国盟信息安全通报

2019 年 1 月 14 日第 184 期

国盟信息安全通报

（第 184 期）

国际信息安全学习联盟

2019 年 1 月 14 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 138 个，其中高危漏洞 44 个、中危漏洞 78 个、低危漏洞 16 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 75 个（占 54%），其中互联网上出现“TP-LinkArcher C5 远程命令执行漏洞、WordPress 插件 Audio Record 任意文件上传漏洞”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 1496 个，与上周（1657 个）环比下降 10%。

主要内容

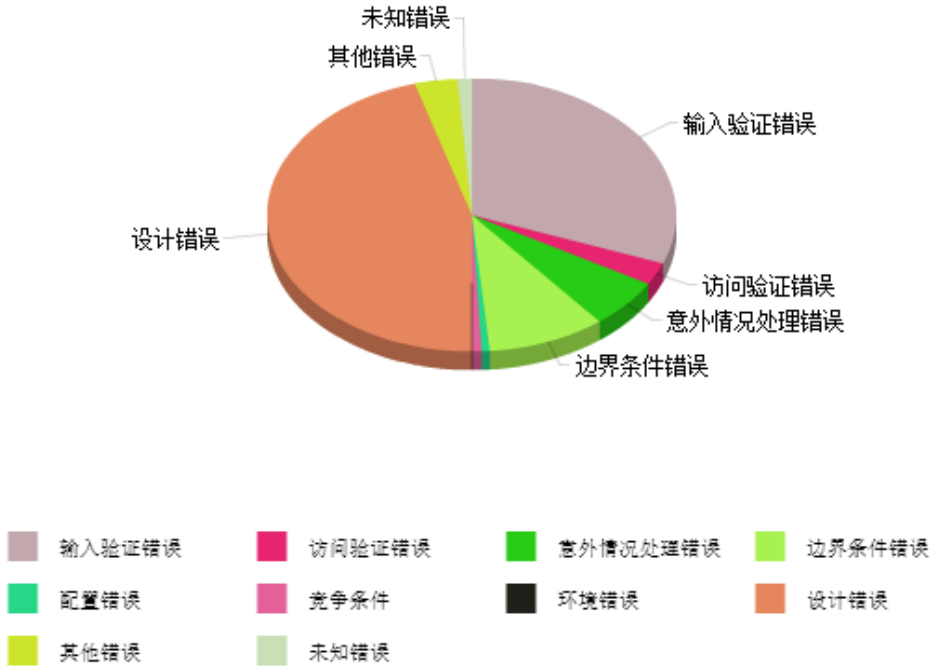
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

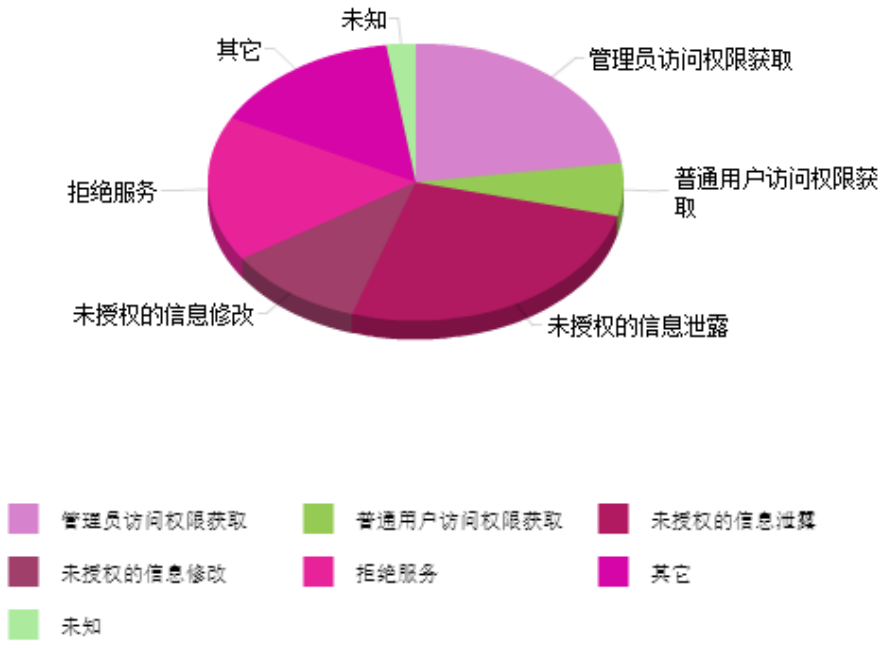
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 138 个，其中高危漏洞 44 个、中危漏洞 78 个、低危漏洞 16 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 75 个（占 54%），其中互联网上出现“TP-LinkArcher C5 远程命令执行漏洞、WordPress 插件 Audio Record 任意文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1496 个，与上周（1657 个）环比下降 10%。

二、安全漏洞增长数量及种类分布情况

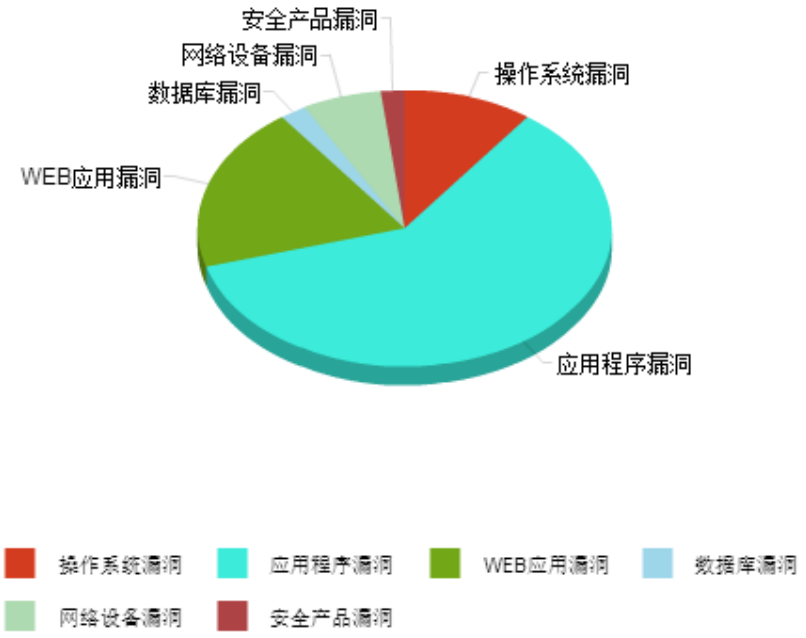
➢ 漏洞产生原因（2019 年 1 月 1 日—2019 年 1 月 14 日）



➢ 漏洞引发的威胁（2019 年 1 月 1 日—2019 年 1 月 14 日）



➢ 漏洞影响对象类型（2019 年 1 月 1 日—2019 年 1 月 14 日）



三、安全产业动态

➢ 让网络生态空间更加风清气朗

近日，针对网络生态问题频发、各类有害信息屡禁不止等突出问题，国家网信办启动网络生态治理专项行动，剑指淫秽色情、低俗庸俗、暴力血腥等 12 类负面有害信息。

据悉，此项行动将持续开展 6 个月，对各类网站、移动客户端、论坛贴吧、即时通信工具、直播平台等重点环节中的上述负面有害信息进行整治，集中解决网络生态重点环节突出问题，充分运用现有行政执法手段，严厉查处关闭一批违法违规网站和账号，有效遏制有害信息反弹、反复势头，促进网络生态空间更加清朗。

互联网是一个社会信息大平台，也是一个文化大平台，对亿万网民的求知途径、思维方式、价值观念有着重要影响。其传播优势和舆论功能，为推动信息交流、促进文化繁荣、凝聚社会共识提供了新的渠道和手段。

网络平台里如果干净纯洁、安全可靠，给网民带来的是新气息、新风尚，营造的是良好的氛围；而如果是污浊混乱，不仅扰乱正常的网络秩序，对个人和社会也都将带来损害。针对有害信息进行专项治理行动，确保网络空间更加清朗、生态良好，符合国家和人民的利益。

此次专项治理行动积极回应了广大网民对风清气正网络空间的呼唤。网络空间是亿万民众共同的精神家园。负面有害信息，污染精神家园，造成信息误导，让人们迷惑、迷惘，不

坚决铲除，后患无穷。加强网络空间治理，加强网络内容建设，既是网民的期盼，也是摆在监管部门、行业主体、从业人员面前的现实课题。

净化网络空间，要推进依法治理，落实主体责任。此次专项行动将严格按照“谁主管谁负责，谁主办谁负责”原则，狠抓责任落实，各地网信部门要切实履行属地管理责任，各网站平台要坚决落实企业主体责任，全力推动网络生态专项治理工作取得实效。

网络是个虚拟世界。离开法治和道德，网络谣言、网络诈骗、网络陷阱等就会大行其道，广大网民就可能深受其害。依法加强网络空间治理，是对社会负责、对人民负责。维护网络空间这个精神家园的风清气朗，是全社会共同的责任。企业要承担企业的责任，政府要提高治理水平，广大网民也应自觉遵守法律和道德规范。

互联网是技术进步带给人类文明的礼物。要让更多的网民能够在互联网的世界中沐浴清风、汲取营养，让互联网成为涵养社会心态、提升公众文明素养的重要载体。也唯有当每个个体都争当网络良好生态营造者之时，风清气朗的网络环境才真正可期。（来源：光明日报）

➢ 加快推进制造强国和网络强国建设 保持工业通信业平稳健康发展

2018 年 1 月 10 日上午，工业和信息化部党组书记、部长苗圩就贯彻落实中央经济工作会议精神，接受了人民日报记者王政、新华社记者张辛欣、中央电视台记者宋菀、经济日报记者黄鑫的联合采访。

