国盟信息安全通报

2019 年 3 月 18 日第 188 期

国盟信息安全通报

（第 188 期）

国际信息安全学习联盟

2019 年 3 月 18 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 240 个，其中高危漏洞 105 个、中危漏洞 122 个、低危漏洞 13 个。漏洞平均分值为 6.38。本周收录的漏洞中，涉及 0day 漏洞 115 个（占 48%），其中互联网上出现“FiberHomeFiberhome AN5506-04-F 跨站脚本漏洞、OFCMS 后台 ueditor uploadScrawl 文件上传漏洞”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 1916 个，与上周（1944 个）环比下降 1%。

主要内容

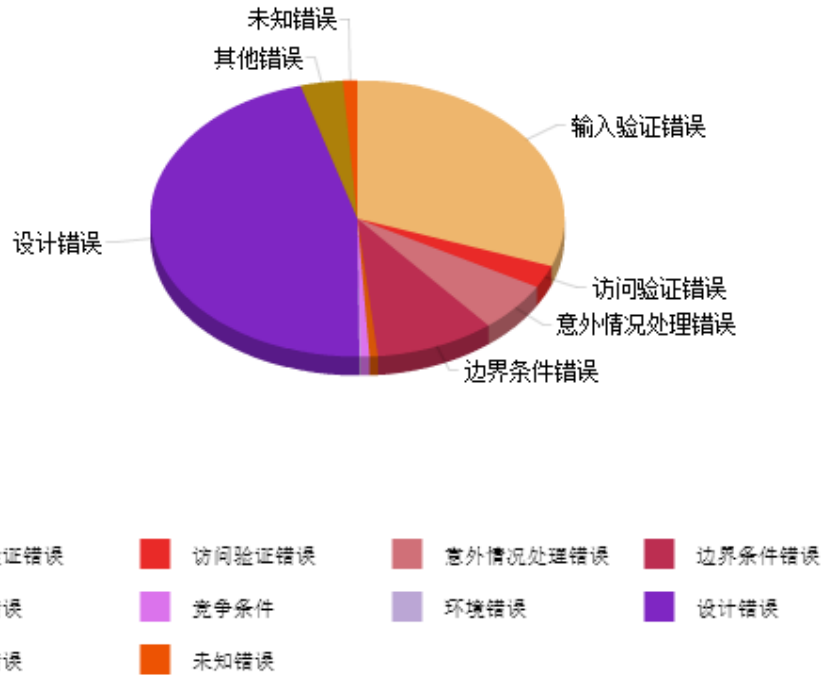
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

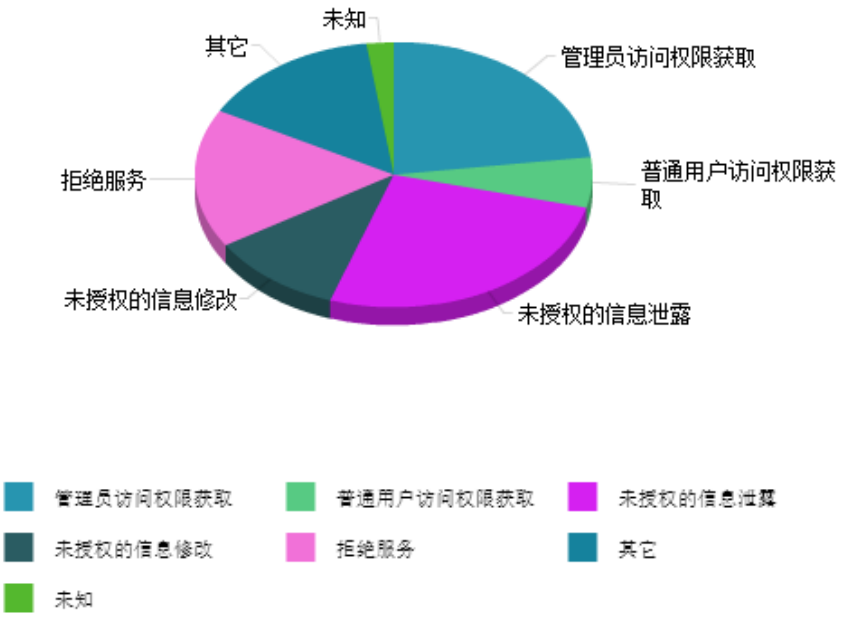
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 240 个，其中高危漏洞 105 个、中危漏洞 122 个、低危漏洞 13 个。漏洞平均分值为 6.38。本周收录的漏洞中，涉及 0day 漏洞 115 个（占 48%），其中互联网上出现“FiberHomeFiberhome AN5506-04-F 跨站脚本漏洞、OFCMS 后台 ueditor uploadScrawl 文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1916 个，与上周（1944 个）环比下降 1%。

二、安全漏洞增长数量及种类分布情况

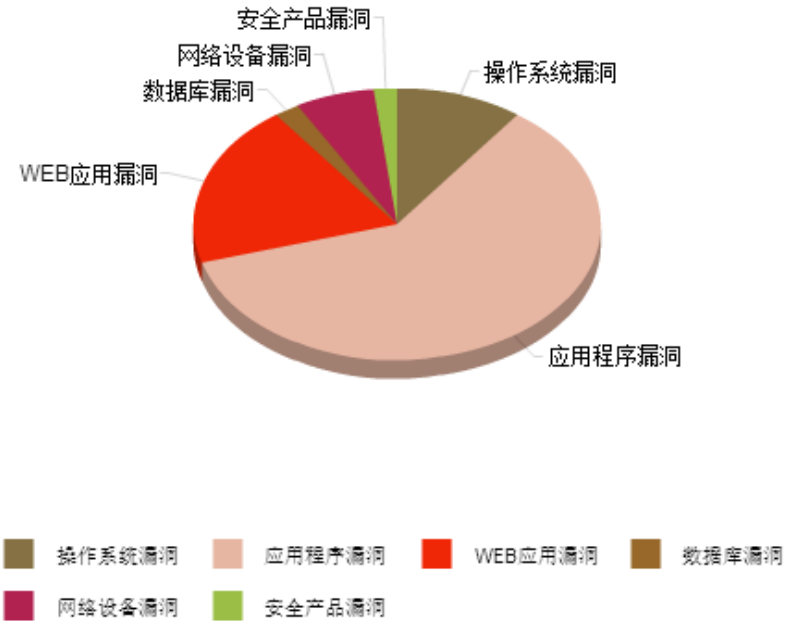
➢ 漏洞产生原因（2019 年 3 月 04 日—2019 年 3 月 18 日）



➢ 漏洞引发的威胁（2019 年 3 月 04 日—2019 年 3 月 18 日）



➢ 漏洞影响对象类型（2019 年 3 月 04 日—2019 年 3 月 18 日）



三、安全产业动态

➢ 十三届全国人大二次会议关于网络安全的相关提案（汇总）

北京 3 月 15 日上午，第十三届全国人民代表大会第二次会议在人民大会堂举行闭幕会，表决关于政府工作报告的决议草案，表决中华人民共和国外商投资法草案，表决关于 2018 年国民经济和社会发展计划执行情况与 2019 年国民经济和社会发展计划的决议草案，表决关于 2018 年中央和地方预算执行情况与 2019 年中央和地方预算的决议草案，表决关于全国人民代表大会常务委员会工作报告的决议草案，表决关于最高人民法院工作报告的决议草案，表决关于最高人民检察院工作报告的决议草案，表决关于确认全国人大常委会接受张荣顺辞去十三届全国人大常委会委员职务的请求的决定草案。

十三届全国人大二次会议：有关网络安全的提案（汇总）

今年，工业互联网首次被写入政府工作报告，预示了工业互联网成为我国产业创新的驱动力，也将引发互联网治理体系的全面变革，更加需要集思广益，构建多方共同治理、协同共赢的良性模式。因此，今年关于工业互联网安全的提案也是亮点之一。

共建国家级网络安全大脑

全国政协委员、360 集团董事长兼 CEO 周鸿祎表示：5G 时代下，线上线下的边界正在消失，网络空间的攻击将会穿透虚拟空间，直接映射到物理世界的安全。当前中国面临的网络安全威胁比较严峻，一是未来联网设备数以百亿计，每一个都可能成为攻击的切入点，防

不胜防；二是漏洞无处不在，没有攻不破的网络。这些威胁只有通过统一大数据来感知网络中未知的攻击才能解决。

周鸿祎提出两点建议：

1. 将国家级网络安全大脑列为国家重大工程专项。建议成立国家网络安全大脑项目总体工作组、专家组、工程推进组，分别负责顶层设计和总体筹划、系统设计、工程建设。

2. 运用新型举国体制，加快推进国家级网络安全大脑建设。其建议由国家相关部门牵头，协调网信、工信、公安、科技等部门和单位，组织国企、民企、科研院所等广泛参与。

工业互联网的影响已渗透到城市安全、人身安全、关键基础设施安全乃至国家安全，造成的后果日益严重。网络安全从“信息安全”时代进入了“大安全”时代。

把网络安全列为智能汽车标配

周鸿祎第二个提案称，万物互联的理念已经在汽车产业得到空前的发展，这也就不可避免的会有网络安全风险。黑客可以通过网络劫持汽车，造成人身伤害、交通事故，严重的甚至可能被用于执行恐怖袭击，进而威胁国家安全。汽车厂商自身的网络安全问题也将威胁到智能汽车的安全。智能汽车都是与汽车厂商的云端服务器远程相连，一旦汽车厂商云端服务器被发现漏洞，攻击者就会对汽车实现远程操控，或者获取车主和汽车相关信息，造成交通事故，甚至威胁社会安全。

周鸿祎提议，制定强制性生产标准，把网络安全列为智能汽车标配。

1. 加装安全联网模块，提高联网防护能力，建立安全接口，加强汽车的控制安全保护，防止控制被劫持。2. 强制安全测试。建立测试评价体系，在汽车上市前进行网络安全测评。3. 建立厂商安全运营平台，提升安全运营能力，及时发现和阻断黑客攻击。

人工智能要智商也要安全

周鸿祎第三个提案称，人工智能正在加速与经济、社会、国防等深度融合，发挥越来越显著的“头雁”效应。但与此同时，人工智能自身所面临的网络安全风险也越来越突出。比如，人工智能的传感器存在被干扰的风险；训练数据存在被污染的风险，可能“教坏”智能机器人；概率判断系统不完善，可能导致车毁人亡；而且，人工智能是通过软件实现的，是软件就有漏洞，就很可能被黑客利用。

周鸿祎建议，加快国家级网络安全人工智能开放创新平台建设。安全应该成为人工智能发展的基础与前提。但是，人工智能网络安全问题非常复杂，迫切需要建立一个开放创新平台，整合各种资源，协同推进和解决。

我国在人工智能网络安全领域的建设还是空白。建议国家支持尽快建设国家级网络安全

人工智能开放创新平台，确保人工智能健康有序发展。

工业互联网安全

全国人大代表、华工科技董事长马新强：尽快制定出台“工业数据保护法”

