国盟信息安全通报

2019 年 8 月 19 日第 199 期

国盟信息安全通报

（第 199 期）

国际信息安全学习联盟

2019 年 8 月 19 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 400 个，其中高危漏洞 62 个、中危漏洞 196 个、低危漏洞 142 个。漏洞平均分值为 5.0。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 11%），其中互联网上出现“WordPress EmailSubscribers&Newsletters 插件跨站脚本漏洞、Microsoft WindowsPowerShell 命令执行漏洞”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 1923 个，与上周（2687 个）环比下降 28%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2019 年 8 月 05 日—2019 年 8 月 18） 4
➢漏洞引发的威胁（2019 年 8 月 05 日—2019 年 8 月 18） 5
➢漏洞影响对象类型（2019 年 8 月 05 日—2019 年 8 月 18） 5
三、安全产业动态 6
➢2019 上半年我国网络安全态势报告:个人信息和数据泄露风险严峻 6
➢移动互联网应用（APP）收集个人信息基本规范解读 7
➢金融科技时代信息安全意识提升之路 17
➢云计算安全的法律风险分析 23
四、政府之声 27
➢国务院办公厅关于促进平台经济规范健康发展的指导意见 27
➢信息安全技术移动互联网应用 App 收集个人信息基本规范（草案）征求意见 28
➢工信部综合整治骚扰电话专项行动工作会在京召开 29
➢《上海市互联网医院管理办法》9 月 1 日施行 29
五、本期重要漏洞实例 31
➢关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告 31
➢IBM Financial Transaction Manager 信息泄露漏洞 32
➢多款 Zoho ManageEngine 产品本地权限提升漏洞 33
➢Cisco IOS Access Points Software 拒绝服务漏洞 33
六、本期网络安全事件 35
➢中信银行“断网”事件再敲警钟 35
➢男子在朋友圈骂人被罚 1000 元 法官:构成名誉侵权 36
➢以信息技术操纵非法集会，谷歌公司被俄罗斯警告！ 38
➢黑客花 2 天就成功入侵 F-15 战机系统美军网络安全漏洞百出 39
➢波音 787 也被爆出安全漏洞 涉及 87 架飞机 41
➢欧洲央行：其外部托管的下属 BIRD 网站遭黑客攻击 42

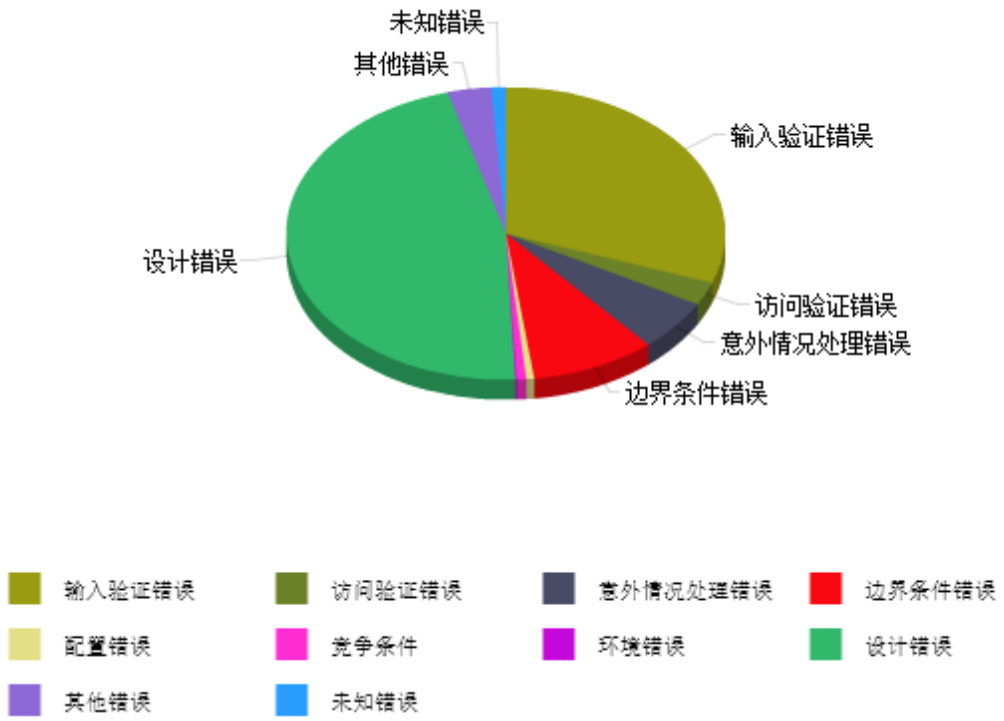
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

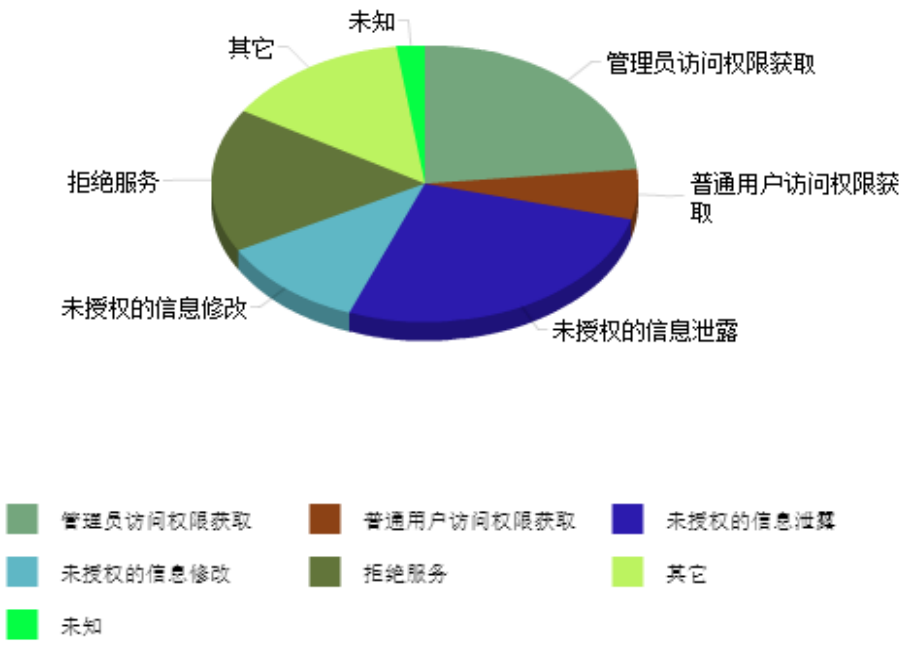
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 400 个，其中高危漏洞 62 个、中危漏洞 196 个、低危漏洞 142 个。漏洞平均分值为 5.0。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 11%），其中互联网上出现“WordPress EmailSubscribers&Newsletters 插件跨站脚本漏洞、Microsoft WindowsPowerShell 命令执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1923 个，与上周（2687 个）环比下降 28%。