苗圩表示，中央经济工作会议把“推动制造业高质量发展”摆在今年七大重点工作任务首位，要求推动先进制造业和现代服务业深度融合，坚定不移建设制造强国。工业和信息化部将坚持以习近平新时代中国特色社会主义思想为指导，按照中央经济工作会议部署和做好“六稳”工作的要求，在“巩固、增强、提升、畅通”上狠下功夫，采取有力措施，保持工业通信业平稳健康发展，开创制造强国和网络强国建设新局面。

记者：中央经济工作会议提出的 2019 年重点工作任务中，“推动制造业高质量发展”被排在首位。针对制造业高质量发展，工信部将有哪些实招？

苗圩：中央经济工作会议上，把“推动制造业高质量发展”作为今年要抓好的第一项重点工作任务，体现了党中央对制造业发展的高度重视，也是中国经济高质量发展，增强国际竞争力的迫切需要。

中国是世界第二大经济体，有巨大的国内市场，完整的产业体系，不断提升的创新能力，便利的基础设施和良好的营商环境，有足够韧性来应对挑战。工业和信息化部将认真贯彻落实中央经济工作会议部署，坚定不移建设制造强国，加快推动制造业高质量发展。

一是建立健全制造业高质量发展的政策体系、指标体系和评价体系。二是加强创新能力建设，继续实施国家制造业创新中心建设工程。打破从基础研究、应用研究到产业化的“死亡之谷”，促进科研成果产业化，加强关键共性技术研究。三是深化制造业结构调整，实施新一轮重大技术改造升级工程，引导传统产业改造提升。推动人工智能、新能源汽车等新兴产业发展。深入实施智能制造工程，培育发展一批先进制造业集群。四是优化制造业发展环境，进一步放宽市场准入，降低制度性交易成本，促进科技、金融、人才与制造业协同发展。推动进一步降低制造业增值税税率，持续降低制造业用电、用水等要素成本。五是进一步扩大对外开放，全面实施准入前国民待遇加负面清单管理制度，落实汽车、船舶、飞机等行业开放政策。

记者：民营企业占了 90%的企业数量，其中大部分是中小企业，中央给民营企业发展吃了“定心丸”，工信部怎么把这颗“定心丸”精准送到位？

苗圩：中小企业与民营企业互为主体，是我国社会主义市场经济发展的重要成果，也是促进高质量发展的生力军。作为国务院负责促进中小企业发展工作的部门，我们坚决贯彻党中央、国务院的部署和要求，会同有关部门重点做好四个方面工作：一是进一步优化中小企业发展环境。以贯彻习近平总书记在民营企业座谈会上明确提出大力支持民营企业发展壮大的 6 个方面政策举措为重点，以落实中小企业促进法为抓手，推动出台促进中小企业健康发展的指导意见。二是进一步提升中小企业专业化能力和水平。培育“专精特新”“小巨人”企业，继续实施中小企业知识产权战略推进工程和信息化推进工程，实施促进大中小企业融通发展三年行动计划。三是进一步提高中小企业服务实效。推进国家中小企业政策信息互联网发布平台建设。发挥国家中小企业公共服务示范平台的作用，继续实施企业经营管理人才素质提升工程。四是进一步推动缓解中小企业融资难融资贵。推动完善应收账款、知识产权等质押融资机制和产融合作试点，发挥国家融资担保基金作用，实施小微企业融资担保业务降费奖补政策，推动建立政、银、企风险分担机制，进一步发挥中小企业发展基金的引领作用。

记者：工信部如何落实“巩固、增强、提升、畅通”八字方针，有哪些实招支撑工业经济平稳发展？

苗圩：2019 年，我们将在“巩固、增强、提升、畅通”八个字上下功夫，进一步深入推进工业供给侧结构性改革，巩固去产能成果，支持重点省份钢铁去产能，持续优化钢铁产业布局。严禁钢铁、水泥、平板玻璃等新上项目扩大产能，严控电解铝新增产能，更多运用市场化、法治化手段，持续推进落后产能依法依规退出，推动更多产能过剩行业加快出清。提升产业链水平，加强关键核心技术和重大短板攻关，把促进传统产业优化升级作为落实高质量发展的重要举措，加大技术改造和设备更新。增强企业发展活力，深化“放管服”改革，不断优化企业营商环境，鼓励和支持非公资本参与制造业领域国有企业改制重组，打造具有全球竞争力的世界一流制造业企业。培育一批专注细分领域的“单项冠军”企业，大力弘扬企业家精神，鼓励企业家聚焦实业、做精主业。畅通工业经济循环，促进工业生产与国内市场良性循环，持续升级和扩大信息消费，支持超高清视频、车联网、新能源汽车等加快发展，引导通用航空、冰雪装备等大众化发展，促进工业经济与金融良性循环，深化产融结合。

记者：中央经济工作会议指出，加快 5G 商用步伐。5G 将带来什么？工信部如何推动？

苗圩：移动通信基础设施对经济社会发展的核心驱动作用日益凸显，5G 具备更高速率、更低时延、更大连接的特点，将与人工智能、大数据、物联网等新技术深度融合，进一步深入到各行各业，加快生产活动向数字化、网络化、智能化方向演进升级，激发出如智能网联

汽车、远程医疗手术等各类创新应用，改变我们的社会。

5G 将构筑万物互联的新一代信息基础设施，成为社会数字经济和各行各业转型升级发展的新引擎。我们不仅要建好 5G，更重要的是想方设法用好 5G。一是加快促进 5G 终端成熟。5G 芯片、终端的研发进程正在全力加速，力争 5G 终端尽快与用户见面，部分企业有望 2019 年中推出供用户测试使用的手机。二是加快网络建设进程。2018 年 12 月，工业和信息化部正式向三家基础电信企业发放了 5G 试验频率使用许可，下一步将开展 5G 规模试验，着力打造城市级的高质量 5G 精品网络。三是加快培育 5G 融合应用。不断深化基于 C-V2X 的车联网标准体系、产业协同和示范应用，加快推进工业互联网和 5G 的融合应用，进一步推动 5G 与农业、交通、医疗、教育等各领域的协同创新。组织开展第二阶段的 5G 应用征集工作，集各方力量共促 5G 应用发展。

记者：2018 年的数据显示，我国信息消费正在快速增长。您认为今年信息消费还将快速增长吗？有哪些助推因素？

苗圩：随着新一代信息通信技术与经济社会各领域的深度融合，信息消费已经成为创新最活跃、增长最迅猛、辐射最广泛的新兴消费领域之一。伴随着居民消费结构的提质升级，新消费理念被广泛认可接受，2019 年信息消费将延续快速增长态势，在推动经济发展质量变革、效率变革、动力变革中发挥着更为重要的作用。其助推因素主要包括促进消费的体制机制日益完善、信息基础设施持续演进升级、新一代信息通信技术活跃创新、制造业加速数字化转型等四个方面。（来源：新华社）

➢ 人工智能时代信息安全监管面临的挑战及对策

当前，全球范围内新一轮科技革命正在萌发，传统互联网正在向万物互联和智能化方向发生深刻转变。大数据的聚合分析、理论算法的革新、计算能力的显著提升及网络设施的迭代演进驱动人工智能发展进入新阶段。作为一项引领未来的战略性技术，人工智能具有显著的溢出效应，它将深刻改变世界竞争格局、改变人类社会生活。

与此同时，人工智能并不是万能的，它是一柄“双刃剑”。

人工智能作为一项影响面极广的颠覆性技术，假如放任其发展，又会对信息安全构成一定的挑战。相较于传统的互联网时代，智慧赋能后的网络信息技术可以通过对现实中真实的人进行上网数据与行为的聚合分析，并对其进行“虚拟行为画像”，从而构建一个比独立个体更加完整的“虚拟人”，进而实现对真实个体的社会行为进行分析与预判。因此，若不对人工智能技术应用加以合理的监管，势必会造成个人数据和个人隐私泄露，引发信息安全风险。

一、智慧赋能的应用对信息安全监管构成潜在挑战

人工智能发展正处于快速上升期，技术水平和质量参差不齐，未来发展趋向也尚不明朗。在个人隐私保护意识越加强化的今天，智慧赋能后的技术应用将会对信息安全造成潜在的风险，引发国家安全稳定风险。同时，从技术层面讲，智能化的技术还不能做到完全科学精确，甚至有可能产生“信息失真”和“行为误判”，从而引发社会伦理道德风险。而最为关键的

是，相对于蓬勃发展的人工智能技术开发与应用，与之相配套的法律制度严重滞后，适应智能化发展需要的信息安全监管体系也尚未形成，智慧赋能后的信息安全监管处于“无法可依”状态，这将对信息安全监管的长久发展带来极大的不确定性和不稳定性。总的而言，人工智能技术的广泛应用有以下几方面潜在风险：

1.内部控制失效

人工智能技术的应用建立在对互联网用户上网数据采集的基础之上，没有大规模的数据存储和数据分析，就不会有智能化的便捷应用和技术服务。针对个人上网数据的大型知识库，主要掌握在拥有先进技术和雄厚资源的大型互联网企业手中，他们一手收集着用户的数据信息，一手分析这些信息并将之智能化应用。由于企业具有逐利的本性，加之信息安全管控高投入的门槛，可能会导致其控制数据泄露的机制形同虚设，无法有效运转。