全国人大代表、华工科技董事长马新强提议，国家安全层面应高度重视工业信息安全，尽快制定出台“工业数据保护法”。随着工业信息化建设不断深化，大部分企业引入了大量与生产制造相关的应用系统，如 OA、CAM、ERP 等，系统内产生的数据和文档，具有高度保密性、高度敏感性，数据被破坏或泄露对企业会造成重大危险。

从国家层面来说，目前的法律制度例如《网络安全法》等多侧重于对个人信息的保护，对于工业制造领域数据采集、加工、使用、储存等诸多环节容易出现的信息安全问题，则没有专门的法律予以保护。

鉴于制造业关键数据保护的紧迫性和当前国内相关立法的缺失，马新强建议，应在重要工业城市加快推进国家网络安全产业基地建设，通过基地建设，大力发展网络安全产业，推进其与工业制造业的协同创新，加快构筑网络安全屏障，推进关键技术及成果的应用推广。

同时，应完善从国家到地方的风险监测体系，及时发现、处置安全风险，制定“工业数据保护法”，吸取地方立法中的得于失，转化成国家层面的法律规范，明确数据在采集、加工、使用、存储中相关方的权利、义务、责任。

全国人大代表、海尔集团总裁周云杰：立法保障工业互联网数据安全

全国人大代表、海尔集团总裁周云杰表示，物联网时代，物联网数据方面的安全立法要强化。物联网的数据应用，既要让消费者得到更好的体验，也要保护消费者的合法权益；既要让各企业在开放的工业互联网平台上共创共享，也要保护工业数据的安全。

保护消费者、用户数据安全分为三个层面：一是立法层面，要建立完善的体系；二是技术层面，要能保护每个个体数据隐私；三是企业文化层面，要建立一种尊重消费者、尊重消费者隐私的文化。对于工业互联网数据安全问题，周云杰认为这关乎国家工业安全，因为工业互联网的交易数据，比消费数据更广泛、结构更复杂，涉及很多设计的数据、风险的要素，也涉及到很多消费者的信息，所以它的信息安全显得更为重要。

数据安全

全国人大代表、苏宁控股集团董事长张近东：加快制定数据安全法律法规

全国人大代表、苏宁控股集团董事长张近东表示，在目前的数据应用领域，由于企业数据保护意识不足加之我国相关立法滞后，个人信息的泄露与滥用层出不穷；而政企之间、行业之间、企业之间的数据缺少交互共享的规范和标准，形成了“信息孤岛”；跨境数据的保

护和合法共享更是缺少有效的国际沟通交流机制。

张近东建议，由国家相关部委牵头，联合互联网技术供应商和互联网服务企业，加快制定数据安全法律法规、安全保护配套标准，从信息的收集、存储、处理、传输、共享、删除等全生命周期管理的角度制定完善的法律体系，确保数据安全。有了数据保护后，还要提高其利用效率。可设定激励机制，引导数据共享服务与公众需求，对于公众迫切需要的，如交通信息、环境信息等数据，率先推进开放共享。

全国人大代表、中国移动浙江公司董事长郑杰

确立数据主权，实现安全风险预警全国人大代表、中国移动浙江公司董事长郑杰表示，目前世界范围内网络攻击、勒索软件、数据泄露等网络安全事件频发。同时，被泄露的公民个人信息经过加工、转卖，可能会被用于网络诈骗、敲诈勒索等违法犯罪。

数据安全关系网络安全、国家安全、公民个人隐私权益和社会安全稳定，应加快制定数据安全法。尽管我们有网络空间主权，但网络空间主权不等同于数据主权，它指的是一国对本国的数据及本国国民跨境数据拥有所有权、控制权、管辖权和使用权。

郑杰提议：要确立数据主权，明确数据安全法的管辖范围；明确境内运营中收集和产生的个人信息和重要数据应当在境内存储；完善数据出境安全评估机制，将机制的适用范围从网络安全法规定的关键信息基础设施运营者拓展至网络运营者；要将相关国家、企业、组织、公民利益的数据活动纳入数据安全法管辖范围。

对安全责任单位采取安全措施的原则、落实数据安全保护责任、采取防范危害数据安全行为技术措施等作出相应规范，建立数据安全投诉举报制度。明晰数据安全监督管理的部门职责，明确数据安全监测预警与应急处置的规定，及时进行数据安全形势研判和风险评估，发布安全风险预警，实现对数据安全风险的全天候实时、动态监测。

全国人大代表，中国移动广东公司董事长魏明：立法明确个人信息收集原则

全国人大代表，中国移动广东公司董事长魏明表示，通过黑客攻击、破坏等其他途径“越界”收集、滥用个人信息的案例不胜枚举。个人信息大量被非法收集、滥用，甚至违法使用，严重侵害公民人身、财产安全。

导致“越界”收集信息常态化的一个重要原因是，当前法律对个人信息的收集原则、范围、方式界定不明确。例如《网络安全法》《全国人大常委会关于加强网络信息保护的决定》等明确要求收集的信息必须与服务有关，需要经被收集者同意，但对是否“有关”没有明确的操作细则，缺乏实操性。

魏明认为，制定一部科学、完整、专门的个人信息保护法律，建立个人信息保护制度已

刻不容缓。他提交了《关于加快制定〈个人信息保护法〉的议案》，并附上了草案。

网络安全治理

全国政协委员、中国证监会信息中心主任张野：加强暗网监管，有效应对黑产威胁

全国政协委员、证监会信息中心主任张野表示，今年将就暗网的管控治理提交相关提案，希望有关部委深入研究美国、欧盟等发达国家的做法和经验，结合中国网络安全治理体制，构建我国应对暗网及相关黑色产业链威胁的有效机制。

具体有三点提议：

1. 加强暗网治理技术手段研究。发现和利用其内部软件缺陷或者漏洞，捕获暗网隐藏的用户信息、破坏暗网的违法网站是治理暗网的关键。应组织网络安全研究机构成立专门的研究团队，抓紧技术攻关，尽快形成适应中国网络空间治理需求的暗网管控技术能力。

2. 加强传统技术与行政执法手段的结合。公安部和网络通信管理部门组织开展联合行动，加强对暗网网站的监测预警，加大违法犯罪行动的打击力度。

3. 加强政府与网络安全企业的合作。鼓励网络安全公司加强暗网治理相关技术、产品研究和专业人员培养，并参与到打击暗网和相关黑色产业链的专项行动中，提升国家治理暗网的整体技术实力。

全国政协委员、众人科技董事长谈剑峰：加大网络安全产业投入，避免受制于人

全国政协委员、众人科技董事长谈剑峰表示维护网络安全就是守护国家安全，中国需要自主、健康的网络安全产业来支撑。谈剑锋的提议分为两方面：一是掌握信息安全核心技术，建立首席信息安全官制度；二是加大网络安全产业投入，避免受制于人。

密码技术是信息安全的核心，与核技术、航天技术并称为国家安全三大支撑技术，如果连“门锁”都用国外技术、国外制造，那就如同大门彻底敞开，更多的安全事件将无法阻挡。因此，在信息安全领域里，必须采用中国自主研发的核心技术。

在网络安全人才培养方面，可以建立首席信息安全官制度，推动安全人才的培养，为产业发展注入新活力，推动网络安全产业的可持续发展。

此外，谈剑锋建议：

1. 从战略层面进行网络安全的体系化和层次化设计。2. 要制定积极的网络安全产业发展政策，实行主动纵向的产业政策 3. 要在政府及国有企业采购中增加网络安全产品和服务采购比例，提振产业空间。

全国政协委员，安天科技集团创始人肖新光：三管齐下提升政企网络安全

全国政协委员，安天科技集团创始人肖新光表示，目前我国大量重要信息系统和信息基

础设施处于“低水平防护”，甚至“无效防护”的状态中，症结包括安全规划能力普遍不足，缺少充分预算资源保障、问责机制未全面落地等问题。

对此，肖新光建议相关机构联合发文，强化帮扶政企单位提升安全能力的赋能工作，提出清晰的战略指引和体系化、框架性防护规划指引，将网络安全防护工作引导到全面建设必要的网络安全防御能力，并将其有机结合以形成动态综合网络安全防御体系的能力导向建设模式。针对网络安全建设缺少预算支撑的现象，建议相关部门对网络安全预算和资源投入落实给出硬性的工作要求，使安全规划实施获得充分保障。

肖新光还建议在现有相关主管部门考核、监管、检查的基础上，积极探索通过国家监察体系对网络安全责任制的落实实施监督审查，对政企机构在网络安全工作中是否及时有效制定规划、配置资源、执行预算，是否达成有效防护效果等督查问效，形成深度问责机制。（来源：互联网综合整理）

➢ 打击勒索软件的法律思考

摘要：现代加密技术和易于获取的现实货币价值为勒索软件的滋生蔓延创造了条件，信息化规模和黑客攻击技术的快速成长使得我国成为勒索软件爆发式增长的“重灾区”。在 FBI 尚发出“公司在感染了勒索软件之后最好支付赎金来找回重要数据”的忠告之下，勒索软件“反抗即损失”的特征愈发明朗化。我国必须加大勒索软件的打击力度，从法律、管理和技术层面实施综合治理。

勒索软件的概念与特征

勒索软件（Ransomware），又称勒索病毒，维基百科将其定义为一种特殊的恶意软件，被归类为阻断访问式攻击，与其他病毒最大的不同在于手法。一种勒索软件单纯地将用户的电脑锁起来；另一种则系统性加密用户硬盘上的文件。所有的勒索软件都会使用户数据资产或计算资源无法正常使用，要求用户支付赎金以取回对电脑的控制权，或是取回用户无从自行获取的加密密钥。勒索软件编写者还在继续开发，导致勒索软件在持续变种，2014 年来针对 Android 系统移动设备的勒索软件陆续出现。McAfee Labs 预测，鉴于配电和医疗保健市场已经出现了物联网设备被劫持的案例，勒索软件随时可能移植到物联网领域。

在法律层面，2016 年 9 月美国加州通过的参议院第 1137 号法案将勒索软件定义为“未经授权的一种病毒，其将计算机病毒或锁死程序放置或感染到计算机、计算机系统或计算机网络中，限制已获授权的用户访问计算机、系统、网络及其所存储的数据，从而要求用户为其支付金钱或其他代价，以移除或通过其他方式修复该计算机病毒或锁死程序”，基本着眼于授权角度再次重申了技术上对勒索软件的定义。

作为病毒的一种，勒索软件的概念自上世纪 90 年代开始出现，但其加剧威胁源自 2005 年开始运用更加复杂的 RSA 加密手段和 2013 年开始利用比特币等虚拟货币作为新的支付形式。暗网中已有越来越多的人提供勒索软件作为服务，勒索软件即服务（Ransomware as a service，RaaS）呈爆炸式发展趋势。我国日渐成为勒索软件泛滥的重灾区，2015 年开始蔓延，2016 年开始强势袭击各大互联网企业和个人用户，成为企业和个人数据安全的重大威胁之一。

