监测、环境监管和公众服务三大信息化体系。据介绍，2018 年福建应用“生态云”平台，开展区域联防联控，减少 50%以上的轻微污染天数，有效提升了空气

质量。

抢占数字经济制高点

电子政务的高效畅行，为我国数字经济的发展开辟了快速通道。

当前，数字经济已壮大为全球最富朝气的经济现象，成为各国比拼实力的新战场，新时代的中国牢牢抓住这一千载难逢的历史机遇。2018 年 4 月，习近平总书记在全国网络安全和信息化工作会议上强调，信息化为中华民族带来了千载难逢的机遇。

致力于转变发展方式、优化经济结构，中国的数字经济成为推动经济变革、效率变革和动力变革的加速器，成为引领经济高质量发展的新引擎。我国信息技术与产业融合发展，不断从网络空间向实体空间扩展，驱动新业态层出不穷、传统业态升级换代。

以 5G 技术为例，当一些发达国家还在无端猜忌和不断争执之时，我国已率先迈开 5G 应用的脚步：今年 1 月，我国完成全球首例 5G 远程外科手术，外科医生在福州利用 5G 网络，操控 50 公里以外一个偏远地区的机械臂，为一头小猪进行了切除肺小叶手术；今年 2 月的 MWC2019（世界移动通信大会）上，中兴正式发布首款 5G 旗舰机；今年 4 月，福州开通首批搭载 5G 设施的公交车，启用首个 5G 全覆盖公园和自动驾驶车智能公园，打通首个基于 5G NSA 网络的 5G 高清语音电话。

在泉州“芯谷”南安园区，三安光电的高端半导体系列项目正在紧张施工建设。三安光电是全世界 LED 产能规模最大的半导体厂商，在 5G 通信芯片等关键领域拥有 1700 多件主流专利积累，在相关知识产权保护方面居于国际领先地位，并以此形成完整的技术优势和竞争优势。三安光电总经理助理陈文欣表示：“三安光电希望给行业合作伙伴提供整套的 5G 布

局解决方案，从而助力‘数字中国’和智能时代的经济发展。”

先行一步的中国，正在抢占数字经济的制高点。日前发布的《中国数字经济发展与就业白皮书（2019 年）》显示，2018 年我国数字经济规模达到 31.3 万亿元，增长 20.9%，占 GDP 比重为 34.8%。据有关机构研究披露，中国数字经济竞争力位居世界第二。

据了解，首届数字中国建设峰会对接落地涉及数字经济相关项目超过 400 个，总投资达 3600 亿元；即将开幕的第二届数字中国建设峰会，共征集、梳理出数字经济对接项目总计 498 个，总投资 4075 亿元。

数字时代造就智慧社会

数字经济和信息技术，不但深刻地影响着世界，而且越来越深入地影响我们的生活。随着我国信息基础设施不断完善、5G 商业化应用不断推进、人工智能不断发展，智慧社会正向我们走来。

2018 年首届数字中国建设峰会期间召开的中国智慧社会发展与展望论坛，明确了智慧社会的定义，总结归纳了智慧社会的八大发展特征、九大发展趋势。也正是在这届峰会上，“e 福州”App 正式上线，2000 平方米的“数字福州”展馆成为“e 福州”的首个体验场所。峰会后，App 新技能不断解锁，“一码通行”版图不断延展。如今，“e 福州”应用范围已扩大到福州整座城市。App 用户数已突破 160 万，日活跃用户突破 15 万，用户累计使用服务超 6000 万次。目前，“e 福州”实现了交通出行、教育缴费、看病就医、政务服务、社区服务、公园景点、图书借阅、不动产交易等九大场景下的应用服务。

当前，我国的智慧社会建设正渐入佳境。北京作为首善之区，全面推进以数据驱动为核心的新型“智慧北京”建设，正式上线“北京通”App，累计发放“北京通”卡 2297 万张。上海打造便民惠民的智慧生活服务体系，推出一站式“互联网+”公共服务平台——“市民云”，已实现公共服务 104 项，实名注册用户超过 760 万人。杭州依托智慧城市建设，最大限度地为人们提供医、食、住、行、游、教等方面细致服务，使每一位居民都能享受到安全、高效、便捷、绿色的城市生活。

智慧社会建设给文化、教育领域带来新气象。日前发布的《2018 年度中国数字阅读白皮书》显示，截至 2018 年，中国数字阅读用户总量达到 4.32 亿，人均数字阅读量达到 12.4 本；我国数字阅读整体市场规模已达到 254.5 亿元，同比增长 19.6%。近日，网龙公司最新研发的“智慧教室”正式亮相，它以集装箱大小的人性化空间为载体，配备高科技设施，堪称移动版的智慧课堂，助力发展中国家能够便捷、快速地普及优质教育资源。据网龙首席执行官熊立博士介绍，埃及政府计划利用网龙现有的教学技术和设备，3 年内在该国建成 26.5

万间像这样的智慧教室。

乘“数字丝路”出海，如今，中国的智慧社会建设不但惠及国人，也日益惠及海外。中国滴滴出行公司与巴西 99 公司建立战略投资伙伴关系，为巴西 1800 多个城市提供专车、快车和出租车服务，2018 年日均订单量达 120 万单，为改善当地人民生活、助推当地经济发展作出贡献。

在数字时代，智慧社会将作为继农业社会、工业社会、信息社会之后的一种更为高级的社会形态加速到来。有关专家表示，建设智慧社会是建设创新型国家的重要一环，是人类社会发展进程中的一次全方位、系统性的变革。推动智慧社会建设步伐，需要加快部署人机共融、万物互联、智能泛在的基础设施，打造信息资源互联互通的社会共享数据平台，从而为方兴未艾的数字中国建设带来更多的机遇。（来源：光明日报）

➢ 个人信息保护国家标准工作情况与思考

个人信息保护国家标准对于个人信息保护工作具有基础性、规范性和引领性作用，是开展个人信息安全监管、指导网络运营者个人信息保护实践的技术基础和重要抓手。本文梳理分析了个人信息保护国家标准和国际标准的工作现状，对我国个人信息保护标准化工作提出了若干建议。

一、个人信息保护国家标准化现状

1.TC260 概述

2002 年 4 月，国家标准化管理委员会（简称“国标委”）批复成立全国信息安全标准化技术委员会（SAC/TC260，简称“信安标委”），负责对网络安全国家标准进行统一技术归口。信安标委是国标委的直属标委会，业务上接受中央网信办指导，主要工作范围包括安全技术、安全机制、安全服务、安全管理、安全评估等信息安全领域的标准化技术工作。

目前，TC260 下设 6 个工作组（WG）和 1 个大数据安全标准特别工作组（SWG-BDS），秘书处设立在中国电子技术标准化研究院。2016 年 4 月，TC260 成立大数据安全标准化工作组，负责大数据和云计算相关的安全标准化研制工作，具体职责包括调研急需标准化需求，研究提出标准研制路线图，明确年度标准研制方向，及时组织开展关键标准研制工作。

2.主要的个人信息保护国家标准

为落实《网络安全法》相关个人信息保护要求，2016 年 TC260 大数据安全标准化工作组开始研究制定个人信息保护国家标准，目前已开展 5 项标准项目，包括已发布 1 项个人信息安全国家标准，正在制定 3 项国家标准，在研 1 项标准研究项目等。主要个人信息保护标准如图 1 所示。

图 TC260 个人信息保护国家标准

GB/T35273-2017《信息安全技术个人信息安全规范》，规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。本标准适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。该标准作为细化支撑《网络安全法》相关个人信息保护要求的重要标准，在已有个人信息保护工作中发挥了重要作用，目前该标准针对个人信息保护出现

的强迫收集、定向推送等新问题，正在进行修订研究。

《信息安全技术个人信息去标识化指南》，描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施，附录 A 和附录 B 分别给出了常用去标识化技术和去标识化模型，附录 C 比较了去标识化技术和模型的特性，并提供了常见标识符的去标识化参考示例。本标准已推进为报批稿，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。

《信息安全技术个人信息安全工程指南》，给出了网络产品和服务在个人信息安全方面的工程实践指南，包括个人信息安全工程目标和系统工程主要阶段的个人信息安全指南。个人信息安全工程也称为隐私工程，是将个人信息保护和个人数据安全关注点整合到系统和软件生命周期过程的工程实践中进行考虑，用于解决在涉及个人信息的信息系统中处理隐私保护问题。本标准适用于设计、开发、采购、供应、运营涉及个人信息的网络产品和服务的组织，可用于指导网络产品和服务在设计开发、采购供应等阶段开展个人信息安全实践。

《信息安全技术个人信息安全影响评估指南》，规定了个人信息安全影响评估的基本概念、框架、方法和流程。个人信息安全影响评估，也称为隐私影响评估（PIA）或数据保护影响评估（DPIA），是针对个人信息处理活动检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。本标准已推进到送审稿阶段，适用于各类组织自行开展个人信息安全影响评估工作，同时为国家主管部门、第三方测评组织等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

研究项目《个人信息告知同意指南》，针对个人信息告知的内容、告知信息的展示形式、告知的时机和频率，同意的模式和实现形式等展开研究，旨在为网络运营者在网络环境中进行个人信息告知同意提供实施指南。

3.技术文件“网络安全实践指南”

为进一步推广网络安全标准，应对网络安全事件，改善网络安全状况，提高网络安全意识，信安标委也开发了一系列技术文件“网络安全实践指南”，这些实践指南不属于国家标准，是支撑国家标准实施的技术指引。

