国盟信息安全通报

2019 年 7 月 08 日第 196 期

国盟信息安全通报

（第 196 期）

国际信息安全学习联盟

2019 年 7 月 08 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 201 个，其中高危漏洞 72 个、中危漏洞 86 个、低危漏洞 43 个。漏洞平均分值为 6.23。本周收录的漏洞中，涉及 0day 漏洞 69 个（占 34%），其中互联网上出现“Creatiwity wityCMS SQL 注入漏洞、Quadbase Systems EspressReport ES 跨站请求伪造漏洞”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 2575 个，与上周（1736 个）环比增长 48%。

主要内容

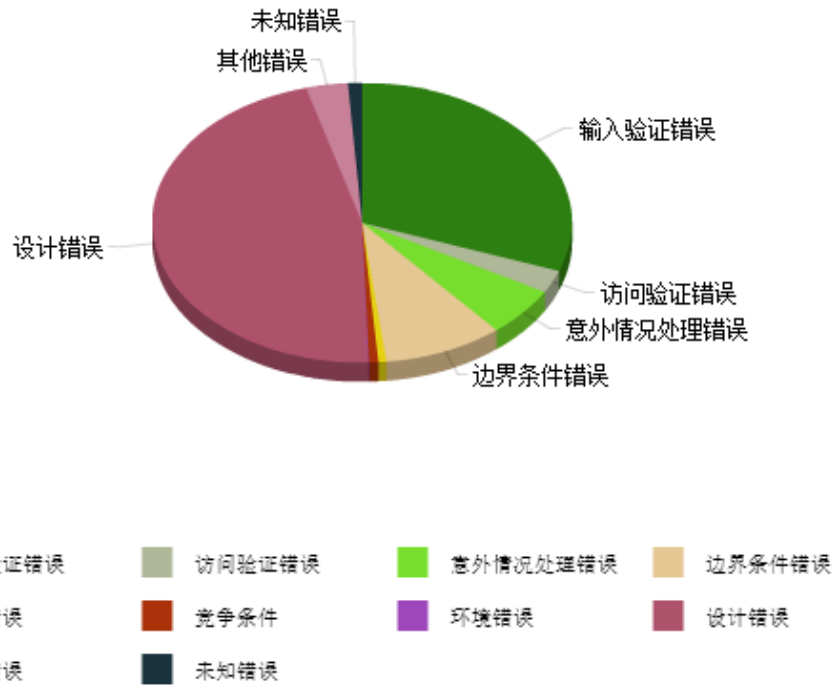
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

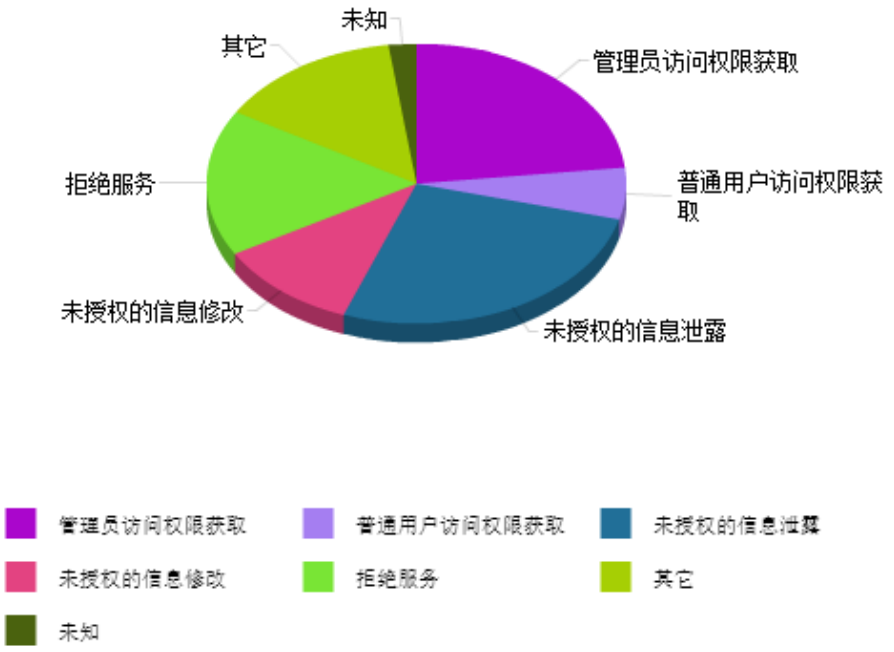
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 201 个，其中高危漏洞 72 个、中危漏洞 86 个、低危漏洞 43 个。漏洞平均分值为 6.23。本周收录的漏洞中，涉及 0day 漏洞 69 个（占 34%），其中互联网上出现“Creatiwity wityCMS SQL 注入漏洞、Quadbase Systems EspressReport ES 跨站请求伪造漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2575 个，与上周（1736 个）环比增长 48%。

二、安全漏洞增长数量及种类分布情况

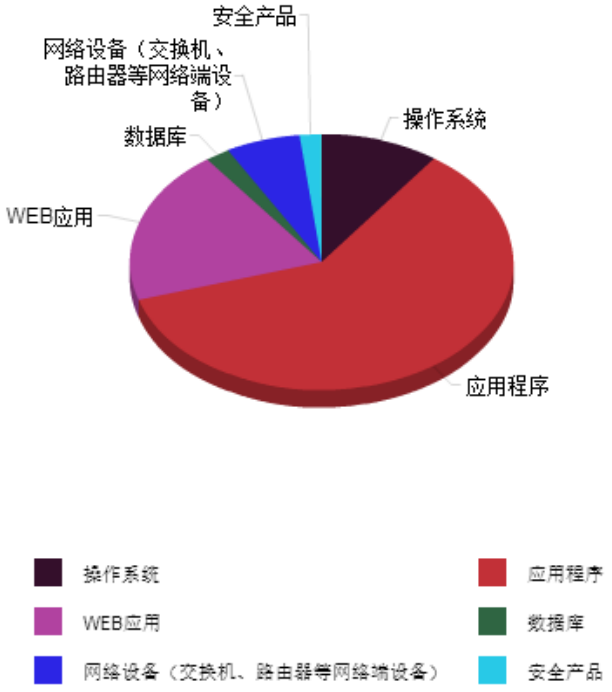
➢ 漏洞产生原因（2019 年 6 月 24 日—2019 年 7 月 8 日）



➢ 漏洞引发的威胁（2019 年 6 月 24 日—2019 年 7 月 8 日）



➢ 漏洞影响对象类型（2019 年 6 月 24 日—2019 年 7 月 8 日）



三、安全产业动态

➢ 树立正确网络安全观的基本路径

“没有网络安全就没有国家安全。”网络安全是国家安全的重要组成部分，是国家安全的基础。维护网络安全，必须树立正确的网络安全观。这是我们党领导全国人民实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要组成部分。树立正确的网络安全观，必须加强党的领导，必须依法治理网络空间，必须依靠人民群众，共筑网络安全防线。这是树立正确网络安全观的必由之路。

加强党的领导是树立正确网络安全观的根本

习近平总书记强调，党政军民学，东西南北中，党是领导一切的。中国共产党是中国特色社会主义事业的坚强领导核心，是最高政治领导力量。只有坚持党对一切工作的领导，才能在更高水平上实现全党全社会思想上的统一、政治上的团结、行动上的一致，进一步增强党的创造力、凝聚力、战斗力，为夺取新时代中国特色社会主义伟大胜利提供根本政治保证。网络安全也是一样。网络安全是综合性、全面性、整体性的安全。它包括政治、经济、军事、文化和社会等国家安全的各个方面。正如习近平总书记所说的“网络安全对国家安全牵一发而动全身”，同许多其他方面的安全都有着密切关系，是关系国家安全和国计民生的重大问题。

新形势下的网络现状，尤其需要加强党对网络安全的领导。网络信息流的巨大快捷便利，

给我国发展带来了难得的机遇。同时，网络安全的复杂性，使得国家安全面临着种种挑战和风险。从国内讲，我国经济社会改革已经进入深水区，随之而来的社会经济快速转型、社会结构深刻变动，使利益格局发生着新的调整，意识形态领域存在着激烈的碰撞。传统安全与非传统安全相互交织，网络信息安全、生态安全、金融安全、能源安全、科技安全、食品安全等风险时隐时现，人民群众面临的安全风险呈现多样化常态化。从世界范围讲，民族宗教矛盾、恐怖主义、气候环境安全、能源安全等风险明显上升。特别是个别西方大国大搞单边主义，利用网军，造谣生事，不断制造事端，妄图遏制我国发展。当前国内安全和国外安全错综交织，国际环境的变化对我国的影响日趋激烈。各种风险的发生具有突发性和叠加性，风险发生的后果具有系统性和巨大破坏性。网络安全的地位和网络安全风险的复杂性都充分表明，树立正确的网络安全观，必须坚持以习近平新时代中国特色社会主义思想为指导，坚持集中统一高效权威的网络安全领导体制，在重大网络安全风险上更好发挥党的统一领导作用，不断增强网络安全保障能力和综合治理能力，确保国家长治久安。

依法治理是树立正确网络安全观的保障

全面依法治国是网络安全的重要保障。党的十八大以来，习近平总书记围绕全面依法治国提出了一系列新理念新思想新战略，涵盖了新时代我国法治建设的性质方向、根本保障和总目标、总路径、总任务、总布局，回答了我国法治建设的一系列重大问题，为加快建设社会主义法治国家提供了根本遵循。我们在网络治理中，“要坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行”。

法律是治国重器，法治是国家治理体系和治理能力的重要依托。我国已经颁布实施了《网络安全法》，它对网络信息、网络运行和信息基础设施安全等方面做了详细规定。同时，国务院、国务院各部门以及各省市自治区还分别出台了一系列行政法规、部门规章及地方政府规章。如《中华人民共和国电信条例》《互联网信息服务管理办法》《互联网域名管理办法》《区块链信息服务管理规定》以及《微博客信息服务管理规定》《互联网群组信息服务管理规定》等，网络信息领域的法律体系正在不断完善之中，为维护网络安全奠定了法治基础。

“网络空间不是‘法外之地’。”对于网络空间的违法犯罪行为，必须违法必究，执法必严。随着互联网的飞速发展，网络安全问题日益凸显，利用网络进行违法犯罪活动形势不容忽视。我国自接入国际互联网以来，国际上反华仇华势力不断对我国进行网络攻击，污蔑我国网络法律制度；国内一些不法分子，也不断利用网络进行犯罪活动，污蔑、造谣，散布种种不良信息，毒化社会风气，扰乱社会秩序。维护网络安全刻不容缓！在维护网络安全的各种手段中，推进网络空间法治化是根本保障。习近平总书记指出：“中国是网络安全的坚定

维护者。”只有对各种违法犯罪活动依法给予制裁，对人民行使网络权利依法予以保护，网络秩序才能好，社会风气才能正。

依靠人民是树立正确网络安全观的基石

习近平总书记指出：“网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。”依法治网，归根到底，是为了保护人民安全行使网络自由的权利，给人民创造一个广阔、明亮、安全、自由的网络空间，最大限度地满足人民精神需求，这是树立正确网络安全观的出发点和落脚点。