新近意义上的勒索软件具有的主要特征在于：一是采用了加密技术（例如 RSA）实现对用户系统、网络的加密和解密，以及支付形式的密码化（例如 Bitcoin）；二是直接损害信息或数据的可用性的同时，也不完全不排除侵入，或在无法实现获取赎金（财物）的“营利目的”时的窃取、破坏等危害保密性、完整性的行为，即其基于勒索行为实施的“成功”与否决策如何进一步实施危害行为。如获取赎金的，可能解密、解锁，也可能窃取数据；如未获取赎金的，则损毁、窃取数据或者披露用户敏感信息 ；部分勒索实施行为甚至无论是否获取赎金，均会窃取、损毁数据。

打击勒索软件的监管难点

《McAfee Labs 2017 年威胁预测报告》预测，2017 年上半年，“勒索软件即服务”模式、在黑市上出售的定制勒索软件、来自开源勒索软件代码的创意衍生攻击方式仍将肆虐横行，“勒索拒绝服务”将成为针对云服务提供商和依赖云开展运营的组织的常见攻击。产生源头

缺乏法律规制和虚拟市场货币监管失控是导致打击勒索软件困难的两大原因。

1、产生源头缺乏法律规制，带动勒索软件的泛在发展和新型商业模式的形成

勒索软件等计算机病毒的“傻瓜化”制作过程和高额赎金暴露了犯罪低成本、高收益的反比特性，使得黑色市场的专业化、精细化、技术化发展趋势愈发明显。以美国执法机构为代表的政府利用漏洞进行情报获取或政治攻击的行为，不断刺激黑客对漏洞的非法挖掘、披露和交易，加上不健全的规范机制，为勒索软件的产生提供了持续的源动力。基于国际社会漏洞治理规则碎片化的现状，从源头上阻断和根除勒索软件变得异常艰难。加密技术的应用已经实现了对制作、传播、实施、支付等所有环节的全面覆盖，现有的公钥加密体系和灰色网络为勒索软件的危害行为提供了“完美”掩护，使其更具隐蔽性。勒索软件的易传递性和获取性激发了“勒索软件即服务”（Ransomware as a service，RaaS）新兴商业模式的形成和兴起。

2、虚拟货币市场的监管失控，导致勒索软件的赎金获取能够隐蔽实现、快速变现并难以执法取证

以比特币为主要类型的“虚拟货币”（virtual currency）近年来也在快速发展，作为技术和交易模式支撑的区块链成为 2016 年炙手可热的话题。各国对虚拟货币的监管缺乏统一规则，为勒索软件的全球网络变现提供了机会，这也是各国立法差异和未建立有效国际合作模式问题的集中体现。全球虚拟货币监管路径尚在不断探索和调整过程中。2013 年底中国人民银行等五部委发布的《关于防范比特币风险的通知》明确比特币为虚拟商品，以严格区别于数字货币并适用不同监管机制。在据称“全球超过 90%的交易量都发生在中国”的 2017 年，央行加强了现场调查并明确提出“四不准”规定：不得违规从事融资融币等金融业务，不得参与洗钱活动，不得违反国家有关反洗钱、外汇管理和支付结算等金融法律法规，不得违反国家税收和工商广告管理等法律规定。为了打击恐怖主义袭击中的虚拟货币使用，欧盟于 2016 年扩大了反洗钱规定的实施范围，美国则在一些法院判例中为比特币的发行货币化提供了长期路径。

此外，以比特币等虚拟货币为支付方式引发了勒索软件的再度泛滥，执法机构无法追踪资金流向，网络犯罪执法取证难上加难。

打击勒索软件的法律规定

勒索软件造成的数据安全威胁成为各国共同面临的挑战。“No More Ransom!（停止勒索）”协作计划、反勒索软件技术的发展和持续执法行动正在全球开展。在法律层面，2016 年 9 月美国加州通过参议院第 1137 号法案（Senate Bill No. 1137- Chapter 725），修订了《刑法典》

第 523 节，在法律层面明确了实施勒索软件行为的刑事责任，规定如果某人以获取钱财或其他利益为目的，直接放置或感染勒索软件，或者指示、引诱他人这样做，从而将勒索软件感染到计算机、计算机系统或计算机网络中，在获取利益后为受感染者提供移除或其他方式的恢复服务的，那么此人将为该勒索软件负责，视情节被处以 2 至 4 年不等的监禁。

我国现行法律没有针对勒索软件的专门性规定，但针对制作传播计算机病毒、敲诈勒索、信息网络技术支持和帮助等危害网络安全方面的法律规定相当完善。2000 年《计算机病毒防治管理办法》明确规定任何单位和个人不得制作、传播计算机病毒，并规定了相应的警告、罚款、没收非法所得等行政处罚；《刑法》第 274 条规定了敲诈勒索罪，并在《关于办理敲诈勒索刑事案件适用法律若干问题的解释》中对量刑标准和提供网络技术支持帮助，规范为他人信息网络犯罪提供技术支持和帮助的行为；《刑法》第 285 条规定了非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪；《刑法》第 286 条将计算机病毒作为破坏性程序的一种，并在《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》中界定了破坏性程序的范围；《刑法》第 287 条之一规定了非法利用信息网络罪，287 条之二规定了帮助信息网络犯罪活动罪；《治安管理处罚法》第 29 条规定故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的，可予以拘留；即将全面实施的《网络安全法》第 27

条强调禁止从事危害网络安全的活动，旨在实现行刑衔接，规定了拘留、罚款、没收违法所得等行政处罚。勒索软件作为计算机病毒的一种，勒索软件实施的危害行为涉嫌违法犯罪的理应属于以上法律法规规制的范围。

勒索软件危害行为及相关罪名分析

勒索软件实施的危害行为，因其阶段不同而可能涉及不同的违法或犯罪行为，同时还可能具有计算机病毒或其他攻击、侵入、干扰、破坏行为的功能，在用户支付赎金后，亦可能留有“后门”而未必能够彻底恢复系统。为便于分析，以下以现行《刑法》为例，参考最高人民法院、最高人民检察院《关于办理敲诈勒索刑事案件适用法律若干问题的解释》和《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》，基于单一勒索目的和功能的理想状态描述归类勒索软件可能涉及的相关罪名。

周期/阶段	制作	提供	实施	获取赎金	未获取赎金	支持/支付
涉及危害行为描述	脆弱性（漏洞）发掘，形成勒索软件（定性为具有入侵软件功能的计算机病毒）	以勒索软件形式销售（收费）或发布（可免费）	通过邮件、网站等形式不特定传播，在特定化对象后进行锁定或加密（同时实际上已经侵入和获取数据）	解锁系统和/或解密数据，恢复用户访问权	披露数据信息，破坏系统、数据	存储、传输勒索软件，并通过虚拟货币等形式结算
可能涉及罪名	非法侵入计算机信息系统罪； 非法获取计算机信息系统数据罪； 破坏计算机信息系统罪； 非法利用信息网络罪	提供侵入、非法控制计算机信息系统程序、工具罪； 破坏计算机信息系统罪； 非法利用信息网络罪	非法侵入计算机信息系统罪； 非法获取计算机信息系统数据罪； 非法控制计算机信息系统罪； 破坏计算机信息系统罪	敲诈勒索罪	敲诈勒索罪	帮助信息网络犯罪活动罪

从上表可以看出，勒索软件“生命周期”的各个阶段主要涉及到对系统和网络漏洞的发掘、侵入、控制、干扰、破坏及获取（权限和数据）等行为，因此与其他危害系统、网络安全的行为具有相似性，但勒索软件突出强调对数据、系统、网络的非法控制和对可用性的危害，使其有别于其他以破坏或获取数据为特征的计算机病毒，以及基于计算机病毒防治所特

定指向的相关犯罪行为；同时也有别于传统意义上的“敲诈勒索”罪。例如，同样在目标系统、网络非法控制和以危害可用性为典型特征的情形，DDoS 等攻击行为通过安装计算机病毒控制并将目标系统、网络作为实施断网的工具，而勒索软件则倾向于以“不可用”为威胁，向目标系统、网络的运营者提示支付赎金。

与具有营利/牟利目的的其他非法获取计算机信息系统数据违法行为比较，勒索软件的获取尽管也属于窃取行为，但行为人就其获取“赎金”向用户提出了明示（尽管可能由于勒索软件的功能缺失或事实上并未实施获取，而具有诈骗性质；或者由于已经“当场”或“事先”获取和占有了数据，而具有“非法获取计算机信息系统数据”性质）。同时，勒索软件的实施行为不需发掘安全漏洞和进行特定披露，亦不以获取数据信息为交易和变现的前提。

与传统意义上的敲诈勒索罪相比，尽管锁定和加密属于“威胁、要挟、恫吓等手段”的具体形式，并可能构成《关于办理敲诈勒索刑事案件适用法律若干问题的解释》（以下简称《解释》）规定的情形，且《解释》第七条规定，“明知他人实施敲诈勒索犯罪，为其提供信用卡、手机卡、通讯工具、通讯传输通道、网络技术支持等帮助的，以共同犯罪论处”。但在行为实施以自动化和工具化的勒索软件形式出现后，其侵入、获取、控制等危害行为和后果将不完全取决于行为人的意志，从而可能涉及危害信息系统、网络安全的多种罪名。换言之，为行为人对软件目的、功能、后果等的认识上提出了主观判定的严格要求。

值得注意的是，对在破坏计算机信息系统的同时索要他人财物的行为如何定性，我国司法实践层面做法并未统一。2007 年我国已出现了勒索软件的司法审判案例。被告人欧阳俊曦 2006 年制作并利用其个人网站传播勒索软件，并以修复丢失资料、获得正版软件序列号为名，向被感染的计算机用户索取财物 2758 元。检察机关主张欧阳俊曦涉嫌破坏计算机信息系统罪和敲诈勒索罪，提请两罪并罚。法院最后认定，欧阳俊曦所为应以破坏计算机信息系统罪论处，因其有自首行为，可以从轻或减轻处罚，因此判处有期徒刑四年。法院在肯定欧阳俊曦行为同时构成破坏计算机信息系统罪和敲诈勒索罪两罪的基础上依据“择一重罪”之原则做出最终认定。二审判决指出，“破坏计算机信息系统罪的动机是多种多样的……对其牟取非法利益的主观犯罪动机和非法取得他人钱财的客观后果，属于破坏计算机信息系统罪的构成要素，对以上情节已在认定此罪过程中给予了评价，不应单独定罪，否则是重复评价。行为人为了牟取非法利益，制作、传播计算机病毒的行为同时触犯破坏计算机信息系统罪、敲诈勒索罪两个罪名这种是基于一个犯罪行为而同时侵犯两个犯罪客体的犯罪，是刑法理论的想象竞合犯。” 这一案例中被告人制作并传播了勒索软件，主观犯罪动机旨在获取财物，其行为分析相对简单，从刑法理论层面认定为想象竞合后即可做出罪名认定。勒索软件

功能在持续发展，新的变种在不断产生，不同的勒索软件案件还需根据其犯罪行为、主观认识等予以一一分析。

打击勒索软件需要多方共同努力

鉴于勒索软件的爆发式增长、全球性蔓延和有效治理手段的缺乏，各国在打击勒索软件具有相似的认同和诉求，开展国际合作成为凝聚多方力量共同应对的重要举措，且已初见成效。2014 年 6 月，美国司法部发布了跨州联合打击“Gameover Zeus” 僵尸网络和“Cryptolocker”勒索软件为代表的破坏性软件的成功行动，参与成员牵涉了全球数国执法、研究机构。该行动针对勒索软件受害者和实施者具有的全球分散性和普遍性特征展开，体现了各国在打击活动中“分段打击”“分布协同”“并行起诉”的新特点。