2018 年 5 月 25 日，TC260 发布《网络安全实践指南-欧盟 GDPR 关注点》，建议相关组织重点关注适用 GDPR 的场景、适用的数据范围、数据处理的基本原则、数据处理的合法正当性事由、对儿童的特别保护规定、数据主体权力、对用户画像的规定、对数据处理者的规定等十四个关注点。

《移动互联网应用个人信息收集指引》，给出了地图导航、网络约车、即时通讯、社区社交、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务等多类移动互联网应用基本业务功能正常运行所需收集的必要个人信息。该指引将于近期发布，适用于移动应用提供者规范个人信息收集行为，也适用于主管监管部门、第三方评估机构等对个人信息收集行为进行监督、管理和评估，还可为移动应用开发者、移动应用商店经营者和移动智能终端厂商提供参考。

4.标准推广应用

衡量一个标准的价值关键是看是否被广泛应用。近年来，TC260 将网络安全标准的研究制定和实施推广工作并重开展，着力强化标准实施落地和应用推广工作。个人信息保护国家标准和实践指南文件，在国家个人信息保护工作中发挥了越来越重要的作用。

（1）隐私条款专项工作

为贯彻落实《网络安全法》，提高网络运营者个人信息保护水平，2017 年 8 月中央网信办、工信部、公安部、国家标准委四部委指导信安标委秘书处组织开展了对京东商城、航旅纵横、滴滴出行、携程网、淘宝、高德地图、新浪微博、支付宝、腾讯微信、百度地图等 10 款网络产品和服务的隐私条款专项工作。该项工作依据《网络安全法》相关个人信息保护要求，参考国家标准《个人信息安全规范》，制定了隐私条款和实现机制的评审要点，督促参评产品自评改进。最后，10 款产品和服务在隐私条款方面均有不同程度的提升，10 家企业也自发签署个人信息保护倡议书，公开做出承诺，保障收集用户个人信息知情权、控制权并尊重用户授权等合法权益，履行个人信息保护责任和义务，保障产品和服务安全可信，抵制黑灰产，自觉接受监督，为行业做好个人信息保护和网络安全工作做出表率。

2018 年 9 月，信安标委秘书处继续开展 2018 年隐私条款专项工作，对出行旅游、生活服务、影视娱乐、工具资讯和网络支付 5 类 30 款产品的隐私条款和实现机制进行评估，并对 2017 年 10 款产品进行复核。本次专项工作信安标委秘书处组织开发了与其配套的个人信息保护专项评审工具，利用工具实现企业、秘书处、专家等角色线上评估，丰富评估结果统计分析和评估报告展示，提高了评审工作效率和展示效果。

（2）App 违法违规收集使用个人信息专项治理工作

为支撑 2019 年四部委开展的 App 违法违规收集使用个人信息专项治理工作，信安标委秘书处组织编制了“大众化应用基本业务功能及必要信息规范”（即《移动互联网应用个人信息收集指引》），用于规范大众化应用收集个人信息的必要性，并研发了 App 专项行动评估辅助工具、App 个人信息保护检测系统等，为专项行动开展提供支撑。

二、国际个人信息安全标准化现状

ISO/IECJTC1/SC27（编号为 SC27）是 ISO/IECJTC1 下属安全技术分委员会，于 1990 年成立，其工作范围主要是信息与通信技术保护的标准研制，包括安全与隐私保护方面的方法、技术和指南。目前 SC27 下设五个工作组，其中 WG5 组负责身份管理和隐私保护方面的标准研制和维护。国际隐私保护标准化工作，目前已形成包含总体框架、管理要求、技术要求、应用领域、实施指南的标准体系。

通用框架类标准主要有 ISO/IEC29100:2011《隐私框架》，规范了隐私保护术语和原则，提供了隐私保护框架。

管理类的标准主要有 ISO/IEC29134:2017《隐私影响评估指南》、ISO/IEC29151:2017《PII 信息保护实用规则》、ISO/IEC27018:2014《公有云中作为 PII 处理者的 PII 保护的行为守则》、ISO/IEC27552《ISO/IEC27001 和 ISO/IEC27002 的隐私管理扩展—要求和指南》、和新标准立项 ISO/IEC27555《在组织建立 PII 删除概念》。其中，29134 为组织开展隐私影响评估（PIA）提供实施指南，国内标准《个人信息安全影响评估指南》在编制时参考了 29134 标准；29151 为组织的个人身份信息（PII）提供了保护控制措施集；27018 面对公有云服务提供商的信息安全风险环境，提出了保护个人可识别信息(PII)的要求；27552 作为 27001 和 27002 的扩展，用于组织建立隐私信息管理体系（PIMS），已推进到第一版 DIS 国际标准草案阶段；27555 提出了组织 PII 的删除流程，已推进为第一版（WD）工作草案。

实施指南类的标准主要有 ISO/IEC27550《系统生命周期的隐私工程》、ISO/IEC29184《在线隐私告知和同意》以及 ISO/IEC29190:2015《隐私能力评估模型》。其中，27550 将隐私保护应用到了 ISO/IEC15288 的系统工程各个阶段，已推进为第三版 TR 技术报告，国内《个人信息安全工程指南》标准编制时参考了该标准；29184 提供了线上隐私告知基本条款，已推进为第三版（CD）委员会草案，国内标准研究项目《个人信息告知同意指南》参考了该标准；29190 提供了一套隐私能力评估流程和隐私能力评估的级别，并为如何将隐私评估能力融入组织运营、评估隐私能力的关键过程区域、隐私评估执行过程人员提供指导。

技术要求类的标准有 ISO/IEC29101:2013《隐私架构框架》、ISO/IEC20889《增强隐私的数据去标识化技术》、ISO/IEC29191:2012《半匿名和部分不可链接的身份认证要求》。其中，29101 提供了 ICT 系统的个人隐私保护技术框架；20889 介绍了统计、加密、抑制、假名、泛化、随机、合成 7 大类的去标识化技术以及 K 匿名和差分隐私 2 大类去标识化模型，国内标准《个人信息去标识化指南》编制时参考了该标准；29191 定义了身份认证相关的四个角色，明确了在具体的认证过程中每个角色对应的基本操作，同时针对半匿名、部分不相关的认证

明确了具体要求。

三、下一步工作建议

随着各种新技术的深入应用，个人信息保护面临更多新场景、新问题，对个人信息保护国家标准提出了新的要求和挑战。

一是加快个人信息保护相关标准研制。针对《网络安全法》等法律法规的个人信息保护要求，结合国家个人信息保护工作的重点和难点问题，围绕个人信息保护主要威胁和风险点，制定关键急需的个人信息保护国家标准。参考国际隐私保护标准体系，广泛制定应用类、指南性标准和网络安全实践指南文件，逐步形成适应我国个人信息保护需求的标准体系框架。

二是积极开展标准应用推广工作。结合政府、企业、用户关注的主题，组织开展重点个人信息保护标准和指引的应用验证和试点示范工作。继续开展隐私条款等专项工作，推广个人信息保护优秀实践，引导网络运营者提升个人信息保护水平。同时研发自动化工具支撑标准有效实施，进一步加强标准的科学性、合理性和可操作性。

三是加强个人信息保护宣传力度。编制重点标准实施指南和宣贯材料，采取标准宣贯会、地方宣贯活动、专题研讨会等多种渠道和形式，加大对个人信息保护重点标准的宣传解读，增强社会各方面对个人信息保护的意识。（来源：《中国信息安全》杂志 2019 年第 4 期）

➢ 敏锐抓住信息化发展的历史机遇

近几十年来信息技术发展迅速，与多学科深度交叉融合，成为推动社会生产新变革、创造人类生活新空间的重要力量。从现实情况看，信息化发展状况事关国家竞争力和民族未来。2018 年 4 月，习近平同志在全国网络安全和信息化工作会议上强调：“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”。实现“两个一百年”奋斗目标、全面建成社会主义现代化强国，必须占据信息化发展制高点，建设网络强国、数字中国、智慧社会，以信息化驱动现代化。

我国信息化发展面临难得机遇

信息技术发展快、渗透性强、影响面广。当前，信息技术与生物技术、新能源技术、新材料技术等的交叉融合正在引发新一轮科技革命和产业变革，将给经济社会发展带来深刻影响。近年来，信息化在我国发展中的战略性、基础性和先导性作用日益突出，我国信息化发展正形成自己的优势，面临难得机遇。

我国经济社会快速发展、信息基础设施不断完善，为信息化进一步发展打下了坚实基础。近年来，随着我国经济社会快速发展，以高速互联、泛在移动、天地一体、智能便捷、综合集成为特征的新一代信息基础设施正在加速形成并不断完善，为我国信息化进一步发展打下了坚实基础。得益于计算能力、存储资源、网络带宽、算法演进、大数据积累等方面的快速发展，我国数字经济异军突起。信息技术与产业融合发展，与各行各业的创新活动日益紧密结合，而且不断从网络空间向实体空间扩展，驱动新业态层出不穷、传统业态升级换代。智能手机的普及为我国进一步推进信息化创造了条件，促进我国电子商务、互联网金融、网络媒体等一大批新兴产业蓬勃发展，而这些产业发展产生的技术需求又为信息技术的创新提供了强劲的驱动力和坚实的物质基础，从而形成良性循环。