二、安全漏洞增长数量及种类分布情况

➢ 漏洞产生原因（2019 年 8 月 05 日—2019 年 8 月 18）



➢ 漏洞引发的威胁（2019 年 8 月 05 日—2019 年 8 月 18）

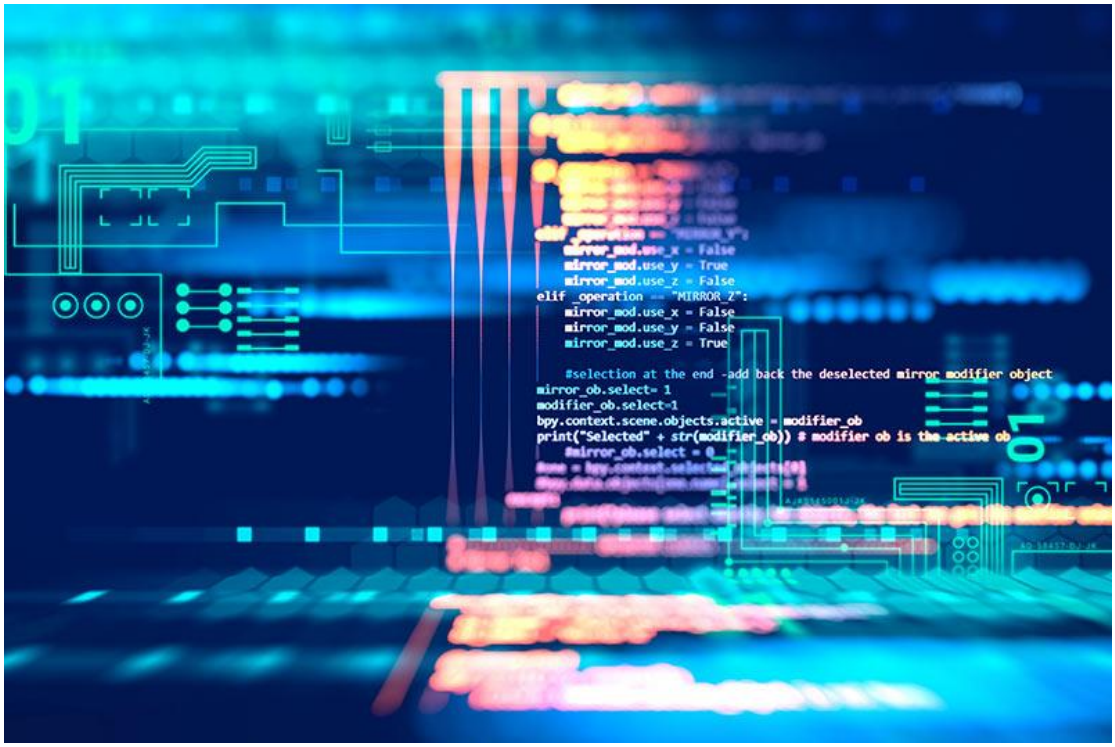


➢ 漏洞影响对象类型（2019 年 8 月 05 日—2019 年 8 月 18）

三、安全产业动态

➢ 2019 上半年我国网络安全态势报告:个人信息和数据泄露风险严峻

2019 年 8 月 5 日，国家互联网应急中心发布《2019 年上半年我国互联网网络安全态势》（以下简称《网络安全形势》）指出，2019 年上半年，我国基础网络运行总体平稳，未发生较大规模以上网络安全事件。但数据泄露事件及风险、有组织的分布式拒绝服务攻击干扰我国重要网站正常运行、鱼叉钓鱼邮件攻击事件频发，多个高危漏洞被曝出，我国网络空间仍面临诸多风险与挑战。



据悉，国家互联网应急中心（以下简称“CNCERT”）从恶意程序、漏洞隐患、移动互联网安全、网站安全以及云平台安全、工业系统安全、互联网金融安全等方面，对我国互联网网络安全环境开展宏观监测。数据显示，与 2018 年上半年数据比较，2019 年上半年我国境内通用型“零日”漏洞收录数量，涉及关键信息基础设施的事件型漏洞通报数量，遭篡改、植入后门、仿冒网站数量等有所上升，其他各类监测数据有所降低或基本持平。

《网络安全形势》显示，利用钓鱼邮件发起有针对性的攻击频发。2019 年上半年，CNCERT 监测发现恶意电子邮件数量超过 5600 万封，涉及恶意邮件附件 37 万余个，平均每个恶意电子邮件附件传播次数约 151 次。钓鱼邮件一般是攻击者伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意

链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动，因欺骗迷惑性很强，用户稍不谨慎就很容易上当。（来源：法制日报）

- **《2019 年上半年我国互联网网络安全态势》报告全文：**
- https://www.cert.org.cn/publish/main/46/2019/20190813163941008331670/20190813163941008331670_.html

➢ 移动互联网应用（APP）收集个人信息基本规范解读

2019 年 8 月 5 日，国家市场监督管理总局和中国国家标准化管理委员会发布了《信息安全技术移动互联网应用（APP）收集个人信息基本规范（草案）》点击链接（以下简称《信息收集规范》），针对 APP 收集个人信息方面提出了更加细化的要求，同时对全国信息安全标准化技术委员会于 2019 年 6 月 1 日发布的《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》（以下简称《基本业务功能规范》）进行了完善，增加了 5 个行业领域的常用服务类型的最少信息。**该规范主要有以下四点主要变化，其次笔者就规范内容逐条进行解读。**

一、发布单位的变化

从《信息安全技术个人信息安全规范》（以下简称《信息安全规范》）、《信息安全技术数据出境安全评估指南》、《信息安全技术个人信息安全影响评估指南》等相关规范来看，发布单位都是中华人民共和国国家质量监督检验检疫总局和中国国家标准化管理委员会，但是本次《信息收集规范》的发布单位是国家市场监督管理总局和中国国家标准化管理委员会。“中华人民共和国国家质量监督检验检疫总局”变化为“国家市场监督管理总局”。

二、适用范围的不同

《信息安全规范》适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。《信息收集规范》适用于移动互联网应用的开发和运营，也可用于移动互联网应用的技术评估、监督检查。

可见，《信息收集规范》的适用范围窄于信息安全规范，仅规范移动互联网应用相关领域。根据《信息收集规范》中“移动互联网应用是指安装、运行在移动智能终端上的应用程序，简称 APP”可知，《信息收集规范》的适用范围仅限于 APP 的开发者、所有者、管理者、

负有技术评估和监督检查的第三方机构以及监管部门。

三、APP 收集个人信息基本要求的细化

《信息收集规范》对 APP 收集个人信息的基本要求做了区分，分别是管理要求和技术要求。管理要求通过“应”、“不得”侧重于 APP 在收集个人信息时的规范要求；技术要求则通过“应”侧重于 APP 在收集个人信息时的具体行为要求。该规范与《信息安全规范》、2019 年 6 月 30 日公布的《信息安全技术个人信息安全规范（征求意见稿）》（以下简称《新版信息安全规范》）、《互联网个人信息安全保护指南》（以下简称《安全保护指南》）、《数据安全管理办法（征求意见稿）》（以下简称《数据安全管理办法》）、《APP 违法违规收集使用个人信息自评估指南》（以下简称《自评估指南》）等文件相比，在个人信息收集部分提出了更加细化的要求。

四、常用服务类型最少信息的变化

首先，从细分服务类型来看，该部分内容与《基本业务功能规范》相比，增加了 5 个行业领域的常用服务类型的最少信息，分别是：运动健身、问诊挂号、浏览器、输入法和安全管理。此外，部分领域的名称也有变化，在《基本业务功能规范》中的“即时通讯社交”变为《信息收集规范》中的“即时通讯”，“社区社交”变为了“博客论坛”，“房产交易”变为“房屋租售”，“汽车交易”变为“二手车交易”。对于前三个领域其业务功能并无实质性变化，而后两个领域的变化明显缩小了适用范围，究其原因是为了更贴近实际 App 的使用情况。

其次，《基本业务功能规范》中的第五部分“通用功能相关必要信息”在《信息收集规范》中并无体现，而后者在附录 B 中列出了“服务类型最小权限范围列表”，主要是针对 Android6.0 及以上的危险权限，给出了二十一类服务类型的最小权限范围，二十一类服务类

型中，无一类服务需要申请通讯录、照相机、麦克风等权限。

第三，从《信息收集规范》附录 A 中各类收集信息所列内容来看，除了在《基本业务功能规范》列表中常见的使用要求说明以外，《信息收集规范》中的列表增加了“法律法规要求的个人信息”一栏，并在相应信息后列出了有此要求的法律规定名称，从实务操作角度为该标准的使用者提供了更好的依据参考以及检索便利。

从具体服务类型要求的最少信息规定表格内容来看，有以下四点值得注意：

首先，依照《网络安全法》和《移动互联网应用程序信息服务管理规定》，所有服务类型均增加可收集“网络日志”信息；除“快递配送”外的所有服务类型均增加了可收集“手机号码”信息，对公众账号信息发布服务使用者增加收集“身份证件号码”。

其次，删减了一部分基本功能可收集信息，在《基本业务功能规范》中“地图导航”功能的“行踪轨迹”，“即时通讯社交”功能的“好友信息”，“新闻资讯”功能中的“关注的账号”，“短视频”功能的“关注的账号”，“婚恋相亲”功能的“身高、学历、收入状况”。此类删减的信息主要为用户画像或个性化展示所需，此处传递出一个信号，即涉及到此类可能精准描述用户的信息需另外经过用户授权同意方可进行收集。

再次，《信息收集规范》中为保持与有关法律要求相一致，对“交易信息”仅做了概念性的列出，在“金融借贷”功能中虽无法律要求，但也只列出了“借贷交易记录”，另外，“房屋租售”功能下也仅列出“业主房产信息”，前述信息具体包含哪些细化内容则没有进一步展示。因此对运营者来说，这类信息收集的细化程度仍具有一定的自主决定权。