2.安全监管缺位

作为一门新的技术应用，人工智能技术应用具有极强的社会颠覆性，属于典型的技术密集型产业，技术更新迭代非常快，始终引领时代发展之大潮。然而，监管具有先天的滞后性，信息安全监管永远落后于信息技术的发展。一方面，信息安全监管是以信息技术发展为前提的，另一方面，信息安全监管又借助信息技术。因此，人工智能时代，信息安全监管面临着极强的压力，监管策略和监管技术的及时调整和补位就显得尤为必要。

3.法律规制滞后

法律与制度是信息安全监管的重要手段，人工智能日新月异，其升级周期随着数据的积累和算法的更新会越来越短。相反，信息安全监管法律的产生具有较大的时间成本和知识消化成本，势必会远远滞后于人工智能新技术的应用发展。当前，人工智能技术应用早已从襁褓中的婴儿成长为茁壮少年，但与之相配套的法律规制却还未迎来新生，这将对人工智能技术的发展应用造成极大的不稳定性。

二、信息安全监管所面临的智能化挑战形成原因与困境

1.智能化挑战形成于科技变革史之中

当前，全球范围内人工智能技术日新月异，人工智能应用蓬勃发展，无人驾驶、工业互联、智能大脑等各种智能化应用场景比比皆是。从科技史角度探究，信息技术革命向人工智能革命的深刻转变，极大地挑战着社会的良性、稳定发展。智慧赋能的信息安全所面临的内部控制失效、安全监管缺位、法律规制滞后等挑战根本上源于这轮信息技术发展具有颠覆性，人类技术发展进入了新的周期、新的层次。意识具有主观能动性，纵观全球，技术的更新迭代总会引起一定程度社会制度的自调整，而这一调整的过程就在于解决技术发展与人类社会

的不相匹配性。

2.智能化挑战对“三维社会结构”的稳定性构成威胁

广义而言，社会具有三个维度，即个人维度、社群维度和国家维度，个人组成社群，社群孕育国家。从人类文明发展的角度来看，人类社会的文明就是在个人、社群和国家三个维度相互作用的情况下辩证发展的。“三维社会结构”作用于文明的进程，文明的进程反过来也作用于“三维社会结构”。以人工智能为代表的新技术革命，是人类文明发展进步的最新成果，也是具有潜在能够裂变人类社会结构的新物种。人工智能技术应用强化了“技术伦理”的重要性，一旦技术失去中立，智能失去理性，势必会影响到“三维社会结构”的稳定性，造成结构性矛盾。

3.信息安全监管体系与智能化应用体系的不匹配性

一定的社会治理体系总是与一定的社会运行体系相作用的，科学的治理体系会有益于社会稳定运行，反之，不良的治理体系将有碍于社会的稳定运行。从智能化挑战的演变态势来看，人类社会并未充分做好适应人工智能发展的准备。现有的信息安全监管体系还停留在条块分割的初始起步阶段，与蓬勃发展的人工智能应用之间存在一定程度的不匹配性，信息安全监管理念和策略严重滞后，信息安全监管手段力不能及，信息安全监管人才储备不足，导致人工智能应用处于野蛮成长状态，如不进行社会自调整，势必会造成技术伦理与人类社会伦理出现偏差，影响社会长治久安。

三、面向智能化信息安全监管需要的应对之策

如前文所言，人工智能来势汹汹、发展迅猛，对人类“三维社会结构”的稳定性构成潜在的挑战。面对人工智能时代的新形势，信息安全监管理念必须主动求变，要在牢牢把握人工智能发展的重大历史机遇期，紧扣产业发展大势，引领信息安全技术产业发展向智能化方向转变的同时，清醒地认识到其潜在的非技术性风险和挑战，主动谋划布局信息安全监管社会支撑与内部控制体系，抢占战略性研究先机，加强前瞻预防与约束引导，积极推动国家信息安全监管相关法律法规的制定与完善，规范做好信息安全相关数据信息的内控工作，更好地服务经济社会发展大局，确保智能化的信息技术产业安全、可靠、可控发展，防范社会发生系统性风险。以三维社会结构为支撑，可以从以下几方面着手应对智能化的信息安全监管挑战：

1.构建面向未来的国家信息安全监管战略体系

战略是思想的高阶，是对未来一段时期行动的指引。积极应对人工智能对信息安全监管带来的挑战，就是要合理把握人工智能发展需要与国家信息安全保障、公民社会与国家安全

之间的平衡，科学谋划智能化应用和信息安全产业发展规划，出台人工智能相关发展行动计划，引领人工智能产业积极、健康发展。同时，构建面向未来的信息安全监管战略体系，这一体系要有一定的可调整性，能够紧跟人工智能技术发展的大潮，能够适应人工智能应用发展的大势。

信息安全监管理念方面，要实现从传统互联网思维到新兴人工智能思维转变，变被动数据流量监管为主动的虚拟行为防范。信息安全监管思路方面，要打破部门监管藩篱，消除数据壁垒，避免消耗性竞争，实现跨部门监管资源的整合。信息安全监管体系方面，要构建从国家到社会，再到个人的三个层次全方位的智能化信息安全保障体系。

2.建立“立体式”的信息安全监管社会支撑体系

技术具有社群性，人工智能技术发展有赖于社群的成长，同时，也服务于一定范围的社群。要充分动员社群力量，建立“共建、共治、共享”的信息安全监管社会支撑体系，积极引导人工智能行业自治组织发展，鼓励信息安全技术创新发展，严格执行网络安全等级保护制度，完善信息安全标准体系，培育公民信息安全保护意识。

信息安全监管法律政策方面，要抢占战略性研究先机，积极推动国家信息安全监管相关法律法规的制定与完善。内部控制方面，要加强前瞻预防与约束引导，规范做好信息安全相关数据信息的内控工作，避免公民个人数据信息的滥用。公民信息安全意识培育方面，要加强普法教育和国家总体安全观宣传，合理增加信息安全监管的公众认知度。人才队伍建设方面，要鼓励跨界研究和跨部门合作，提升信息安全研究的综合竞争力。（来源：国家计算机网络与信息安全管理中心　邓文兵）

➢ 2018 年中国信息安全从业人员现状调研报告

人才问题已成为落实网络强国战略进程中最受关注的议题之一。网络安全人才资源是开展和推进我国网络安全工作的核心引擎，只有人才工作做强才能把网络安全各方面工作做大做强。4·20 全国网络安全和信息化工作会议上，习总书记强调“要研究制定网信领域人才发展整体规划，推动人才发展体制机制改革，让人才的创造活力竞相迸发、聪明才智充分涌流。”

锻造人才队伍的第一步是摸清当前信息安全人才家底，做好基础调研，把握从业人员的发展需求，从而找出当前信息安全人才队伍培养建设的问题与痛点。在此背景下，中国信息

安全测评中心启动“2018 年度中国信息安全从业人员现状调研”活动，以期为广大安全从业人员和准从业人员提供职业发展指导，为安全行业创新发展提供指引，为国家网络安全人才队伍建设提供决策参考。

此次调研历时三个月，通过在线问卷调查、实地访谈、会商研讨等方式，深度调研信息安全从业人员现状。调研共回收有效样本 4349 份，覆盖了全国所有省、市、自治区和直辖市，囊括了各重要行业和关键基础设施领域。在调研维度和内容上，本年度报告不仅反映了信息安全从业人员的基本情况，更注重综合分析从业人员职业发展状况、薪酬待遇情况、能力提升情况、用人单位队伍建设情况，以及从业人员对安全发展态势的观点意见。篇幅所限，本文仅呈现报告部分要点内容。完整版报告将于近期发布，敬请期待。

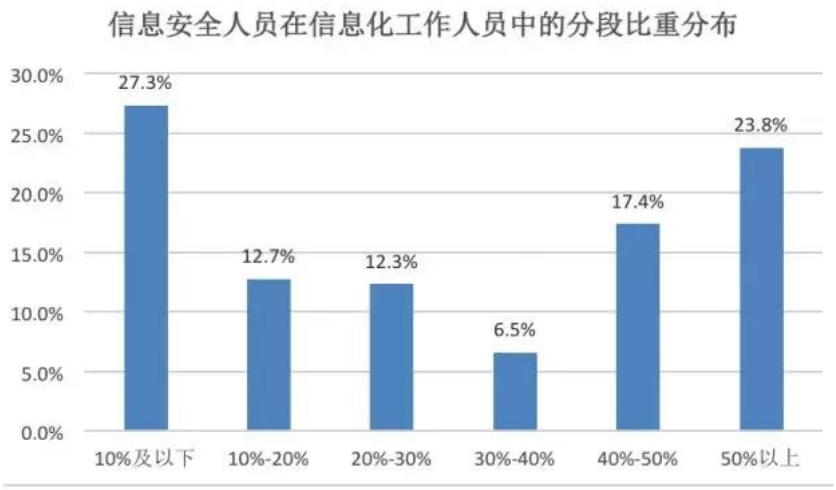
一、调研对象篇

1. 首次对信息安全从业人员进行分类定义

本报告将信息安全从业人员定义为“以信息安全为主要工作职责，会对所在单位信息安全状况造成影响的人员”。根据工作内容的不同，我们将信息安全从业人员工作职责分为 6 个类别，包括 15 个子类：1. 监管治理，包括战略法规和执法监督；2. 规划管理，包括策略规划和组织管理；3. 安全建设，包括分析设计、开发与集成；4. 安全运营，包括安全运维、数据处置、应急响应、审计与评估和安全态势分析；5. 内容安全，包括内容分析、内容安全评估和舆情分析；6. 科研教育，包括安全研究、培训和教学。本次调研将我国各行业领域承担上述 6 大类别工作职责角色的人员认定为信息安全从业人员，将其确认为抽样总体开展问卷调查工作。