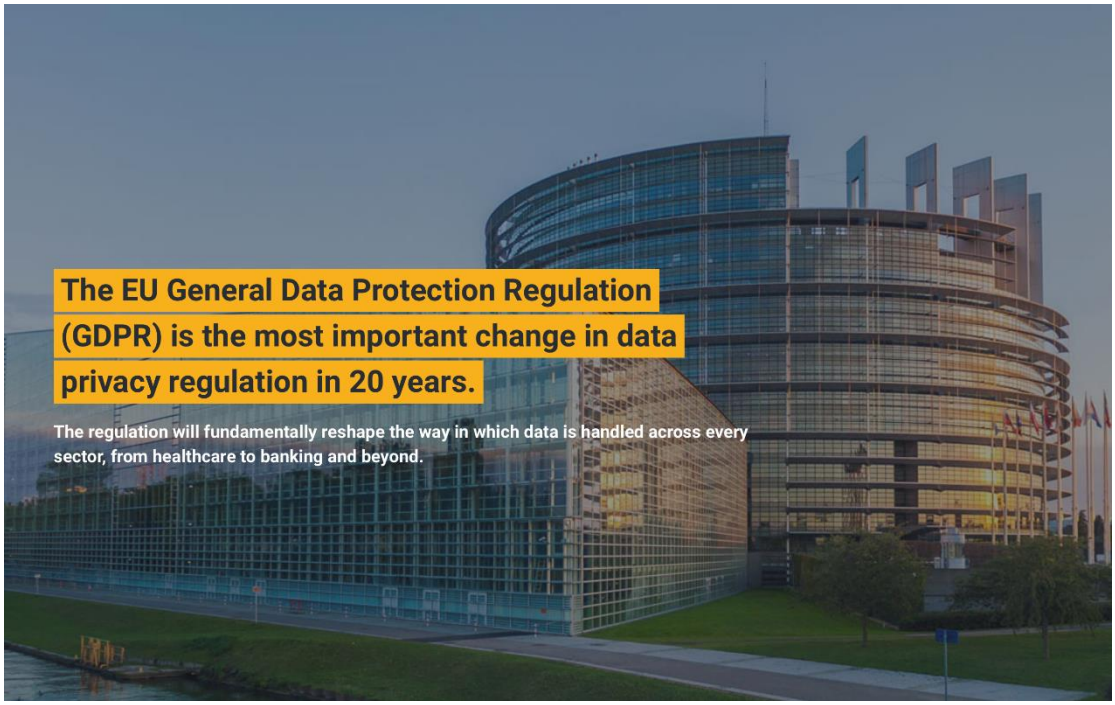
树立正确的网络安全观，必须坚持人民主体地位。人民是历史的创造者，是决定党和国家前途命运的根本力量，也是维护网络安全的基石。网络安全工作的根本在于扎根网络群众。网络安全为人民，网络安全靠人民。维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。在网络治理过程中，各地各部门应本着对社会负责、对人民负责的态度，坚持走网络群众路线，发动群众、组织群众，积极培育网络安全意识，创造更多“与网民共建”的好经验。实践证明，只有把党的群众路线贯彻到网络治理的全部活动之中，网络治理才能落地生根，才能构筑起国家网络安全的坚固长城。

总之，确保网络安全，就必须树立正确的网络安全观，构筑好网络安全屏障，将维护网络安全的各项具体举措落到实处。为此，我们必须以习近平新时代中国特色社会主义思想为指导，加强党中央对网络安全工作的集中统一领导，确保网络安全事业始终沿着正确方向前进，在奋力推进网络强国建设中更好实现亿万人民的伟大梦想。（来源：　光明日报）

➢ 《数据安全管理办法》对我们来说意味着什么？

2018 年 3 月，Facebook 剑桥分析事件的爆出，一把扯下了科技公司各自在用户数据保护方面披上的遮羞布。随后 5 月，欧盟正式开始执行“史上最严的数据隐私保护法案”《通用数据保护条例》（GDPR），更是把关于数据隐私的讨论推向了巅峰。

无论是连番的数据泄漏丑闻还是各国政府和机构组织的纷纷表态，2018 年一整年，隐私和数据安全都是一个绕不开的话题，公司和用户都不得不开始重视它背后的经济效益、利用关系以及个人权利。



据中国互联网网络信息中心的数据显示，截至 2018 年底，中国网民达 8.29 亿，手机网民 8.17 亿。在这个背景下，无论是对管理者的要求还是民意的诉求，数据安全管理规章化不可避免。

2019 年 5 月 24 日，国家网信办联合国家发改委等 12 个部门起草了《网络安全审查办法(征求意见稿)》（以下简称《办法》）。四天后，5 月 28 日，中国国家互联网信息办公室（以下简称“网信办”）发表《数字安全管理办法（征求意见稿）》，发布《数字安全管理办法（征求意见稿）》，向社会公开征求意见。6 月 28 日，《数据安全管理办法》的意见反馈正式截止。

《办法》只针对“网络运营者”，要求它们保护国家、社会、个人在网上的信息和数据安全，包括个人要给企业多少数据，哪些不必再给，企业无权再要；企业要如何保护用户个人数据，如何利用和处理已有的数据，在何种情况下把用户数据交与政府；政府如何监管企业不滥用个人数据。在《办法》出台之前，因为此前条例的模糊性，网络运营者得以钻了数据收集的漏洞。现在，《办法》就个人隐私和数据收集、广告和新闻精准投放、app 和平台对权限的无理索求以及账户、平台在停用后数据归宿等近几年来多发的数据隐私争议点上作出了明确地要求，《办法》也可能将成为中国首个围绕网络安全和数据管理落实的规章。

堵上所有能钻的空子

近几年的移动应用的普及，新入网用户激增，但同时，零基础直接上手的移动互联网用户对数据和隐私的权利概念模糊，绝大多数用户在这方面意识薄弱，因此导致了不少互联网公司肆意收割数据的现状。在五章四十条的《办法》中，有诸多条例都体现着对当前互联网

乱象的“对症下药”。

•《用户协议》要“说人话”

每当用户注册一个新网站的账号时，总是习惯把那些长篇累牍的《平台数据手机条约》一拉到底，点击同意。对此，《办法》第二章第八条要求：收集使用规则应当明确具体、简单通俗、易于访问，并给出了九小点的“具体要求凸显的条例”。**对运营方面向用户的条款作出明确规定：**第八条 收集使用规则应当明确具体、简单通俗、易于访问，突出以下内容:

（一）网络运营者基本信息;

（二）网络运营者主要负责人、数据安全责任人的姓名及联系方式;

（三）收集使用个人信息的目的、种类、数量、频度、方式、范围等;

（四）个人信息保存地点、期限及到期后的处理方式;

（五）向他人提供个人信息的规则，如果向他人提供的;

（六）个人信息安全保护策略等相关信息;

（七）个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法;

（八）投诉、举报渠道和方法等;

（九）法律、行政法规规定的其他内容。

换句话说，满篇堆砌法律名词，用尽各种语言技巧的“数据收集条约”将被取缔。尽管用户和平台之间“不同意就不能用”的协议不会改变，但平台必须让用户明确地知晓数据收集的意图，或者说用户自己使用服务的代价。

• 用不到的信息不许强行收集

在第十一条中，《办法》明确规定了“网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。”

即网站和应用用不到的信息，运营方不能强行收集，更不能因为用户不同意提供这些“用不到”的信息，就拒绝提供服务。系统层上，苹果在 iOS12 和 iOS13 的更新中也作出了类似的规范和限制。

• 拒绝大数据杀熟

在十三条中，《办法》则规定了禁止对个人信息分析后进行定价歧视，此举也明显针对的就是去年国内频繁曝出的“大数据杀熟”现象。

• 治理垃圾推送消息

在《办法》第三章《数据处理使用》中第二十三条规定，运营者利用用户数据和算法推

送新闻信息、商业广告等，应当以明显方式标明“定推”字样；要对用户提供停止接收定向推送信息的功能，并且当用户关闭该功能后，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

• 标注机器生成内容

随着人工智能的愈发成熟，机器替代人工回复消息甚至生产内容正在慢慢成为一种趋势。比如前几年开始在社交网络上流行的各类 bot 就属于该类，各类服务中的自动客服回复和智能助手也可归为该类。在《办法》第二十四条规定，利用大数据和人工智能合成的新闻、博文、帖子、评论等信息，应以明显方式表明“合成”字样。

• 设立“数据安全负责人”职位

《办法》中也要求网络运营方要有“数据安全负责人”职位，这个职位要求有数据安全专业知识的人员担任，专员需要参与有关数据活动的重要决策，且运营方要保证这个职位“独立履行职责”。

• 对已有数据的保护

《办法》第三章规定，如运营方被兼并或破产，所拥有的数据要么交接要么删除，不得保留；个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，及时告知用户并向网信部门报告。

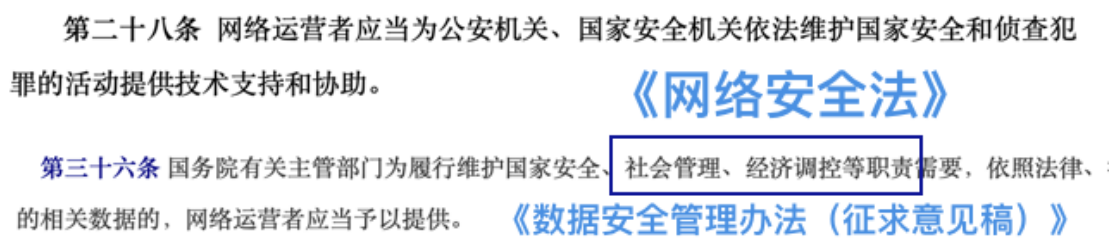
网络运营者在用户注销账号后应当及时删除其个人信息，保存个人信息也不应超出收集使用规则中的保存期限，继要求运营方“只收集最必要的，有期限的保留，且当用户要求平台方删除或离开平台后，运营方要主动删除用户数据。”

• 强制“溯源”

《办法》中还规定“对于用户通过社交网络转发他人制作的信息，应自动标注信息制作者在该社交网络上的账户或不可更改的用户标识。”换言之，这是一种强制“溯源”，新浪微博在最新版本更新中加入了标注“博主”的功能，可以在评论区中明显辨认出“原博”。但该条例规定的则是在社交网络中常见的“转发链条”里，无论多少人转发，社交网络平台需要对“原博”作出不可更改的标注。此规定的前提，是网络运营者要督促提醒用户对自己的网络行为负责、加强自律。

在“大数据杀熟”、个人信息被贩卖、私密信息被盗用或流传、注销删除账号难、商业广告和新闻推送霸屏的当下，《办法》对网络运营方作出了诸多规定，并且将执法部门从中央下发至“地（市）及以上网信部门”，这将使执法难度下降，用户更易维权，这无疑是数据保护上的提升。但另一方面，《办法》中许多条例的模糊性也容易使得网络运营方明确知

晓自己的义务，但个人用户却不知自己有何权利。同时，对网络运营方数据管理的要求也是双向的，一方面个人用户将更“被动地”保护自己数据，另一方面，政府也更“主动地”对运营方提出了数据审查要求。



变化内容

《办法》是中国版 GDPR 吗？

虽说《办法》有望成为中国首个围绕网络安全和数据管理落实的规章，从内容上也是政府站在用户角度，对网络运营方就用户数据作出收集、处理、删除等各个环节的要求。

《办法》发布之后难免被拿来与 GDPR 相比。两者相同之处颇多。

两部法案都提到了数据保护官类似岗位的设置；数据在泄露后，运营方告知用户的职责；也对国际间数据转移作出了要求，GDPR 仅允许数据控制者将数据转移到欧洲经济区 EEA 以外的、当地法律已被欧盟批准为充分保护的国家或地区，中国并未在此名单中，GDPR 的目的更倾向于“把数据放在有法律监管的地区”，换言之，你不能把 GDPR 范围区的数据转移到非范围区的地方，然后再故技重施滥用数据。