与具有直接攻击危害的漏洞与数据非法交易等行为相比，借助于加密技术和暗网等隐秘模式的勒索软件具有更大的成本效益优势和可变现性。网络社会已经与现实社会融为一体，勒索软件不仅体现出牟利性，更可能通过对个人设备、基础设施等的控制危及个人合法自由和社会公众安全。在对勒索软件缺乏有效反制技术的当下，除了理性适用《治安管理处罚法》《刑法》《网络安全法》的基本规定和加强国际合作之外，个人和企业也应积极采取行动。对个人而言，应不断提高对不明链接打开、不明文档下载的抵制意识，善于利用现有法律规定维护自身合法权益；从企业视角出发，应加强网络技术人员的从业培训，提高文件的加密技术，增加数据的备份渠道；就政府治理考虑，应制定特殊的人才培养政策，招揽白帽子黑客等尖端技术人才，形成违法犯罪分子的制衡力量。（来源：《中国信息安全》杂志 2017 年第 4 期、公安部第三研究所）

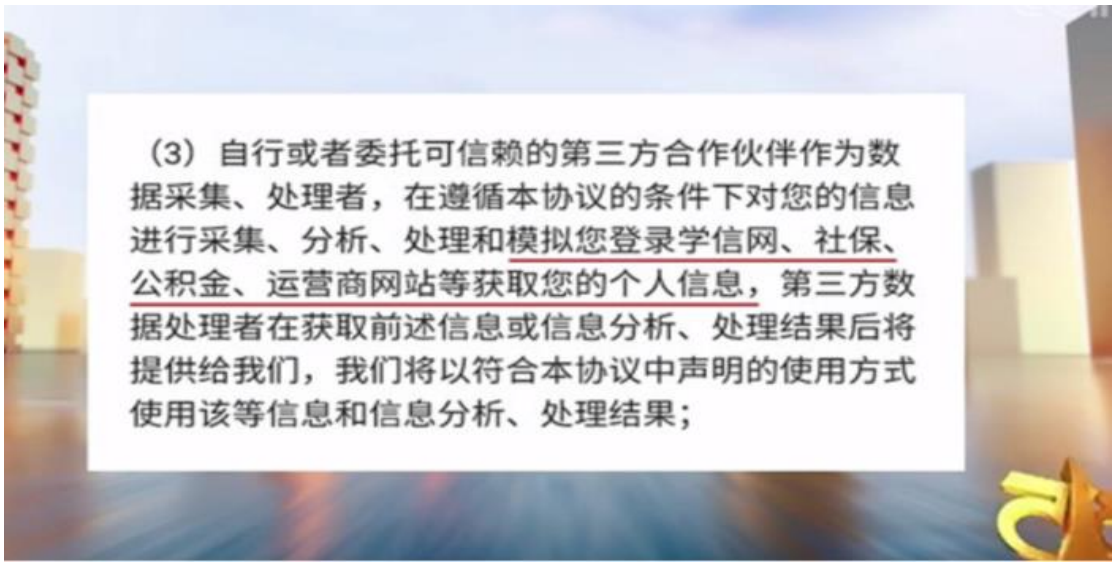
➢ 央视 315 曝光 AI 骚扰电话背后的高科技灰色产业链

科技是把双刃剑，而 AI 是这把剑最锋利的部位，315 晚会“AI 骚扰”电话的曝光，让人工智能的反面效应昭然若揭。令人震惊的是，AI 只是引爆骚扰电话的最后一环，一通最普通不过的骚扰电话的背后牵扯出了 APP 安装（隐私截取）、探针盒子（隐私下载）、大数据分析（隐私数据整理）和 AI 语音电话骚扰（隐私变现）等一连串环环相扣、产业链成熟、科技含量极高的灰产。不良商家正是利用人工智能和高科技，一环扣一环，织就了一张无形的大网，我们的手机隐私如同草原上毫无保护的“羔羊”，时时刻刻被这个虎视眈眈的灰产“围猎”。

我们来反向复盘一下这次参与隐私信息围猎的链条：用户下载 APP（信息被截取）——探针盒子（通过无线网—MAC 地址找到电话号码和用户信息，并整理成大数据）——AI 外呼系统（自动拨打骚扰电话）。

1、用户下载 APP（信息被截取）——你输入到 APP 的每条隐私都有可能被泄露

晚会现场，315 节目组现场为我们演示了 APP 是如何窃取我们的隐私的，在这款社保 APP 上只要输入我们的社保信息，所有的信息都会在用户毫不知情的情况下被截取并不法利用。这些 APP 往往会在使用条款中暗藏许多强制条款，并会对个人信息进行采集、分析、处理和模拟登录学信网、社保、公积金、运营商网站等，以获取个人信息。



社保信息被截取：事实上我们几乎每天都会用到这些第三方的信息查询软件，比如很多人买火车票不用 12306，转去一些第三方的购票平台；查询车辆违章信息等，同样会有信息被截取并泄漏的风险。而在信息时代，你买的每一份外卖、订的每一张电影票都时刻记录着所有的行为，你使用手机的行为越频繁，你的隐私就会越透明。

警惕非官方 APP 隐私泄漏

现实情况是没有人会仔细阅读 APP 中密密麻麻的条款，想要避免自己在不良商家面前“一丝不挂”，首先要从源头上堵住隐私泄漏的漏洞。使用官方出品的 APP，从官方渠道下载软件，关闭肆意索取信息的 APP 权限，都是保护个人隐私的良好开端。

2、探针盒子（MAC 地址找到电话号码和用户信息）——通过无线网汇聚成黑暗大数据

315 上被曝光的李经理表示，目前已经获取全国 6 亿用户的手机信息。而庞大的手机号码主要获取方式是通过手机的 MAC 地址，很简单的得到 IMEI（手机串号），然后进行大数据匹配就可以很轻松获取。甚至关于个人的人物画像也可以匹配，其中包括性别、年龄，手机设备的具体型号都可以得到，就连用户经常使用的 APP 和搜索关键词也了如指掌。

WiFi 探针技术是指基于 WiFi 探测技术来识别无线访问接入点的，附近有已开启 WiFi 功能的智能设备，WiFi 探针就能够识别用户的信息。当用户走进探针信号覆盖区域内，同时将 WiFi 功能打开，测试手机设备就能被探针探测出来，无论是 iOS 或者安卓系统都能轻易检测到，并且获取设备的 MAC 地址。

不管你是否连接 WiFi，探针盒子都能获取到 MAC 地址，之后上传数据到后台，利用大数据匹配的算法对 MAC 地址进行深度分析，这样便可轻松得到客户常用的 APP、兴趣爱好等信息。智能硬件不断升级，探针盒子也不例外。目前最先进的探针盒子技术还能实现一键拨打电话、群发信息等功能，同时还配备智能电话营销系统。相当于在探针盒子原有的功能上，增加了电话机器人的功能，电话机器人可以自动拨打电话，对搜集到的潜在客户进行一键电话营销，这也就是大家在 315 晚会上看到的那一幕暗访的情景。

探针盒子到底藏在哪里？

探针盒子一般情况下就放在人流密集的公共场所，这样可以获取庞大的用户信息。一般情况下学校、地铁站、商场、写字楼、商铺、旅游景点等都是放置探针盒子的最佳场所。由于探针盒子体积小巧，因此安放在屋内的天花板上相当隐蔽。只要给这些固定场所的负责人，每个月一定的“好处费”，就算是完成“姜太公钓鱼”了。

探针盒子安装在很隐蔽的商城内根本不易察觉

探针盒子不光搜集你的手机号，还会通过 APP 掌握我们所有的行踪，而我们的行为越多，我们的画像就越清晰，通过大数据我们就被彻底扒了个精光。接下来我们的信息就会被各种销售密集型企业接手，并通过一个个人工智能机器人外呼系统给我们推销相应的业务。

比如你有孩子，就会推荐补习班和家教；你刚结婚就会收到贷款和房地产的电话等等，兵法云知彼知己百战不殆，在这场信息战中，我们就是销售眼里待宰的羔羊，而我们却浑然不觉。

3、AI 外呼系统（自动拨打骚扰电话）——原来我一直和机器人在说话

没有泄露就没有伤。AI 骚扰功能看起来已经相当“人工智能”，电话沟通仿真能力相当逼真，沟通语言流畅自然，不知疲倦，永远爱岗敬业，甚至还可以模仿林志玲姐姐的接线声音。很难想象，其实大家平时接到的很多骚扰电话都是来自于智能骚扰电话。

这其中涉及到智能语音技术、一键拨打、大数据等前沿科技手段，代替了人工接线的同时还提升了拨打效率，AI 骚扰可以每天完成 800 到 1000 通电话。

据了解，这些机器人是以每个 3000 元的价格从中科智联科技、壹鸽科技等科技公司购买的。之前传统的人工外呼打电话的营销方法，一天最多只能打 300 到 500 个电话，而这些机器人一天最多可以打 5000 个电话。其中一家提供外呼系统的科技公司经理更是告诉记者，在过去的一年多时间里，他们筛打出去的电话共达 40 亿个，目前已受到贷款、房地产、收藏品、金融、整形等三十几个行业的营销公司的欢迎。

4、银联卡默认开通闪付 安全还是第一要素

今年没有大牌企业上榜，而银联的出现倒是颇为意外，原因是银联卡会默认开启“闪付”功能(Quick Pass)，存在风险。央视记者发现，使用新开的支持闪付功能的银行卡，轻靠 POS 机接口消费，无需密码就能完成交易。闪付不用输入密码就能产生交易，每日额度 600 元-50000 元不等，在办理业务的时候为默认开通，银行工作人员在办理开通时也不予提示。而在某电商网站上，通过搜索特定关键词可搜索购买到支持银联免密支付的 POS 机，并能成功支付。

根据公开资料显示，“闪付”（Quick Pass）代表银联的非接触式支付产品及应用，具备小额快速支付的特征。用户选购商品或服务，确认相应金额，用具备“闪付”功能的金融 IC 卡

或银联移动支付产品，在支持银联“闪付”的非接触式支付终端上，可快速完成支付。

如何让你远离潜在安全风险

探针盒子搜集信息，大数据提供支持，智能机器人外呼，我们的隐私就这样肆无忌惮的被收集着，作为互联网时代的弱势群体的人类难道只能这样坐以待毙吗？答案是否定的。

国家在不断加强通信行业的监管，已经有了对于骚扰电话有更强的打击力度，相信在 315 晚会的曝光之后，这样的黑色行业将会有灭顶之灾。除此之外，我在这也为您支几招，方便您在大数据时代能够保护好自己的隐私。