2. 超三成信息化工作人员须承担信息安全工作

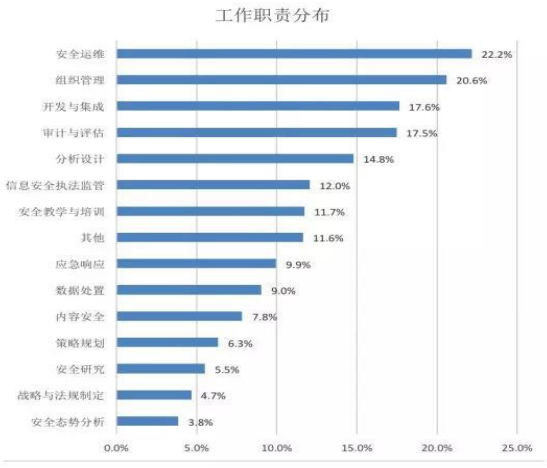
受访者认为，自己所在工作单位中信息安全人员在整体信息化工作人员中的比重平均为36.1%。但在具体分布上呈两极分化，认为信息安全人员在信息化人员中占比在 10%以下与50%以上的占比最高，分别达到 27.3%和 23.8%。



信息安全人员在信息化工作人员的分段比重分布图（样本量 4349 人）

3. 从业人员工作职责集中在安全运营和安全建设

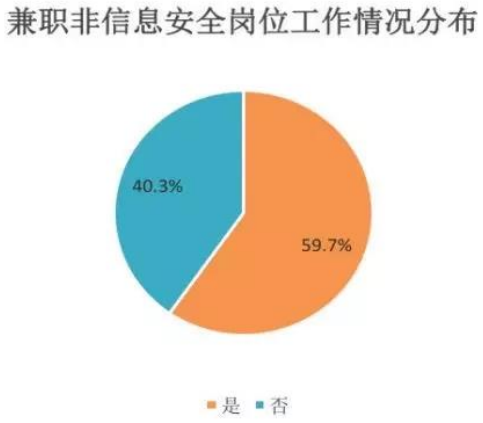
62.4%的信息安全从业人员承担的工作职责是安全运营，包括安全运维、数据处置、应急响应、审计与评估和安全态势分析；承担安全建设的从业人员占比为 32.4%，包括分析设计、开发与集成；其余工作职责类别依次是规划管理（26.9%）、科研教育（17.2%）、监管治理（16.7%）和内容安全（7.8%）。



受访者兼职非信息安全岗位工作情况分布图（样本量 4349 人）

4. 信息安全从业人员兼职非安全工作现象普遍

调研数据显示，近六成信息安全从业人员需要同时承担非信息安全岗位工作。在这部分人群中，有 40%的人员承担的非信息安全岗位工作在日常工作中占比在 25%到 50%之间；33.8%的人员一半以上的工作时间用于处理非信息安全工作。

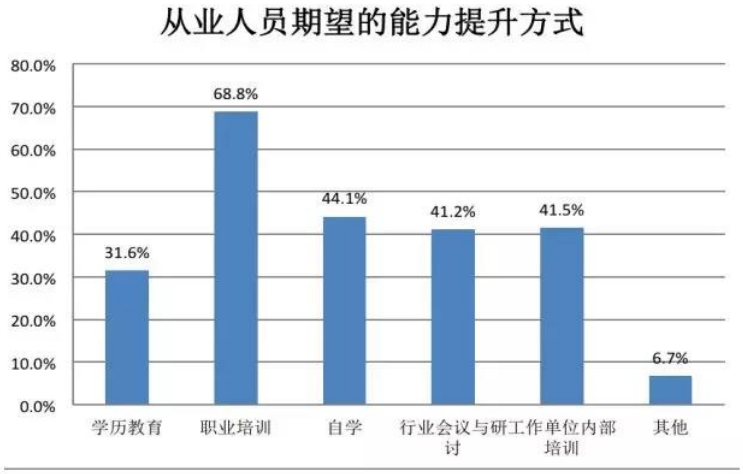


受访者工作职责分布图（样本量 4349 人）

二、能力提升篇

1. 职业培训成为从业人员首选的能力提升方式

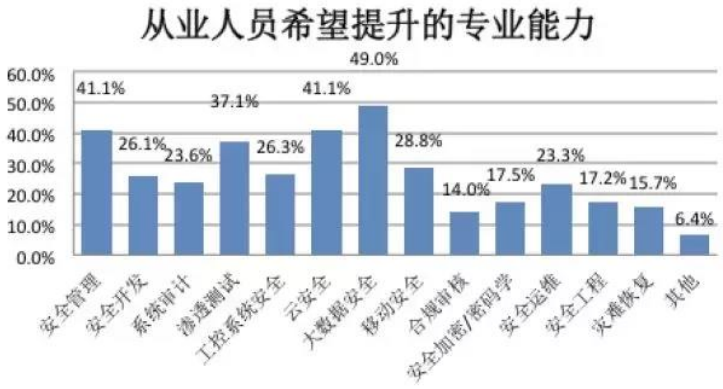
2018 年调研数据显示，“职业培训”以周期短、针对性强，以及紧密结合业界前沿趋势的优势取代了 2017 年的“自我学习”成为最受信息安全从业人员青睐的自我能力提升方式，近七成从业人员表示更倾向通过职业培训提升自身能力和知识水平。



受访者期望的能力提升方式分布图（样本量 4349 人）

2. 从业人员希望提升新技术新应用细分方向专业能力

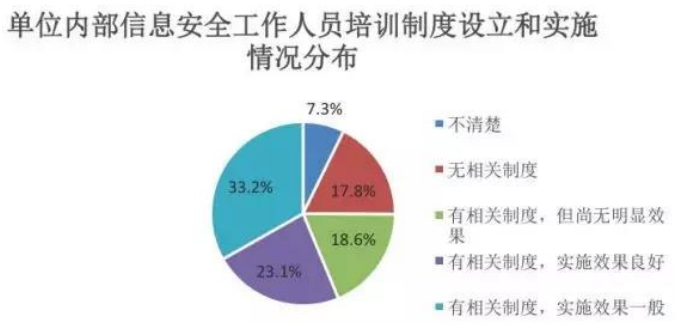
大数据安全、云安全、安全管理和渗透测试是我国信息安全从业人员最希望提升的专业能力。



受访者希望提升的专业能力分布图（样本量 4349 人）

3. 内部信息安全工作人员培训制度实施效果不佳

信息安全从业人员所在工作单位大部分建立了内部的信息安全工作人员培训制度，占比约 74.9%，但仅 23.1%的受访者认为相关的培训制度取得了良好的实施效果。



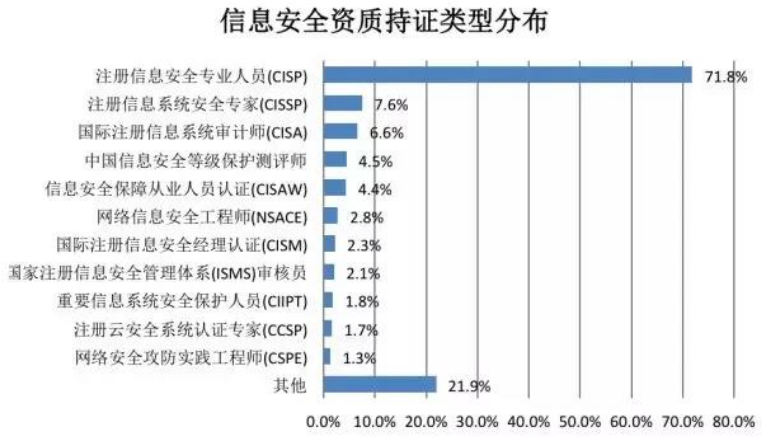
单位内部信息安全工作人员培训制度设立和实施情况分布图

（样本量 4349 人）

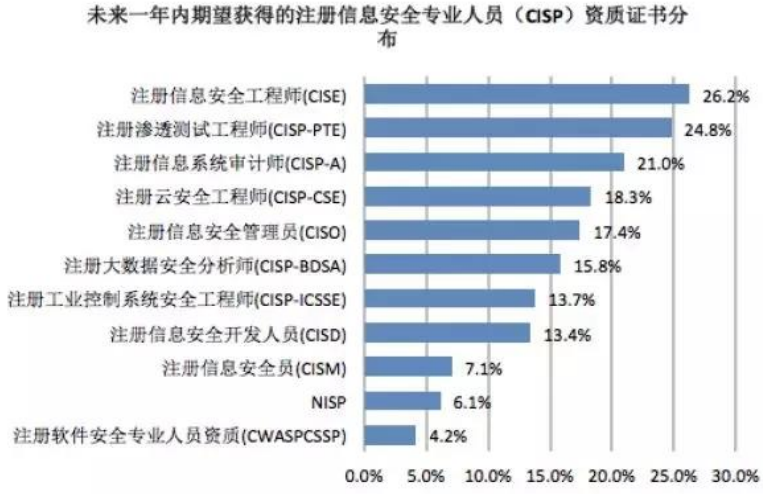
4. 从业人员持有最多、最希望获取 CISP 资质证书

调研显示，超过六成持有相关资质证书的信息安全从业人员认为职业培训和资质认定的过程有助于促进职业发展和能力提升。目前，国内持有权威资质证书占比最高的是注册信息安全专业人员（CISP）（71.8%），其中注册信息安全工程师（CISE）持证人数最多，占比达到 44.1%。83.7%的从业人员期望在未来一年内获得信息安全资质证书，最希望获取注册信息安全专业人员（CISP）证书的人群占比高达 68.9%，其中最受欢迎的子品牌分别是注册信息安全工程师（CISE）、注册渗透测试工程师（CISP-PTE）、注册信息系统审计师（CISP-A）和注册