又比如，对企业不能再使用难以理解的冗长语言来让用户签订隐私政策；用户对自己数据的“被遗忘权”，在主动提出删除账户后，运营方对过往数据不再有保留权等。

还有一些问题，GDPR 和《办法》有共同认识，但实施做法和思路不尽相同。

《办法》对境内境外数据流通做出要求的目的就不同于 GDPR。《办法》要求网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；境内用户访问境内互联网的，其流量不得被路由到境外。此规定是为了防止潜在的流量劫持。

另一方面，横向对比两部法案，GDPR 比《办法》会更细致一些，GDPR 是站在用户一方，对数据收集方提出了在当下的“数据隐私权”以及维护这一权利所建立起的法律保护框架。而《办法》则更多地是针对数据的提供者和使用者要如何对待数据。

从两部法案的保护主体个人用户的角度来看，GDPR 给予了个人用户对其数据更大的控制权，并明确了这些权利，而《办法》则更强调给予用户“知情权”，运营方像是在被《办

法》推着走，而非被用户监管和维权。在个人敏感数据方面，GDPR 给出了七类可视为个人敏感数据的数据类型，从种族民族性取向到个人生物识别技术和基因数据都在这个范围内，《办法》中则并未详细展开“个人信息”的覆盖数据类型。而用户，也就是 GDPR 中所提到的“数据主体”，GDPR 中用了三个章节详细阐述了数据主体对数据的知情权、访问权、更正权和可携权、删除权、限制处理权、反对权和自动化个人决策相关权利。这些权利在《办法》中不难找到对应的法规，但个人用户到底对自己的数据有哪些权利，这是在《办法》中并未明晰的。

在 GDPR 中，还用了大量的篇幅来传递一个概念：“意愿”。GDPR 要求用户要在意愿自由、不存在被胁迫或欺诈、知情权明确、运营方提供给用户的信息明确到用户都不能轻易忽略……诸多前提条件后，用户按下的“同意协议”才是真的“同意”，才会真正从法律层面让协约生效。这个同意不能有任何不明确的空间，只要用户还对协议有合理的怀疑，就判定用户的意愿不明确。

而后 GDPR 还就“同意意愿”分为了儿童对同意的判断、有效同意的要件、同意的法律框架等做了更详细的要求和阐述。用户意愿是 GDPR 中的一个高频词，而在《办法》中，更多出现的则是“要求运营方”。

尽管在《办法》最后规定，若网络运营者违反《办法》，将面临公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。但用户通过何种途径可以得知平台滥用数据，得知后如何投诉举报立案，对运营方的惩罚措施和力度等细节都并未在《办法》中得到具体说明。

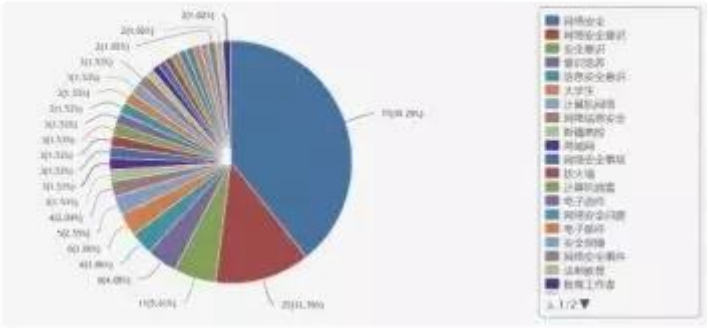
无论《办法》如何落地，至少表达了一个信号：运营者必须重视数据安全和用户个人隐私管理。对用户来说，也不是有了法规就万事大吉。保护个人数据隐私，无论对于个人、企业还是政府，仍旧是一个漫长且艰巨的博弈过程。（来源：GeekPark）

➢ 网络安全意识研究综述

随着信息化的深入发展、互联网对社会生活的全面渗透，网络环境日益复杂多变，信息系统的脆弱性也逐渐凸显，而网民的网络素养仍处于较低层次，这些因素共同决定了网络威胁的客观存在。技术层面讲，网络安全是一种相对的安全，并不存在一劳永逸的技术，所以增强用户的网络安全意识就成为了实现网络安全的重要措施。欧洲网络信息安全局在一份题

为《提高信息安全意识》的文件中指出，大量研究表明，在所有的信息安全系统框架中，人这个要素往往是最薄弱的环节。只有革新人们陈旧的安全观念、提高认知水平与认知能力，才能真正抵御网络威胁。因此，如何提高网络安全意识等问题逐渐进入了学者的视野。

图 1 网络安全意识相关文献主题分布



在中国知网数据库中以篇名为“网络安全意识”为检索条件对 2000 年以来的期刊、硕博论文、会议论文、报纸进行检索，共获得中文文献共有 111 篇（截至 2019 年 1 月 15 日）。从总体趋势来看，2000—2014 年文献数量相对较少，2015 年开始明显增加，主题分布主要包括网络安全、网络安全意识、安全意识、信息安全意识等。

一、网络安全意识的相关概念研究

尽管网络安全意识研究的重要性已经被学界认同，也经常作为重要概念出现在研究中，但并没有清晰、系统性的理论发展脉络与明确的概念界定。网络安全是网络安全意识的目标与来源，而网络安全风险决定了网络安全意识的具体内涵。因此，本文总结了现有研究中关于“网络安全”与“网络安全风险”的相关研究，试图厘清网络安全意识这一概念的界限并明确其内涵。

早期的网络安全主要指数据内容安全、信息系统安全、网络结构安全等。在网络作为信息工具的时代，网络安全可以理解为传统的信息安全，强调信息（数据）本身的安全属性，包括信息的秘密性、完整性和可用性。2004 年，李炅等人提出，网络安全是一个系统性的概念，不仅包括计算机上信息储存的安全性，还要考虑信息传输过程的安全性，即通信安全和主机安全共同构成了网络安全。全面聚焦电子商务面临的网络安全威胁，将网络安全目标的最小集合总结为身份真实性、信息机密性、信息完整性、服务可用性、不可否认性、系统可控性、系统易用性、可审查性。何德全提出，人是网络发展的基本动力和信息安全的最终防线，所以网络安全机制要面向用户，保障用户的网络应用。可见，虽然这个时期也有学者意识到“人”作为主体的重要性，但没有将“人”放在网络安全概念的核心位置进行深入研究。如今，网络安全的内涵正在不断变化，从最初的硬件安全扩展到包括全球、国家、社会、

个人在网络空间中的安全状态。安静指出，目前，个人网络安全的重要性明显提升，这种个人的网络安全可以从个人财产安全、个人人身安全、个人心理安全三个方面来认识。

时至今日，互联网的作用早已超出了工具范畴，逐渐成为一种社会空间。随着相关领域研究的深入，网络安全的内涵也得到了丰富和扩展，与相关概念“信息安全”之间的关系辨析进入研究视野。张焕国认为，网络安全应当包含设备安全、数据安全、内容安全和行为安全四个层次，提出网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境的信息安全。然而，目前学者对于信息安全问题的研究已经不再局限于个人隐私，也涉及商业机密和国家安全的各个方面。例如，黄奕信结合国情将信息安全定义为保证信息主体（国家、组织和私人）的信息不受到内部和外部的威胁、侵害以及误导，确保信息的独立性和隐私性。正是由于“信息”这一概念的扩展，所以也有学者对上述分类持不同观点，刘仁认为网络安全的内涵比信息安全的内涵要狭义，因为信息的概念比较宽泛、更多元化，而网络安全是从网络环境出发，只需要保证使用者在网络环境中的信息得到保护，处于安全状态即可，故更多的是设计网络层面上的信息数据安全。可见，虽然学界对于“信息安全”与“网络安全”的范围存在争议，但不可否认的是，对于传统信息安全领域的研究奠定了如今网络安全研究领域的发展基础。

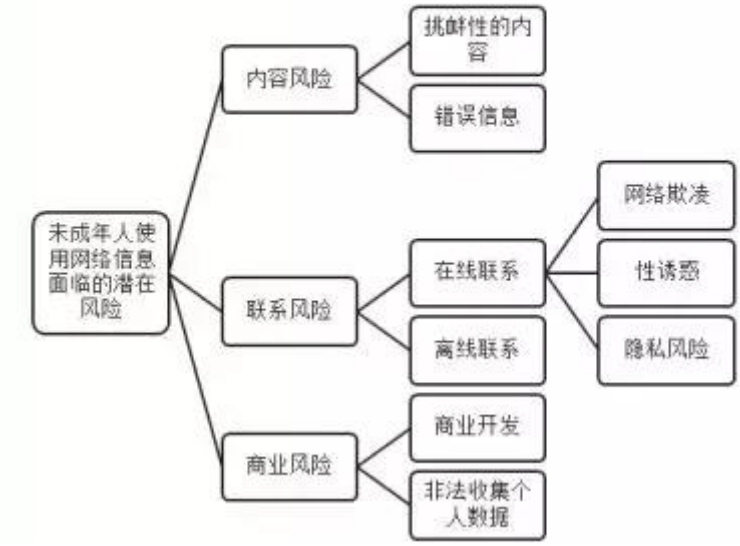
互联网的基本特点是全球性的广泛连接，这种广泛连接使信息资源的作用得到了充分的发挥，但也不可避免地导致了众多不安全因素的进入，这些网络安全风险决定了网民应当具备的网络安全意识的基本内容。因此，关于网络安全风险的研究成果对梳理网络安全意识的内涵具有重要意义。

在早期的研究中学者认识网络安全风险的主要视角为信息系统和网络本身的安全性，认为网络安全威胁主要来源有恶意攻击、安全缺陷、软件漏洞、结构隐患等几个方面，威胁产生的主要原因包括人为故意、偶然失误、自然灾害等。相应地，这一时期的研究热点包括新型加密技术、入侵检测 IDS、病毒识别与清除技术等，着力提升网络信息、网络数据安全的发展。目前，网络环境中的不安全现象除了包括上述技术方面的客观安全威胁，还包括主要受个人主观因素影响的网络诈骗、个人信息泄露、网络暴力、网络谣言、网络成瘾等问题。

在所有网民中，未成年人面临的网络安全风险又格外典型，引起了学者们的关注。对于他们而言，网络风险不一定会造成实际的伤害，而是会提高未成年人遭遇风险的可能性。政策条款不能够消除所有风险，其目的是管理风险，以便利用所有资源，将网络对未成年人的危害降至最低。2012 年，英国未成年人互联网安全理事会就倡议应该在 5 ～ 11 岁年轻人