最后，所有涉及到“第三方支付”的信息均只有“第三方支付方式”被规定为服务类型所需的最少信息。相较于《基本业务功能规范》，《信息收集规范》中缺少了“支付状态”。虽然从一定程度上划分了 App 运营者与第三方支付运营者之间的权限，但是若此类信息在 App 上进行记录及向用户对付款状态作出提示也需要用户额外进行授权，是否会因此对客户体验造成影响仍然值得商榷。

除了上述变化外，笔者就规范的内容进行如下逐条解读：

1. 管理要求

a) App 运营者应履行个人信息保护义务，采取必要安全措施，保障用户个人信息安全。

《网络安全法》	第四十二条	网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。
《信息安全规范》	10.3 条	个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失。

从上述文件可知，本条的“安全措施”可以理解为管理措施和技术措施等，具体包含身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等措施。

b)当用户同意 App 收集某服务类型的最少信息时，App 不得因用户拒绝提供最少信息之外的个人信息而拒绝提供该类型服务。注:附录 A 列举了 App 常见的服务类型以及服务类型对应的最少信息。

《数据安全管理办法》	第十一条	个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。
《信息安全规范》	5．2	收集个人信息的最小化要求。

尽管上述文件中都提到了应收集核心业务功能所对应的最少信息，但是何为“最少”并没有予以明确，实践中，各家 App 还是按照自己判断的最少标准收集个人信息。《基本业务功能规范》曾对十六个行业的 App 所应收集的必要信息进行具体的描述，但是该文件位阶较低，仅具有指引作用，不能成为行政约束的参考文件，该文件公布后，也没有在市场中引起特别大的回声。

本次《信息收集规范》对二十一个行业的 App 收集服务类型的最少信息进行明确，同时限制了该等最少信息所对应的使用目的。该规范作为国家标准，其位阶高于《基本业务功能规范》，可以成为行政约束的参考性文件。

实践中，对于一些具有垄断地位的 App，在个人信息主体没有其他交易选择的情况下，只能授权该 App 收集非必要个人信息。可以预测，该规范落地后，对于 APP 收集非必要个人信息的行为必然具有警示和约束作用。

但是，也会存在一个疑问，该规范附录 A 中的二十一个领域的最少信息是合理的吗？如果实践中依据该规范对企业进行约束，是否会造成企业运营上的障碍？据笔者了解，即使同一行业中，由于运营者的差异，所需要收集的必要信息也有差异。比如在金融借贷类 App 中，不同企业的反欺诈措施不同，风控手段不同，所需要收集的必要个人信息亦不同，仅仅通过中国人民银行个人信用报告以及第三方个人信用评分，并不能有效支持企业做出授信决策。

笔者认为，收集最少信息起码应该是整个行业平均水平的企业所能够做到的，仅仅行业头部或者少数企业做到，可能会限制行业的发展；另外，对于每个行业中新萌芽的创新力量，严苛的最少信息收集可能会限制企业产品或服务的改善、更迭、获客、推广等，反而易造成行业垄断，头部企业由于已经收集了大量的个人信息，强者恒强，导致新生力量的发展门槛

变高。

最少信息的收集是否会依据《信息收集规范》中的附录 A 或者作为重要的参考依据，仍需拭目以待，但是不可否认的是，该附录将成为企业收集个人信息范围的重要指导内容。

c) App 不得收集与所提供的服务无关的个人信息。

本条在《自评估指南》评估项 7-27 中以及《APP 违法违规收集使用个人信息行为认定方法（征求意见稿）》（以下简称“《认定方法》”）第四条中均有提到，在此不赘述。

实践中，大多数 App 都有收集与所提供的服务无关的个人信息的情形，而该等收集授权也仅仅是在隐私政策中通过诸如“公司可能会收集和使用您的相关信息，您一旦选择使用 XX 软件及相关服务，即意味着同意公司按照本隐私政策收集、使用(含商业合作使用)、储存您的相关信息”等表述一揽子获得。

本条款再一次强调 App 不得收集与所提供的服务无关的个人信息，根据《信息收集规范》的上下文，意即，超出附录 A 最少信息以外的其他个人信息都不应收集，如需收集，App 应证明该等信息与其提供服务的相关性。

d)对外共享、转让个人信息前，App 应事先征得用户明示同意。当用户不同意,则不得对外共享、转让用户个人信息。

根据《信息安全规范》8.2 b）向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意。

本条款将“授权同意”进一步细化为“明示同意”，提高了同意的授权标准，与收集个人敏感信息划归为一类。根据《信息安全规范》，“明示同意”指个人信息主体通过书面主动声明或自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。（肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”等）。

同时，本条款将之前文件中的“应事先征得个人信息主体的授权同意”强化为“用户不同意，不得对外共享、转让用户个人信息”，从“应”到“不得”，可见规范度在进一步加强。

e) App 不得收集不可变更的设备唯一标识(如 IMEI 号、MAC 地址等)，用于保障网络安全或运营安全的除外。

根据《信息安全规范》附录 A，设备唯一标识(如 IMEI 号、MAC 地址等)属于个人信息，但是不包含在附录 B 个人敏感信息中。本条款强调“不得收集”，可见设备唯一标识也是重要个人信息之一。

据笔者了解，设备唯一标识并不是 App 保障网络安全和运营安全的必要收集信息，相

当 App 收集设备唯一标识的目的是用于广告分析、定向推送或间接获得其他个人信息。比如 MAC 地址与 IP 地址结合，可以获得手机移动轨迹；App 与广告公司合作，可以基于设备唯一标识追踪获得个人信息主体的其他信息。但是在一些 App 中，确实需要通过收集设备唯一标识保障安全，比如金融交易类 App，在发生用户交易纠纷的时候，需要明确什么账号，在什么时间，通过什么设备，什么 IP，提交的交易请求。

如果该条款落地，企业需要对其是否收集设备唯一标识进行评估，其所提供的理由能否达到保障网络安全或运营安全这个除外标准。

f)用户明确拒绝使用某服务类型后，App 不得频繁(如每 48 小时超过一次)征求用户同意使用该类型服务，并保证其他服务类型正常使用。

《新版信息安全规范》	5.3-d)	个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意。
	附录 C-C3-b)	个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，个人信息控制者不应反复征求个人信息主体的同意。除非个人信息主体主动选择开启扩展功能，在 24 小时内向用户征求同意的次数不应超过一次。
《认定方法》	第四条第 8 项	用户明确拒绝 App 收集个人信息请求，App 仍频繁征求用户同意，干扰用户正常使用。
《自评估指南》	评估项 7-28	对于用户明确拒绝使用、关闭或退出的特定业务功能，App 不应再次询问用户是否打开该业务功能或相关系统权限。

从上述文件中可以看出，对于限制“频繁”征求用户授权同意包括两个场景，第一个场景是使用、关闭或退出特定业务功能场景，第二个是收集个人信息场景。本条款指的是第一种场景，即，拒绝使用某服务类型后，App 不得“频繁”征求用户同意。

本条通过示例的方式对“频繁”进行界定，但是 48 小时也仅仅是示例，到底是参照 48 小时即可，亦或不能少于 48 小时，还是说 App 向用户明示本平台的“频繁”程度即可，不得而知。另外需要说明的是，此处的“48 小时”与《新版信息安全规范》附录 C 中的“24 小时”并不冲突，因为两者讲的并不是一个场景的情形。

g) App 应对其使用的第三方代码、插件的个人信息收集行为负责。第三方代码、插件收集个人信息视同 App 收集，App 应防止第三方代码、插件收集无关的个人信息。注:如第三方代码、插件自行向用户明示其收集、使用个人信息的目的、方式、范围，并征得用户同意，则第三方代码、插件独立对其个人信息收集行为承担责任。

《信息安全规范》	8．6 条	注:个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件(例如网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口)，且该第三方并未单独向个人信息主体征

		得收集、使用个人信息的授权同意，则个人信息控制者与该第三方为共同个人信息控制者。
《新版信息安全规范》	8．7 条	当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用本标准 8.1 和 8.6 的，对个人信息控制者的要求包括……
《数据安全管理办法》	第三十条条	网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