1、不论在网上做什么事情，只需要填写必要信息，如果将全部信息交给网络，最后吃亏的是你自己。2、探针盒子是通过 WIFI 获取你手机信息的，所以公共场所尽量关闭手机 WIFI。3、二手手机在出售时，尽量做好“滴水不漏”的工作，将手机完全格式化。4、网络测试不可信，尤其是那些需要提交个人信息的小游戏，切不可为了一时好奇将自己暴露在互联网之上。5、社交平台尽量标注“假信息”，做到让不法分子无机可乘。

除此之外，手机上的一些设置也可以避免类似案件发生，不要给 App 全部权限，如读取联系人、读取位置信息等，很多朋友都懒得看，直接一路点击同意。这正是给了不法 App 有机可乘的机会。（互联网综合整理）

➢ 组织机构的数据安全人员能力要求

数字经济时代，数据安全成为网络空间安全领域最受关注的热点问题。无论从法律要求、企业保护自身利益，还是对自己客户负责的角度说，一个组织构建自身的数据安全能力，成为极为紧迫的需求。但是，企业在建设自身数据安全能力时，离不开数据安全专业人员能力建设。企业数据安全人员能力不等同于传统网络系统安全人员的能力。过去几年，对很多企业数据安全能力的测评或咨询结果显示，缺乏数据安全专业人员是企业数据安全能力不足的关键短板之一。因此，企业或者任何组织需要怎样的数据安全人员能力，是一个需要引起足够重视的问题。

一、企业面临的数据安全问题十分复杂

数据正成为所有行业和企业不可或缺的生产资料。如今，数据的存在形式和使用方式都和过去有极大不同，数据不再仅仅是一个文件或者数据库里的完整记录，而是形式多样、非常碎片化并且在复杂的业务合作链条中快速流动。因此，今天的数据安全概念与过去有本质

的不同。这种不同至少体现在以下几个方面：

一是业务环节复杂，应用多变。一架飞机或者一部手机的制造，以及一个软件系统的编写，都会用到各种元器件或者程序模块，人们已经意识到，存在日益严重的供应链安全问题。但是，人们对数据使用链的安全挑战了解还不多。如今，在网络上购买一件商品，数据需要流经商家、独立软件供应商、物流供应商（可能是多个）、支付支持方和平台服务方等环节，才能确保完成这个任务。这个“数据链”上的每个环节都可能出现数据安全问题，从而影响自己的客户、业务或者带来说不清的法律责任。同时，业务本身的各种活动、业务模式调整、支持业务的应用更新等的频率，都远超传统模式，会不断带来新问题，需要快速调整适应。

二是数据存储使用环境复杂。需要保护的数据，从采集或者产生，到中间的存储、使用以及最后的删除或销毁，涉及各种终端设备、在线业务系统和数据库、离线数据库和存储等不同的设备和网络环境，以及不同用户和权限管理等。

三是黑灰产对抗无孔不入。数据同样也日益成为黑灰产的生产资料，成为被窃取的目标。黑灰产的产业链日益完整，黑客攻击技术手段、大范围社会协作、收买内部人员甚至直接派遣卧底应聘等方式，无孔不入地窃取数据。

四是面对的法律要求复杂。很多国家相互效仿，不断出台与数据相关的各种法律政策。与此同时，对数据安全究竟该如何管理、如何与数字经济发展实现平衡等问题，全球处于摸索的混沌状态，法律政策也在不断调整中。

显然，企业的数据安全工作需要面对上述问题，对数据安全的专门人员能力要求也比较

复杂，包括对业务以及数据流动的深度理解，数据防泄露、打标脱敏、数据管理、数据库审计及各种保护隐私相关技术，传统攻防技术，以及业务所在地或所服务的用户牵涉的法律合规等。

二、企业数据安全岗位人员能力要求

因为数据并不会仅仅存留在某个应用软件、某个设备或者某个数据库中，传统的以系统为中心的安全思路并不能满足企业的数据安全需求，而是必须转到“以数据为中心的安全”上来，即要对一个组织掌握的数据全面负责，无论这些数据是从哪些应用、设备、系统、业务中产生、存储或处理，或者涉及哪些不同的业务及人员。一种可能的办法是按照数据在组织内的生命周期进行梳理，实际上，这会涉及多个部门、多个岗位人员的支撑及互相配合。

参考数据安全能力成熟度模型（DSMM）标准的描述，组织内的相关岗位大概涉及数据管理岗、开发岗、信息安全岗、合规岗、人力资源岗、运维岗、审计岗及其他数据安全岗位等。这些岗位的数据安全相关能力要求，根据不同的数据生命周期阶段的安全需求，对可涉及岗位的数据安全能力要求有所不同，大致描述如下。

表 1 数据采集阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据采集	数据合理分类分级	数据管理岗	*1. 理解组织机构内数据所处的业务场景，及数据一旦发生泄露所造成的风险 2. 能够定制化制定适用于组织的分类分级制度标准，能够根据数据重要及敏感程度等对数据落实合理分类分级
	数据采集安全管理	数据管理岗 / 开发岗	*1. 能够充分理解数据采集的法律合规要求、安全和业务需求，并能够根据组织机构内的业务场景提出针对性的解决方案 *2. 能够制定数据采集的信息共享方案，并不断提升组织机构内相关人员对合规要求以及对业务场景的理解
	数据源鉴别及记录	数据管理岗 / 开发岗	*1. 具备对数据源鉴别标准的一致性理解和执行的准确性 *2. 能够制定数据源鉴别及记录的技术方案并执行落地
	数据质量管理	数据管理岗 / 数据质量管理岗	*1. 具有数据质量管理的相关理论基础，并能够基于组织机构的实际数据质量管理需求开展相关工作 *2. 具备对数据质量标准的一致性理解能力、建立数据质量管理过程的有效性和效率目标能力、在组织机构层面实现数据质量管理的持续优化能力等 3. 制定统一的数据质量管理规范，并可以对各业务的数据管理人员进行规范的培训

表 2 数据传输阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据传输	数据加密传输	开发岗 / 安全岗 / 数据管理岗	* 了解市场主流的安全通道和可信通道建立方案、身份鉴别和认证技术、数据加密算法，并能够根据具体的业务场景选择合适的数据传输安全管理方式
	网络可用性安全管理	网络管理岗 / 运维岗	*1. 精通网络安全基础技术知识，具备网络安全管理经验 *2. 了解网络安全对可用性的安全需求，并根据不同业务对网络性能需求制定有效的可用性安全防护方案

表 3 数据存储阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据存储	存储介质安全	运维岗 / 数据管理岗	* 熟悉介质使用的相关合规要求，熟悉不同存储介质访问和使用差异性，能够主动根据政策变化更新管理要求
	逻辑存储安全	数据管理岗 / 开发岗	1. 明确整体的数据逻辑存储系统、存储设备安全管理要求并能够推进相关要求的落地实施 *2. 熟悉相关的数据存储容器技术架构，并能够基于安全管理的原则判断出相关的风险，从而能够保证对各类数据存储容器的有效安全防护
	数据备份和恢复	运维岗 / 数据管理岗	* 了解数据备份介质的性能和相关数据的业务特性，能够确定有效的数据备份、恢复工作开展的方式

表 4 数据处理阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据处理	敏感数据脱敏	数据管理岗	*1. 熟悉常规的数据脱敏技术，能够分析数据脱敏过程中存在的安全风险，基于数据脱敏的具体场景，保证业务和安全之间的需求平衡 *2. 具备对数据脱敏的技术方案定制化的能力，能够基于组织机构内部各级别的数据建立有效的数据脱敏方案 3. 管理岗人员还需具备定期对数据脱敏工作人员的脱敏操作能力进行考核评估的能力（DSMM 4 级要求）
	数据分析安全	数据分析岗	*1. 能够基于合规性要求、业界标准对大数据安全分析中可能引发的数据聚合的安全风险进行有效的评估，并能够针对分析场景提出有效的解决方案 2. 精通对大数据分析的安全技术，能够及时跟进先进的最佳实践以保证对相关技术的合理应用（DSMM 5 级要求）
	数据正当使用	权限管理岗 / 安全运营岗	*1. 能够建立有效的身份及访问管理方案 2. 具备对数据正当使用的相关风险的分析和跟进能力（DSMM 4 级要求）
	数据处理环境安全	数据管理岗 / 信息安全岗	* 了解在大数据环境下的数据处理系统 / 平台的主要安全风险，并能够在相关的系统设计、开发阶段通过合理的设计以及运维阶段的有效配置规避相关风险

表 5 数据交换阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据交换	数据导入导出安全	数据管理岗	* 充分理解组织机构的数据导入导出策略，并根据数据导入导出的业务场景执行相应的风险评估，提出实际的解决方案
	数据共享安全	数据管理岗 / 信息安全岗	* 理解组织机构的数据共享策略，并根据数据共享的业务场景执行相应的风险评估，提出实际的解决方案
	数据发布安全	数据管理岗 / 合规岗 / 信息安全岗	* 充分理解数据安全发布的制度和流程，通过岗位能力测试，并能够根据实际发布要求建立相应的应急方案
	数据接口安全	信息安全岗 / 开发岗	* 充分理解数据接口调用业务的使用场景，具备充分的数据接口调用的安全意识、技术能力和风险控制能力

表 6 数据销毁阶段的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
数据销毁	数据销毁安全	运维岗 / 数据管理岗 / 开发岗	* 熟悉数据销毁的相关合规要求，熟悉不同业务对数据销毁需求的差异性，能够主动根据政策变化和技术发展更新相关知识和技能
	介质销毁处理安全	运维岗 / 数据管理岗	1. 整体把控组织机构内部数据销毁的原则，并明确各类数据销毁的规范做法 *2. 能够依据数据销毁的整体需求明确使用的介质销毁工具

表 7 全生命周期基础通用支撑的数据安全人员能力要求

数据生命周期阶段	安全需求	可涉及岗位	数据安全人员能力要求（标 * 的基本对应 DSMM 3 级要求）
全生命周期基础通用支撑	制定数据安全策略规划	数据管理岗 / 高级管理层	*1. 具备制定数据安全顶层方针、策略的能力，了解组织机构的业务发展目标，并能够将数据安全工作目标和业务发展目标进行有机的结合 *2. 精通信息安全管理体系建设的基础知识、数据安全相关技术知识和规范撰写的能力 3. 能够及时评估策略规划的实施效果，根据实施效果修订数据安全策略规划文件，并制定数据安全策略规划的提升计划（DSMM 4 级要求） 4. 具有一定的业务趋势洞察能力，能够洞察业务变化、行业的变化对安全带来的挑战（DSMM 5 级要求）
	人力资源安全	人力资源岗	1. 能够充分理解整体数据安全建设策略及工作目标，有定义数据安全职能部门 / 岗位的能力，并能够根据组织内部情况合理设定岗位并确定职责及分工 2. 职能岗位设计时能考虑职责分离原则，合理建立组织机构内部监督管理职能部门，对组织机构内部的数据安全管理相关职能岗位的操作行为进行安全监督管理 3. 能够持续优化组织机构的数据安全岗位及职能设置，以实现整体业务目标的优化 *4. 负责人力资源安全管理的人员应充分理解人力资源管理流程中可对安全风险进行把控的环节 *5. 固化针对员工、第三方人员入职过程中的数据安全教育环节，通过培训、考试等手段提升整体的数据安全意识水平 *6. 负责执行数据安全职能设置的人员能够明确组织机构的数据安全工作目标
	合规管理	合规岗 / 法务岗	* 具备对数据安全合规要求解读能力和对数据安全合规现状的理解力
	数据资产管理安全	数据管理岗	1. 充分了解所管理的数据资产的相关信息，并具备判断对数据资产的相关使用是否能够保证其价值不受损害的能力 *2. 负责组织机构统一的数据资产管理工作人员了解组织机构内部数据资产管理需求，以及对数据资产所涉及业务范围的整体理解，能够建立适用于组织机构业务实际情况的可落地的管理制度
	数据供应链安全	供应链管理岗 / 外包管理岗	* 对组织机构上下游数据供应链的整体了解，熟悉供应链安全方面的法规和标准，并具备推进供应链管理方案落地的能力
	元数据管理	数据管理岗	* 了解元数据管理的理论基础，理解组织机构的元数据管理的业务需求
	终端数据安全	主机管理岗 / 数据管理岗	* 了解终端的数据出入口以及相应的数据安全风险，可利用相应的工具实现整体的安全控制方案
	监控与审计	审计岗 / 运营岗	* 了解数据访问和操作涉及的数据范围和合法性，具备安全风险的判断能力，并能制定合理的监控审计方案