面临的网络风险方面加强研究，以便为学校、家长和青少年制定未来的教育策略。

图 2 DeMoor 等人研究得出的未成年人使用网络信息过程中面临的潜在风险



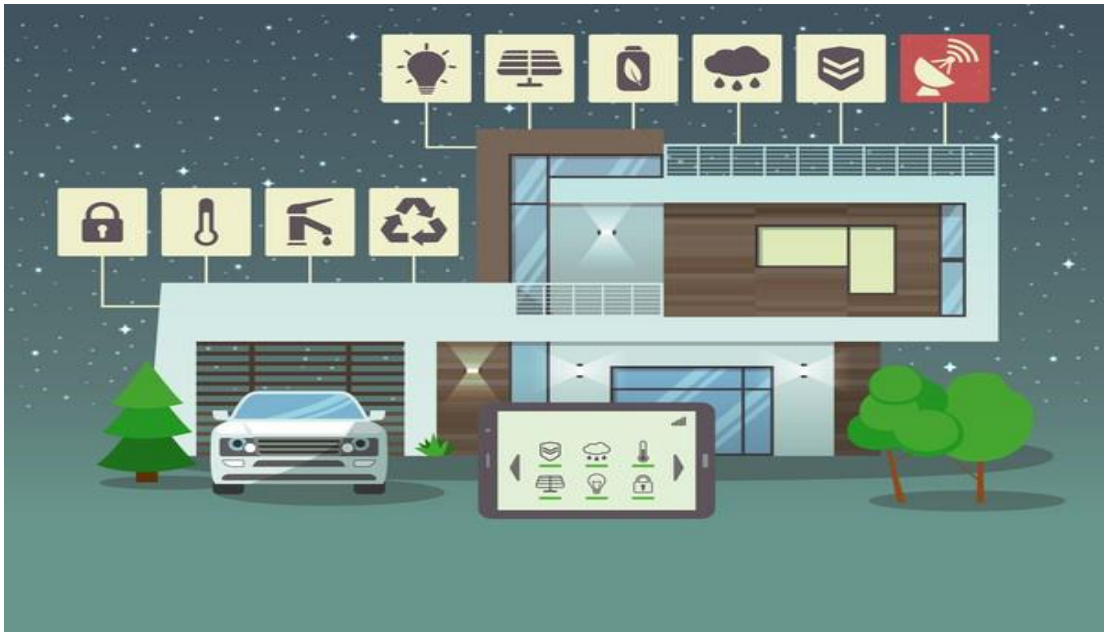
DeMoor 等人将未成年人互联网利用中面临的风险用结构图进行表达（图 2），包括内容风险、接触风险和商业风险，成为多数学者接受并认可的一种模式。其中，内容风险指未成年人使用网络信息时可能受到的网络信息资源内容的负面影响，包括不良网络信息资源内容和错误、不可信的信息。联系风险包括在线联系风险与离线联系风险，如网络欺凌、性诱惑、隐私风险等。对于未成年人来说，其网络行为涉及到商业活动的主要包括参与电子商务或电子广告活动，其中一个相当隐蔽的风险就是对未成年人个人数据的收集和商业开发。

综合网络安全与网络安全风险的相关研究成果，网络安全意识的概念与内涵也逐渐清晰。

早期，网络安全意识的概念相对比较狭隘，Siponen 将网络安全意识定义为一种教育模式，使所有网民对各种各样的网络威胁、计算机和数据漏洞保持敏感。Shaw 等人在研究中将网络安全意识的内涵综合考量为用户理解信息安全重要性的程度、控制信息的能力、保护个人和组织信息的能力。互联网发展初期，我国学者对网络安全意识的最初认识体现在网络社会责任感，即用户作为主体对网上信息内容的发布和接受负有社会责任，要自觉抵制不良信息的传播，要有“网络安全人人有责”的观念。张卫清曾在网络文化和安全文化的基础上提出“网络安全文化”的概念，指人们对网络安全的理解和态度，以及对网络事故的评判和处理原则，是每个人对网络安全的价值观和行为准则的总和，包括网络

安全物质文化、网络安全制度文化和网络安全精神文化三个层面。

网络安全是网络安全意识的目标，而网络安全风险决定了网络安全意识的实际内容，因此，网络安全意识的内涵随着上述两方面研究领域的深入逐渐得到扩展。当前的网络安全意识指遭遇网络不安全因素时所表现出来的判断、分析、应对等综合能力，体现在面对网络安全风险时“发现问题—应对难题—化解危机”的整个过程当中。具体来讲，包括对个人所处的网络或空间有一定的认知，对网络环境可能具备的危险性有一定认知，并且对网络空间中的不安全因素有一定认知。按照网络安全意识的对象划分，现有的研究主要包括网络设施安全意识、网络信息安全意识、网络运营安全意识和网络行为安全意识。在实证研究中，魏德才在调查大学生群体网络安全意识时选取了五项指标，包括网购时防侵权意识、网络安全知识的获取、注册网络用户信息是否留有真实信息、对待未证实的社会敏感消息的态度、在遭受网络侵权后的维权途径调查；王炎龙、邓倩通过未成年人对网络语言的使用的角度透视了未成年人的网络安全观，包括网络接触环境和途径、对网络不洁字眼的态度、对网络语言内涵的认知力、使用网络语言的目的、网络文明意识等。可见，在具体的实证研究中，研究者往往会根据自己的研究目的将“网络安全意识”概念的外延拆分成不同的层面，通过不同的表现形式进行测量和评估，缺少系统性的理论框架。



二、网络安全意识现状与问题研究

随着人们对于互联网的使用频率和嵌入程度越来越高，在享受互联网带来的生产、生活等方面的便利和优势的同时，网络安全意识也应该引起相应的重视，以免阻碍对互联网的进一步利用乃至个人的成长与发展。学者们开始通过实证方法对部分群体网络安全意识

的现状进行了研究。

卢伟在 2009 年，通过问卷调查的方法，收集了 475 位在校大学生的网络安全知识掌握情况、网络安全经历和防范措施情况，并把网络安全知识划分为物理安全、网络系统安全、信息系统安全、信息基础设施安全和设施安全。调查结果显示，大学生平时已习惯并喜爱利用网络获取信息资料、与朋友交流、放松娱乐等，但与此同时他们对网络安全知识了解不足，并缺乏自我保护和防范意识，比如对文件加密、用户权限限制、提高密码设置的复杂程度等都不够重视。2011 年，刘新华、巢传宣对大学生网络安全意识和教育状况进行调查后认为，行为是意识的外在表现，所以外在行为和内在意识之间存在较高相关性，于是依据学生的网络危险行为，来评估学生的网络安全意识高低。二人把网络危险行为具体为 18 种：制造或传播网络病毒、在网上阅读或制作反动宣传资料、浏览“黄赌毒”站点、与别人色情聊天、上网时不利于防火墙软件监视数据流动、不定期升级杀毒软件、不及时修补系统漏洞、从网上下载的文件或软件使用前不杀毒、随意打开垃圾邮件、收到不明邮件后打开邮件中的链接、在公共场所上网后不及时关闭所登录过的网站、不定期更改 QQ 密码或电子银行登录口令、将自己的照片或其他真实资料发给陌生人或发布在网上、主动邀请网友见面、应邀与网友见面、收到虚假中奖信息后按要求登录指定网站填写信息、网上购物时不仔细核对网站地址和网络成瘾。并基于调查结果强调了网络安全意识教育的重要性。魏德才和陈胜男于 2015 年在海南省对大学生网络安全意识做了调查和研究，将网络安全意识分为网购时防范意识、获取安全知识途径、注册用户留存信息真实度、信息核实判断能力和被侵权后维权意识。问卷调查的结果表明，当代大学生在网络空间中言行随意，轻信虚拟世界中的言论，过度依赖虚拟世界中的交往，因此放松警惕，不注意隐私保护，并且在网购时，防范侵权意识差，高于六分之一的学生都曾在网购中被侵权。尽管如此，多数大学生依旧对于网络安全知识主动获取的意愿不高，能力不强，仅有 24.89% 的学生有意识地了解过网络安全知识。

近年来，网络安全意识的研究也开始向其他群体扩散。2017 年，刘志林对我国民众的网络安全意识现状进行调查和分析，结果显示，民众已开始重视网络安全，其中中老年群体的网络安全意识相对较差。据数据显示，18 ～ 29 岁的年轻人对网络认识和理解程度较其他年龄段更高，50 岁以上的中老年群体由于年龄、学习能力和知识水平的限制，没有足够的意愿或能力接触和学习网络安全知识，此外，思想观念停留在被动接受而非主动防御，也是重要原因之一。因此，民众网络安全意识仍然需要进一步加强。

学者对网络安全意识的划分可归类为信息甄别、自我防范和行为伦理规范。信息甄别

一方面指在不同环境下对个人信息披露的真实程度和尺度的把控能力；另一方面是指在芜杂泛滥的网络信息中过滤垃圾信息、虚假信息和有害信息，筛选有价值的信息的能力。自我防范指人们在运用网络时没有做到科学合理，而引起如网络攻击、病毒感染、网络篡改、信息泄密等网络安全事故频发。行为伦理规范是指人在缺乏网络礼仪的情况下产生的行为失范而影响自身乃至社会发展。网络的隐匿性、虚拟性使青少年容易规避现实社会的约束而成为网络的破坏者。轻者表现为发泄不满、肆意谩骂、散布谣言等，重者则包括参与实施网络诈骗、传播病毒、传播违法信息等犯罪活动。网络道德素养和网络法律意识等规范意识的缺失还有可能导致青少年被不法分子利用，无意识地成为不法信息的携带者、传播者和受害者，既危及自身发展，也伤害到他人和社会。值得一提的是，青少年群体是网络“非主流”文化的主要接触者和接受者。以图片、文字、网站为主的“非主流”文化以其个性化的特点，对青少年的网络安全意识产生着不可避免的消极影响。由于非主流文化具有一定的蒙蔽性，人们对非主流文化的价值标准和价值判断存在模糊不清的问题，加上网络安全知识缺乏，网络安全意识不强，制约着青少年整体网络安全水平的提升。

三、网络安全意识的教育与培训研究

教育是提升网络安全意识的最佳途径。我国近年来已愈加重视相关教育和培训，既有可圈可点之处，也存在一些不足。

3.1 网络安全意识教育存在的问题

网络安全意识的提高势在必行，凸显了网络安全意识教育的必要性和紧迫性。卢伟指出，我国大学生对信息安全知识掌握不到位，操作能力欠缺，但计算机应用基础课程中相应的网络知识不足，网络安全专题的活动、讲座很少。同年，肖红光、谭作文和周亚卉三人对比研究了中美两国信息安全教育的情况发现，美国在《信息系统保护国家计划》中制定了四个信息安全教育培训项目：联邦计算机服务（FCS）项目、服务奖学金（SFS）项目、中小学拓广项目和联邦范围内的培养项目。相比之下，我国的信息安全教育未得到足够重视，导致有如下问题：从政府到学校再到学生信息安全意识不足；从事信息安全工作的人员较少，且大多数都是网络管理人员通过短期自学或培训后上岗；信息安全专业的课程设置仍然停留在技术防护层面，难以涵盖信息安全的其他主要内容，比如有关网络安全的多数内容基本是相近学科的翻版或外延，缺少系统观点和方法，仅仅强调密码学、防火墙、入侵检测等安全理论和技术知识的教育；作为应用型教育，高质量的信息安全教材不足，大多是技术类和专业理论书籍；网络信息安全是一门实用性较强的学科，但是目前我国多数高校尚未建立高质量信息安全仿真环境，所以实验条件非常落后。2011 年，刘新

华、巢传宣提到了几点我国高校网络安全教育的不足：一是未得到高度重视；二是网络安全教育不够完整，没有包含网络法治、道德、安全防范和心理健康四部分；三是网络安全教育没有针对性，随着学生的年级提升，网络安全法制教育应该更重要，不能简单地统一教学；四是网络安全教育不够深入，绝不能“头痛医头脚痛医脚”。

近年来，情况日渐改善。张俊强调，目前对于网络安全教育的认识，主要是对其重要性和紧迫性认识不足，足够透彻的认识才能正确指导行动，但是在某些地方政府或高校相关教育依然零散随意，甚至边缘化。网络安全教育的管理机制同样不够健全，很多高校都成立了网络安全教育领导小组，但分工不明、运转不力，或仅停留在文件层面没有实施，多数高校的方式僵化，比如开学时进行网络安全教育或举办一次讲座，之后分发传单介绍杀毒软件以及一些网络安全知识，这些举措显然收效甚微。除此之外，网络安全教育并未被真正纳入教学计划，多数课程依旧强调技术和理论，极少涉及网络安全乃至伦理道德问题。

当下我国网络安全教育存在的各类问题在不断发展和进步中已得到一定解决，但依旧存在问题：像国家教育部→省市教育单位→高校党政→二级院系→相关教学人员类似的管理负责机制未能明确建立，有关网络安全教育到的法规体系尚不成熟——包括从国家层面的法规到教育部层面的指导性文件再到各高校或单位层面根据自身实际情况制定的管理规定；积极主动的宣传引导不够，不论是高校用多种形式发声，还是社会组织以各种形式宣传。