云安全工程师（CISP-CSE）。



信息安全资质持证类型分布图（样本量 2819 人）



未来一年内期望获得的注册信息安全专业人员（CISP）资质证书分布
（样本量 2461 人）

三、工作环境篇

1. 网络安全管理制度和操作规程落实情况堪忧

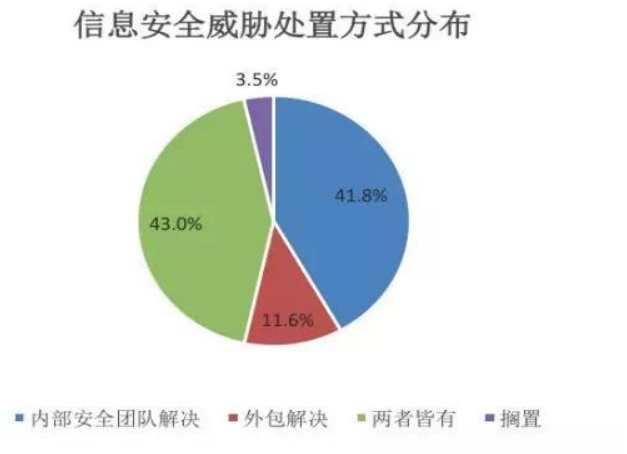
78.0%的信息安全从业人员表示，其所在工作单位设立了内部网络安全管理制度和操作规程；但是仅四分之一的从业人员反馈相关制度实施效果良好（25.0%），半数以上从业人员认为实施效果一般或较差（53.0%）。

网络安全管理制度和操作规程设立和实施效果情况分布图

（样本量 4349 人）

2. 自建团队和安全外包相结合应对信息安全威胁

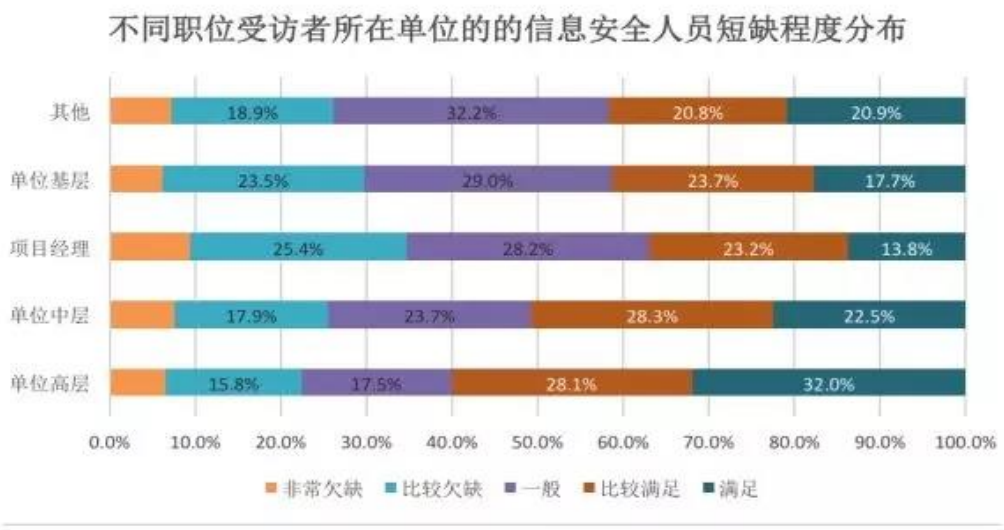
内部安全团队解决以及内部和外包结合解决（43.0%）是目前各企事业单位处置网络安全威胁的主要方式，完全交给第三方外包解决（11.6%）的企业并不多。



信息安全威胁处置分布图（样本量 4349 人）

3. 政企单位高层对信息安全工作的认知有待提高

本次调研发现，各企事业单位高层管理者对信息安全人员短缺情况明显比中层和基层人员更乐观，更倾向于认为当前单位信息安全人员队伍规模能够满足工作需要。此外，超过一半的从业人员认为单位高层对信息安全工作不重视是安全事件发生的主要原因之一。



不同职位受访者所在单位的信息安全人员短缺程度分布图

（样本量 4349 人）

4. 已有的职业晋升通道和激励机制作用尚不明显

职业晋升通道和激励机制设置情况分布图

（样本量 4349 人）

为了招得来、留得住信息安全“高精尖”人才，65.5%的从业人员表示其所在工作单位建立有信息安全从业人员职业晋升通道和工作激励机制，21.3%明确表示没有职业晋升通道和激励机制；只有不足 13.2%的受访者认为相关机制取得了良好效果，46.3%的受访者认为实施效果一般或尚无明显效果。（来源:《中国信息安全》杂志 2018 年第 12 期）

四、政府之声

➢ 27 项信安标委归口国家标准获批发布

2019 年 1 月 2 日，全国信息安全标准化技术委员会归口的《信息技术 安全技术 带消息恢复的数字签名方案 第 3 部分：基于离散对数的机制》等 27 项国家标准正式发布。

清单如下：

1.GB/T 15851.3-2018 《信息技术 安全技术 带消息恢复的数字签名方案 第 3 部分：基于离散对数的机制》 代替标准号：GB/T 15851-1995 实施日期：2019-07-01

2.GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》 代替标准号：GB/T 28449-2012 实施日期：2019-07-01

3.GB/T 36629.3-2018 《信息安全技术 公民网络电子身份标识安全技术要求 第 3 部分：验证服务消息及其处理规则》 实施日期：2019-07-01

4.GB/T 36950-2018 《信息安全技术 智能卡安全技术要求（EAL4+）》 实施日期：2019-07-01

5.GB/T 36951-2018 《信息安全技术 物联网感知终端应用安全技术要求》 实施日期：2019-07-01

6.GB/T 36957-2018 《信息安全技术 灾难恢复服务要求》实施日期：2019-07-01

7.GB/T 36958-2018《信息安全技术 网络安全等级保护安全管理中心技术要求》实施日期：2019-07-01

8.GB/T 36959-2018 《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》 实施日期：2019-07-01

9.GB/T 36960-2018 《信息安全技术 鉴别与授权 访问控制中间件框架与接口》 实施日期：2019-07-01

10.GB/T 36968-2018 《信息安全技术 IPSec VPN 技术规范》 实施日期：2019-07-01

11.GB/T 37002-2018 《信息安全技术 电子邮件系统安全技术要求》 实施日期：2019-07-01

12.GB/T 37024-2018 《信息安全技术 物联网感知层网关安全技术要求》 实施日期：2019-07-01

13.GB/T 37025-2018 《信息安全技术 物联网数据传输安全技术要求》 实施日期：2019-07-01

14.GB/T 37027-2018 《信息安全技术 网络攻击定义及描述规范》 实施日期：2019-07-01

15.GB/T 37033.1-2018 《信息安全技术 射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别》 实施日期：2019-07-01

16.GB/T 37033.2-2018 《信息安全技术 射频识别系统密码应用技术要求 第 2 部分：电子标签与读写器及其通信密码应用技术要求》 实施日期：2019-07-01

17.GB/T 37033.3-2018 《信息安全技术 射频识别系统密码应用技术要求 第 3 部分：密钥管理技术要求》 实施日期：2019-07-01

18.GB/T 37044-2018 《信息安全技术 物联网安全参考模型及通用要求》 实施日期：2019-07-01

19.GB/T 37046-2018 《信息安全技术 灾难恢复服务能力评估准则》 实施日期：2019-07-01

20.GB/T 37076-2018 《信息安全技术 指纹识别系统技术要求》 实施日期：2019-07-01

21.GB/T 37090-2018 《信息安全技术 病毒防治产品安全技术要求和测试评价方法》 实施日期：2019-07-01

22.GB/T 37091-2018 《信息安全技术 安全办公 U 盘安全技术要求》 实施日期：2019-07-01

23.GB/T 37092-2018 《信息安全技术 密码模块安全要求》 实施日期：2019-07-01

24.GB/T 37093-2018 《信息安全技术 物联网感知层接入通信网的安全要求》 实施日期：2019-07-01

25.GB/T 37094-2018 《信息安全技术 办公信息系统安全管理要求》 实施日期：2019-07-01

26.GB/T 37095-2018 《信息安全技术 办公信息系统安全基本技术要求》 实施日期：2019-07-01

27.GB/T 37096-2018 《信息安全技术 办公信息系统安全测试规范》 实施日期：2019-07-01。

（来源：全国信息安全标准化技术委员会）

➢ 公安部发布《公安机关办理刑事案件电子数据取证规则》

2019 年 1 月 2 日，公安部发布《公安机关办理刑事案件电子数据取证规则》，新规则自 2019 年 2 月 1 日起施行。

规则总共四章，与此前的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》相互配套，为刑事案件中的电子取证提供了更为详细的指引。（来源：公安部）

- **《公安机关办理刑事案件电子数据取证规则》**
- **全文：**http://www.mps.gov.cn/n2254314/n2254409/n4904353/c6337154/content.html

➢ 国家网信办发布《区块链信息服务管理规定》

2019 年 1 月 10 日，国家互联网信息办公室发布《区块链信息服务管理规定》(以下简称“《规定》”)。国家互联网信息办公室有关负责人接受采访，就《规定》的相关问题回答了记者提问。

问：请您介绍一下《规定》出台的背景?