本条中的第三方代码、插件有两种性质，第一种不在 App 上露出，不单独向用户获得授权，用户难以感知，根据《信息安全规范》8.6 条的注释部分，该类第三方代码、插件与 App 属于共同个人信息控制者，用户无从约束该类第三方代码、插件，只能通过约束 App 来间接实现对该类第三方代码、插件的约束，当然，相应的责任也应该由 App 来承担。

比如，2017 年 8 月，第三方广告 SDK“个信”因被发现内置后门，在未经用户允许的情况下收集用户隐私数据，获取用户设备已安装 App 的列表信息，导致嵌入该 SDK 的 500 多款 App 被 Google Play 下架。

第二种会与用户进行交互，单独向用户获得授权，根据《新版信息安全规范》8.7 条，该类第三方代码、插件属于接入第三方，App 可以通过事前评估、记录、协议约定、审计等措施来约束该类第三方代码、插件，但《新版信息安全规范》并没有明确 App 是否对接入第三方的行为承担责任以及承担怎样的责任。

那么问题来了，根据《数据安全管理办法》第三十条：网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。该条款中的“第三方应用”指的是什么？是对应《信息安全规范》中共同个人信息控制者中的第三方还是《新版信息安全规范》中的接入第三方，亦或两者兼具？

第三方应用是由第三方运营且可以在 App 上实现单独的功能，如果对应共同个人信息控制者中的第三方，显然不露出的代码、插件等并不能实现单独的功能，仅仅是辅助角色。所以第三方应用更有可能对应《新版信息安全规范》中的接入第三方。根据上文，App 对第三方应用承担无过错推定责任，而本条中，对于单独露出的第三方代码、插件，App 不承担责任。

如前所述，单独露出的第三方代码、插件属于接入第三方，对应《数据安全管理办法》

中的第三方应用，在 App 的责任承担上存在两个文件上的差异。从文件的层级效力来看，《数据安全管理办法》显然高于《信息收集规范》，是否可以理解为，对于单独获得用户授权的第三方，仍旧应按照无过错推定责任来约束 App。鉴于这两份文件目前都属于征求意见稿，后续还需等待进一步的明确。

2. 技术要求

a) 当收集的个人信息超出服务类型的最少信息时，超出部分的个人信息，App 应逐项征得用户明示同意。

《新版信息安全规范》	5.3-a)	不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意各项业务功能收集个人信息的请求。
	附录 C-C.3-a)	在扩展业务功能首次使用前，应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意。

上述文件仅对扩展业务功能提出了逐项选择同意的要求，而本条款不仅针对扩展业务功能，还包括基本业务功能中收集非必要信息时也应逐项选择同意，App 不能在隐私政策中进行一揽子授权，意即，除了基本业务功能中的最少信息可以在隐私政策中直接获得授权外，基本业务功能中非必要个人信息以及扩展业务功能中所需个人信息的收集均需个人信息主体通过弹窗、填写框等逐项选择同意。

b) 当同一 App 有 2 种或 2 种以上服务类型时，App 应允许用户逐项开启和退出服务类型，开启或退出的方式应易于操作。

根据《新版信息安全规范》5.3-c）关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动。

与上条相比，本条款进一步强调了“逐项”，且将“开启”和“退出”并列进行说明。意即，App 不仅应向个人信息主体逐项展示关闭和退出的路径，还应逐项展示开启的路径，且该等路径应易于发现和操作。

c) 当用户退出某服务类型后，App 应终止该服务类型收集个人信息的活动，并对仅用于该服务的个人信息进行删除或匿名化处理。

根据《新版信息安全规范》5.3-c）关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动；同时，用户注销账户、退出个性化

展示或者超出个人信息保存期限后，应对个人信息进行删除或匿名化处理。

之前的文件仅规定了用户注销账户、退出个性化展示或者超出个人信息保存期限后三个场景的删除或匿名化处理行为，并未明确用户退出某服务类型后的删除或匿名化处理行为，本条款补充增加了该场景中的删除或匿名化要求。该条款与上条款中的逐项开启和退出呼应，上条款为本条款的实现提供了可能。

d)当申请个人信息相关权限或要求用户输入个人信息时，App 应向用户同步明示申请权限或收集信息的目的。

《信息安全规范》	5.4-a)	收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围，并获得个人信息主体的授权同意。
《数据安全规范办法》	第八条（三）	收集使用个人信息的目的、种类、数量、频度、方式、范围等。

上述文件均明确了 App 在收集个人信息之前应告知收集使用个人信息的目的。但是本条款更加细化到了申请个人信息相关权限或要求用户输入个人信息这两种场景中。

目前市场上的诸多 App 存在一个普遍的情形，即在用户打开 App 后展示隐私政策前，该等 App 通过弹窗的形式要求获得用户手机号码、IMEI、IMSI 权限，设备定位权限以及访问照片、媒体内容和文件的权限等，该等弹窗并未明示申请权限或收集信息的目的，以至于用户在点击“允许”的时候产生诸多质疑；部分头部 App 在用户一打开 App 时，即弹出隐私政策，通过隐私政策先行的方式获得用户的授权，但是在该等隐私政策中，也少有对于申请权限或收集信息的目的进行完整细致的描述。

本条款中提到了“同步”二字，笔者理解，App 通过隐私政策集中描述收集目的的方式无法实现“同步”，还应在获取用户权限和用户输入个人信息当下页面展示收集目的，用户在明确知晓收集目的后再决定是否授权。可见，本条款在之前文件的基础上，对这两种情形下的授权提出了更高的要求。

e)App 应向用户提供实时查询已收集个人信息类型的功能;查询结果应以独立界面展示，且查询方式应易于操作。

《新版信息安全规范》	5.5-a)-5)	个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法……等
《数据安全规范办法》	第八条（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。
	第二十一条	网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号。

上述文件均要求 App 提供查询方法，但没有具体明确何种方法，实践中，相当数量的 App 通过留存客服电话的方式提供查询，然而客服需要一定的反馈时间。本条款通过“实时查询”“功能”以及“独立界面展示”的标准对查询方法提出了新的要求，意即，App 应在展示页面上设置查询功能，且能实现实时输出查询结果，查询结果还须以独立界面展示以便于用户浏览和保存。

f) 存在对外共享、转让个人信息的，App 应向用户提供查询数据接收方身份的功能;查询结果应以独立界面展示，且查询方式应易于操作。

《信息安全规范》	8.2-b）	向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意。
《安全保护指南》	6.6-c)	在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息。
《自评估指南》	评估项 3-14	如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确接收方的类型或身份。

上述文件均提到了向个人信息主体告知数据接受方的类型，但是请注意，“接受方的类型”和“接受方的身份”是两个不同的概念，《自评估指南》中曾同时出现两个概念。接受方的类型我们可以理解为广告服务商、物流服务商等一个范围的界定，而数据接受方的身份似乎需要明确具体指向，但是需要明确到何种程度，以及是否会造成商业秘密的泄露，还需要后观。

g) 在技术可行且不影响终端和服务正常的情况下，App 应优先在用户终端中存储、使用所收集的个人信息。

对存储技术提出要求作为收集个人信息方面的标准来说，是否存在超出范围的问题尚存在讨论空间。该要求如何在具体的评估和监管中落地也需要进一步进行明确，例如如何定义“技术可行”、“不影响终端和服务正常”等前提条件。而用户终端存储所涉及的具体功能也无法进行细化并提出统一标准。

就笔者了解，微信聊天记录等信息以及 cookie 的相关记录可实行用户终端存储，但终端存储是否一定安全？以 cookie 为例，App 以外的第三方也可以实现调用用户访问 App 时放置的 cookie 并对用户的行为进行追踪。另外，如何对此类信息是否被备份至数据库并经 App 运营者进行进一步分析处理，用户无法对此进行感知，而通过技术手段测试对监管部门也提出了较高的成本要求。因此在之后该条技术要求是否会进行完善有待进一步观望。

h) App 应以实现服务所必需的最低合理频率向后台服务器发送个人信息。

《信息安全规范》	5.2-b）	自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率。
《认定办法》	第二条第 2 项	没有逐一列出收集个人信息的类型、频率，特别是针对个人敏感信息。

与之前的文件相比，该条款的“频率”指的是发送频率而不是收集频率，App 需要向用户告知收集个人信息的频率，但是收集后是否就一定会向后台服务器发送呢？笔者了解，不是所有 App 收集的个人信息都需要发送，有些缓存信息，当用户关闭 App 后即清除，App 后续也无法使用这些不存储在设备中的缓存信息，对个人信息主体造成的影响就非常有限。这样看来，真正影响用户的应是发送频率。