3.2 网络安全教育的方式方法研究

研究显示，我国网络安全教育方式方法主要有：制度建设、优化管理、宣传知识。

制度建设主要有法律，政府和高校三种层次。法律层次是与网络安全教育和管理相关的法律法规的出台，例如《中华人民共和国计算机信息系统安全保护条例》等；政府层次是教育部、省市教育厅（局）出台指导性文件并进行指导督查；高校内部则是各自根据具体情况，建立多种计算机网络管理制度、宿舍管理制度、网上巡查制度网络言论引导制度等，规范学生的上网行为习惯，引导学生的使用网络规范和知法懂法守法。

优化管理，指大学生网络安全教育组织管理体系，秉承“谁主管谁负责，谁建设谁负责”的原则，建设中央到省市到高校到院系到老师的管理制度，比如高校中应当成立由校领导牵头，党委宣传部、网络管理中心、教务处、保卫处等部门负责人组成网络安全教育领导小组，逐步落实。成立学生网络安全委员会、校网宣联合会等组织团体来发挥学生主观能动性，引导学生自我管理，加强自律。

宣传知识，分为课堂讲学、知识讲座和活动与宣传。我国有关网络安全意识教育的材料和书籍在不断完善，课堂讲学从原先不规范，过于理论化和技术化，转向更深入、全面、具体的教学。知识讲座是目前大多数高校常用的网络安全意识教育的手段，通常在开学初期，邀请相关学者或业界专家来校为学生普及相关知识。活动与宣传既包括最广泛的布置橱窗展板宣传，也包括举行线下的网络安全知识竞赛、组织模拟法庭等网络安全法律的普法活动，以及部分高校建设的网络安全意识教育网站，来为大学生提供多种获取网络安全知识的渠道。

3.3 国外网络安全意识教育的经验研究

张慧敏梳理了国外全民网络安全意识教育的特点，归纳为以下四点：政府为主、各方合作；目标明确、保证投入；对象具体、方法多样；主题多元、内容丰富。对于大学生群体的网络安全意识教育，许多学者建议学校开设相关课程，或在现有课程中加入网络安全意识、网络道德规范、网络法律法规等相关内容。管理方面，学校应加强对校园网络的管理，包括 IP 地址管理、不良网站屏蔽、论坛实名制等，还要加强网络舆情分析，形成统一协调、反应灵敏、高效畅通的网上舆情收集反映回馈机制，化解潜在的隐患。对于未成年人的网络安全教育，王国珍梳理了新加坡中小学的网络素养教育模式，认为其核心内容是培养孩子们的自我保护能力，应当将引导学生自尊自重使用网络，不浏览有害网站、不参与非法网络活动作为教育重点，加强对网络潜在风险的辨识能力，学会如何保护自己。在此基础上，加强责任感的教育，要求学生们认清自己网络使用行为产生的后果，保护自己的同时也保护他人。

许畅和高金虎二人对美国的网络安全意识教育进行了研究，并对我国提出了一些建议。早在 1993 年，克林顿政府颁布了《国家信息基础设施条例》来规范信息基础设施的各项标准。之后历任政府不断完善和调整，增强对网络安全的重视。到奥巴马执政时期，网络安全上升到国家安全战略核心地位。奥巴马政府试图建立一个全方位多层次的网络安全环境，为达此目的，发起了多项全国性公民网络安全常识普及和教育活动，并吸引和雇佣了大量网络空间安全专家。2010 年，美国政府部署推行了“国家网络安全教育计划”，经过两年的反复征集意见和调整修改，主要面向在校学生、一般公民和网络空间从业人员推广，并尊重和强调差异化，针对不同区域、不同年龄阶层的公民的安全意识和技术水平做了详尽安排。

对我国而言，可以借鉴美国对顶层设计的重视，加快推进网络安全意识培养体系。此外应统筹社会资源，完善网络安全管理机制，尽快建设完善以政府管理为核心，社会力量

为协作主力的架构，充分调动企业、行业协会、学校、科研机构等社会资源，针对专职人员、学生、中老年人群体等使用不同策略，丰富教育方式和载体如各类专门网站、网络信息安全大赛、课程和培训项目，从而全面提升国民网络安全意识。

通过以上的学习和借鉴，最终形成符合我国实际情况的全社会全方位多层次的网络安全意识实施体系，即安全（Security）—安全信息（Information）—安全知识（Knowledge）—安全认识（Perception）—安全行为（Behaviour）。

四、总结

综合上述研究结果来看，目前学界对于网络安全意识的内涵还没有一个全面、系统的理论框架。虽然大部分学者已经认识到互联网时代网络安全意识的重要性，部分学者也分析了互联网时代网络安全意识概念范畴的发展演变，但是在实际操作化方面仍缺乏系统性方法，导致在实证研究中大部分学者都是按照各自的研究目的与研究问题将网络安全意识进行不同层面的拆分，因此目前的研究领域略显杂乱。在研究对象方面，大学生群体、青少年群体成为主流研究关注的焦点，多数实证研究会选择在大学或高中开展调查，导致此类群体的研究已经较为丰富和成熟，而针对未成年人、儿童群体的研究还相对薄弱。其中，关于青少年网络使用特征与现状的研究数量较多，聚焦在网络安全意识的专门文献较少。本文认为，由于网络安全意识正凸显出日益重要的地位，学界应当加强此方面的研究，从不同维度提出完整的理论框架来评估、调查和引导青少年的网络安全意识。在网络安全意识教育部分，很多学者根据国外相关经验提出了针对我国的提升策略，但结合我国自身特色方面略显不足，也是日后研究中应当加强的部分。（来源：《信息安全与通信保密》）

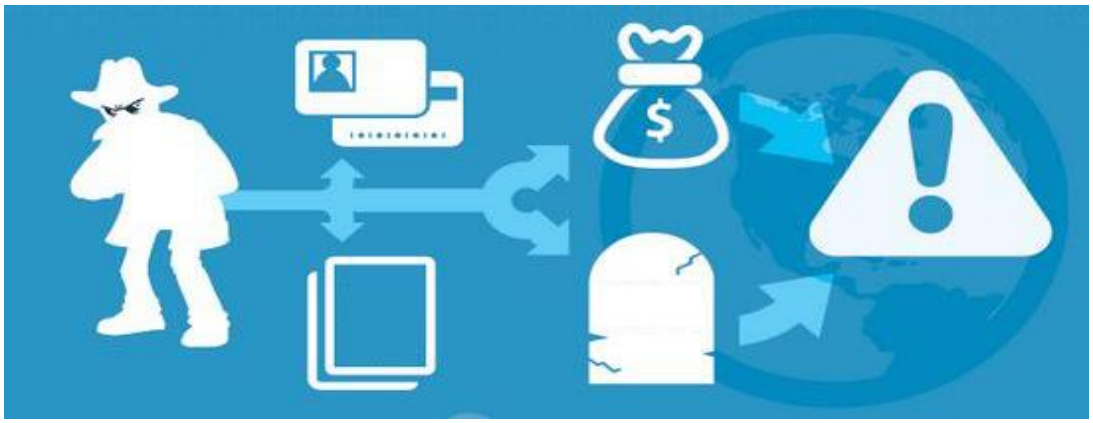
➢ Gartner：2019 年七大安全和风险趋势

在一次业务战略会议上，一家国家交通运输系统的首席信息安全官播放了一张幻灯片，内容是该机构的拟定风险偏好声明：

公司没有可能导致公众、乘客或工作人员受伤或失去生命的安全风险。所有安全目标都已实现并逐年改善。我们愿意接受可能导致经济损失的风险。公司在运算性能网络的可靠性和能力以及资产状况方面只容忍低到中的总体风险。

首席信息安全官一直致力于说明根据风险作出决策的重要性，而且他们发现创建风险偏好声明是让企业机构保持 IT 风险管理与业务目标一致性的最有效工具。首席信息安全官可通过创建简单、实用和务实的风险偏好声明消除网络安全团队与各业务部门之间的文化脱节。Gartner 预计，这将是 2019 年影响首席信息安全官的七大网络安全和风险管理趋势之一。

Gartner 研究副总裁 Peter Firstbrook 在 2019 年 Gartner 安全与风险管理峰会（Gartner Security and Risk Management Summit 2019 inNational Harbor，MD）上表示：“这些重要趋势突显了安全生态系统正在发生战略性转变，而这些转变目前尚未得到广泛的认可，但是具有广泛的行业影响力和巨大的颠覆潜力。这些发展趋势使安全和风险管理领导者（SRM）能够提高抵御能力、更好地支持业务目标并提升自身在企业机构中的地位。”



趋势一：领先的安全和风险管理领导者正在创建与业务成果相关的务实风险偏好声明，以更有效地吸引利益相关者。

根据 Gartner 客户的询问，安全和风险管理领导者所面临的最严峻挑战之一是无法与业务领导者进行有效沟通。尽管首席信息安全官参与战略会议较多，但业务领导者往往无法判断某项技术或某个项目是否具有过高的风险或者企业机构是否因为过度规避风险而错失机会。

风险偏好声明将业务目标和风险应对计划相联系，以便在承担风险时向利益相关者和合作伙伴告知企业机构的意图。风险偏好声明必须明确、一致和具有相关性，并且必须为企业机构选择正确的实现方式。

趋势二：重新关注安全运营中心（SOC）的实施情况或成熟度，把重点放在威胁检测和响应上。

由于网络安全攻击的复杂性和影响日益增加以及网络安全工具产生警报的复杂性不断提高，企业机构希望能够建立或重新激活安全运营中心或者将这一功能外包。到 2022 年，50%的安全运营中心将转变为集成了事件响应、威胁情报和威胁搜寻能力的现代安全运营中心，而在 2015 年，这一比例还不到 10%。

企业机构正在投资更敏感的工具并专注于维持响应和检测或预防之间的平衡。由于复杂的警报和工具数量增加，因此对于运营集中化和优化的需求也在增加，这意味着安全运营中心如今已是一种业务资产。

趋势三：领先的企业机构正在利用数据安全治理框架来确定数据安全投资的优先级别。

数据安全不仅仅是一个技术问题。为了实现有效的数据安全，可能需要建立数据安全治理框架来获得以数据为中心的蓝图；并通过该蓝图确认所有企业计算资产中的结构化和非结构化数据集并加以分类，同时制定数据安全策略。当安全和风险管理领导者确认了业务战略和风险承受能力时，该框架就可以作为技术投资优先级别指南。

趋势四：受市场需求以及生物识别技术与强大的基于硬件认证技术的推动，“无密码”认证正受到市场青睐。

无密码认证是一个长期目标，但直到现在才开始真正受到市场的青睐。密码会吸引攻击者，并且易受到社会工程学、网络钓鱼、撞库和恶意软件等多种攻击。

随着新的无密码标准的出现以及兼容无密码身份验证的设备数量日益增加，无密码认证的普及率正在提高。生物识别技术因具有强大的身份识别能力而成为一项越来越受欢迎的“无密码”技术。其他技术包括硬件令牌（hardware tokens）、电话令牌（phone as a token）、在线快速身份验证（fast IDentity Online）和被动行为分析（analytics based on passive behaviors）。

趋势五：越来越多的网络安全产品供应商开始提供优质的服务，帮助客户获得更直接的价值并协助客户进行技能培训。

全球空缺的网络安全职位预计将从 2018 年的 100 万个增加到 2020 年的 150 万个。企业机构正在想方设法填补空缺的职位，但它们可能会发现即便是留住现有的员工也十分困难。与此同时，网络安全软件正在日益扩散和复杂化。一些技术，尤其是人工智能技术的运用，需要人类安全专家不断进行监控或调查。