5G 的商业化应用将进一步拓展我国信息技术应用的深度与广度。目前，5G（第五代移动通信技术）正从技术标准化和网络测试阶段转向试商用部署阶段。2020 年我国 5G 将实现商业推广，2025 年我国 5G 用户预计将达到亿级规模。5G 对经济社会发展和人们的生产生活将产生十分深刻的影响，从交通、工业、农业到生活家居、健康管理，5G 都将发挥重要作用。5G 的商用推广不仅能提升我国网络基础设施和智能设备的技术水平，还能加速半导体、车联网、人工智能等新兴领域的发展，成为开启万物互联、深度融合的“万能钥匙”。

人工智能的发展将把我国信息化发展提升到新高度。近年来，人工智能已成为国际竞争的焦点，对经济社会发展产生了重大影响。例如，人工智能推动电子政务从信息型、交互型、业务型向感知型方向发展，已逐步应用在身份认证、在线客服、信息检索、行政审批、辅助决策、应急处置、态势感知等各个政务公共服务领域，大幅提高了政府管理效率。我国发展人工智能具有良好的基础与条件。从构成人工智能的三要素——算法、算力、数据来看，近

几年全世界关于机器学习算法的论文有超过 1/3 是我国学者发表的；我国“天河”系列、“太湖之光”等超级计算机的计算速度世界领先；我国医疗、金融、城市治理等领域的数据不仅数量大，而且数据获取能力强。我们要注重人工智能核心算法的突破、大数据和应用场景公共平台的建设，推动我国信息化发展跃上新的台阶。

着力解决信息化发展面临的主要问题

机遇与挑战并存。新时代，我国要推动互联网、大数据、人工智能和实体经济深度融合，发展数字经济、共享经济，培育经济新增长点，形成发展新动能，以信息化驱动现代化，必须正视挑战，着力解决信息化发展面临的主要问题。只有解决好主要问题，才能更好抓住信息化发展的历史机遇。

一些关键核心技术受制于人问题。尽管我国在电子商务、智能终端、5G、超级计算机等方面的技术水平在世界上已经处于并行甚至引领的位置，但也应清醒认识到，我国在信息技术领域取得的优势仍然是局部的，而且并不稳固，特别是核心芯片与软件受制于人的状况尚未得到有效解决，尚未摆脱对西方发达国家的依赖。最近，美国提出了“电子复兴”等计划，要通过多学科跨领域的大规模长期合作，大幅度提高各类商用和军用电子系统的性能、效率和能力。这些计划关注的重点包括：用于电子设备的新材料、将电子设备集成到复杂电路中的新体系结构和软硬件设计上的创新等。我国应在信息化关键核心技术上奋起直追，努力掌握信息化的主动权。

网络安全问题。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。当前，传统网络边界越来越模糊，新型网络攻击愈演愈烈，有增无减的网络安全威胁干扰和破坏着社会正常生产生活，甚至威胁国家安全和社会稳定。网络安全问题还对民生造成严重影响，网络金融诈骗、隐私泄露等事件频频发生，对民众危害巨大。近年来，我国对网络安全核心技术研发和产业发展加大了支持力度，在网络安全态势感知、拟态安全、威胁情报等领域已经进行布局，同时与人工智能、金融风控、5G 等相关领域形成相互支撑。应进一步在这些方面加大力度，在信息化过程中做到发展与安全相辅相成。

信息基础设施建设不均衡问题。信息基础设施是我国经济社会发展无形的“大动脉”，对经济社会发展具有重要影响。目前，我国信息基础设施建设不平衡、不充分的问题仍然较为突出。农村互联网相关基础设施建设仍然比较滞后，城乡之间互联网普及率仍有较大差距。不同区域之间信息化程度差异也比较明显，东西部地区信息基础设施建设失衡的局面亟待改变。信息基础设施建设不平衡、不充分问题不利于区域协调发展。应进一步加大投入，推进信息基础设施建设，尤其要注重城乡之间、区域之间信息基础设施建设的均衡，防止形成“数

字鸿沟”。

信息化理念滞后问题。当前，一些地区对信息技术应用的认识还停留在通信应用、图文处理等低端层次，缺乏利用信息化手段提高政府管理水平、企业生产效率等的理念与能力。一些基层政府和普通群众信息化理念不能与时俱进，信息技术普及还不到位，致使许多信息基础设施处于闲置状态。还要看到，一些地区和部门在信息化过程中从一开始就是分头建设，缺乏统一规划，造成不同部门之间信息传递不顺畅，在管理、财务、人事等方面形成“信息孤岛”，造成资源无法共享、信息资源闲置，为未来信息化升级换代埋下隐患。应根据信息技术的发展趋势不断更新信息化理念，注重统一规划，更好发挥信息化的巨大作用。

信息领域基础理论“变道超车”问题。当前，信息领域的基础理论研究正处于拐点期，亟待突破。2018 年 1 月国务院印发的《关于全面加强基础科学研究的若干意见》提出，要促进基础研究与应用研究融通创新发展。信息领域的基础研究、应用研究、技术开发和产业化边界现在已经越来越模糊，科技创新链条更加灵巧。这更要求我们打通基础研究和技术创新相衔接的绿色通道，力争以基础研究带动应用研究、技术开发实现新突破。科技发展的历史一再证明，没有基础理论突破，很难有技术突破；没有大规模的技术积累，就无法产生爆发性创新。我们必须积极布局前沿基础理论研究，在信息领域基础理论方面实现“变道超车”。

（来源：人民日报　作者：毛军发，上海市习近平新时代中国特色社会主义思想研究中心）

➢ 企业提高全员安全意识的六个方向

很多企业安全部门可能因为将预算和资源都投入到软/硬件安全解决方案的采购与部署，侧重技防，而选择性忽略或者根本没有更多预算投入人防。实际上人防与技防处于同等重要的位置，基于技术的解决方案能够覆盖的领域是有限的，即使企业花了很多钱来构建安全防线，有时候一个来自内部人员的小错误就可能将企业置于岌岌可危的境地。

从攻击端来看，攻击者越来越重视终端用户的行为心理研究，不断通过各种方法绕过企业的安全防御策略来达到目的，水坑式攻击和鱼叉式钓鱼攻击是两种典型的方式。要建好“人民防线”，离不开良好的人员操作机制和安全意识提升计划。通过制定周密的安全意识提升项目，员工能够主动担负起责任，更好地保护企业数字资产和识产权。此外，从更高的角度来看，员工还能将所学的安全知识延伸到个人生活中，使得更多的家庭受益。

2016 年，Gartner 曾发布了一篇安全指南，提出了一些帮助中小型企业在预算十分紧张

的情况下提升员工安全意识的建议。三年过去了，网络空间的形态发生了很多变化，因此 Gartner 的安全专家重写了这篇指南，提出了几种简单可行、立竿见影的方法，仍坚持“调动最少的资源”这一原则。

方法一、简单明了的消息通知

- **内网横幅**

采用网络广告的思路在企业内部网页顶端添加横幅，推进安全意识的树立和安全消息的传达能力。

- **登录消息**

诸如 Microsoft Word 和 Unix 等应用和操作系统为管理员提供了系统登录时发送消息的通道。管理员可以自定义消息推送以提醒用户要遵守哪些安全要求、推送最新的安全提示或传输任何可以强化安全能力的消息。不过要注意信息要保持简短且不要经常发送，如果信息很复杂或者持续推送会降低它对用户产生的印象，并且在部分国家和地区可能存在违反法律规定的风险。

- **“阻止的站点”页面**

限制员工访问各类网站（包括社交媒体、搜索、购物等正规网站）或阻止访问被视为有风险的网站是一种企业内部常见的安全策略。不过要注意不要只使用 Web 屏蔽服务供应商提供的默认“阻止的站点”页面，只写一句“违反企业安全策略”。最好在页面上为被阻止的网站创建自定义消息，告知用户不能访问该网站的原因。用好“阻止的站点”，为员工提

供额外内容供他们阅读或查看以及相关联系人的信息，这样可以创造一个很好的主动学习机会。

方法二、各种类型的会议

- **远程培训**

如果企业规模比较大，将所有员工集中到一起进行培训不方便，可以开展在线视频培训，员工无需离开办公桌即可参与，一般适用于分享安全提示、进行问答等简单的安全培训活动。

- **与安全主管共进午餐**

与安全管理人员一起举办午餐会是向特定受众传达关键信息的简单且有效的方式，从另外一个层面看，真人讨论也能提升员工的参与度。

- **行业专家现场培训**

邀请外部行业专家（如执法部门或专业公司）进行现场演示，为观众提供与安全行业领袖和从业者互动的机会。邀请的行业专家可以通过讲故事分享真实的信息和经验，让整体内容更加有趣，更能吸引观众。

方法三、增加安全专家的出镜率

- **拍摄短视频**

企业内部安全专家可以尝试拍摄一些针对特定主题来拍摄一些小视频，每次讲解一个问题并提供解决方法，清晰、有意识地传达消息，拉动员工与企业内部安全人员的距离。增强安全专家的出镜率有助于提升员工对专家的熟悉度，从而增加视频的点击率和未来线下会议的参与率。这些视频可以存放在内网主页的某个固定区域。

- **专门的沟通邮箱**

企业可以在内部设置一个专门用于安全问题的邮箱，保持与员工的持续沟通渠道，提供必要的信息交流。该邮箱可用于解答安全问题或提供反馈。然后，邮箱的管理人员可以将问题与解答定时上传至企业内部的常见安全问题与解答页面。这种方式不用与人面对面进行交流，是一种低投入的互动形式，对于部分员工可能更有吸引力。

- **布置安全专家的工位**

可以将安全专家的工位布置得更加开放，增加饮食供应和舒适的座椅等，从形式上鼓励员工坐下来与安全专家聊一聊，在舒适的环境中员工会更愿意发言并提出一些关键问题。除了被动接受员工的咨询外，也可以主动发送座谈的邀请。