发送频率可以将个人信息类型转化，比如，某 App 为了提供服务必须收集位置信息，如果频繁收集且同时发送，该位置信息就会转化为行踪轨迹，而行踪轨迹属于个人敏感信息范畴，该类信息会对个人信息主体的人身、财产、名誉等产生重大影响。意即，App 即使由于提供服务所需必须频繁收集个人信息，也可以不回传至后台服务器，但是“最低合理频率”如何界定，恐怕还需要看市场的发展和反应。

总结，总体来看，当前的监管文件体现出监管部门倾向于通过加强对 App 运营者的管理作为主要的个人信息收集使用方面的安全控制手段。因此作为与用户使用具有直接关联的运营者，不仅需要对 App 的收集使用个人信息相关机制建立起符合要求的合规体系，而且在涉及到合作者及间接接触用户（如 SDK 等不向用户直接露出）的数据收集处理相关事项中也要发挥重要的安全保障功能。尽管该信息收集规范的细化要求是否会再进行调整，以及是否在正式通过后能在实践中发挥出监管预期的效果仍有待进一步观望，但可以确定，监管对 App 的合规要求在今后会进一步提高，运营者唯有将合规融入到产品从设计到推出以及与外部合作的与个人信息相关的全部流程中，才能在愈加规范的市场环境中获得用户的认可。（来源：数据法盟 作者：张丹、刘晓霞）

➢ 金融科技时代信息安全意识提升之路

金融科技时代，随着人工智能、大数据、云计算、区块链等新兴技术的蓬勃发展及其在风险控制、精准营销、运营管理等领域的广泛应用，运用个人信息实现“比你更懂你自己”的场景已经屡见不鲜。但正如习近平总书记所说，“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”，我们必须清醒地认识到，随着

金融科技的发展，金融企业和客户面临的网络安全问题日益突出，网络安全建设必须跟信息化建设同步规划、部署和实施。

为做好网络安全，金融企业往往借助于安全技术产品和服务来进行防护，但是“技防”永远无法完全取代“人防”的作用，内外部人员安全意识薄弱而导致的信息安全事件很难完全避免，所以需要形成体系化的安全意识提升机制，使安全意识建设成为一种企业文化，才能达到综合化、一体化、纵深化防御的效果。

一、安全意识概念辨析

安全意识，从本质上说，是对于风险感知并主动回避的能力。要理解安全意识，需要从以下三方面着手：

首先，要认识到安全意识不是一种虚幻的概念或感觉，而是一种能力，就像各种岗位必备的其他知识或者技能一样。这种能力应该被准确定义，所有岗位应该被精准赋能。具体而言，对内要放入岗位的基本能力要求，对外（合作伙伴、外部客户）要持续地培训和教育，而且均能通过一定手段计量、监测和考核。

其次，要认识到这是相关人员必须具备的能力，要实现横向到边、纵向到底、内外兼修的覆盖，即横向要跨业务条线，纵向要跨岗位、跨机构，整体覆盖上到董事会和高管层、下至基层员工的各级人员；外部要延伸到相关的合作伙伴和客户。各岗位、各层级、内外部干系人都必须具备安全意识，形成一张覆盖企业全范围及外部干系人的“安全意识网”。否则，

任何一个点的缺口一旦被攻破，整个企业的安全防护措施可能就会被击穿得千疮百孔。

第三，安全意识提升的目的，既需要防止主动违反安全规定，又需要防止被动违规。所谓主动违规，就是罔顾安全要求，主动从事风险事件，甚至主动规避风险防范措施；所谓被动，就是意识不到自己行动可能导致的风险，所谓“无知者无畏”。安全意识提升，就是要让主动违规的人员，能有震慑感、能认识到违规导致的风险，不敢不愿“铤而走险”；对于被动违规的人员，要培养敏感性，提升风险规避和应对能力。

二、金融企业安全意识提升的必要性

金融企业信息安全培训的必要性体现在四个方面：

1．金融企业涉及信息的敏感性极高。金融企业面向广大客户提供金融服务，涉及的信息主要包括与客户相关的信息（包括客户基本信息、客户账户信息以及客户交易信息等），以及金融企业经营管理活动相关的内部信息（包括战略规划信息、金融产品信息、经营活动信息等）。大多数信息安全事件的发生都源自于员工主动或被动地泄露敏感信息。

2．金融企业信息安全的核心问题是人的安全意识。任何的安全管理体系、安全技术、安全产品或服务，都无法保护每一个人远离每一种可能存在的安全风险。因为无论多么严密的管理体系、多么先进的设备、多么严谨的系统、多么完备的数据，如果员工的安全意识不足，将导致管理流于形式、设备形同虚设、数据空中楼阁。

3. 金融企业安全意识仍然普遍较为薄弱。大部分金融企业已经投入大量的资金购买安全技术，但是在人员安全意识提升上却投入甚少，往往忽略了人的安全意识薄弱是信息安全管理的最短板。

4. 金融企业安全事件层出不穷。客户信息泄露、网站被攻击或篡改、应用漏洞导致资金损失、钓鱼攻击导致勒索事件……，金融企业的信息安全事件，每出现一次都会造成很大的损失，引起广泛的关注。而根据信息安全研究机构的统计，在所有企业的信息安全事件中，70%-80%是由于内部员工的疏忽或有意泄露造成的。

三、金融企业安全意识提升面临的问题

增强员工安全意识，主要通过培训和教育来实现，但培训和教育存在五大问题：

1．未建立系统化的安全意识提升管理体系。安全意识培训是零散的、随需而做的，尚未形成整体的、有机的、立体的安全意识提升规划。

2．安全意识培训针对性不足，培训内容不接地气。由于需求分析不到位，经常是一套培训材料就“放之四海而皆准”，结果自然收效甚微。

3．安全意识培训形式单一、内容枯燥、素材匮乏、资源不足。采用课堂教学方式培训，

缺乏日常碎片式、体验式的素材，枯燥的培训方式自然效果不佳。

4．安全意识培训参与度不高。大部分金融企业的员工都非常忙碌，培训过程成了应付式的参与，往往“身在曹营心在汉”，导致培训效果大打折扣。

5．未建立安全意识提升的考核机制。未建立起有效的量化考核机制，缺乏技术手段、检查手段、考核机制来实现。

四、安全意识提升方法论

要实现安全意识有效提升，需要遵循四个步骤：

（一）找准对象

金融企业不同的工作岗位，接触的信息重要性和面临的风险状况不同，需要的信息安全知识和信息安全培训的侧重点也是不同的。

1．金融企业高管。金融企业高管应该首当其冲地成为信息安全培训受众，主要原因一是接触的信息面广、层次高、敏感信息多，是“性价比最高”的重点攻击对象；二是可以对全员安全意识提升起到表率作用。高管的安全培训重点应该放在信息安全战略和安全意识宣导方面，了解金融企业信息安全战略方向、信息安全相关法律法规、主要的信息科技监管要求和监管趋势、金融科技时代下信息安全新形势和管理新特点、信息安全组织架构、金融企业信息安全的特性、需要保护的主要信息类别和分布情况、主要的风险事件案例等。

2．中层管理者。金融企业的中层管理人员，是“承上启下”地执行战略和政策的中坚力量，需要贯彻执行企业的信息安全战略，同时带动基层员工主动落实信息安全防护措施。中层管理人员的信息安全培训，应侧重于信息安全基本概念、信息安全相关法律法规、信息科技监管要求及趋势、信息安全管理体系、主要的风险事件案例、业界最新风险防控思路及措施等。

3．所有部门基层员工。基层员工由于数量众多、接触的具体信息丰富，是最容易泄密的群体。基层员工的安全培训应侧重于银行信息安全相关的制度和流程的具体内容、信息安全行为相关的法律法规、敏感信息保护要求、敏感信息泄露行为导致的不良后果和真实案例、违规处罚措施、基本的信息安全操作技能和防护手段等。

4．信息科技员工。信息科技部门员工是信息安全政策落地的核心力量，更是信息安全管理和技术措施的直接执行者和捍卫者。信息科技部门各个不同团队的信息安全培训，有不同的侧重点：