可能在不久之后，就没有足够的技术人员来使用这些产品。因此，越来越多的供应商开始提供优质的服务，将产品与实施、配置和长期运营服务相结合。这意味着供应商可以帮助客户从工具中获得更直接的价值，并且企业机构可以提升网络管理员的技能水平。

趋势六：由于云已成为主流计算平台，因此领先的企业机构正在投资云安全能力并使这项能力变得更加成熟。

随着越来越多的企业机构开始使用云平台，网络安全团队将会遇到更加多样和复杂的云安全挑战。为了应对这个快速变化的环境，领先的企业机构正在建立云卓越技术中心团队并对人员、流程和工具加以投资。云访问安全代理（CASB）、云安全状态管理（CSPM）和云工作负载保护平台（CWPP）等工具能够提供多重云安全能力来应对风险，但企业机构仍须对人员和流程进行投资，例如采用安全开发运维（SecDevOps）的工作方式等。

趋势七：持续自适应风险与信任评估网络安全策略开始出现在更传统的网络安全市场中。

持续自适应风险与信任评估（CARTA）是一种安全策略方法。该策略方法承认没有完美的保护方法，因此需要随时随地调整安全策略。局域网网络安全和电子邮件安全这两个传统市场正在开始采用持续自适应风险与信任评估的思维模式，侧重于周界内检测以及检测与响应能力。（来源：Gartner）

四、政府之声

➢ 中华人民共和国密码法（草案）征求意见

2019 年 7 月 5 日，第十三届全国人大常委会第十一次会议对《中华人民共和国密码法（草案）》进行了审议。现将《中华人民共和国密码法（草案）》在中国人大网公布。

关于《中华人民共和国密码法（草案）》的说明：

一、立法的必要性

密码工作是党和国家的一项特殊重要工作，直接关系国家安全，密码在我国革命、建设、改革各个历史时期，都发挥了不可替代的重要作用。进入新时代，密码工作面临着许多新的机遇和挑战，担负着更加繁重的保障和管理任务，制定一部密码领域综合性、基础性法律，十分必要。一是核心密码和普通密码维护国家安全方面的基本制度、密码管理部门和密码工作机构及其工作人员开展核心密码和普通密码工作的保障措施等，需要通过国家立法予以明确，进一步提升法治化保障水平。二是近年来密码在维护国家安全、促进经济社会发展、保护人民群众利益方面发挥越来越重要的作用，国家对重要领域商用密码的应用、基础支撑能力的提升以及安全性评估、审查制度等不断提出明确要求，需要及时上升为法律规范。三是传统对商用密码实行全环节许可管理的手段已不适应职能转变和“放管服”改革要求，亟需在立法层面重塑现行商用密码管理制度。全国人大常委会和国务院将制定密码法列入了立

法工作计划。

2017 年 4 月至 5 月，国家密码管理局将《中华人民共和国密码法(草案征求意见稿)》向社会公开征求了意见，并于 2017 年 6 月向国务院报送了《中华人民共和国密码法(草案送审稿)》(以下简称送审稿)。收到此件后，司法部广泛征求了各地各部门意见，会同国家密码管理局对送审稿作了研究修改，并反复与中央网信办、工业和信息化部、商务部等单位沟通协调，形成了目前的《中华人民共和国密码法(草案)》(以下简称草案)。草案已于 2019 年 6 月 10 日经国务院常务会议讨论通过。

二、立法的总体思路

一是明确对核心密码、普通密码与商用密码实行分类管理的原则。草案在核心密码、普通密码方面，深入贯彻总体国家安全观，将现行有效的基本制度、特殊管理政策及保障措施法治化；在商用密码方面，充分体现职能转变和“放管服”改革要求，明确公民、法人和其他组织均可依法使用。

二是注重把握职能转变和“放管服”需要与保障国家安全的平衡。草案在明确鼓励商用密码产业发展、突出标准引领作用的基础上，对涉及国家安全、国计民生、社会公共利益，列入网络关键设备和网络安全专用产品目录的产品，以及关键信息基础设施的运营者和国家机关采购、使用的部分，规定了适度的管制措施。

三是注意处理好草案与网络安全法、保守国家秘密法等有关法律的关系。密码是保障网络安全的核心技术和基础支撑，草案在商用密码管理和相应法律责任设定方面与网络安全法的有关制度，如强制检测认证、安全性评估、国家安全审查等作了衔接；同时，鉴于核心密码、普通密码属于国家秘密，草案在核心密码、普通密码的管理方面与保守国家秘密法作了衔接。

三、草案的主要内容

草案共五章四十四条，主要内容如下：

（一）关于密码工作的领导和管理体制

草案明确：坚持中国共产党对密码工作的领导；中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设（第四条）。国家密码管理部门负责管理全国的密码工作；县级以上地方各级密码管理部门负责管理本行政区域的密码工作；国家机关和涉及密码的单位在其职责范围内负责本机关、本单位或者本系统的密码工作（第五条）。

（二）关于密码的分类管理原则

草案明确规定密码分为核心密码、普通密码和商用密码，实行分类管理（第六条）。提出了密码分类保护的原则要求：核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级；核心密码、普通密码属于国家秘密，由密码管理部门依法实行严格统一管理（第七条）。商用密码用于保护不属于国家秘密的信息；公民、法人和其他组织均可依法使用商用密码保护网络与信息安全（第八条）。

（三）关于密码发展促进和保障措施

草案总则对核心密码、普通密码和商用密码在发展促进和保障措施方面的共性内容作了规定：一是规定国家鼓励和支持密码科学技术研究、交流，依法保护密码知识产权，促进密码科学技术进步和创新，建立密码工作表彰奖励制度（第九条）；二是规定国家加强密码宣传教育（第十条）；三是规定县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级预算（第十一条）；四是规定任何组织或者个人不得窃取或者非法侵入他人的加密信息或者密码保障系统，不得利用密码从事违法犯罪活动（第十二条）。

（四）关于核心密码、普通密码

为了确保核心密码、普通密码安全，增强密码通信服务和网络空间密码保障能力，草案第二章规定了核心密码、普通密码的主要管理制度：一是明确传递、存储、处理国家秘密信息时的核心密码、普通密码使用要求（第十四条）；二是规定密码工作机构应当依法建立健全安全管理制度，采取严格的保密措施（第十五条）；三是规定密码管理部门依法对核心密码、普通密码工作进行指导、监督和检查，会同有关部门建立核心密码、普通密码安全协同联动机制，明确了相关案事件处置程序（第十六条、第十七条）；四是规定国家加强密码工作机构和核心密码、普通密码人才队伍建设（第十八条）；五是明确了核心密码、普通密码有关物品和人员享有免检等便利（第十九条）；六是规定了密码管理部门、密码工作机构对其工作人员的监督和安全审查机制（第二十条）。

（五）关于商用密码

为了贯彻落实职能转变和“放管服”改革要求，规范和促进商用密码产业发展，草案第三章规定了商用密码的主要制度：一是规定国家鼓励商用密码技术的研究开发和应用，健全商用密码市场体系，鼓励和促进商用密码产业发展（第二十一条）；二是规定了商用密码标准化制度（第二十二条、第二十三条、第二十四条）；三是建立了商用密码检测认证制度，并鼓励从业单位自愿接受商用密码检测认证（第二十五条）；四是对列入网络关键设备和网络安全专用产品目录的商用密码产品、用于网络关键设备和网络安全专用产品的商用密码服

务实行强制性检测认证（第二十六条）；五是规定关键信息基础设施应当依法使用商用密码、开展安全性评估及国家安全审查（第二十七条）；六是对特定范围的商用密码实行进口许可和出口管制制度（第二十八条）；七是规定了电子政务电子认证服务管理制度（第二十九条）；八是支持商用密码行业协会积极发挥作用，加强行业自律，促进行业健康发展（第三十条）；九是规定了密码管理部门和有关部门建立商用密码事中事后监管制度（第三十一条）。

此外，草案规定了相应的法律责任（第四章）。（来源：中国人大网）

- **关于《中华人民共和国密码法（草案）》**
- **全文：**http://www.npc.gov.cn/npc/flcazqyj/2019-07/05/content_2090842.htm

➢ 工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》

2019 年 7 月 1 日，为贯彻落实党中央、国务院决策部署要求，积极应对新形势新情况新问题，切实做好新中国成立 70 周年网络数据安全保障工作，全面提升电信和互联网行业网络数据安全保护能力，工业和信息化部近日印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，在行业内部署开展为期一年的提升网络数据安全保护能力专项行动。

本次专项行动围绕新中国成立 70 周年等重大活动数据安全保障和行业网络数据安全保障体系建设，明确两个阶段的工作目标，并从加快完善网络数据安全制度标准、开展合规性评估和专项治理、强化行业网络数据安全管理、创新推动网络数据安全技术防护能力建设、强化社会监督和宣传交流 5 个方面提出 14 项重点任务。（来源：工业和信息化部办公厅）

- **工业和信息化部办公厅关于印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》的通知 工信厅网安〔2019〕42 号 全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c7021335/content.html

➢ 《国家网络安全产业发展规划》正式发布

2019 年 6 月 30 日，在中国软件产业发展情况新闻发布会上，《国家网络安全产业发展规划》正式发布，工业和信息化部与北京市人民政府决定建设国家网络安全产业园区。根据规划，到 2020 年，依托产业园带动北京市网络安全产业规模超过 1000 亿元，拉动 GDP 增长超过 3300 亿元，打造不少于 3 家年收入超过 100 亿元的骨干企业。加快构建“高精尖”

经济结构，推进首都“四个中心”建设，增强网络安全产业发展的高端引领作用，保障网络时代国家安全利益。

到 2025 年，依托产业园建成我国网络安全产业“五个基地”：

一是国家安全战略支撑基地。以国家安全、网络空间安全等重大战略需求为核心驱动力，超前部署、加速推进一批网络安全关键共性技术研究。二是国际领先的网络安全研发基地。搭建面向全球的协同研发平台，汇聚全球创新资源，推动网络安全核心技术创新和科研成果转化。三是网络安全高端产业集聚示范基地。培育一批具有全球竞争力的骨干企业，打造产学研用一体化的网络安全产业生态链，在全国形成高端产业示范引领效应。四是网络安全领军人才培育基地。依托北京市技术、人才、科研、教育等优势资源，建设一批总部型、基地型培训基地，吸引国内外高端网络安全人才。五是网络安全产业制度创新基地。加强政府统筹引领作用，推动园区体制机制创新，积极研究探索建立适应新时代网络安全产业发展需求的、创新的、先进的、高效的园区管理运营体制机制，实现政府、行业、企业、社会共建共享。（来源：中国经济网）

➢ 工业和信息化部关于电信服务质量的通告（2019 年第 2 号）

2019 年 7 月 1 日，工业和信息化部发布了《工业和信息化部关于电信服务质量的通告》（2019 年第 2 号）。根据《中华人民共和国电信条例》相关规定，现将 2019 年第一季度电信服务有关情况从电信和互联网用户个人信息保护监管情况、电信用户申诉举报情况、电信服务监管情况、经营及消费提示等四个方面通报了有关情况。

并发布消费提示：（一）工业和信息化部提醒广大用户提高安全防范意识，不要轻信来历不明的电话、短信，接到营销骚扰或疑似诈骗电话，请拨打 12321 或电信企业客服热线及时举报。（二）工业和信息化部提醒广大用户从正规渠道下载手机应用软件，安装时注意阅读服务协议、用户隐私政策和手机权限调用说明，增强防范意识，维护自身合法权益。（三）工业和信息化部提醒广大用户增强电信网络诈骗防范意识，谨防冒充“航空公司客服”“信用卡服务”“贷款业务服务”等的境外诈骗短信，此类短信多利用用户个人信息进行精准诈骗，迷惑性较强。（来源：工业和信息化部）