答：出台专门规范区块链信息服务的管理规定，主要基于以下三个方面的考虑。

一是深入推进网络信息安全管理的需要。《中华人民共和国网络安全法》、《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》已经颁布实施，明确规定了网络运行和信息安全管理以及新技术新应用安全评估有关制度要求。建立区块链信息服务备案管理制度，制定《规定》，是落实相关法律、行政法规，加强网络信息安全管理的需要。

二是促进区块链信息服务健康发展的需要。加强区块链信息服务管理、指导区块链信息服务提供者(以下简称“服务提供者”)履行备案手续是建立健全信息安全管理制度和技术保障措施的重要途径，有利于促进区块链技术及相关服务的健康发展。

三是区块链信息服务安全风险防范的需要。区块链技术快速发展，相关应用蓬勃涌现，

给国家经济社会带来巨大发展机遇，便利了人民群众的工作和生活，但同时区块链技术被一些不法人员利用，作为存储、传播违法违规信息，实施网络违法犯罪活动的工具，扰乱互联网信息传播秩序，严重损害公民、法人和其他组织合法权益，亟需依法推动服务提供者主动健全安全保障措施，提升安全风险预警防范效果。

问：《规定》中所指的区块链信息服务是什么？

答：《规定》中所指的区块链信息服务是指基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供信息服务。

问：《规定》中所指的区块链信息服务提供者是什么？

答：《规定》中所指的区块链信息服务提供者是指向社会公众提供区块链信息服务的主体或者节点，以及为区块链信息服务的主体提供技术支持的机构或者组织。

问：《规定》对服务提供者落实区块链信息服务安全主体责任作出了哪些要求？

答：《规定》对服务提供者主体责任进行了明确规定。主要包括：一是落实信息内容安全管理责任。二是具备与其服务相适应的技术条件。三是制定并公开管理规则和平台公约。四是落实真实身份信息认证制度。五是不得利用区块链信息服务从事法律、行政法规禁止的活动或者制作、复制、发布、传播法律、行政法规禁止的信息内容。六是对违反法律、行政法规和服务协议的区块链信息服务使用者，应当依法依约采取处置措施。

问：《规定》对服务提供者履行备案义务作出了哪些要求？

答：《规定》要求服务提供者应当在提供服务之日起十个工作日内通过国家互联网信息办公室区块链信息服务备案管理系统填报备案信息，同时明确备案信息审查、备案信息变更、备案编号标注、备案信息定期查验等相关事宜。

问：《规定》对服务提供者履行安全评估和配合监督检查义务作出了哪些要求？

答：《规定》要求服务提供者：一是开发上线新产品、新应用、新功能的，应当按有关规定报国家和省、自治区、直辖市互联网信息办公室进行安全评估。二是信息服务存在信息安全隐患的，应当进行整改，直至符合法律、行政法规等相关规定和国家相关标准规范后方可继续提供服务。三是记录备份应当保存不少于六个月，并在相关执法部门依法查询时予以提供。四是应当配合网信部门依法实施的监督检查，并提供必要的技术支持和协助。五是接受社会监督，设置便捷的投诉举报入口，及时处理公众投诉举报。

问：对违反《规定》要求的区块链信息服务提供者和使用者，有哪些处罚措施？

答：违反《规定》相关规定的，由国家和省、自治区、直辖市互联网信息办公室依据本规定和有关法律、行政法规予以相应的处罚;构成犯罪的，依法追究刑事责任。（来源：国家互

联网信息办公室）

- **《区块链信息服务管理规定》**
- **全文：**http://www.cac.gov.cn/2019-01/10/c_1123971164.htm

➢ 《网络短视频平台管理规范》《网络短视频内容审核标准细则》发布

2019 年 1 月 9 日，中国网络视听节目服务协会发布《网络短视频平台管理规范》及《网络短视频内容审核标准细则》。

两份文本从机构把关和内容审核两个层面为规范短视频传播秩序提供了依据。《网络短视频平台管理规范》对平台应遵守的总体规范、账户管理、内容管理和技术管理规范提出了 20 条建设性要求；《网络短视频内容审核标准细则》面向短视频平台一线审核人员，针对短视频领域的突出问题，提供了操作性审核标准 100 条。《网络短视频平台管理规范》及《网络短视频内容审核标准细则》的发布必将有助于进一步规范短视频传播秩序。（来源：中国网络视听节目服务协会）

- **《网络短视频平台管理规范》及《网络短视频内容审核标准细则》全文**
- http://www.csrc.gov.cn/pub/zjhpublic/zjh/201812/t20181221_348485.htm
- http://www.cnsa.cn/index.php/infomation/dynamic_details/id/68/type/2.html

五、本期重要漏洞实例

➢ Cisco Prime Infrastructure 信息泄露安全漏洞

发布日期：2019-01-10
更新日期：2019-01-11
受影响系统：
Cisco Prime Infrastructure
描述：

CVE(CAN) ID: CVE-2018-15457
Cisco Prime Infrastructure（PI）是一套通过 LMS 和 NCS 技术进行无线管理的解决方案。
Cisco Prime Infrastructure 在基于 Web 的管理界面存在跨站脚本漏洞，该漏洞源于程序没有充分的验证用户提交的数据。远程攻击者可通过诱使用户点击恶意制作的链接，利用该漏洞在受影响界面的上下文中执行任意脚本代码或访问基于浏览器的敏感信息
<*来源：vendor
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190109-cpi-xss
*>
建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190109-cpi-xss）以及相应补丁：
cisco-sa-20190109-cpi-xss：Cisco Prime Infrastructure Cross-Site Scripting Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190109-cpi-xss

➢ Adobe Connect 信息泄露漏洞

发布日期：2019-01-08
更新日期：2019-01-11
受影响系统：
Adobe Connect <= 9.8.1
描述：

BUGTRAQ ID: 106469
CVE(CAN) ID: CVE-2018-19718

Adobe Connect 是网络会议软件。
Adobe Connect 9.7.5 及之前版本，在实现上存在会话令牌泄露漏洞，成功利用后可导致敏感信息泄露。
<*来源：vendor
链接：https://helpx.adobe.com/security/products/connect/apsb19-05.html
*>

建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB19-05）以及相应补丁:
APSB19-05：Security updates available for Adobe Connect
链接：https://helpx.adobe.com/security/products/connect/apsb19-05.html
补丁下载：https://helpx.adobe.com/adobe-connect/release-note/adobe-connect-10-1-release-notes.html

➢ Microsoft Exchange Server 远程信息泄露漏洞

发布日期：2019-01-08
更新日期：2019-01-10
受影响系统：
Microsoft Exchange Server 2019
Microsoft Exchange Server 2016
Microsoft Exchange Server 2013
描述：

BUGTRAQ ID: 106437
CVE(CAN) ID: CVE-2019-0588
Microsoft Exchange Server 是一套电子邮件服务程序，它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。
Microsoft Exchange PowerShell API 在 calendar contributors 权限管理中存在信息泄露漏洞。远程攻击者可利用该漏洞查看日历通常隐藏的其他详细信息。
<*来源：Cameron Vincent
链接：https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/b4384b95-e6d2-e811-a983-
*>

建议：

厂商补丁：
Microsoft

Microsoft 已经为此发布了一个安全公告（January 2019 Security Updates）以及相应补丁:
January 2019 Security Updates：January 2019 Security Updates
链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0588

➢ Linux Kernel 'can_can_gw_rcv in net/can/gw.c' 本地拒绝服务漏洞

发布日期：2019-01-04
更新日期：2019-01-07
受影响系统：
Linux kernel <= 4.19.13
描述：

BUGTRAQ ID: 106443
CVE(CAN) ID: CVE-2019-3701
Linux kernel 是开源操作系统 Linux 所使用的内核。
Linux kernel 4.19.13 及之前版本，net/can/gw.c 文件的 can_can_gw_rcv 在实现中存在安全漏洞。攻击者可利用该漏洞造成系统崩溃。

<*来源：Muyu Yu
*>
建议：

厂商补丁：
Linux

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：
http://www.kernel.org/
https://bugzilla.suse.com/show_bug.cgi?id=1120386
https://marc.info/?l=linux-netdev&m=154651842302479&w=2

六、本期网络安全事件

➢ 涉嫌窃取近千政界人士信息德国 20 岁黑客遭逮捕

2019 年 1 月 9 日，据 The Verge 报道，一名 20 岁的德国学生承认泄漏了大约 1000 名政治家、记者和演艺人士的私人数据，因为他对这些人的“公开声明感到愤怒”。德国网络犯罪办公室检察官 Georg Ungefuk 告诉记者，警方于周日逮捕了这名未透露姓名的嫌犯并搜查了他的公寓。据报道，这名男子在审讯期间供认，称他没有出于政治动机而独自行事。

泄漏的数据是在 12 月持续公开的，但据报道当局上周才了解到这一情况。这影响了大约 1000 人，包括德国总理默克尔，众多说唱歌手和记者，以及议会中每个政党的成员，除了极右的德国选项党。根据《华尔街日报》报道，大部分泄露的信息都是联系方式和其他相对不敏感的数据。大约有 50 到 60 人的更多私密细节被泄露，包括银行账户报表，照片和聊天记录。

《卫报》提供了一些关于嫌犯的更多细节，Ungefuk 说这名嫌疑人没有正式文凭，但拥有“渊博的计算机知识”以及“广泛的兴趣和大量的时间。”调查人员据称在追踪“数字轨道”并联系后逮捕了他。据彭博社报道，他通过对其他案件提供某种帮助与警方合作。他们