（1）对于开发测试人员，应侧重于企业信息安全政策和制度、监管和行业组织发布的应用安全相关技术规范、密码技术和应用、需求分析安全要求、设计安全要求、编码安全要

求、安全测试要求，代码审计相关知识，以及系统和应用安全常见漏洞的原理、现象、漏洞扫描等发现方法、扫描结果评估方法和安全防范措施等；

（2）对于运维人员，应侧重于企业信息安全政策和制度、监管和行业组织的信息系统运维相关技术规范、机房安全、网络安全、主机及系统安全、终端安全、信息安全技术工具、故障应急、业务连续性等；

（3）对于信息安全岗员工，是信息安全培训体系的制定者和维护者，一方面应该掌握设计信息安全培训体系的方法，另一方面应接受有关监管趋势及要求、风险评估和安全检查知识和技能、信息安全技术工具的策略和操作技能等方面的培训。

5．外包人员。外包人员可能接触到金融企业的客户信息、系统开发和设计文档、源代码等大量的敏感信息，安全意识培训应侧重于外包制度和流程的具体内容、金融企业信息的分类和信息安全保护具体要求、与信息安全行为相关的法律法规、泄密行为导致的不良后果和真实案例等。

6．外部客户。大量的风险案例是由于客户对于个人客户信息保管不当、误安装病毒木马软件、误点击钓鱼邮件等原因造成的。外部客户的安全培训应侧重于具体的案例说明、主要的诈骗手段拆解、简明扼要的信息安全宣传标语等。

（二）用对方法

1．现场培训。现场培训是最常见的一种集中开展的培训形式，好处是大家精力比较集中，交流较为充分，在主题的选择上可以更为聚焦，讲解上可以更为深入。专题培训和交流会议，是两种常见的现场培训方式。

2．在线培训。由于 3A 的特性（Anytime，Anywhere，Anyway，任何时间、任何地点、多种方式），在线培训最适合针对全员的培训，特别适合普及性的、内容相对简短的培训，推荐的方式是选择一些重要的知识点，用案例的方式生动活泼地表现出来，其中穿插讲解风险要点、规避措施和管理要求。

3．开办内外部信息安全专栏。一方面在内部门户系统或办公自动化系统中开设信息安全专栏，随时发布信息安全相关的内容，包括主要的信息安全法律法规要点、国家和监管层面关于网络安全防范的重要战略和指示精神、信息安全事件及防范措施等；另一方面开设外部专栏，例如在微信公众号上发布安全意识相关的文章、图片、视频，向客户宣贯信息安全相关热点新闻、案例和风险防范技巧。

4．以赛代训。通过竞赛的方式，提高培训对象的参与度，调动培训对象的热情。竞赛方式包括合规知识竞赛（针对信息安全知识和技能要求设计形式活泼的考题）、信息安全创

意作品大赛（征集征文、摄影、视频、诗歌、宣传画报、漫画等各种各样的创意作品）、微信游戏比赛（在微信中设置一些信息安全小游戏，例如答题闯关、有奖查漏、捉对厮杀、双人 PK 等）、CTF 攻防大赛（在比赛规则中设计漏洞查找、问题解答、安全加固、相互攻击等模式，通过实战提升安全专业技能）等。

5．信息安全实战演练。采用“真演实练”的方式，模拟真实的攻击场景，检验员工的安全意识和面对攻击的应对水平。常见演练场景包括钓鱼邮件和病毒木马、社会工程学方式、撞库测试、弱口令测试等，测试结束后必须开展专题的案例分析和总结，详解攻击原理和过程，向员工宣导正确的防范措施。

6．信息安全活动宣传周/宣传月等。借助国家网络安全宣传周、科技宣传周等契机，在金融企业内部成立自己的信息安全活动宣传周/宣传月，通过视频、走马灯、画报、宣传手册、有奖知识问答、微信或微博展示等形式，向全行及外部客户推广、宣传信息安全理念。

7．无处不在的安全宣传。安全意识宣传“抬头不见低头见”，例如在电梯口的视频电视中持续播放安全意识宣传动画，在食堂墙报上张贴安全意识的口诀或者漫画，在过道拉起安全意识的宣传“易拉宝”，在办公环境中的会议室、文印室、办公座位等场所张贴“信息安全温馨提示”，在办公电脑的桌面屏保推送“信息安全宣传口号”或者“信息安全宣传墙纸”，人手一册发放有安全知识的笔记本等。

8．定期发送风险提示。针对防钓鱼、弱口令、外发邮件安全、客户信息保护等常见的信息安全风险，制作风险提示或者电子期刊，结合实际案例讲解安全风险的常见表现、解决措施等，主动推送给企业内部员工和外部客户。

9．信息安全智能机器人系统。参照智能客服的模式，以人工智能技术构建自动客服系统，建立信息安全智能知识库，涵盖信息安全基础知识、信息安全制度、信息安全案例、信息安全风险防范技巧等丰富的内容。

10．外部提供的信息安全培训组合服务。针对信息安全专业团队资源不足的情况，购置第三方信息安全培训组合服务。培训组合服务可以通过信息安全动画、宣传片、视频课程、宣传画、知识手册、屏保、电子期刊、现场培训等多种形式提供。

（三）抓住时机

1．全员每年例行做。例如，每年固定一个时间开展信息安全现场培训或者交流，或者每年固定一个时间组织全员参与在线培训等。

2．员工入职马上做。新员工在入职后一个月内需要开展信息安全培训，最好采用现场培训的方式开展，帮助新员工了解企业的信息安全文化和信息安全管理原则，初步掌握信息

安全相关的基本知识与技能，养成良好的安全习惯。新员工的安全意识培训考核结果，可以与员工的转正相结合。

3．高危人士时常做。针对接触企业大量数据的信息科技人员、接触大量客户敏感信息的营销人员、掌握战略或人力资源管理等内部信息的关键岗位员工等“高危人士”，需要加大信息安全培训的频率，至少每半年接受一次培训，部分内容可以一直重复、常讲常新。

4．专业人士专场做。针对信息科技开发、运维、安全等直接从事信息安全风险防范工作的人士，定期组织专场的培训，深入学习最新的信息安全技术和理论知识，形成体系化的知识结构。

5．特殊事件重点做。在出现安全事件等特殊情况后，立即开展案例分析，分析事件发生的原因、影响、后续措施等，着重于分析采取何种措施可以避免今后发生类似问题。

6．客户嵌入流程做。将针对客户的培训嵌入到业务流程中，在客户办理业务的时候配套提供，例如自助设备、手机银行、网银操作中嵌入关于防止密码泄露、防止电信诈骗的风险提示，发现可疑操作后的电话或短信提示，以及客户登录密码错误后的提醒等。

（四）效果衡量

1．衡量培训组织情况。包括培训计划执行率、培训覆盖率（细分为全员培训覆盖率、新员工培训覆盖率、外包人员培训覆盖率等指标）。

2．衡量直接的培训效果。一般先组织笔试，然后将笔试结果作为衡量因素，可以设置的指标包括培训平均分、培训合格率等。

3．衡量培训执行效果。通过日常信息安全检查工作的结果来衡量，包括“信息安全日常行为抽检合格率”、“制度执行抽检违规率”、“信息安全泄密事件”、“重大信息安全责任事件”等。（来源：《中国信息安全》杂志 2019 年第 6 期）

➢ 云计算安全的法律风险分析

随着计算机技术的快速发展，传统的互联网技术和服务已无法满足大数据及计算服务的需求，在这种背景下，云计算应运而生。自 2006 年云计算概念第一次被提出开始，十几年来，它的发展一直备受国内外关注，被看作是信息技术变革和商业模式变革的核心。

具体来说，云计算是一种模型，它能支持用户便捷地按需通过网络访问一个可配置的共享计算资源池（包括网络、服务器、存储、应用程序、服务）。共享池中的资源，能够以最

少的用户管理投入或最少的服务提供商介入实现快速供给和回收。

目前，云计算还面临着很多的安全风险。从技术层面上来说，云计算提供的服务可分为 Iaas、PaaS 和 SaaS 三个层面，IaaS 的虚拟化技术、PaaS 的分布式处理技术以及 SaaS 的应用虚拟化技术是构建云计算核心架构的关键技术，也是云计算所面临的技术风险的主要来源。从管理层面上来看，由于云计算中数据的所有权和管理权相分离，用户将自己拥有的数据存储到云服务提供商处，由云服务提供商进行全面管理，用户并不能直接控制云计算系统；而云服务提供商没有对云数据的所有权，无法直接对数据本身进行查看和处理。另外，云服务提供商无法得知用户使用的终端及进行的相关操作是否安全，由此可能引发许多不可控的、意料之外的风险。因此，与传统的 IT 架构相比，云计算面临着许多新的管理风险。