- **工业和信息化部关于电信服务质量的通告（2019 年第 2 号）全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c7021505/content.html

五、本期重要漏洞实例

➢ IBM WebSphere MQ 信息泄露漏洞

发布日期：2019-06-20
更新日期：2019-06-27
受影响系统：
IBM WebSphere MQ 9.1.1
IBM WebSphere MQ 9.1.0.1
IBM WebSphere MQ 9.1.0.0
描述：

BUGTRAQ ID: 108068
CVE(CAN) ID: CVE-2018-1925
消息队列（MQ）是一种应用程序对应用程序的通信方法。IBM WebSphere MQ 产品支持应用程序通过不同组件如处理器、子系统、操作系统以及通信协议的网络彼此进行通信。
IBM WebShere MQ 9.1.0.0,9.1.0.1,9.1.1 使用了比预期更弱的加密算法，这些算法可能允许攻击者解密高度敏感的信息。
攻击者可以利用此问题获取对敏感信息的访问权限；这可能会导致进一步的攻击。
<*来源：IBM （ncsupp@ca.ibm.com）
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10744713
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（IBM10744713）以及相应补丁:
IBM10744713：IBM MQ Console is vulnerable to a man in the middle attack
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10744713

➢ SQLiteManager SQL 注入漏洞

发布日期：2019-07-03
更新日期：2019-07-03
受影响系统：
SQLiteManager SQLiteManager 1.2.4
SQLiteManager SQLiteManager 1.2
描述：

BUGTRAQ ID: 108640

CVE(CAN) ID: CVE-2019-9083
SQLiteManager 是一个能够支持多国语言基于 Web 的 SQLite 数据库管理工具。
SQLiteManager 1.20 和 1.24 允许通过/sqlitemanager/main.php dbsel 参数进行 SQL 注入。
利用此问题可能会使攻击者破坏应用程序，访问或修改数据，或利用底层数据库中的潜在漏洞。

<*来源：Rafael Pedrero
*>

建议：

厂商补丁：
SQLiteManager

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：

➢ Cisco IOS 和 IOS XE Software 拒绝服务漏洞

发布日期：2019-07-03
更新日期：2019-07-03
受影响系统：
Cisco IOS
Cisco IOS XE Software
描述：

BUGTRAQ ID: 107604
CVE(CAN) ID: CVE-2019-1737
Cisco IOS XE Software 是一系列思科系统 的“广泛部署的互联网操作系统（IOS），用 ASR 1000 系列。
Cisco IOS 为互联网络操作系统，是许多 Cisco Systems 路由器和当前 Cisco 网络交换机上使用的一系列网络操作系统。
Cisco IOS 软件和 Cisco IOS XE 软件处理 IP 服务水平协议（SLA）数据包时的漏洞可能允许未经身份验证的远程攻击者在受影响的设备上引起接口楔入和最终拒绝服务（DoS）情况。该漏洞是由于 IP SLA 响应程序应用程序代码中的套接字资源处理不当造成的。
攻击者可以通过向受影响的设备发送精心设计的 IP SLA 数据包来利用此漏洞。攻击可能允许攻击者使接口变为楔入，从而导致受影响设备上的最终拒绝服务（DoS）条件。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-ipsla-dos
*>

建议：

厂商补丁：

Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190327-ipsla-dos）以及相应补丁:
cisco-sa-20190327-ipsla-dos：Cisco IOS and IOS XE Software IP Service Level Agreement Denial of Service Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-ipsla-dos

➢ GlusterFS 任意代码执行漏洞

发布日期：2019-07-03
更新日期：2019-07-03
受影响系统：
RedHat Virtualization 4
RedHat Virtualization Host 4
RedHat Redhat Gluster Storage Server for On-premise 3 for RHEL 7 0
RedHat Redhat Gluster Storage Server for On-premise 3 for RHEL 6 0
RedHat Enterprise Linux Server 7
RedHat Enterprise Linux Server 6
Gluster Glusterfs
描述：

BUGTRAQ ID: 107577
CVE(CAN) ID: CVE-2018-10929
GlusterFS 系统是一个可扩展的网络文件系统，相比其他分布式文件系统，GlusterFS 具有高扩展性、高可用性、高性能、可横向扩展等特点，并且其没有元数据服务器的设计，让整个服务没有单点故障的隐患。
在 glusterfs 服务器中使用 gfs2_create_req 在 RPC 请求中发现了一个缺陷。
经过身份验证的攻击者可以使用此漏洞创建任意文件并在 glusterfs 服务器节点上执行任意代码。
<*来源：Michael Hanselmann
链接：https://lists.debian.org/debian-lts-announce/2018/09/msg00021.html
*>

建议：

厂商补丁：
Debian

Debian 已经为此发布了一个安全公告（DLA 1510-1）以及相应补丁:
DLA 1510-1：glusterfs security update
链接：https://lists.debian.org/debian-lts-announce/2018/09/msg00021.html

六、本期网络安全事件

➢ 酒店内藏偷拍摄像头引关注 消费者隐私如何保护？

2019 年 6 月 30 日，最近，针孔摄像头偷拍事件频发，涉及场所和范围也越来越广。试衣间、酒店、民宿、出租房等堪称“重灾区”，河南某酒店经理称 “八成酒店都有针孔摄像头”，一时间震惊公众，虽酒店方事后为不负责任言论道歉，但也引发不少网民担忧。那么出门在外住宿，你是否会检查房间内有无摄像头偷拍？

(福建三明市民 张先生)：会检查，但是检查手段比较简单，但之前看到那个介绍说那个螺丝里面有(偷拍设备)，那我感觉我们这种手段检查不出来。

(河南郑州市民 李女士)：一般会看一下，但是有时候会看不出来，就是打开灯，看一下这个天花板，还有角落这些地方。

(上海市民 姚小姐)：如果是晚上入住的话，先把所有的灯都关掉，然后把手机的摄像头打开看一下，从墙壁或者床的对面，然后以及天花板还有浴室，这些地方有没有隐藏的摄像头的红外线，有没有发亮的地方。

今年 5 月，女大学生去写生入住安徽黟县某饭店，就发现客房厕所安装有针孔摄像头。6 月 20 日，深圳警方通报优衣库偷拍事件：科技公司员工为求刺激安装针孔摄像头，目前被依法处以行拘 10 日处罚。近日，一对情侣入住河南某酒店竟然发现插座内藏有针孔摄像头，目前涉事男子已被刑事拘留。6 月 22 日，广东佛山邓先生在出租屋内发现针孔摄像头

频繁发生的针孔摄像头事件，人们不禁担忧：以后住酒店要带帐篷？住宿要进行“地毯式”侦查？当遇到类似情景时，公众应当如何维护自身合法权利？(西南政法大学法学院副教授 法学博士 张武举)

首先发现偷拍行为之后，应该第一时间先固定证据。第二个步骤应该报警，报警之后也协助警方来搜集和固定相关的证据。 第三个步骤可以通过警方和其他司法机关来协调，就民事责任展开协调。第四个如果是协调不当或双方达不成一致，达不成和解的话，可以提起民事诉讼行政诉讼，甚至刑事诉讼。

那么在类似针孔摄像头偷拍案件中，对于偷拍者的责任认定有什么区分呢？

第一种责任是行政责任，可能会处以 500 元以下罚款或 5 日以下的拘留，情节严重的要处以 5 日以上 10 日以下的行政拘留。第二种责任是民事责任，侵害被害人的名誉权，肖像权或隐私权的，行为人应该承担消除影响，停止侵害，赔偿损失等民事责任。 第三项是刑事责任，如果偷拍者利用偷拍的内容，侮辱或者诽谤被害人的，可以依照刑法规定追究他的刑事责任，侮辱罪或者诽谤类的刑事责任。第二，如果是利用偷拍的内容对被害人敲诈勒索的，数额较大的成立刑法规定的敲诈勒索罪，如果是利用这种偷拍来的信息，如果偷拍的信息涉及到了相关的包括性等暴露性的事情内容在内的，那么这些信息的传播，可能就成立咱们刑法中的传播淫秽物品罪。如果把这个信息透露出去，为了牟利的话，可能成立咱们刑法中规定的传播淫秽物品牟利罪，

在层出不穷的偷拍事件中，酒店等经营场所在此类事件中是否需要承担法律责任？

对于偷拍者偷拍行为，如果发生在酒店的话，酒店在经营管理过程中疏于告知，保密等等义务的履行，在偷拍者不能充分赔偿受害人的损失的情况下，酒店可能要承担补充赔偿责任。

据报道，这类案件中的针孔摄像头设备大多是网购。记者在一些网络购物平台以“针孔摄像头”“微型摄像头”等关键词搜索，显示“没有找到相关宝贝”。但检索“摄像头小型”、“微型摄像”，结果出现不少商品，价格在百元至千元不等。“一元大小”、“夜晚不发光”、“不用接电待机一年”等广告语十分醒目，且可批量下单。

(贵州省社会科学院法律研究所副研究员　法学博士 张可)

网络销售平台要有严格的限制，一定要加大对商家在网络上出售这样的商品的限制，做到及时发现，及时清理，并且向公安机关提供相应的线索，同时相关部门也一定要严格地落实国家关于窃听窃视器材的生产销售的规定，依法严惩这样的这个违规者，从源头上治理，包括销售这种犯罪的这种摄像头乱象。

(民革上海市委会法律服务工作站首席律师　魏建平)

网络的销售可能比较门槛比较低，从现在看来，我们觉得网络的销售是不是有许可资质要打一个问号，现在看到我们相应的几个案件中间处理都是处罚的是什么？使用者。那么另外紧接着刑法第 283 条，它有一个非法生产的问题和销售的问题。查到了以后，往上要一直处罚到销售方和相应的生产方，这样才能从根本上来解决斩断非法销售和非法使用这样一个链条。

(西南政法大学法学院副教授 法学博士 张武举)

目前的法律法规如下几个方面值得完善。第一就是需要明晰间谍专用设备窃听窃照专用设备等等这些概念的它的范围，明晰它的范围和标准。第二，进一步规范这些专用设备的生产销售的渠道，使用的途径等等。第三，进一步明确情节严重的标准。这样在执法、司法中才有章可循。 现在现行规定都失之于笼统，而且也授权性的规定，比如授权公安机关对相关的器材涉案器材作出认定，认定标准目前还没有一个规范性文件加以规制，这容易造成执法的困难，也容易引起一些争议，(另外)需要加大惩治力度，像经济制裁的力度就比较弱，而行政拘留的期限的规定也比较短。（来源：中新网）

➢ 美国安局再被曝监控丑闻:非法监控公民通讯记录

2019 年 6 月 28 日，6 年前因“棱镜门”丑闻备受指责的美国国家安全局，近来再次被曝监控丑闻。有组织曝光，美国国安局在去年十月，非法收集美国公民的通讯记录。

据今日俄罗斯网站报道，美国公民自由联盟组织 26 号公布的文件显示，美国国安局在未获得《涉外情报监视法》授权的前提下，于去年 10 月期间持续多天，对美国公民的手机数据进行非法监控。

文件显示，这些手机数据来自美国一家电信公司。该公司以“通讯数据记录”出现了“异常状况”为借口，向美国国安局提供了大量“未经授权的”公民手机通话和短信记录。文件没有公布具体数字，只公开了提供数据的具体时间：是 2018 年 10 月 3 号开始，直到 10 月 12 号才结束。