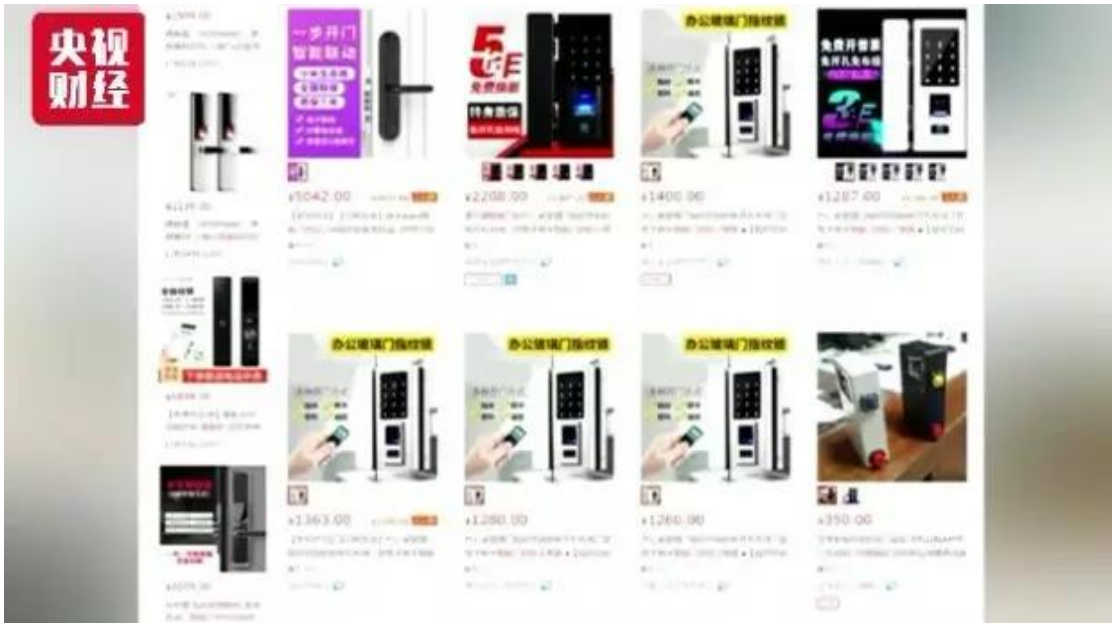
没有准确描述嫌疑人如何发现泄露的信息，除了暗示“非常简单”的密码使他的工作变得容易。

这种泄漏符合早期政治动机对包括德国在内的几个国家的攻击模式。那些与俄罗斯国家赞助的黑客有关。但 Ungefuk 表示“没有证据表明存在第三方的参与。”“被告表示，他的行动动机是出于对受影响的政治家、记者和公众人士的公开声明的愤怒，”据彭博社援引德国联邦刑事警察局的一份声明表示。然而，后果可能是广泛的，因为这次攻击加剧了人们对数据安全的担忧，并促使人们就更严格的隐私规则进行对话。“我们正在研究收紧法律是否有意义或是否必要，”德国司法部长卡塔琳娜·巴利（Katarina Barley）在回应泄密事件时表示。

（来源：The Verge）

➢ 40 款智能门锁 15%被轻易打开,抽检人脸识别开锁无一合格

2019 年 1 月 7 日，央视新闻报道智能门锁近几年逐渐进入越来越多的家庭，截至 2018 年 6 月底，我国智能门锁生产企业已超过 1500 家，2018 年预计销量 2100 万套。作为传统门锁的升级版，智能门锁是否更加安全?



《每周质量报告》的调查发现：

调查：“小黑盒”几秒钟能打开智能门锁：不久前，网传视频显示，有人用一个烟盒大小的盒子在几台智能门锁前来回晃动，几秒钟后，门锁就自动打开了。这个“小黑盒”真的这么神奇?

记者来到广州市区一个规模较大的五金建材批发零售市场，在一家店铺，销售人员介绍，主推的智能门锁两千多块钱，可通过指纹、密码、感应卡等多种方式开锁，安全性高。销售人员表示，他们的智能门锁绝对安全，包括“小黑盒”都打不开的。

风险监测：利用电磁场干扰电路 “小黑盒”开锁只需几秒

广州的国家通用电子元器件及产品质量监督检验中心，对全国范围内的智能门锁产品进行了一次风险监测。

质检中心专家 邵鄂：网上这个“小黑盒”，专业术语叫特斯拉线圈，只要按下按键，它就产生一个瞬间的电磁场。专家告诉记者，这个特斯拉线圈个头虽然不大，但是能够产生的电磁场强度却不小。记者注意到特斯拉线圈在开启时，瞬间产生的强大电磁场，能将节能灯泡点亮。

检测人员给记者演示了电磁兼容测试过程，利用电磁场干扰电路。当特斯拉线圈靠近一款正常工作的智能门锁附近时，门锁在几秒钟内自动打开。15%的门锁能被“小黑盒”打开：这次风险监测，分别从实体店及网络电商平台采集了 38 个品牌、40 款型号的智能门锁产品，涉及的标称产地有广东、浙江、福建等 7 个省市，除了 7 批来自实体店，其余 33 批次来自京东商城、天猫商城、苏宁易购等网络平台。

结果显示：四十个样品中，有 6 个批次被特斯拉线圈也就是所谓的小黑盒打开了，占比达到了 15%。专家告诉记者，解决这一问题在技术上并不难，只是成本会提高，目前市场上主流企业的产品已经解决了这一问题。

哪款智能门锁更不安全?

除了“小黑盒”的问题，这些智能门锁还有哪些安全风险?市场监管总局组织了涉及全国范围的智能门锁风险监测，共涉及识别方式安全、信息安全、电子安全和功能安全四个方面。

①指纹识别锁：存较高风险

质检中心专家 李乐言：采样 40 批次的智能门锁里，有 36 批次是具备这个指纹识别功能的，有 10 批次是存在风险隐患，风险程度比较高的。

专家演示：首先在智能门锁指纹识别区贴上一小块胶带，然后用已经录入指纹的手指进行几次开锁，随后找来 6 位不同年龄的没有录入任何指纹信息的检测人员逐一随机用手指尝试开启门锁，结果门锁都能开启。

②人脸识别锁：照片就能开

记者了解到，有人脸识别开锁功能的智能门锁同样存在较高风险，4 批次高端产品，不

合率 100%。4 批次产品存在的共同问题是无法准确分辨真实的人脸和面部照片的区别。

专家演示：通过相机拍摄同一个测试对象面部不同角度的照片，打印出黑白照片，利用这些不同角度的照片靠近智能门锁的摄像头前方进行测试，当使用这张正面的照片靠近摄像头某一位置时，门锁开启了。

③感应卡开锁：感应卡可被复制

这次风险监测中，30 批次有感应卡开锁功能的智能门锁，发现 28 批次有风险，占比 94%。专家将一张感应卡放进书包，同时打开手机 NFC 功能，也就是近距离无线通信功能。当这部手机靠近书包一定距离后，一组数据出现在手机上，据专家介绍，攻击者完全可以利用这些读取到的信息复制一张和书包里感应卡开锁信息完全一样的感应卡。

④远距离控制门锁：存信息安全问题

此外，一款智能门锁的 APP，专家通过简单操作后，不仅能远距离控制门锁状态，获取用户手机信息，甚至可以反向进入厂商服务器，获取大量使用该品牌智能门锁用户的手机信息。专家表示，有 10 批次远距离控制门锁产品，支持用移动应用远程控制，对门锁有进行开锁及查看记录的功能，其中，8 批次存在信息安全问题。

根据这次风险监测的结果，市场监管总局近日专门发布关于智能门锁质量安全消费警示：

- 建议消费者尽量不使用或关闭人脸识别功能和远程开锁功能，在日常使用中妥善保管好信息识别卡，防止被非法读取和复制。
- 在使用带有指纹识别功能的智能门锁时，建议消费者应在日常使用中留意指纹识别模块是否存在残留异物或物理损坏，若发现指纹识别模块出现异常，应立即停止使用指纹识别功能，并联系生产企业解决。（来源：央视新闻）

完整视频：https://v.qq.com/x/page/e08245ccony.html

➢ 国家税务总局：个人所得税 App 存在 62 例木马为误传

2018 年 12 月 30 日，根据国家税务总局官方微博的消息，经过调查，税务总局“个人所得税”App 存在 62 例木马为误传。官方称自税务总局官方“个人所得税”App 上线以来，未发现存在木马病毒问题。税务总局一直以来高度重视“个人所得税”App 安全，将继续采取各种手段加强安全监测和保护。

12 月 27 日，根据媒体的报道，个税 App 上线一天，就占据了安卓和苹果双榜第一。但是国内安全研究团队发现“个人所得税”App 被恶意广告木马盯上，12 月 27 号上线一天，就检测到 62 例伪装木马样本。

国家税务总局表示，自税务总局官方“个人所得税”App 上线以来，未发现存在木马病毒问题，并提醒纳税人，通过国家税务总局(www.chinatax.gov.cn)和各省税务局官网以及主要手机应用市场下载应用，并警惕来历不明的二维码链接。（来源：国家税务总局）

➢ 澳洲灾害早期预警网络服务系统遭黑客入侵

2019 年 1 月 8 日，澳洲灾害早期预警网络（EWN）服务系统遭黑客入侵，数万澳人接获预警系统发来的消息——EWN 遭攻击，个人数据不安全。昆州警方和澳洲网络安全中心（ACSC）已经开始调查这起事件。EWN 发言人表示，黑客有意毁坏 EWN 的名誉。

事故发生在上周六晚大约 9 点 30 分，黑客非法侵入系统后，利用电子邮件、手机短信和固定电话给系统订户发送了一条消息：“早期预警网络已经被骇，你的个人数据不安全。赶紧修复安全问题。”这条信息还向人们提供了取消订用预警服务的链接。

“早期预警网络的员工及时发现了攻击行为，立即关闭了系统，限制了发送出去的信息数量。但不幸的是，数据库中仍有一小部分人收到了这条信息。我们目前正在和警方合作来调查这起事件，并解决这一问题。”早期预警网络发表声明说。