需要说明的是，DSMM 本身按照能力成熟度分层，这里主要描述的是 3 级要求，而当前能达到 DSMM 3 级的组织其实还很少。

三、企业需要有数据安全官

可以看出，一个组织全面的数据安全人员能力要求是很复杂的，涉及很多方面。要想建设相对完善的数据安全能力，任何组织都需要一个抓总的数据安全岗位，可以称之为“数据安全官”。数据安全官负责整体统筹规划数据安全战略目标，实施策略，协调各部门共同协作进行体系化建设。原则上，任何一个企业或者机构组织，都需要有这样的岗位。欧盟《通用数据保护条例》（GDPR）要求企业设置数据保护官（DPO），但是，DPO 更偏向于高级咨询者和合规监督者，负责合规、监督、外部合作，提供数据相关处理建议、风险分析和解决建议等。

本文建议的数据安全官则更偏向于数据风险的治理者，除了负责合规监督外，还要根据一个组织的数据安全需求切实落地和提升数据安全能力建设，控制数据安全风险，因此，需要完成合规、内部协调和外部合作、数据安全战略统筹规划和方案设计与落地、数据安全能力建设和风险控制等,以提升组织的数据安全整体能力，并以达到最终保障数据安全效果为最终目标。中国是互联网业务形态最丰富的国家，也是数据安全面临的挑战最复杂的国家，因此，最有机会拿出最好的数据安全治理经验。数据安全官将是非常广泛的数据安全人才需求。（来源:《中国信息安全》杂志 2019 年第 2 期）

四、政府之声

➢ 市场监管总局中央网信办关于开展 App 安全认证工作公告

2019 年 3 月 13 日，市场监管总局中央网信办，发布“市场监管总局中央网信办关于开展 App 安全认证工作的公告”：为规范移动互联网应用程序(以下称 App)收集、使用用户信息特别是个人信息的行为，加强个人信息安全保护，根据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》，市场监管总局、中央网信办决定开展 App 安全认证工作。

现将有关事项公告如下：

一、App 安全认证活动依据《移动互联网应用程序(App)安全认证实施规则》(见附件)开展。

二、从事 App 安全认证的认证机构为中国网络安全审查技术与认证中心，检测机构由认证机构根据认证业务需要和技术能力确定。

三、认证机构和检测机构应按有关规定，客观、公正地开展认证和检测活动，并对认证和检测结果负责。

四、国家鼓励 App 运营者自愿通过 App 安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 App。

附件：移动互联网应用程序(App)安全认证实施规则（来源：国家市场监管总局）

- **《移动互联网应用程序(App)安全认证实施规则》全文：**
- http://gkml.samr.gov.cn/nsjg/rzjgs/201903/W020190315324290664848.docx

➢ 工信部、国家标准委联合印发《工业互联网综合标准化体系建设指南》

2019 年 3 月 8 日，工业和信息化部 国家标准化管理委员会关于印发《工业互联网综合标准化体系建设指南》的通知、工信部联科〔2019〕32 号。

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门、通信管理局、市场监督管理部门，有关行业协会、中央企业、标准化技术组织、标准化专业机构：

为发挥标准在工业互联网产业生态体系构建中的顶层设计和引领规范作用，推动相关产业转型升级，加快制造强国和网络强国建设步伐，工业和信息化部、国家标准化管理委员会共同组织制定《工业互联网综合标准化体系建设指南》，现予印发。（来源：工业和信息化部 国家标准化管理委员会）

- **《工业互联网综合标准化体系建设指南》全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c6667001/part/6667027.pdf

➢ 教育部办公厅印发《2019 年教育信息化和网络安全工作要点》通知

2019 年 3 月 13 日，教育部印发《2019 年教育信息化和网络安全工作要点》(下称《工作要点》)。

《工作要点》提出，成立国家数字教育资源公共服务体系联盟，实现省级平台全部接入体系，完善大资源开发利用机制，“一师一优课、一课一名师”活动晒课 100 万堂，认定 800 门国家精品在线开放课程。

《工作要点》明确，网络学习空间应用不断深入，全国师生网络学习空间开通数量新增 1000 万个，继续推选网络学习空间应用优秀地区 40 个和优秀学校 200 所。完成中小学校长和骨干教师“人人通”专项培训 6000 人，推动逐步实现“一人一空间、人人用空间”。

《工作要点》要求，数字校园建设与应用加快推进，印发《高等学校数字校园建设规范》，开展学校联网攻坚行动，全面改善学校网络接入和带宽条件，中小学宽带接入率达到 97%以上、出口带宽达到 100Mbps 以上，并探索采用卫星通信等多种技术手段实现学校互联网全覆盖。

《工作要点》提出，深化基础教育数字教育资源开发与应用。继续做好统编三科和普通高中的“人教数字教材”开发。深入开展数字教材教学模式研究，推进义务教育“人教数字教材”在不同数字化教学环境下与教育教学的深度融合和应用推广，培育形成 3 个区域及 10 个学校示范案例。

《工作要点》明确，推进继续教育资源建设。继续推动国家开放大学网络学习课程、通识课程、五分钟课程、全媒体数字教材建设，使上线的网络课程总量超过 350 门，完成 1 万个 5 分钟课程规划和建设，推进 110 门通识课程建设，启动 100 门大规模在线开放课程建设。

《工作要点》要求，全面规范校园 APP 的管理和使用。开展校园 APP 专项调研，摸清底数，研判形势。与网信部门开展联合行动，治理校园 APP 乱象。研究制定规范校园 APP 管理的意见，规范第三方校园 APP 的引入和自主开发校园 APP 的建设，探索建立规范校园 APP 管理的长效机制，促进移动互联网有序健康发展。推动落实《教育部办公厅关于严禁有害 APP 进入中小学校园的通知》，重点加强学习类 APP 的规范管理。（来源：教育部）

- **教育部办公厅关于印发《2019 年教育信息化和网络安全工作要点》的通知全文：**
- http://www.moe.edu.cn/srcsite/A16/s3342/201903/t20190312_373147.html

➢ 生态环境部要求认真落实网络安全法

2019 年 3 月 14 日，生态环境部党组书记、部长李干杰在该部日前召开的生态环境部网

络安全和信息化领导小组会议上强调，要深入贯彻习近平总书记关于网络强国的重要思想，推动生态环境网络安全和信息化工作更好更快发展，为打好污染防治攻坚战、推进生态环保事业发展提供有力支撑。

会议首先听取了关于生态环境部网络安全工作、生态环境信息化工作和 2019 年生态环境部网络安全和信息化工作要点等情况的汇报，并观看了生态环境部综合业务门户、网站群、“互联网+政务服务”平台、生态环境信息“一张图”等系统演示。

会议指出，党中央、国务院高度重视网络安全和信息化工作，先后作出一系列重大决策、提出一系列重大举措，推动网信事业取得历史性成就。2018 年以来，生态环境部党组提出并实施一大批改革创新举措，组建网信领导小组和网信办，独立设置信息中心，全面加强“四统一、五集中”（统一规划、统一标准、统一建设、统一运维，数据、人员、技术、资金、管理集中），形成在用信息系统整合上云、建成部系统网站群、非涉密公文处理实现远程办公、行政审批事项“一网通办”四项标志性成果，信息化工作取得明显成效。但总体来看，生态环境信息化建设的基础依然薄弱，对标打好污染防治攻坚战提供坚强保障的要求仍然存在不小差距，必须加快推动信息化高质量跨越式发展。

会议强调，加强网络安全和信息化工作，是贯彻习近平总书记关于网络强国的重要思想的具体行动，是落实党中央、国务院决策部署的必然要求，是提高生态环境管理水平的内在需要。要认真学习领会习近平总书记关于网络强国的重要思想，树牢“四个意识”，做到“两个维护”，充分认识网络安全和信息化工作的极端重要性，切实增强信息化应用和发展的责任意识，切实增强信息化工作思维，推动互联网与生态文明建设深度融合，充分运用互联网技术和信息化手段高水平推进生态环境保护工作。

会议要求，要紧紧围绕支撑打好打胜污染防治攻坚战，服务生态环境质量总体改善目标，全面推进网络安全和信息化重点任务，突出抓好“五个落实”，即严格落实“四统一、五集中”要求，落实现有标志性成果巩固深化任务，落实支撑污染防治攻坚战重点任务，落实信息化体系设计工作任务，落实信息化体制机制改革任务。要认真落实网络安全法、网络安全工作责任制要求，树立正确网络安全观，全面加强网络安全检查，落实具体安全防护措施，健全网络安全工作机制，坚决守住网络安全底线。要大力加强网信工作推进保障，抓好政治建设、组织领导、制度建设和队伍建设，促进生态环境信息化事业更好更快发展。（来源：法制日报）

五、本期重要漏洞实例

➢ Microsoft Windows 本地权限提升漏洞

发布日期：2019-03-12
更新日期：2019-03-14
受影响系统：
Microsoft Windows Server 2019
Microsoft Windows Server 2016
Microsoft Windows 10
描述：

BUGTRAQ ID: 107280
CVE(CAN) ID: CVE-2019-0766

Microsoft Windows 是一套个人设备使用的操作系统。Windows AppX Deployment Server 是其中的一个应用程序部署服务器。
Microsoft Windows AppX Deployment Server 在实现中存在权限提升漏洞。攻击者可通过登录系统并运行特制的应用程序，利用该漏洞在任意位置创建文件。

<*来源：Wayne Low

链 接： https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ac45e477-1019-e911-a98b-
*>
建议：

厂商补丁：
Microsoft

Microsoft 已经为此发布了一个安全公告（March 2019 Security Updates）以及相应补丁:
March 2019 Security Updates：March 2019 Security Updates
链 接： https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ac45e477-1019-e911-a98b-000d3a33a34d