- **写博客**

写博客是一种增加长期关注者的方式，还能巩固安全专家在相关领域的权威性。写博客

是建议不要特别高瞻远瞩，最好的方式就是“保持真实”，要有故事，有细节，增加员工的代入感，有助于建立长期联系，推进员工安全意识的培养。其次，博客篇幅不必很长，在讲清事情的前提下越短越好。

方法四、让员工多多参与

- **摄影比赛**

企业可以通过一些并非很直接、接地气的活动从侧面推进员工安全意识的培养。比如举办摄影比赛，流程比较简单，用户体验也很友好，能够接触和吸引各个部门的员工。摄影比赛可以围绕安全主题设定比赛目标和规则，比如让员工提供能够表现安全的照片。让企业高管参与可以大大提升活动的影响力，也可以表现高管对于安全的重视程度。此外，此类活动的宣传力度要广要大，除了群发电子邮件这种公共方式之外，还可以通过管理层通道在开例会时进行重点强调。当然，奖品的好坏也直接决定了活动能够吸引到的人数和质量。

- **安全小站**

安全小站的形式可以是一个公共的展示和互动区域，可以提供部分经过处理的数据图表让员工更直观地看到安全态势，如果能够提供模拟安全攻防的互动项目或者小游戏那就更好了，比如在看到勒索软件在电脑上肆虐时该如何进行适当的补救，高互动的形式能够让参与者更加投入来解决安全问题。

- **攻防竞赛**

根据企业的自身情况，可在严格限定范围和手段的情况下开展一系列网络攻防竞赛。比如针对企业员工面临的主要网络风险——钓鱼邮件，开展竞赛。比赛可分为攻击者和防御者，攻击者对防御者进行网络钓鱼攻击，而防御者则要在处理海量的邮件是避免踩坑，成功次数最多的攻击者和踩坑最少的防御者均能获得企业的奖励。要注意竞赛的手段和分寸，明确与企业正常业务的边界。

- **将安全延伸到私人时间**

可以让员工携带不再使用、准备丢弃的老旧设备到公司，由安全专家说明和指导如何抹去个人信息，消除丢弃或者转卖时造成的安全风险，以后在处理客户或者企业的数据时也该采取相同的行动。

方法五、正面激励

- **正面反馈员工的进步**

当企业高级管理层看到员工在保障企业安全时做出的努力和成果时，可以通过颁发奖状、留下手写消息卡片、通过电子邮件发送感谢信、提供礼品卡来奖励这些员工，感谢他们的安

全行为，加强员工在企业安全建设过程中的主观能动性。

- **建立积分规则**

建立积分规则的目的是推行长期的奖励计划，该计划向员工授予可用于在企业内部商店或者外部供应商处购买商品的积分。这种持续的奖励系统能够不断激励员工，构建长期的安全意识，表达对员工感谢。

- **给与虚拟的勋章**

如果企业的内部通信或者协作软件支持虚拟勋章或者自定义头像的话，可以给与积极参与企业安全建设的员工开通虚拟安全勋章。虽然这种形式并不能给员工带来任何实际的奖励，但是可以推动安全意识的发展。

- **与 CEO 共进午餐**

员工与 CEO 或其他高级管理人员面对面相处的时间可能很少。企业可向员工提供与 CEO 或平时比较少见的管理层人员共进午餐的机会，以表明高层对于安全建设的重视。可以同时邀请数名员工共进午餐，不设置任何正式议程，员工可以提出问题并了解企业领导和其他情况。

- **提拔做得好的员工**

业务负责人可以将在企业安全建设中表现好的员工提拔至安全运营领导者的角色，赋予业务流程中的更多的安全话语权并加强其领导力。企业可以将这一环节添加到 KPI 考核机制中的加分部分，在晋升评定中给与看得见的积极反馈，并在企业内部通报结果，为员工参与安全建设添加更多动力。

方法六、保持头脑清醒

- **安全日历：**通过电子邮件、海报、内网消息或上文中提到的内网横幅等渠道定期推送的简短安全提示，通知目前流行的安全威胁和公司可能面临安全事件。并与公司内部的数字营销团队合作，通过点击率了解数字流量和员工的关注度。

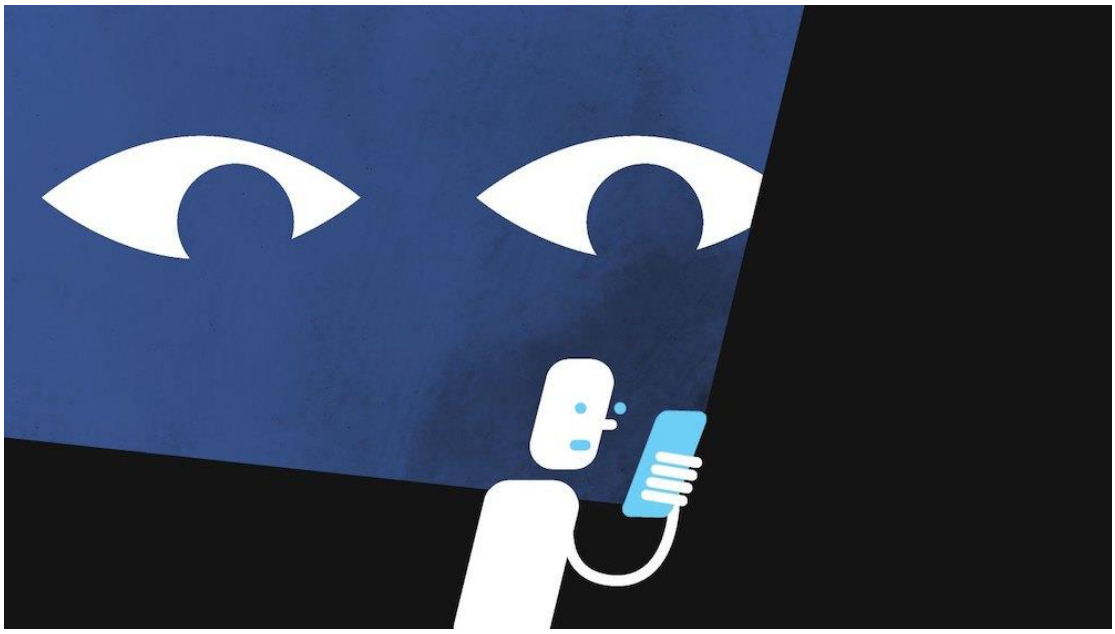
- **梳理谈话要点：**安全专家可以为管理人员一份备注清单，用于在团队会议中加强安全信息内容部分。安全建设的核心内容应当保持一致，但每位团队管理者都可以根据各自团队文化进行自定义。

- **假想练习：**团队领导可以在内部会议期间提出一些安全威胁的假象情况，让大家一起讨论。通过倾听对话，团队领导可以判断团队是否理解他们在保护企业安全方面的责任，并且可以在他们识别问题时提供额外的帮助和培训。这种方法也是促进合作思维的好途径，使得员工在安全的群体环境中表达想法和落实行动。（来源：FreeBuf）

四、政府之声

➢ App 违法违规收集使用个人信息行为认定方法（征求意见稿）发布

2019 年 5 月 5 日，App 专项治理工作组发布了关于征求《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》通知。



通知全文如下：

各有关单位及专家：为落实《关于开展 App 违法违规收集使用个人信息专项治理的公告》，App 专项治理工作组在中央网信办、工信部、公安部、市场监管总局指导下，开展了 App 违法违规收集使用个人信息安全评估，发现一些 App 存在强制授权、过度索权、超范围收集个人信息等问题。

为了明确界定 App 收集使用个人信息方面的违法违规行为，为 App 运营者自查自纠提供指引，为 App 评估和处置提供参考， App 专项治理工作组起草了《App 违法违规收集使用个人信息行为认定方法(征求意见稿)》，现向社会公开征求意见。（来源：App 专项治理工作组）

- **《App 违法违规收集使用个人信息行为认定方法（征求意见稿）通知》全文：**
- http://pip.tc260.org.cn/assets/wz/2019-05-05/5bcd8d9f-a06c-4d20-80bf-b3b64c9eb816.pdf

➢ 《医疗机构医疗大数据平台建设指南》（征求意见稿）发布

2019 年 5 月 6 日，《医疗机构医疗大数据平台建设指南》（征求意见稿）（以下简称“《建设指南》”）发布会在北京成功举办。在内容设置上，《建设指南》从深化医院信息化改革和推广医疗大数据应用入手,结合大数据时代下的国内外医疗现状,给出了医疗大数据平台的建设内容和建设要点，包括总体架构、技术路线和功能范围；其次，针对不同医疗业务场景,介绍了基于医疗大数据平台的临床、科研和公共卫生等各种大数据应用，并解析了医疗大数据为医疗机构提供何种数据服务的问题，同时，给出了一些详细介绍医疗大数据平台实际建设和应用情况的案例；最后，行业专家围绕建设医疗大数据平台给出了一些具有建设性的意见和建议，并展望了医疗大数据平台的后续发展。

《建设指南》全文八万五千字，其中正文五万字，共包括四个章节：第一章引言，介绍医疗大数据发展的政策背景、现状和问题，以及医疗大数据及平台的概念、意义和作用；第二章总体设计，明确医疗大数据平台的需求和建设目标，介绍医疗大数据平台的总体架构、技术路线和功能范围；第三章建设要点，详细介绍了医疗大数据平台建设的安全体系、硬件部署、数据接入以及数据治理策略；第四章应用场景，从临床应用、科研应用、医院管理、患者管理和药物临床试验等方面介绍了医疗大数据的建设及应用。