经调查，早期预警网络周一再次发布声明说，上周六晚的非法入侵是一个未经授权的人所为，他使用非法获得的信息登录了预警系统，并发送了一条滋扰性的垃圾通知给部分用户。信息中包含的网络链接没有危害，用户的个人信息也并没有被泄露。

早期预警系统面向全澳，与当地政府合作，为民众提供恶劣天气及自然灾害预警。最近的一次预警是提醒悉尼居民留意他们当地潜在的危险雷暴。

该网络总经理普洛赖特（Kerry Plowright）表示，并不是所有的用户都受到了此次事故的影响，但那些受影响的用户包括地方政府、州政府和联邦政府机构。昆州受影响的地方政府已经在各自的社交媒体上向当地居民通报了入侵事件。

普洛赖特对澳洲广播公司说：“当这种事情发生时，我的心都要跳出来了。我想，喔，这是我能想像到的最糟糕的事情。”他还表示，早期预警网络只是一个小公司，名声就是一切，客户的信任极其重要。他说，公司会尽一切努力，防止此类事件再次发生。（来源：大纪元）

➢ 买机票后被骗十余万:个人信息疑遭泄露携程被判赔 5 万

2019 年 1 月 3 日，申女士通过携程购买机票后收到航班取消退费短信，骗子通过详尽的个人信息骗取了申女士信任，一天内将 10 余万元转账到骗子账户。申女士认为携程未尽到安全保障义务，导致其身份信息及订票信息泄露，支付宝未依法实施注册实名制，存在漏洞，将上海携程商务有限公司(以下简称携程公司)、支付宝(中国)网络技术有限公司(以下简称支付宝)以侵权责任纠纷诉至法院，要求两公司连带赔偿经济损失并赔礼道歉。近日，北京市朝阳区人民法院认定携程公司在信息安全管理方面存在漏洞，未尽到对个人信息负有的信息保管及防止泄露义务，判决携程公司赔偿申女士经济损失 5 万元并向其赔礼道歉。

在携程买机票落入骗局，个人信息疑遭泄露起诉索赔

2017 年 8 月 9 日零时许，申女士通过携程公司 APP 为同事订购东方航空公司承运的两张联程航班机票。首乘飞机起飞前申女士收到+85295672718 号码向其订购机票所留的手机号发送的短信，短信内容为**“尊敬的旅客：你好!您原订于 2017 年 8 月 10 日航班因起落架**

故障已被取消。请及时致电客服 008617710402984 办理改签或退票。 [东方航空]”。

申女士称其按照短信提示拨打了“客服电话”，“客服”准确地说出了乘机人信息，并再次告知申女士因航班取消需退款 1250 元，“客服”向申女士提出通过支付宝或微信途径退款，申女士将其支付宝账户提供后，“客服”以无法操作为由向申女士提出以更为快捷的支付宝亲密付方式支付。申女士遂开通支付宝亲密付功能，申女士通过其绑定在支付宝的中国工商银行账户以支付宝亲密付方式分四次向支付宝会员“开通航空服务”付款共计 19008.99 元。

申女士称其看到工商银行提示短信后，挂断“客服”电话欲与工商银行核实时，“客服电话”回拨给申女士并表示因申女士挂断电话影响后台操作，导致申女士的上述款项被划走，现需要将划走的款项转回给申女士，因亲密付有限额，需要用申女士的网银转账，后申女士到楼下的工商银行柜台开通了工商银行手机银行、网上银行。按照“客服”的要求分两次共计转账 99976 元，因仍未收到退款，申女士意识到被骗。后申女士向派出所报案，目前该刑事案件尚未侦破。

申女士认为，携程公司作为专业的机票代理机构，未尽到安全保障义务，导致其身份信息及订票信息泄露，使得诈骗分子能够依此获取其信任，导致损失发生，携程公司在安全措施上存在重大疏漏，其基于携程公司违反安全保障义务要求携程公司承担相应的赔偿责任。支付宝公司作为专业的第三方支付公司，未按照国家相关法律实施注册实名制，支付宝软件亦存在缺陷，在其亲密付支付功能中未尽到充分的风险提示义务，导致诈骗分子能够以所谓“开通航空服务”的名义与其进行交易，获取其信任最终导致其发生经济损失，亦应承担相应的赔偿责任，故诉至法院，要求携程公司、支付宝公司公开赔礼道歉，连带赔偿经济损失 118900 元、精神损害抚慰金 1 万元。

法院：携程未尽保管防泄义务，支付宝与受骗无因果关系

庭审中，携程公司提交的 2018 年敏感信息管理规则显示，订单信息属于一级信息，内部传输可不加密。携程公司未向法庭提供内部员工授权进行访问涉案订单的人员范围、访问敏感信息的授权记录、监控情况、操作记录、内外部传输审批情况的相关证据。在携程应用界面及短信确认内容中也没有充分明显地告知消费者对于航班信息诈骗的注意。

法院认为：携程公司在信息安全管理的落实方面存在漏洞，未尽到对个人信息负有的信息保管及防止泄露义务，具有过错，应承担侵权责任。因携程公司违反了网络运营主体的安全保障义务，存在个人信息保护上的安全维护漏洞，导致申女士遭遇诈骗形成财产损失。法院综合案情及携程公司的过错责任程度，酌情确定携程公司在 5 万元赔偿数额的范围内对

申女士承担补充责任。

庭审中出示证据显示，在申女士主张的 11 万余元损失中只有近 2 万元是通过亲密付支付，支付原因是申女士在陷入骗局时比较着急，无视支付宝的多次提示，没有尽到核实交易相对公司的谨慎义务。剩余 9 万余元，是申女士在其陷入骗局后在工商银行转账的款项，即使没有亲密付，申女士也会转账该 9 万余元，支付宝对于上述所有财产损失不具有任何过错和侵权行为。

法院认为，从已有证据来看，申女士因受骗先后开通了支付宝亲密付功能和工商银行手机银行功能并转款，虽然支付宝亲密付的授权消费对象没有实名制，但在手机银行功能存在实名制以及支付宝、手机银行均对申女士进行了开通提示的情况下，申女士仍完成了转账行为。因此可看出，在该过程中申女士受骗原因是其过于轻信和轻率的思想状态，而与是否实名制及是否尽到风险提示义务并无直接因果关系。故在本案中申女士请求支付宝公司承担侵权责任，法院不予支持。

法官说法：电商平台、网络服务提供者应承担安全保障义务

第一，携程公司在提供网络服务的过程中，通过对用户数据的搜集和维护，获得了巨大的财产收益，从危险中获取利益者应负担制止危险的义务。因此，携程公司作为网络服务提供者既然从自己架构的数据系统中获得了利益，就应当对系统危险隐患所造成的损害后果承担责任。携程公司作为知名旅行产品网络服务提供者，已成为大数据时代的主要个人信息处理者，其对个人信息的处理包含了从信息被收集，到被处理和利用，再到传递等一系列行为，其商业行为的获利模式亦主要在于信息的处理与传递。因此，携程公司对于申女士订票所生成的个人信息负有信息安全保管及防止泄露、控制危险的义务。

第二，从电商平台的运营模式来看，用户对电商平台保障其消费流程的数据安全具有合理的信赖，基于网络环境下的基本安全需求，实际已经形成了用户预期免受第三人侵害的合理信赖利益，因此从保护用户信赖利益的角度出发，法律也应对电商平台提出安全保障的义务。本案中，申女士正是对携程公司不会违法向第三人泄露机票行程信息的状态产生了合理的信赖，才会对诈骗分子形成轻信，进而导致了财产损失。

第三，通过攻击或利用系统安全漏洞实施的侵权行为，具有发生的经常性和影响的广泛性特点，而网络服务提供者作为系统安全的直接维护者和受益者，对于这类行为无论是在反应机制和技术储备，还是人力财力的支持，都具有高度的应对便利和条件，因此对网络服务提供者规范其安全保障责任，将最有利于被侵权人得到合理的救济，也最符合侵权法的整体效率的实现。在此类案件中，赋予网络服务提供者安全保障义务，无疑将推动网络运营主体

进行协助追查和收集证据，并提高网络运营主体的防范意识和手段，从而使受害人获得救济的可能性大大提高。（来源：人民法院报）

➢ 470 余万条疑似 12306 用户数据遭贩卖嫌疑人被刑拘

2018 年 12 月 28 日，北京市公安局网络安全保卫总队(以下简称网安总队)工作中发现，网传有人利用互联网贩卖 470 余万条疑似 12306 铁路订票网站的用户数据，引发社会广泛关注。中国铁路总公司官方微博回应“网传信息不实，12306 网站未发生用户信息泄露”。

获此情况后，网安总队立刻会同西城分局成立专案组开展工作。经查，一网络用户“deepscorpions”在网上贩卖疑似 12306 铁路订票网站的用户数据，包含 60 余万条用户注册信息和 410 余万条铁路乘客信息。经专案组网上侦查、溯源追踪，成功锁定犯罪嫌疑人为北京市西城区某科技有限公司员工陈某(男，25 岁，河北省邢台市人)，后于 29 日在该公司所在地将其抓获归案。

经讯问，陈某供述 60 余万条用户注册信息，系其前期在网上非法购买所得，并非通过对 12306 官方网站技术入侵获取。其余 410 余万条铁路乘客信息，系其利用上述用户注册信息，通过第三方网络订票平台非法获取。目前，嫌疑人陈某因涉嫌侵犯公民个人信息罪被西城分局刑事拘留。案件正在进一步审理中。（来源：首都网警）

信息安全意识产品免费大赠送

isa@spisec.com