补丁下载：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0766

➢ WordPress Contact Form Email 插件跨站脚本漏洞

发布日期：2019-03-11
更新日期：2019-03-12
受影响系统：
WordPress Contact Form Email < 1.2.66
描述：

CVE(CAN) ID: CVE-2019-9646

WordPress 是一套使用 PHP 语言开发的博客平台。Contact Form Email plugin 是使用在其中的一个电子邮件收、发管理插件。
WordPress Contact Form Email 插件 1.2.66 之前版本，wp-admin/admin.php 页面中存在跨站脚本漏洞。远程攻击者利用该漏洞可在应用程序的上下文中执行 JavaScript 代码。

<*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/contact-form-to-email/#developers

➢ Cisco NX-OS 未授权文件系统访问漏洞

发布日期：2019-03-06
更新日期：2019-03-12
受影响系统：
Cisco NX-OS
描述：

CVE(CAN) ID: CVE-2019-1601

Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。
Cisco NX-OS Software 由于文件系统权限问题，在实现中存在安全漏洞。远程攻击者可通过访问并对关键配置文件写操作，利用该漏洞使用配置文件，绕过身份验证安全限制。

<*来源：vendor

链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-file-ac
*>

建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190306-nxos-file-access）以及相应补丁：
cisco-sa-20190306-nxos-file-access： Cisco NX-OS Software Unauthorized Filesystem Access Vulnerability
链接：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-file-access

➢ IBM WebSphere Application Server 跨站脚本漏洞

发布日期：2019-03-04
更新日期：2019-03-07
受影响系统：
IBM Websphere Application Server 9.0
IBM Websphere Application Server 8.5
描述：

CVE(CAN) ID: CVE-2019-4030

IBM WebSphere Application Server（WAS）是一款应用服务器产品。
IBM WAS 8.5 及 9.0 版本，在实现中存在跨站脚本漏洞。远程攻击者可利用该漏洞向 Web UI 中注入任意的 JavaScript 代码，导致会话信息泄露。

<*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：
http://www-01.ibm.com/support/docview.wss?uid=ibm10869406

六、本期网络安全事件

➢ 日本拟对 IT 巨头收集个人信息追责

2019 年 3 月 10 日，日媒称，日本公平交易委员会基本决定，在美国谷歌和脸书等 IT 巨头非法收集、使用个人信息时，对其适用《反垄断法》。

据共同社 3 月 6 日报道，日本公平交易委员会考虑，把企业与个人之间的服务和信息交换看作交易，并视为触犯《反垄断法》中规定的“滥用优势地位”条款。对 IT 巨头，日本此前一直以企业间交易为中心重点监视，今后将目光扩大至个人。

报道称，IT 巨头有强势地位，在人们使用信息检索和社交网站时收集个人信息，日本公平交易委员会将认定这种行为属于触犯规定，加以管制。

日本公平交易委员会事务总长山田昭典在当天的记者会上指出，对于 IT 巨头是否处于优势地位、是否造成损失，适用时“有必要展开个别讨论”。

报道还指出，该组织将基于 1 月起对 IT 巨头开展的实际交易情况调查结果以及围绕强化管制的政府专家研讨会议论情况，进一步完善法律制度。

另据共同社此前报道，日本公平交易委员会 2 月 27 日开展正式调查，以弄清楚美国亚

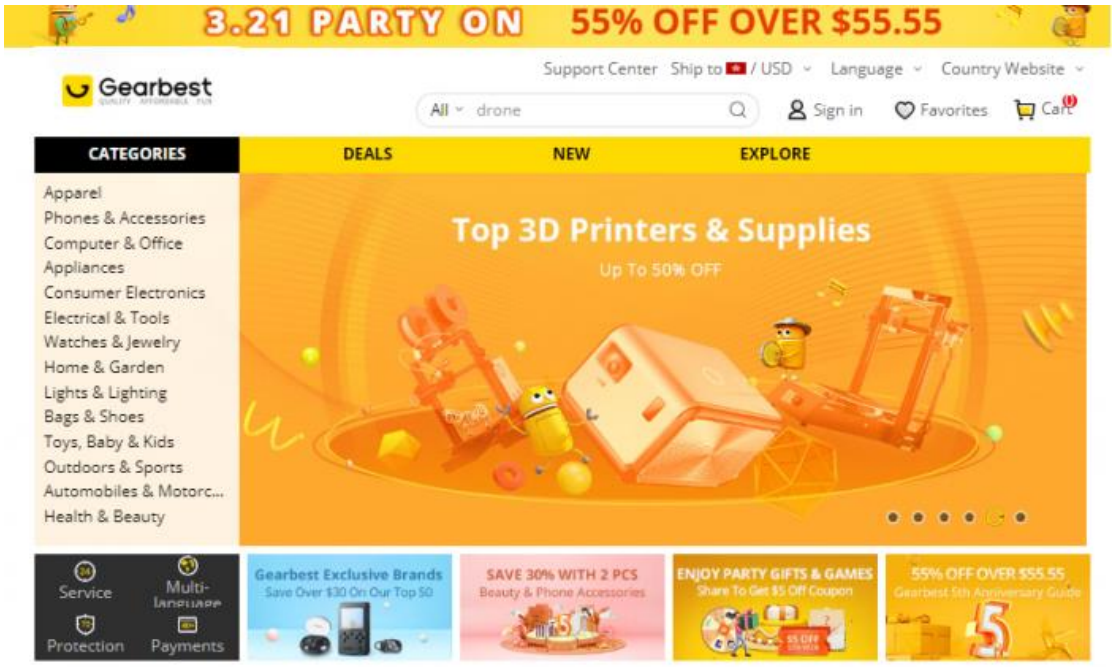
马逊及苹果等 IT 企业巨头的实际交易情况。这是因为担忧 IT 巨头通过垄断市场加强影响力而推进掌控、给交易对象造成不当压力的问题。

报道称，日本政府开始对提供网络服务基础、被称为“平台公司”的 IT 巨头加强限制。如果企业不配合调查，将基于《反垄断法》第 40 条行使强制调查权限，以严厉姿态应对。（来源：参考消息）

➢ 中国跨境电商巨头 Gearbest 泄露数百万消费记录

2019 年 3 月 16 日，TechCrunch 报道称，总部位于深圳的 A 股上市公司跨境通旗下自营跨境电商平台 Gearbest 泄露了数百万用户的个人信息和购物订单。

Gearbest 是以电子类业务为主的综合电商平台，它为华硕、华为、英特尔和联想等品牌提供服务。Gearbest.com 在全球购物类网站中流量排名在 40 名左右，在全球所有网站中位于前 250 名，月访问流量有 1.22 亿。



安全研究员 Noam Rotem 发现，一个 Elasticsearch 服务器每周都会泄露数百万条记录，包括客户信息、订单内容和付款记录等。该服务器未受密码保护，允许任何人搜索数据。

根据 Noam Rotem 目前公布的信息，泄露的数据中包含用户姓名、地址、电话号码、电子邮箱和订单及产品信息。该数据库还包含支付和发票信息，附带有支付金额以及半隐藏的姓名和电子邮件地址。其中一些会员订单还包含护照号等身份信息。Rotem 称，这些数据

可能会危及世界上部分自由受限地区的消费者。例如，一些来自禁止 LGBTQ 和婚前性行为国家的客户购买了性玩具等用品，这可能会给他们招致麻烦。

在阿拉伯联合酋长国和巴基斯坦等出台了相关严格法律的国家中，他们可能会被判死刑。

Rotem 表示，该数据库并没有多少加密措施，有的甚至完全没有加密。他还在相同的 IP 地址上发现了另外一个网络数据库管理系统，让所有人都可以操纵和破坏 Gearbest 母公司跨境通的数据库。目前尚不清楚这些数据库曝光了多长时间。互联网扫描网站 Binary Edge 数据显示，这些数据库是在 3 月 7 日首次被探测到的。

TechCrunch 称，他们已经通过该公司的专用安全页面与之取得联系。但 Gearbest 尚未作出回应，也没有对数据加以保护。

Gearbest 从成立之初就专注于小语种新兴市场，在西班牙、波兰、捷克等国家都设有仓库。它有可能会在当地受到欧洲隐私数据保护法的制裁。欧盟地区有着目前世界上最严格的隐私保护政策，任何违反《通用数据保护条例》（GDPR）的企业都有可能面临最多相当于其全球年度营收 4% 的罚款。

跨境通 2018 年财报显示，该公司去年实现营业总收入为 216.26 亿元，比去年同期上升 54.28%。其中，营业利润为 12.43 亿元，利润总额为 13 亿元。基本每股收益为 0.67 元，上年同期为 0.52 元。2018 年，跨境通在“黑五”期间跨境出口 GMV 超过 14 亿元，同比增长 45%，其中 GearBest 同比增长了 55%。该公司在互动易平台公布的信息显示，“黑五”期间该公司自营网站销售额排名前十的国家分别是：美国、德国、西班牙、法国、意大利、英国、以色列、波兰、葡萄牙、加拿大。截至发稿，跨境通股价为 12.08 元人民币，下跌了 0.25%。（来源：新浪科技）

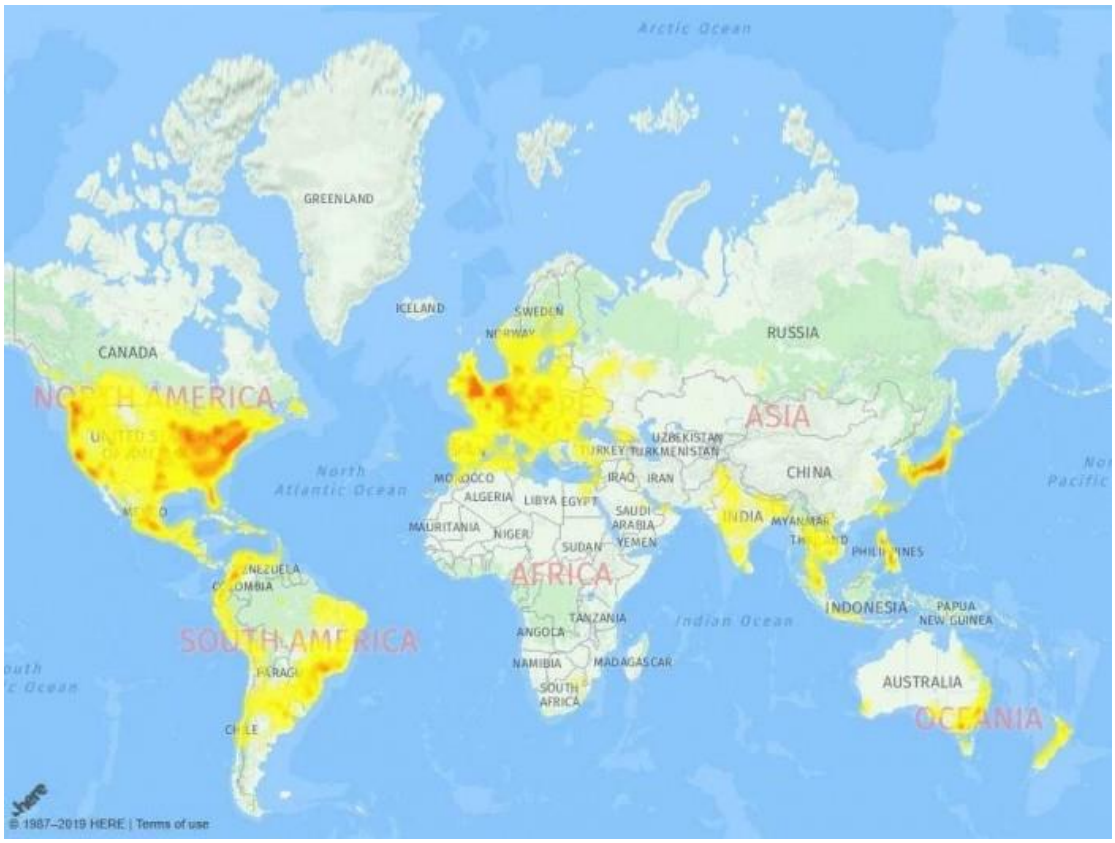
➢ Facebook、Instagram 和 WhatsApp 发生严重宕机事故