此外，本指南还设有附录，包括：专门为本指南主题征集的专家观点，回应了业界关心的医疗大数据的建设中存在的热点、难点问题，以及建设经验；医院大数据平台的建设案例，大数据平台的数据管理制度等。

为全面展示当前医疗大数据建设成果，《建设指南》针对性地选取了有代表性的典型案例，包括解放军总医院、北京大学第三医院、上海市第十医院、福建省立医院和北京大学肿瘤医院，分享其建设情况及研究成果，供读者参考。

衡反修主任介绍，《建设指南》编写的初衷是力图根据当前医院信息技术应用水平、医院管理和技术能力，以及国内医疗大数据建设现状，形成适合国内医院发展、可落地的建设方案，为医院建设大数据平台提供借鉴。（来源：中国医院协会信息管理专业委员会）

- **《医疗机构医疗大数据平台建设指南》（征求意见稿）**
- **全文：**http://www.chima.org.cn/uploadfile/2019/0506/20190506071559563.pdf

➢ 国务院办公厅印发国务院 2019 年立法工作计划的通知

2019 年 5 月 1 日，国务院办公厅关于印发国务院 2019 年立法工作计划的通知、国办发〔2019〕18 号。其中，第二条指出：坚决贯彻落实党中央决策部署，科学合理安排立法项目

——围绕打好三大攻坚战，提请全国人大常委会审议固体废物污染环境防治法修订草案，制定非存款类放贷组织条例、处置非法集资条例、私募投资基金管理暂行条例、排污许可管理条例、地下水管理条例，修订外资银行管理条例、报废机动车回收管理办法。

——围绕推动经济高质量发展，提请全国人大常委会审议契税法草案、税收征收管理法修订草案，制定优化营商环境条例、反走私工作条例、企业名称登记管理条例，修订国家科学技术奖励条例、粮食流通管理条例、企业所得税法实施条例、个体工商户条例。

——围绕加强社会主义文化建设，提请全国人大常委会审议著作权法修订草案，**制定未成年人网络保护条例**，修订水下文物保护管理条例。

——围绕提高保障和改善民生水平，提请全国人大常委会审议退役军人保障法草案，制定保障农民工工资支付条例、消费者权益保护法实施条例、城镇住房保障条例、住房租赁条例、社会保险经办管理服务条例、生物技术研究开发安全管理条例、生物医学新技术临床应用管理条例、建设工程抗震管理条例、城市公共交通管理条例，修订民办教育促进法实施条例、失业保险条例、食品安全法实施条例、生猪屠宰管理条例、医疗器械监督管理条例、化妆品卫生监督条例、收费公路管理条例。

——围绕加强和创新社会治理，提请全国人大常委会审议社区矫正法草案、治安管理处罚法修订草案、海上交通安全法修订草案，制定社会组织登记管理条例、**公共安全视频图像信息系统管理条例**。

——围绕有效维护国家安全，提请全国人大常委会审议**密码法草案**、原子能法草案、出口管制法草案、监狱法修订草案，制定领事保护与协助工作条例、外国人永久居留管理条例、**关键信息基础设施安全保护条例**、人类遗传资源管理条例。

——围绕深化国防和军队改革，提请全国人大常委会审议有关法律草案，制定、修订有关行政法规。

——围绕深入推进依法行政、加强政府自身建设，提请全国人大常委会审议档案法修订草案，制定重大行政决策程序暂行条例、政府督查工作条例、司法所条例，修订预算法实施条例。

为配合中国特色大国外交，推动构建“人类命运共同体”，推动我国积极参与国际规则

制定，开展有关国际条约审核工作。抓紧办好政府职能转变和“放管服”改革、优化营商环境等涉及的法律法规清理工作。抓紧制定外商投资法相关配套法规。配合全国人大及其常委会审议有关法律案。对于其他正在研究但未列入立法工作计划的立法项目，由有关部门继续研究论证。对于党中央、国务院交办的其他立法项目，抓紧办理，尽快完成起草和审查任务。（来源：中国政府网）

- **《国务院办公厅关于印发国务院 2019 年立法工作计划的通知》**
- **全文：**http://www.gov.cn/zhengce/content/2019-05/11/content_5390676.htm

➢ 公安部：等级保护 2.0 标准 5 月 13 日发布

2019 年 5 月 10 日，公安部网络安全等级保护中心通报：网络安全等级保护制度 2.0 标准将于 5 月 13 日正式发布。随后，由公安部网络安全保卫局指导、公安部信息安全等级保护评估中心主办的“网络安全等级保护制度 2.0 国家标准宣贯会”将于 5 月 16 日在北京召开，参会人数预计将达到千人规模。

网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。随着信息技术的发展和网络安全形势的变化，等级保护制度 2.0 在 1.0 的基础上，注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。网络安全等级保护制度 2.0 国家标准的发布，对加强我国网络安全保障工作，提升网络安全保护能力具有重要意义。

网络安全等级保护新标准具有三个特点，第一，等级保护的基本要求、测评要求和设计技术要求框架统一，即：安全管理中心支持下的三重防护结构框架；第二，通用安全要求+新型应用安全扩展要求，将云计算、移动互联、物联网、工业控制系统等列入标准规范；第三，把可信验证列入各级别和各环节的主要功能要求。基于此，等保 2.0 时代，应重点对云计算、移动互联、物联网、工业控制以及大数据安全等进行全面安全防护，确保关键信息基础设施安全。（来源：公安部网络安全等级保护中心 ）

五、本期重要漏洞实例

➢ Cisco Firepower Threat Defense Software 拒绝服务漏洞

发布日期：2019-05-01
更新日期：2019-05-08
受影响系统：
Cisco Firepower Threat Defense Software 6.3
Cisco Firepower Threat Defense Software 6.2.3
Cisco Firepower Threat Defense Software 6.2.2
Cisco Firepower Threat Defense Software 6.2.1
Cisco Firepower Threat Defense Software 6.2
Cisco Firepower Threat Defense Software 6.1
Cisco Firepower Threat Defense Software 6.0.1
Cisco Firepower Threat Defense Software 6.0
描述：

BUGTRAQ ID: 108170
CVE(CAN) ID: CVE-2019-1703
Cisco Firepower Threat Defense（FTD）Software 是由美国思科（Cisco）公司开发的程序，是一套提供下一代防火墙服务的统一软件。
用于 Cisco Firepower 2100 系列的 Cisco Firepower Threat Defense Software 中，内部数据包处理功能存在一个漏洞，允许未经身份验证的远程攻击者导致受影响的设备停止处理流量，从而导致拒绝服务（DoS）条件。该漏洞是由于逻辑错误导致的，该逻辑错误可能会阻止在特定流量条件下补充入口缓冲区。攻击者可以通过向受影响的设备发送一系列精心设计的数据包来利用此漏洞。成功利用此漏洞可能允许攻击者使用在所有接口之间共享的所有输入缓冲区，从而导致所有活动接口中的队列楔形条件。
<*来源：Oracle
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-dos
*>
建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-20190501-frpwr-dos）以及相应补丁：
cisco-sa-20190501-frpwr-dos：Cisco Firepower Threat Defense Software Packet Processing Denial of Service Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-dos

➢ Oracle WebLogic Server 反序列化远程命令执行漏洞

发布日期：2019-04-25
更新日期：2019-05-05
受影响系统：
Oracle WebLogic Server 12.1.3.0.0
Oracle WebLogic Server 10.3.6.0.0
描述：

BUGTRAQ ID: 108074
CVE(CAN) ID: CVE-2019-2725
Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。
Oracle Fusion Middleware 的 Oracle WebLogic Server 10.3.6.0.0 和 12.1.3.0.0（子组件：Web 服务）版本存在一个漏洞，允许通过 HTTP 进行网络访问的、未经身份验证的攻击者破坏 Oracle WebLogic Server。成功利用此漏洞可能导致 Oracle WebLogic Server 的接管。

<*来源：Badcode, Liao Xinxi, ZengShuai Hao, Zhiyi Zhang, and Hongwei Pan, Lin Zheng, Song Keya, and Tianlei
链接：https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
*>
建议：

厂商补丁：
Oracle

Oracle 已经为此发布了一个安全公告（CVE-2019-2725）以及相应补丁：
CVE-2019-2725：Oracle Security Alert Advisory - CVE-2019-2725
链接：https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

➢ ImageMagick 缓冲区溢出漏洞

发布日期：2019-04-29
更新日期：2019-05-05
受影响系统：
ImageMagick ImageMagick 7.0.8-43 Q16
描述：

BUGTRAQ ID: 108102
CVE(CAN) ID: CVE-2019-11597
ImageMagick 是一个用来创建、编辑、合成图片的软件，可以读取、转换、写入多种格式的图片。

ImageMagick 7.0.8-43 Q16 版本在 coders/tiff.c 的 WriteTIFFImage 函数中有一个基于堆的缓冲区过读，允许攻击者通过精心制作的图像文件导致拒绝服务或可能导致信息泄露。

<*来源：galycannon
链接：https://github.com/ImageMagick/ImageMagick/issues/1540
*>
建议：

厂商补丁：
ImageMagick

ImageMagick 已经为此发布了一个安全公告（#1540）以及相应补丁：
#1540：heap-buffer-overflow in WritePNMImage of coders/pnm.c
链接：https://github.com/ImageMagick/ImageMagick/issues/1540