针对这些技术和管理上的风险，2019 年 5 月 13 日，《网络安全等级保护基本要求》正式发布。相对于旧版的等级保护制度，新版的等级保护制度对云计算在技术和管理两方面的安全问题提出了具体的措施，例如在“网络架构”、“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”、“云计算环境管理”、“云服务上的选择”等方面提出了具体化的要求。但是，云计算作为一种新型的服务模式，除了技术和管理上的风险，其具有的虚拟性及国际性等特点也催生出了许多法律和监管层面的问题，使云服务面临着多方面的法律法规风险。

法律风险分析

第一个法律风险是数据跨境存储和传输问题。

云计算具有地域性弱、信息流动性大的特点，一方面，当用户使用云服务时，并不能确定自己的数据存储在哪里，即使用户选择的是本国的云服务提供商，但由于该提供商可能在世界的多个地方都建有云数据中心，用户的数据可能被跨境存储；另一方面，当云服务提供商要对数据进行备份或对服务器架构进行调整时，用户的数据可能需要转移，因而数据在传输过程中可能跨越多个国家，产生跨境传输问题。因此，云服务商需要熟悉各国关于数据跨境的相关规定。例如，欧盟的《通用数据保护条例》规定：欧盟公民的个人数据只能在满足该条例的条款下流动，居民个人信息（这些个人信息可能是不包含任何隐私的）数据进行合法的跨境存储和传输，则该云服务提供商需要满足某些条件。而在一般情况下，涉及欧盟业务的云服务提供商很难满足条件的要求。

因此，云服务提供商必须筛选出那些包含欧盟居民个人信息的数据，并将它们严格存储在欧盟境内的数据中心内部，否则就违反了欧盟法律的相关规定。

我国于 2016 年发布的《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国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。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。这条规定就限制了云计算服务商必须将存储有我国公民各种信息的服务器部署在中国。

第二个法律风险是隐私保护问题。

在云计算环境中，用户数据存储在云中，加大了用户隐私泄露的风险。在云服务中，云服务提供商需要切实保障用户隐私，不能让非授权用户以任何方法、任何形式获取用户的隐私信息。然而，一些国家的隐私保护法却明确规定，允许一些执法部门和政府成员在没有获得数据所有者允许的情况下查看其隐私信息，以切实保护国家安全。

因此，云服务中的隐私保护策略与某些国家的隐私保护法的相关规定可能产生矛盾。例如，美国的爱国法法案授权美国的执法者为达到反恐的目的，可以经法庭批准后，在没有经过数据所有者允许的情况下查看任何人的个人记录。这意味着，如果云用户的数据存储在美国境内，那么美国的执法者可以在经过法庭批准后，在用户毫不知情的情况下获取用户的所有云数据，查看用户的所有隐私信息，而这势必会对公民的隐私造成一定威胁。

在我国，2017 年出台了《中华人民共和国个人信息保护法》（草案），该草案提出：信息处理主体应当采取合理的安全措施保护个人信息，防止个人信息的意外丢失、毁损，非法收集、处理、利用。但同时又指出，国家机关因履行法定职责，并为实现收集个人信息的目的，

可以处理和利用个人信息。对于云服务商来说，如何既确保用户数据不被泄露、又不危害国家安全便成为一个棘手的问题。

第三个法律风险是犯罪取证问题。

在云环境中进行犯罪取证时，首先要进行数据采集，即在可能存有证据的数据源中鉴别、标识、记录和获得电子数据。由于云中的数据不再是保存在一个确定的物理节点上，而是由云服务提供商动态提供存储空间，因此数据源可能存储在不同的司法管辖范围内，使司法人员难以采集到完整的犯罪证据。另外，云数据的流动性很强，如果数据的采集顺序不合理，短时间内很多重要的数据就可能丢失且很难被找回。此外，云环境下的犯罪取证过程至少需要涉及云服务提供商和客户端，由于多租户环境下有海量的客户端接入到云服务中，因此云服务提供商和客户端之间的依赖关系是动态变化的。另外，云服务提供商和云计算应用大都依赖于其它的提供商和应用，这样就又形成了一条依赖链。在这种情况下，犯罪取证需要针对多条依赖链进行，若任何一条依赖链断开，都可能影响取证过程和取证结果。进行犯罪取证时，既需要获取和保存相关证据，又不能给其他用户的数据带来安全风险。由于云数据共享存储设备，因而如何进行数据分离使其他用户的隐私信息不因实施犯罪取证而泄露，也是云环境下犯罪取证的一大难题。

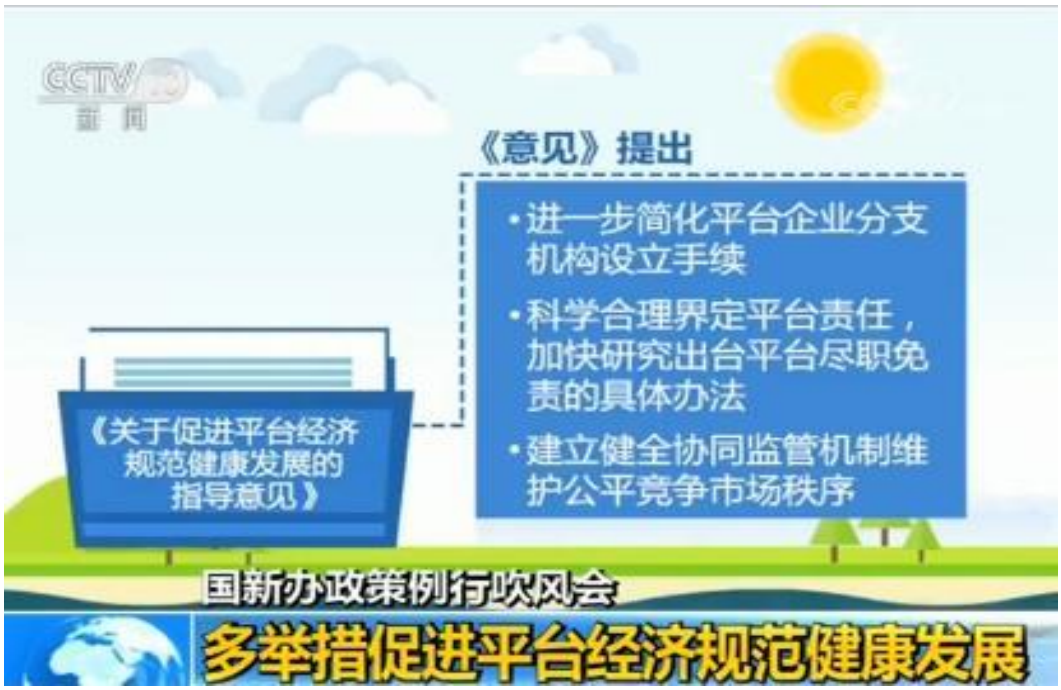
总述

从以上分析可以看到，虽然这几年云计算的发展十分迅速，甚至可以说进入了成熟发展的阶段，但如何保障云计算的安全却仍然是一个重大的课题，特别是针对云计算这种有别于传统 IT 结构的新型服务模式，相关的立法工作仍处在比较滞后的阶段。当前的信息技术发展很快，但是相关的法律法规的更新却需要一个极为漫长的过程，在这个过程中，难免会有很多人钻法律空子，利用这种发展不对等来实施一些危害他人或社会的行为。我认为，在一个新的技术发展过程中，有关部门应该及时给予关注和引导，主动同该技术领域的专家进行合作，及时的制定和颁布规章制度，这样不仅有利于新技术的合法发展，也能有效的保护社会和国家的利益。（来源：中国保密协会科学技术分会）

四、政府之声

➢ 国务院办公厅关于促进平台经济规范健康发展的指导意见

2019 年 8 月 1 日，国务院办公厅印发《关于促进平台经济规范健康发展的指导意见》（以下简称《意见》）。《意见》指出，要坚持以习近平新时代中国特色社会主义思想为指导，持续深化“放管服”改革，围绕更大激发市场活力，聚焦平台经济发展面临的突出问题，加大政策引导、支持和保障力度，落实和完善包容审慎监管要求，推动建立健全适应平台经济发展特点的新型监管机制，着力营造公平竞争市场环境。为促进平台经济规范健康发展，《意见》提出了五个方面政策措施。