2019 年 3 月 14 日世界各地的 Facebook 用户都报告称，他们在登录 Facebook 网站以及 Instagram 和 WhatsApp 时遇到了问题，也无法发帖。Facebook 并未给出服务中断的原因，除了承认该公司已经获悉某些地区的服务宕机以外几乎并未提供其他信息。Facebook 股价几乎并未因此受到影响，该股周三收盘上涨 0.84%。

Facebook 周三发布 Twitter 消息承认了此次服务中断，该公司称：“我们知道，目前有些人在访问 Facebook 旗下各个应用程序时遇到了困难。我们正在努力尽快解决这个问题。“

随后 Facebook 证实，这个问题不是 DDoS 攻击带来的结果。DDoS 攻击即“分布式拒绝服务攻击”，是指黑客通过向一个站点输送大量虚假流量来发动攻击。

据专供用户报告应用程序和站点问题的 DownDetector 网站称，从全球范围来看，上报 Facebook 问题的报告最多达到了 1.1 多万。用户报告了各种各样的问题，从根本无法加载网站到无法发布评论等。Facebook 用户纷纷在 Twitter 上发布截图，这些截图显示了他们试图加载 Facebook 应用时的错误信息。在加载网站时，有些用户的屏幕上会显示出“账号暂时不可用”(Account Temporarily Unavailable)的消息。



从以往历史来看，Facebook 的技术问题经常都会给使用该平台甚至其他网站的广告主带来严重问题。去年 11 月，Facebook 为广告主提供的工具遭遇故障，当时营销人员正试图投放“黑色星期五”(Black Friday)和“网络星期一”(Cyber Monday)广告。

在 2013 年，Facebook 经历了一次故障，其结果是导致多个网站瘫痪，Facebook 当时表示故障的原因是其登录功能已经遍及整个互联网。根据当时的报道，当用户试图使用 Facebook 资料登录网站时，会被引导至一个 Facebook 错误页面。报道称，这一故障只持续了几分钟，对《纽约时报》和 CNN 等网站造成了影响。（来源：新浪科技）

➢ 委内瑞拉电力系统再遭攻击: 再次大停电

2019 年 3 月 9 号当地时间周六，大量民众涌入首都加拉加斯表示对停电的不满，甚至有部分极端的抗议者与警方发生了严重的肢体冲突。但有更多的民众选择走出家门，表达对总统马杜罗的支持，并谴责国内外反动势力对和平的蓄意破坏。

“这里没有电，他们用发电机来游行，而不是把发电机送到需要它们的医院里去。”

据央视新闻报道：委内瑞拉总统指责美国对该国电力系统进行高科技“电磁攻击”，并表示连日来美国针对委内瑞拉电力系统的攻击旨在制造政治和社会不稳定。他呼吁民众保持平静，同时表示政府将竭尽全力确保食品供应、供水和医疗服务。他说，电力系统工作人员正在进行“谨慎、细致”的工作，以确保供电稳定性。

马杜罗还表示：“本来截至(9 日)中午我们已经恢复了受影响地区将近 70%的供电，但此时又一台正常运转的发电机遭到了新一轮网络攻击，这打乱了恢复供电的部署，我们之前所做的一切努力都被破坏了。”

事情起源于 3 月 7 日，委内瑞拉开始大规模停电，当日傍晚，从安第斯山脉到加勒比海岸地区陆续进入断电状态。停电以后委内瑞拉的主要交通系统全部瘫痪，基础设施陆续失效。8 日，委内瑞拉全国停班停课。虽然在当天晚些时候部分地区恢复了供电，但次日早上又开始断电，这加剧了民众的恐慌。

此次停电是自 2012 年以来委内瑞拉持续时间最长、影响地区最广的停电。委内瑞拉电力部长(Luis Motta Domínguez)说，停电是因为委内瑞拉东部的大型水力发电站受到“电子攻击”。委内瑞拉新闻部长罗德里格斯(Jorge Rodríguez)也表示，此次停电的原因是国内最重要的古里水电站遭到反对势力蓄意破坏，目前正在抢修恢复。但是很明显，持续的“高科技网络攻击”让委内瑞拉电力部门的修复工作频频受阻，全面恢复供电举步维艰。

委内瑞拉电力供应逾六成来自水力发电，而其中绝大多数发电量由古里水电站提供。

今年 1 月 23 日，委内瑞拉议会主席、反对派领导人胡安·瓜伊多自封“临时总统”，获得美国政府承认。美国继而加大对委内瑞拉的制裁力度，公开表示不排除军事干预。而早在 3 月 7 日，委内瑞拉电力系统遭到第一轮网络攻击进入瘫痪之时，委政府就已经表示：已按照总统马杜罗的命令在全国采取相关措施，保护人民生命和财产安全，全国将在几小时内恢复供电。然而第二轮的网络攻击很快让委内瑞拉政府一度恢复的电力系统再次崩溃。

马杜罗表示：

美国支持反对派领导人“自立总统”，企图推翻马杜罗政权，使本就处于经济危机中的委内瑞拉雪上加霜，此举也为国际社会所指责。而这次大规模的停电和旋即而来的游行，也无疑将给委内瑞拉带来不可估量的损失。（来源：央视新闻）

➢ 团伙做假证还有黑客团队专门负责入侵考试网站

2019 年 3 月 16 日，一团伙做假证，不但细分到接单中介、假证中介、制贩假证等环节，竟有专门的黑客人员，负责入侵各地人事考试的网站。15 日，四川省公安厅通报泸州警方

破获的一起做假证的案件，抓获嫌疑人 24 人，现场查获伪造的证件 1.2 万本。

去年 5 月，泸州网安部门发现犯罪嫌疑人龙某涉嫌为网络制贩假证团伙提供虚假的“网查”服务，随后立即成立专案组开展侦破工作。经查，整个团伙主要分为黑客人员、接单中介、假证中介、制贩假证人员 4 个环节。

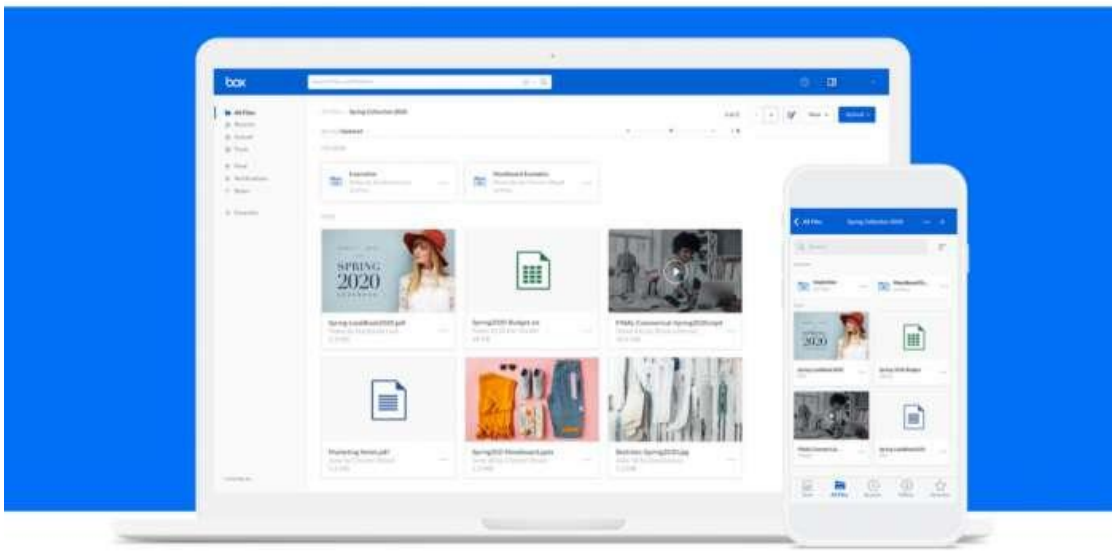
其中，黑客人员负责入侵各地人事考试网等网站，获取网站权限后，再非法添加黑链并为假证团伙提供“网查服务”（将假证信息添加指定网站中）。接单中介负责在 QQ 群、网站中打广告招揽客户。假证中介收到订单信息后，联系黑客将要办理的证件信息非法添加进各地网站，安排制作假证人员印制假证，并将网站查询页面链接发送给接单中介。制贩假证人员接到订单后按照假证中介要求印制假证，并通过快递邮寄给下级中介或购买假证人员。

去年 6 月，在掌握了该犯罪团伙成员结构和身份信息后，专案组对犯罪团伙展开集中收网，一举打掉“黑客入侵、网上接单、窝点制作”为一体的黑产一条龙新型伪造证件犯罪团伙，抓获犯罪嫌疑人 24 人，端掉制贩假证窝点 2 个，现场查获伪造证件成品、半成品 12000 余本、制证设备 2 套，及大量黑客工具。（来源：封面新闻）

➢ 云盘服务 Box 帐号配置不当致数十家公司敏感数据泄露

2019 年 3 月 12 日，据美国科技媒体 TechCrunch 报道，网络安全公司 Adversis 发现，有数十家公司因为员工公开分享云盘服务 Box 企业存储帐号的文件链接，而无意间泄露了敏感的企业和客户数据。

虽然存储在 Box 企业帐号内的数据默认设置称私密状态，但用户可以与任何人分享文件或文件夹，因而只需要一个链接就可以公开接触这些文件。但 Adversis 表示，这些秘密链接还可以被其他人发现。使用脚本扫描和枚举的方式，Adversis 发现有 90 多家公司的文件夹都可以公开访问。



Box 自己的员工也未能幸免。

该公司表示，虽然多数数据都是合法公开的，而且该公司也向用户发送了建议，帮助其尽可能减少风险。但很多员工可能并不知道敏感数据被分享出去，甚至可以被其他人找到。更糟糕的是，一些公共文件夹还可以被搜索引擎索引，导致信息更容易被发现。

Adversis 表示，Box 应该重新配置默认共享链接，限制为“公司内部的人员”，从而降低意外暴露敏感信息的概率。（来源：新浪科技）