➢ Lenovo XClarity Administrator 信息泄露漏洞

发布日期：2019-05-01
更新日期：2019-05-08
受影响系统：
Lenovo XClarity Administrator 2.3
Lenovo XClarity Administrator 2.2
Lenovo XClarity Administrator 2.0
不受影响系统：
Lenovo XClarity Administrator 2.4
描述：

BUGTRAQ ID: 108165
CVE(CAN) ID: CVE-2019-6158
Lenovo XClarity Administrator（LXCA）是中国联想（Lenovo）公司的一套集中式的资源管理解决方案。
Lenovo XClarity Administrator 的 HTTP 代理凭据被以明文形式写入日志文件。该漏洞仅在配置 HTTP 代理凭据时影响 LXCA。受影响版本为 2.0.0 到 2.3.x.
<*来源：Lenovo
链接：https://support.lenovo.com/us/zh/solutions/len-26141
*>
建议：

厂商补丁：
Lenovo
Lenovo 已经为此发布了一个安全公告（len-26141）以及相应补丁：
len-26141：XClarity Administrator (LXCA) Service Data May Include Proxy Credentials
链接：https://support.lenovo.com/us/zh/solutions/len-26141

六、本期网络安全事件

➢ 2.75 亿条印度公民信息 MongoDB 数据库被曝光公开索引

2019 年 5 月 10 日，援引外媒 Security Discovery 报道，他们于 5 月 1 日发现了一个未经保护和公开索引的 MongoDB 数据库，其中包括了涉及印度公民的个人身份信息的 275,265,298 条记录。这些信息中包括姓名、电子邮件地址、性别、教育水平和专业领域、专业技能和职称、手机号码、就业经历和当前雇主、出生日期以及当前的薪资水平。


```
"_id" : ObjectId("5cbf0fd076da82177d173910"),
"Course(2nd Highest Education)" : NaN,
"Name" : "[redacted]",
"Current Location" : "[redacted]",
"Industry" : "Catering/Food Services/Restaurant, Hotel/Travel/Tourism/Airlines/Hospitality",
"Institute(Highest Education)" : "Others",
"Specialization(2nd Highest Education)" : NaN,
"Resume Id" : "[redacted]",
"Specialization(Highest Education)" : "Other B.A.",
"Current Employer" : "[redacted]",
"Mobile No" : "[redacted]",
"Preferred Location" : "Anywhere in India",
"Course(Highest Education)" : "B.A.",
"Key Skills" : "GPs, PNL, stocks, guest care, staff developement and training, IT skills, gener
"Previous Employer" : "[redacted]",
"Date of Birth" : "1986-04-14 00:00:00",
"Address" : "[redacted]",
"Area of Specialization" : "Food & Beverage, Guest Relation, Restaurant",
"Institute(2nd Highest Education)" : NaN,
"Resume Title" : "f&b operational expert and has got graduation from london",
"Current Salary" : "6,00,000 annually",
"Email Id" : "[redacted]yahoo.com",
"Gender" : "Male",
"Level" : "Others",
"Functional Area" : "Hotel/Restaurant",
"Alternate Number" : "[redacted]"
```


在这个曝光的数据库中并没有泄露源或者从属关系的标签。这个 MongoDB 数据库本身是托管在亚马逊 AWS 基础架构上的，反向 DNS 也没有显示任何结果。数据库中的结构和名称暗示这个曝光的数据库仅仅只是黑客大规模手机数据中的一部分。根据 Shodan 的历史数据，MongoDB 于 2019 年 4 月 23 日首次被索引。

Collection Statistics

_id	Collection	Count	Size	Storage Size	Avg Object Size	Indexes	Index Size	Padding
	mediafire_csv_last_final	275265298	110.0 GiB (118,0...	114.6 GiB (123,0...	428 B (428)	1	8.3 GiB (8,942,7...	1.0
	mediafire_csv_4	33279137	12.1 GiB (13,02...	12.7 GiB (13,59...	391 B (391)	1	1.0 GiB (1,080,6...	1.0
	mediafire_csv_final_2	4250988	1.9 GiB (2,092,6...	2.6 GiB (2,828,7...	492 B (492)	1	133.1 MiB (139,...	1.0
	mediafire_csv_2	1945618	1.1 GiB (1,132,6...	1.1 GiB (1,164,9...	582 B (582)	1	60.2 MiB (63,14...	1.0
	mediafire_csv	1459614	152.4 MiB (159,...	232.0 MiB (243,...	109 B (109)	1	45.2 MiB (47,37...	1.0
	mediafire_csv_final_3	339894	229.3 MiB (240,...	320.3 MiB (335,...	707 B (707)	1	10.5 MiB (11,04...	1.0
	jalandhar	20000	9.4 MiB (9,821,4...	10.7 MiB (11,18...	491 B (491)	1	638.8 KiB (654,...	1.0
	daman	4638	8.0 MiB (8,375,8...	10.7 MiB (11,18...	1.8 KiB (1,805)	1	159.7 KiB (163,...	1.0
	mediafire_csv_final_1	3426	8.8 MiB (9,178,8...	10.7 MiB (11,18...	2.6 KiB (2,679)	1	119.8 KiB (122,...	1.0
	mediafire_csv_final_4	2374	7.7 MiB (8,097,9...	10.7 MiB (11,18...	3.3 KiB (3,411)	1	87.8 KiB (89,936)	1.0
	mediafire_csv_3	585	28.1 KiB (28,736)	40.0 KiB (40,960)	49 B (49)	1	31.9 KiB (32,704)	1.0
	my_collection_keys	585	28.1 KiB (28,736)	40.0 KiB (40,960)	49 B (49)	1	31.9 KiB (32,704)	1.0
	mediafire_csv_final	484	102.2 KiB (104,...	168.0 KiB (172,...	216 B (216)	1	24.0 KiB (24,528)	1.0
	Medical_test	297	296.4 KiB (303,...	680.0 KiB (696,...	1021 B (1,021)	1	24.0 KiB (24,528)	1.0
	system.indexes	17	1.9 KiB (1,904)	8.0 KiB (8,192)	112 B (112)	0	0 B (0)	1.0
	yeppi	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0
	test_collect111ion	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0
	test_collection	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0

随后外媒将此事报告给了印度 CERT 团队，不过截至目前这个数据库依然是公开和可搜索的，是被名为“Unistellar”的黑客集团所抛弃的。尽管实际信息被窃的人数可能少于暴露的记录数量，但依然是印度地区报告的最大规模信息泄露事件。（来源：Security Discovery）

➢ 爱彼迎民宿路由器暗藏摄像头：官方回应已移除房源

2019 年 5 月 5 日，有媒体报道称，在山东青岛一家爱彼迎(Airbnb)的民宿中，住客在无线路由器内发现了隐藏的摄像头和存储卡，拍摄方向正对卧室。5 日晚间，爱彼迎公关人员对此正式回应称，爱彼迎十分重视隐私保护，对任何侵犯隐私的行为都秉持零容忍态度，目前平台方已经永久性移除涉事房源。

爱彼迎方面表示：“5 月 2 日晚上 10 点房客与我们联系后，我们当晚做了全额退款处理，并承诺会支付他的酒店费用。同时我们是专人专线，并安排了个案经理专门跟他沟通。”

此外，爱彼迎还再次向房客表达诚恳歉意，并承诺“会继续跟进妥善安排后续事宜”。

据了解，发现路由器隐藏摄像头的住客从事信息安全工作，整个过程被一些网友称为“教科书式反偷拍”：

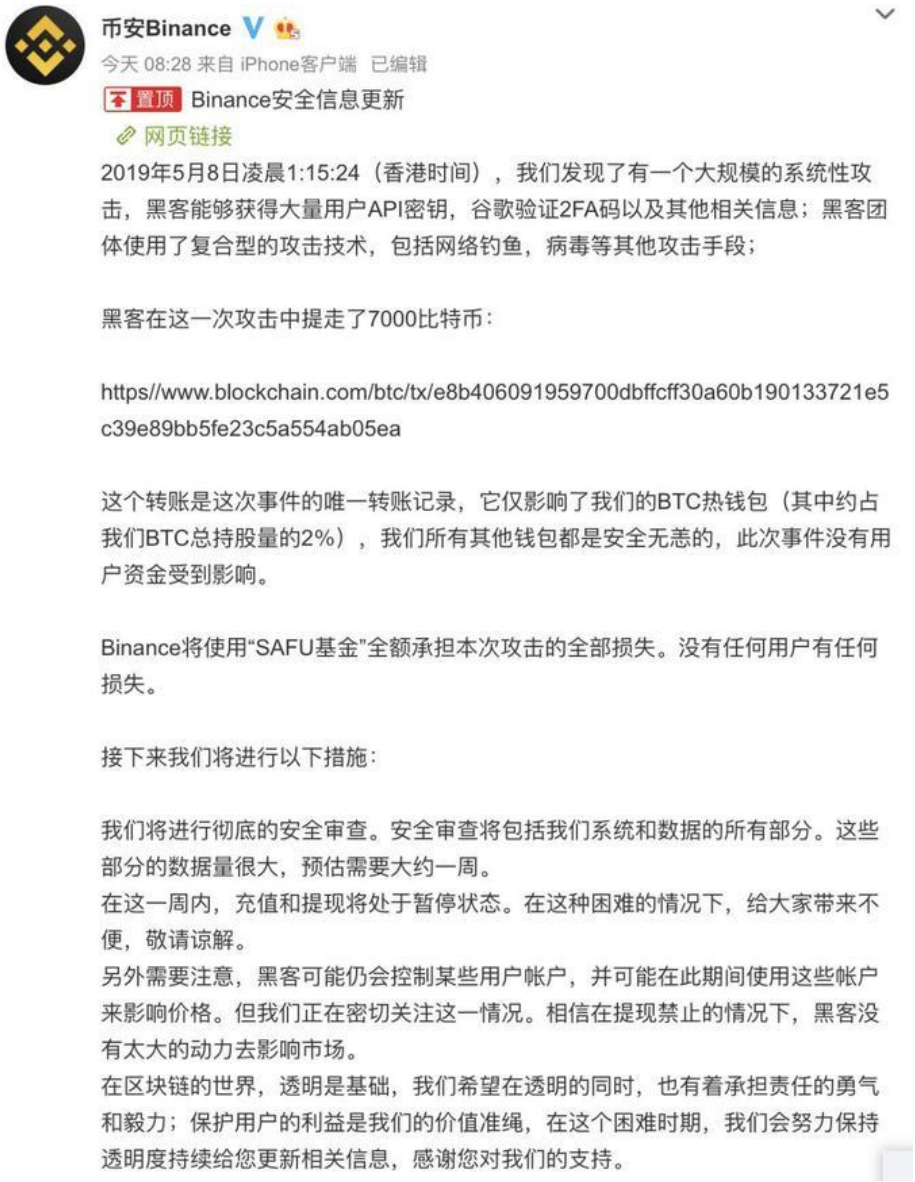
入住后在玄关和卧室发现三个动态感应器，但屋内并无智能家居。随后检查路由器，发现一根排线异常，对比官方产品照片后确认路由器进行了改造，拆开后发现内有存储卡，立