公民自由联盟组织表示，这一事件对公民隐私和权利有“严重影响”，但受影响的美国公民却并不知情。

加强监听审批 国安局依旧状况百出

2013 年，美国防务承包商前雇员斯诺登，曝光了美国国安局在全球进行大规模监控活动。其范围之广、程度之深令人咋舌，用斯诺登自己的话来说“这一系列监控项目形成的网络，可以让美国对全球大部分通信进行监控。”这一丑闻被称为“棱镜门”。

“棱镜门”丑闻曝光后，美国国会于 2015 年立法，加强了对监控项目的审批。但美国国安局近年来仍被曝出以各种“异常状况”为由非法收集个人信息的情况。今年 1 月，美国国安局曾表示已经改变了相关做法，并销毁了自 2015 年以来获取的 6 亿份通讯记录。（来源：央视新闻）

➢ 日本便利店试用手机支付 几天内盗刷频发被叫停

2019 年 7 月 5 日，经调查，截止 4 日上午 6 点，已有约 900 名用户的手机被盗刷，损失金额可能达到 5500 万日元（约合 51 万美元）。据日媒报道，可以在大型连锁便利店 7-11 中使用的手机支付服务 7pay 自 7 月 1 日开始提供服务，然而仅在 7 月 2 日凌晨，该服务便出现了问题。

据 7&I 控股公司（旗下拥有 7-11 等公司）表示，7 月 2 日，有客户提出了“好像被盗刷了”的询问。经调查，截止 4 日上午 6 点，已有约 900 名用户的手机被盗刷，损失金额可能

达到 5500 万日元（约合 51 万美元）。

7 月 4 日下午 2 点，7pay 董事长小林强召开了紧急记者会，他表示目前正在调查详细的受害人数以及损失金额。此外小林强还指出，将会对所有的损失提供补偿，并对开通了客户服务中心紧急电话。报道指出，由于该服务在开通初期便出现了盗刷现象，这会使用户的心态发生动摇。

遭受了近 5 万日元损失的用户小林勇树表示，原本对 7pay 手机支付服务非常期待，但是现在变得很失望。同样被盗刷 6 万多日元的用户村上慎悟则表示，已经不会信任手机支付服务了，他决定还是使用已经被普及的支付方法（信用卡支付等）。目前，7pay 的充值、以及新用户注册服务均已停止。

此外，多家日媒报道称，日本警视厅已于 4 日以盗刷他人 7pay 的嫌疑逮捕了 2 名中国人（张某与王某）。据悉，此 2 人利用他人的 7pay 账号与密码购买了大量电子烟，其金额达到了 73 万日元。面对调查张某表示，有人在社交媒体上向他发送了 7pay 的账号和密码，并指示他去购买电子烟。（来源：环球科技）

➢ 南京警方破获外挂案:境外编写境内销售半年获利 5000 多万

2019 年 7 月 3 日，激战正酣，突然屏幕上红光一闪，游戏人物被打死了。哪里来的敌人，从何处射来的子弹，都不知道。“爆头、透视、远距离狙杀……”信手拈来，“拥有它，你就是游戏里面最靓的仔！”半年时间内，这款外挂就让他们非法获利 5000 多万元。近日，南京警方破获的这起“黑客”侵入、破坏计算机信息系统程序案件，让民警们也都大吃一惊。

此事还得从 2018 年说起，当年南京警方曾破获过一起“绝地求生”游戏外挂案件，抓捕了 141 人。自那以后，游戏市场上安静了一段时间。然而自今年以来，民警发现“绝地求生”游戏中，又开始重现各种神人，爆头、透视、远距离狙杀……无一不能。

凭借办案经验，民警们怀疑又有外挂“重现江湖”。据民警表示，经常在一些 APP 软件上能看见，主播邀请广大网友围观自己的“神操作”：游戏人物在地图中转了几下，突然就开枪了，远处“有人”中弹；很快又开枪，又“有人”倒下了。而在一些网络游戏论坛里面，有不少人也在吐槽：“我蹲在一个黑暗的角落，背后都是墙，突然就被人打死了；我刚出屋子就被人爆头了；我连人都没看见就被打死了……”

南京市公安局网安支队联合南京市公安局建邺分局组成专案组，对此案进行侦查。专案组民警在论坛上搜索很快有了发现，一个活跃于多个卡盟网站的外挂软件销售团队，对外销售“XYZ 游戏外挂”，且有在南京的销售记录。这个外挂销售价格为 35 元，只能使用 24 小时。这个团伙一共有 14 人，其中两人为游戏外挂的程序编写者，长期在国外，另外 12 人则是国内的代理销售商。

“这个团伙非常狡猾，程序编写者躲在国外进行非法软件开发，将验证服务器架设在国外。外挂程序开发好后，他们给国内的 12 名代理商发放制卡端，玩家花钱购买卡密，代理

商将支付金额通过银行卡打给程序编写者。程序编写者收到钱后，生成卡密给玩家，玩家在游戏中输入相应的卡密即可打开外挂使用。”办案民警表示。

在侦查中警方还发现，国内的 12 名代理商直接或间接向下级销售外挂软件，或者通过卡盟销售。该团伙有着非常严格的销售规章，对涉案的外挂实施控价管理、审核管理，对低价销售的人员会有完善的处理措施。同时经游戏相关公司确认，该款外挂软件已占市场份额的 70%左右，严重影响了游戏使用者的使用体验。经侦查实验及软件的功能性鉴定，“XYZ”游戏外挂属于破坏性程序。

这个外挂在半年时间内，团伙非法获利达到了惊人的 5000 多万元。12 名总代理拿卡是 14 元一张，只能使用 24 小时。而卖到玩家手上，售价达到 35 元。办案民警说：“在明确了犯罪嫌疑人的组织架构及犯罪事实后，在专案组统一指挥下，自 2019 年 5 月中旬起，先后在内蒙古、浙江等地共抓获王某健等犯罪嫌疑人 15 人，其中 7 名总代理、下线代理人 8 名。所有嫌疑人都对游戏外挂的功能表示明知，且对销售游戏外挂卡密的行为供认不讳。”目前，对于剩余的 5 名总代理以及境外涉案人员，也在进一步的调查中。

制作和销售游戏外挂为何违法？

南京市公安局网安支队建邺大队民警：《中华人民共和国刑法》第二百八十五条非法侵入计算机信息系统罪的认定标准为：违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制；提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具。

依据以上条款，警方目前认定被抓的 15 人都属于提供侵入、非法控制计算机信息系统程序、工具，涉嫌非法侵入计算机信息系统。（来源：南京晨报）

➢ 假三星固件更新应用欺骗超过 1000 万 Android 用户

2019 年 7 月 6 日，据报道超过 1000 万用户被骗安装了一款名为“Updates for Samsung”的假三星应用，该应用声称会更新固件，但实际上，它会将用户重定向到一个充斥着广告的网站，并对固件下载收费。CSIS 安全集团的恶意软件分析师阿莱克塞斯·库普林斯（Aleksejs Kuprins）今天在接受 ZDNet 采访时表示，“我已经联系了谷歌 Google Play 应用商店，请求他们考虑移除这款应用。”

三星手机在更新固件和操作系统上比较棘手，假应用 Updates for Samsung 趁虚而入，安装了它的用户数量很高。

“我们不该指责人们在购买了新的 Android 设备后，错误地前往官方应用商店寻找固件更新。”库普林斯指出，“要知道，供应商经常将他们的 Android 操作系统版本与数量惊人的软件捆绑在一起，这很容易让人混淆。”“用户可能会对(系统)更新过程感到有点茫然。因此，可能会错误地前往官方应用商店查找系统更新。”

限速“免费下载”

“Updates for Samsung”应用承诺为非技术用户提供一站式的服务，让三星手机用户可以同时获得固件和操作系统更新，从而解决上述问题。但库普林斯认为，这是该应用的开发者的一个诡计。该应用程序与三星无关，它只在 WebView (Android 浏览器)组件中加载 updato[.]com 域。

在浏览这款应用的评论时，你可以看到数百名用户抱怨说，该网站是一个充斥着广告的鬼地方，他们中的大多数人都找不到自己想要的东西——而这只是在该应用运行正常、不会发生崩溃的前提下。该网站提供免费和付费(正统)的三星固件更新，但在深入研究了该应用的源代码后，库普林斯表示，该网站将免费下载速度限制在 56kbps，一些免费固件下载最终会定时失效。

“在我们的测试中，我们也观察到下载没有完成，即使网络条件相当良好。”库普林斯说道。然而，通过让用户无法下载所有的免费固件，这款应用迫使用户购买 34.99 美元的高级套装，以便下载任何的文件。

这里的问题是，该应用违反了 Google Play 的规则，使用自己的支付系统，而不是使用

谷歌官方提供的支付通道；截取用户的支付数据，或者由第三方记录这些数据，而不是由谷歌的安全防护更好的支付通道来处理数据。同样，该应用还提供了 19.99 美元的 SIM 卡解锁服务；然而，目前尚不清楚这一服务是否如它所说的那样可行，还是只是另一个攫取钱财的伎俩。

不是恶意软件，而是欺诈和骗局

总而言之，该应用程序不是传统意义上的恶意软件，因为它不会代表用户或未经用户同意执行任何的恶意行为。相对而言，“诈骗”、“欺诈”、“广告软件”这些词能更准确地描述其运作模式。“我没有发现该应用程序在设备上执行任何的恶意行为，”被问及是否存在其他的可疑行为时，库普林斯向 ZDNet 证实，“然而，当应用程序打开时，它确实会显示很多的全屏广告，几乎是每次点击屏幕都会弹出这些广告。”

库普林表示，他是在谷歌 Play Store 中搜索“update”（更新）这个词时发现这个应用程序的。他认为这种搜索很可能会呈现一些不好的应用。他说，“‘Updates for Samsung’应用之所以出现在靠前的搜索结果里，是因为它的安装量很大。”

Updates for Samsung 应用的安装量已经突破 1000 万之多，因此要避免让它给广大用户带来更大的损失，谷歌需要动用它的 Play Protect 保护服务，直接在用户的手机上禁用该款应用。（来源：网易科技）

➢ 宝贝回家寻子公益论坛因遭黑客攻击暂时闭站维护

2019 年 6 月 30 日，一个名为“宝贝回家”的民间志愿者寻子公益网站的官方论坛无法正常访问。官方公告称，遭受黑客攻击导致部分数据丢失，目前仍然在闭站维护中。截至 7 月 1 日下午发稿之时，该网站仍未恢复访问。

据了解得知，宝贝回家寻子网是隶属于宝贝回家志愿者协会的公益网站，主要宗旨是为帮助寻找失踪儿童及一些流浪乞讨的孩子找家，为孩子家长及志愿者提供一个信息沟通的平台。

因儿子一次意外走散让全家人度日如年，此后吉林的张宝艳、秦艳友夫妇于 2007 年创建“宝贝回家”网站，志在为许许多多孩子走失或者被拐走的家庭提供帮助。目前，宝贝回家论坛已经成为大量有类似遭遇的父母寻求帮助的渠道之一。谁也没想到这一公益网站也会遭遇黑客攻击，不知道这会影响多少父母及时获取关键消息。

由于数据丢失，该论坛已经停站维护，宝贝回家网站首页大量显示寻子信息均已成空白。而为了及时发布消息，“宝贝回家”依然通过微博、微信公众号等渠道持续发布最新的寻子信息。

对于黑客攻击“宝贝回家”这种公益性论坛的行为，已经引发了大量网友的愤慨。也有业内人士表示“愿意联合其他安全公司为宝贝回家网站提供义务的技术支持，保障网站平稳运行。”2019 年 7 月 3 日下午宝贝回家论坛得各方安全力量相助在停站维护三天后，宝贝回家论坛终于恢复正常访问。（来源互联网综合整理）

信息安全意识产品免费大赠送

isa@spisec.com