即报了警。

据悉，涉案民宿房主自 2019 年 3 月开始，在房间内正对床的位置安装针孔摄像头，拍摄他人隐私视频进行观看，目前已被行政拘留 20 日，并处罚金 500 元，擅自经营的旅馆被依法取缔。（来源：快科技）

➢ 货币交易所币安受到黑客攻击被盗 7074 枚比特币

2019 年 5 月 8 日下午消息，据路透社报道，全球最大加密货币交易所之一的币安（Binance）今天宣布，黑客从该公司窃取了价值 4100 万美元的比特币。这也是全球各地发生的一系列加密货币交易所失窃案中的最新一起



币安Binance

今天 08:28 来自 iPhone客户端 已编辑

置顶 Binance安全信息更新

网页链接

2019年5月8日凌晨1:15:24（香港时间），我们发现了有一个大规模的系统性攻击，黑客能够获得大量用户API密钥，谷歌验证2FA码以及其他相关信息；黑客团体使用了复合型的攻击技术，包括网络钓鱼，病毒等其他攻击手段；

黑客在这一次攻击中提走了7000比特币：

https//www.blockchain.com/btc/tx/e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

这个转账是这次事件的唯一转账记录，它仅影响了我们的BTC热钱包（其中约占我们BTC总持股量的2%），我们所有其他钱包都是安全无恙的，此次事件没有用户资金受到影响。

Binance将使用"SAFU基金"全额承担本次攻击的全部损失。没有任何用户有任何损失。

接下来我们将进行以下措施：

我们将进行彻底的安全审查。安全审查将包括我们系统和数据的所有部分。这些部分的数据量很大，预估需要大约一周。

在这一周内，充值和提现将处于暂停状态。在这种困难的情况下，给大家带来不便，敬请谅解。

另外需要注意，黑客可能仍会控制某些用户帐户，并可能在此期间使用这些帐户来影响价格。但我们正在密切关注这一情况。相信在提现禁止的情况下，黑客没有太大的动力去影响市场。

在区块链的世界，透明是基础，我们希望在透明的同时，也有着承担责任的勇气和毅力；保护用户的利益是我们的价值准绳，在这个困难时期，我们会努力保持透明度持续给您更新相关信息，感谢您对我们的支持。

对此，币安创始人赵长鹏在 AMA 中首次披露了黑客盗币的细节。他表示，黑客此前已发现系统存在的安全漏洞，但一直很耐心，直到系统出现大额交易才出手。此外，赵长鹏还对外披露，币安在 5 月 7 日凌晨就发现了“大规模的安全漏洞”，该漏洞导致黑客能够访问用户应用程序接口密钥（API keys）、双因素身份验证码、以及其他信息。按照安全通知中公布的一笔交易，黑客从币安交易所中取走了价值大约 4100 万美元的比特币。

赵长鹏的文章表示，用户不必担心自己的损失，因为该公司会使用其安全资产基金来补偿这部分损失。赵长鹏在 Twitter 上表示，包括 Coinbase 在内的其他加密货币交易所都针对与此次入侵事件有关的地址进行了存款冻结。受到黑客窃取消息影响，比特币价格 8 日早些时候在亚洲一度下跌 4.2%，随后跌幅收窄。（来源：快科技）

➢ 80 后银行女员工偷拍金融机密文件被判“故意泄露国家机密罪”

2019 年 5 月 9 日，新华社报道：“你只告诉我一个人，我不会给别人说的。”相信许多人在向别人打听秘密的时候都会做出这种保证，但是又有几个人能做到？泄密的后果又由谁来承担？最近，80 后研究生李某就掉进了这样的“坑”。


中国裁判文书网
China Judgements Online

关联文书

二审 河北省衡水市中级人民法院 （2018）冀11刑终479号 2018-12-11 律予撤回上诉

李某故意泄露国家秘密一审刑事判决书

发布日期：2019-05-06 浏览：389次

河北省衡水市冀州区人民法院
刑 事 判 决 书
（2018）冀1181刑初149号

公诉机关衡水市冀州区人民检察院。
被告人李某，女，1986年9月25日出生。
辩护人郑某斌，北京方宏律师事务所律师。
辩护人潘慧凤，河北合明律师事务所律师。
被告人李某犯故意泄露国家秘密罪一案由河北省高级人民法院指定本院管辖。衡水市冀州区人民检察院以冀检公诉刑诉[2018]127号起诉书指控被告人李某犯故意泄露国家秘密罪，于2018年8月27日向本院提起公诉。本院依法

事情是这样的：1986 年出生的李某（女）研究生毕业后，自 2011 年 7 月开始在廊坊银行工作，2016 年 6 月至 12 月被中国银监会借调工作，借调期满后，因工作原因继续借调至 2017 年 2 月底。

李某当时在中国银监会法规部法制顾问处工作。2017 年 2 月 16 日下午，法规部法律顾问处保密机上的 OA 系统收到一份文件，文件名称是“关于商请提供意见的函”，附件就是《指导意见》（也就是处于内部征求意见阶段的资管新规）。李某看见后找到潘某副处长汇报情况，潘某让其负责处理，李某便向潘副处长申请将文件打印出来再处理。潘副处长同意之后，李某就到综合处将文件打印了出来，并且在涉密机打印登记本上进行了登记。

2017 年 2 月 17 日上午 9 时许，李某通过微信和原来单位（廊坊银行总行）法律合规部总经理郑某聊一些工作，告诉郑某中国人民银行近期可能会出台对统一资管业务的指导意见。郑某问是否有文件，李某说有文件，是涉密的，不能外传。

郑某说他个人学习一下，于是李某拍照之后，通过微信点对点的发给了他。一共拍了三十多张照片（总共大概七、八十页），发给了郑某。但是由于李某知道这份文件是秘密文件，不能随便给别人看，她发给郑某的照片上就没有拍带有机密标识字样的页面。

根据李某证言，她把文件处理完毕之后，按照领导安排出差了。回来后李某在一个微信公众号上看到了类似的照片，因为这些照片和发给郑某的特别像，但不敢确定就是她发给郑某的文件照片，于是她就把微信公众号的链接发给了郑某，问郑某怎么回事。

郑某说他也不知道怎回事，他只是把文件照片发给了廊坊银行总监费某一个人，没有发给别人。

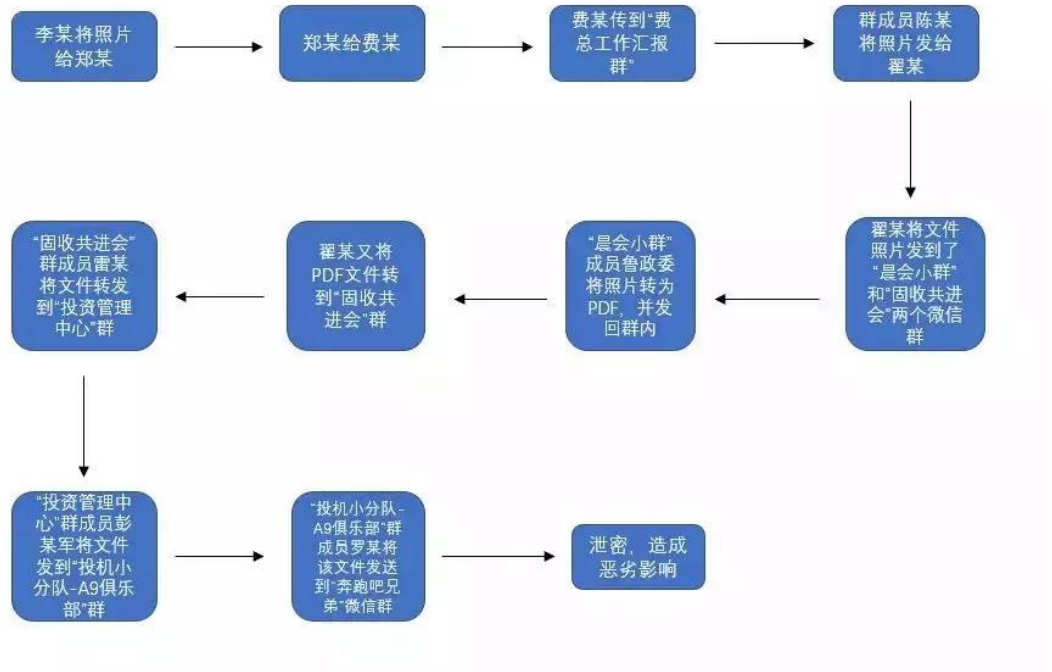
然而，费某将文件照片发布到了名为“费总工作汇报群”的下属工作微信群，该群成员廊坊银行金融同业管理部总经理陈某将文件照片发给了兴业经济研究咨询股份有限公司员工翟某。

结果该文件就开启“一传十、十传百”的扩散模式。

2017 年 2 月 21 日 7 时 03 分许，翟某将文件照片发到了“晨会小群”和“固收共进会”两个微信群。2017 年 2 月 21 日 8 时 41 分许，“晨会小群”微信群成员兴业经济研究咨询股份有限公司员工鲁政委，将上述 36 张图片转换成为 PDF 格式文档，文件名为《20170221 资产管理办法》并发回“晨会小群”。2017 年 2 月 21 日 9 时 08 分许，翟某将该文件发到了“固收共进会”微信群。2017 年 2 月 21 日 9 时 22 分许，“固收共进会”微信群成员，民生银行总行投资管理中心员工雷某将该文件发送到“投资管理中心”微信群。2017 年 2 月 21 日 9 时 42 分许，“投资管理中心”微信群成员北京光大银行工作人员彭某军，将该文件发送

到“投机小分队-A9 俱乐部”。

“投机小分队-A9 俱乐部”群成员罗某随后将该文件发送到“奔跑吧兄弟”微信群。进而导致该文件在多个金融行业微信群及有关人员微博、博客、微信公众号中不断转发，最终造成涉密信息在互联网上被大范围公开传播，影响恶劣。



事实上，李某借调到银监会后，集体开会的时候就强调过保密教育，但其法律意识过于淡薄。

法院认为：被告人李某违反保守国家秘密法的规定，故意泄露国家秘密，情节严重，其行为已构成故意泄露国家秘密罪，依法应予惩处。被告人李某对起诉书指控的犯罪事实及确定的罪名无异议。

综合考虑被告人的犯罪事实、性质、情节、悔罪表现及对社会的危害程度，最终判决如下：被告人李某犯故意泄露国家秘密罪，判处有期徒刑一年，缓刑一年。李某的这种行为确实造成了很恶劣的影响，有可能严重影响到国家对金融市场的调控，若是当初李某泄露的文件给市场造成扰动，那造成的损失可能是无法挽回的。（来源：新华社）

➢ 网络公司后台被攻击损失近千万元 民警千里抓“黑客”

2019 年 5 月 11 日，去年 12 月，回龙观派出所接到辖区内一网络公司报警，称其开发

的软件被黑客攻击，公司服务器全面瘫痪。警方经过近半年的侦查，通过层层数据梳理成功锁定嫌疑人，近日远赴成都将雇佣黑客实施网络攻击的两名嫌疑人抓获归案。目前案件正在进一步工作中。

随着网络化的普及，扫码点餐、大屏互动等功能在餐厅、酒吧等场所已经比较普及。每年的年底，不少餐厅、酒吧会承接公司年会等活动，正是客流高峰。但就在此时，一提供相关服务的网络公司后台遭到了黑客的攻击。

“当时真的是绝望了。”该网络公司法定代表人刘先生告诉记者，他们开发的应用主要为饭店、酒吧提供点餐、互动等平台服务，没想到公司主服务器被攻击而宕机，数百家合作商户无法进行结账、互动，导致了不少商户门店出现混乱。

网络公司查询后台数据发现，其应用被“肉鸡”软件攻击上亿次，前后持续了近半个月。初步统计，该公司的损失近千万元。

接报警后，昌平公安分局警务支援大队网络侦查中队和回龙观派出所的民警立即将网络公司的服务器数据进行了全面保全，并从中寻找到数十万条攻击日志，逐条排查以找出线索。

经层层跳转，警方确定了其中一个攻击源，民警立即来到江苏省某市开展侦查。此时，本案涉案的黑客人员已因实施其他犯罪行为被江苏警方刑事拘留，审讯后，黑客交代了雇佣其实施网络攻击的“上线”。

通过数据梳理，警方锁定了位于成都的两名嫌疑人。半个月前，在四川省成都市，民警陆续将犯罪嫌疑人周某、陈某抓获归案。

据悉，这一案件是昌平区破获的首起涉黑客网络犯罪案件。目前，两名嫌疑人已因涉嫌非法破坏计算机信息系统罪被昌平分局刑事拘留，案件仍在进一步工作中。

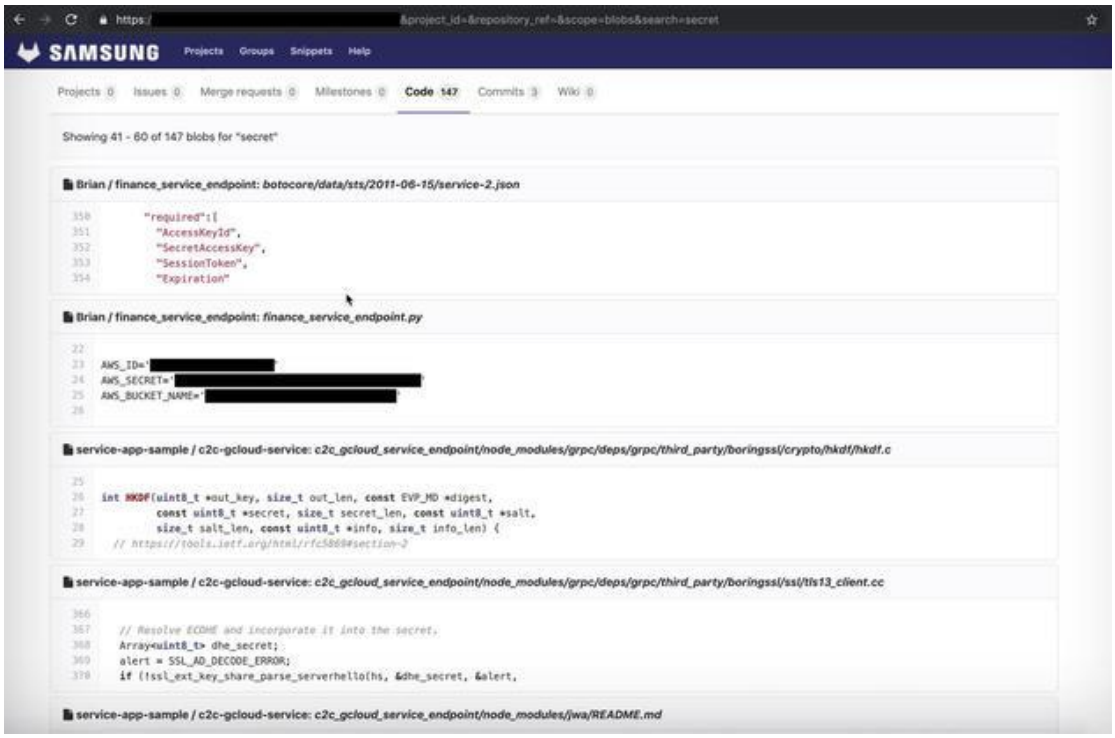
昌平公安分局警务支援大队网络侦查中队刘警官表示：网络犯罪是非接触性犯罪，警方要想获得并固定证据格外困难。而此案对相关从事网络服务的公司也是一个提醒，提升公司的日常维护意识，“不光能建起来，还得能守得住”。 （来源：北京晚报）

➢ 三星内部数据不设防涉及源代码、密码和员工资料

2019 年 5 月 9 日，美国科技媒体报道称：一名信息安全研究员近期发现，三星工程师使用的一个开发平台泄露了多个内部项目，包括三星 SmartThings 敏感的源代码、证书和密钥。三星数十个自主编码项目出现在旗下 Vandev Lab 的 GitLab 实例中。该实例被三星员工用于分享并贡献各种应用、服务和项目的代码。由于这些项目被设置为“公开”，同时没有受到密码的保护，因此任何人都可以查看项目，获取并下载源代码。

迪拜信息安全公司 SpiderSilk 的安全研究员莫撒布·胡赛因（Mossab Hussein）发现了这些泄露的文件。他表示，某个项目包含的证书允许访问正在使用的整个 AWS 帐号，包括 100 多个 S3 存储单元，其中保存了日志和分析数据。

他指出，许多文件夹包含三星 SmartThings 和 Bixby 服务的日志和分析数据，以及几名员工以明文保存的私有 GitLab 令牌。这使得他可以额外获得 42 个公开项目，以及多个私有项目的访问权限。



三星回应称，其中一些文件是用于测试的，但胡赛因对此提出质疑。他表示，在 GitLab 代码仓库中发现的源代码与 4 月 10 日在 Google Play 上发布的 Android 应用包含的代码相同。这款应用随后又有过升级，到目前为止的安装量已经超过 1 亿多次。

胡赛因说：“我获得了一名用户的私有令牌，该用户可以完全访问 GitLab 上的所有 135 个项目。”因此，他可以使用该员工的帐号去修改代码。胡赛因还提供了多张屏幕截图和视频作为证据。泄露的 GitLab 实例中还包括三星 SmartThings 的 iOS 和 Android 应用的私有证书。（来源：TechCrunch）