一是优化完善市场准入条件，降低企业合规成本。推进登记注册便利化，进一步简化平台企业分支机构设立手续，放宽新兴行业企业名称登记限制；清理和规范制约平台经济健康发展的行政许可、资质资格等事项，指导督促有关地方评估网约车、旅游民宿等领域的政策落实情况，优化完善准入条件、审批流程和服务；加快完善新业态标准体系，为新产品新服务进入市场提供保障。

二是创新监管理念和方式，实行包容审慎监管。探索适应新业态特点、有利于公平竞争的公正监管办法，分领域制定监管规则和标准，在严守安全底线的前提下为新业态发展留足空间；科学合理界定平台责任，加快研究出台平台尽职免责的具体办法；建立健全协同监管

机制，积极推进“互联网+监管”，维护公平竞争市场秩序。

三是鼓励发展平台经济新业态，加快培育新的增长点。发展“互联网+服务业”，支持社会资本进入基于互联网的医疗健康、教育培训、养老家政、文化、旅游、体育等新兴服务领域；发展“互联网+生产”，推进工业互联网创新发展；推进“互联网+创业创新”，依托互联网平台完善全方位创业创新服务体系；加强网络支撑能力建设。

四是优化平台经济发展环境，夯实新业态成长基础。加强政府部门与平台数据共享，上线运行全国一体化在线政务服务平台电子证照共享服务系统；加大全国信用信息共享平台开放力度，支持平台提升管理水平；建成全国统一的电子发票公共服务平台，尽快制定电子商务法实施中的有关信息公示、零星小额交易等配套规则。

五是切实保护平台经济参与者合法权益，强化平台经济发展法治保障。抓紧研究完善平台企业用工和灵活就业等从业人员社保政策，开展职业伤害保障试点；加强消费者权益保护，督促平台建立健全消费者投诉和举报机制；完善平台经济相关法律法规。

《意见》要求，各地区各部门要按照职责分工抓好贯彻落实，压实工作责任，密切协作配合，切实解决平台经济发展面临的突出问题，推动各项政策措施及时落地见效。（来源：国务院办公厅 ）

- **《国务院办公厅关于促进平台经济规范健康发展的指导意见》**
- **全文：**http://www.gov.cn/zhengce/content/2019-08/08/content_5419761.htm

➢ 信息安全技术移动互联网应用 App 收集个人信息基本规范（草案）征求意见

2019 年 8 月 8 日，《信息安全技术移动互联网应用收集个人信息基本规范（草案）》发布，面向社会公开征求意见。移动应用程序提供服务调取用户信息将有规范可依。草案提出：App 运营者应履行个人信息保护义务，采取必要安全措施，保障用户个人信息安全。草案对网贷 App 提出了要求，应允许用户在金融借贷应用中手动输入紧急联系人信息，而不应强制读取用户的通讯录。

全国信息安全标准化技术委员会秘书处工作人员何延哲介绍，“金融借贷 App 这一类，我们提出紧急联系人是可以收集的，有的 App 是通过上传通讯录的方式收集紧急联系人，我们认为它超出了必要信息的范围。”草案还列出了地图导航、网络约车、即时通讯等 21 种常用类型的 App 可收集到的最少信息及使用要求。当用户拒绝提供最少信息之外的个人信

息时，App 不得以任何理由拒绝该类型服务。何延哲说：“一定要是用户可选的、用户可知的，用户如果愿意上传、愿意使用创新功能，那是可以的。”

草案提出：App 不得收集与所提供的服务无关的个人信息。对外共享、转让个人信息前，App 应事先征得用户明示同意。App 应对其使用的第三方代码、插件的个人信息收集行为负责。（来源：国家互联网信息办公室）

- **《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》**
- **全文：**http://www.cac.gov.cn/2019-08/08/c_1124853418.htm

➢ 工信部综合整治骚扰电话专项行动工作会在京召开

2019 年 8 月 15 日，工业和信息化部信息通信管理局在北京组织召开综合整治骚扰电话专项行动工作会，会议主题是深入贯彻落实党中央“不忘初心、牢记使命”主题教育相关要求，进一步加大骚扰电话源头治理力度，深入推进骚扰电话综合整治，切实解决人民群众关注的突出问题。最高人民法院、最高人民检察院、教育部、公安部、司法部、人力资源和社会保障部、住房和城乡建设部、文化和旅游部、国家卫生健康委员会、中国人民银行、国家市场监督管理总局、中国银行保险监督管理委员会、中国证券监督管理委员会等十三部门参加会议。

会上，各部门交流了本行业骚扰电话治理工作开展情况，通报了骚扰电话问题严重的源头企业情况，并结合当前出现的新情况新问题，对后续治理重点和举措进行了深入交流和探讨。

各部门均表示将继续按照党中央“不忘初心、牢记使命”主题教育相关要求，切实落实国务院治理骚扰电话有关部署，加强各自行业内部管理，健全完善行业内电话营销规则，建立完善行业营销主体名单库，依法查处违规拨打商业营销电话的企业，共同推进综合整治骚扰电话工作，以显著的治理成效迎接建国七十周年。（来源：工业和信息化部）

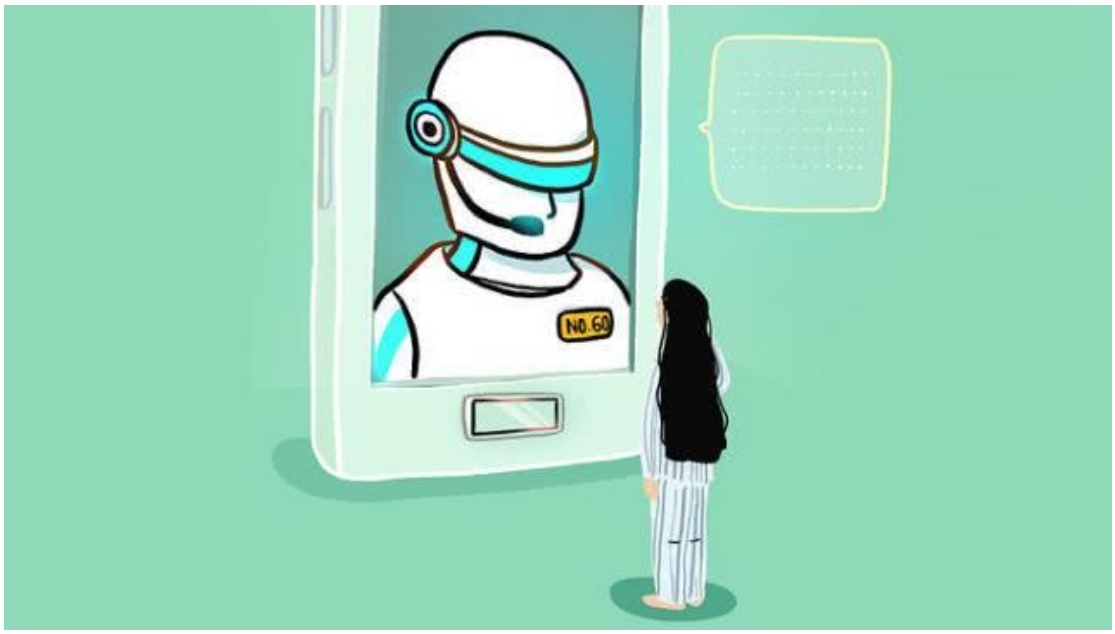
➢ 《上海市互联网医院管理办法》9 月 1 日施行

2019 年 8 月 12 日，上海市卫健委发布《上海市互联网医院管理办法》，这一管理办法将于 9 月 1 日起施行。这一文件明确将“互联网医院”定义为“包括作为实体医疗机构第二

名称的互联网医院，以及依托实体医疗机构独立设置的互联网医院”。

互联网医院的诊疗服务范围有哪些?

这一文件明确规定，互联网医院开展的诊疗服务应符合实体医疗机构或依托实体医疗机构的功能定位，并在《医疗机构执业许可证》登记的执业范围内，主要包括：常见病和慢性病患者随访和复诊、家庭医生签约服务。同时，文件还明确了准入标准、监督管理等，明确卫生健康行政部门通过管理平台对互联网医院实施监管，重点监管互联网医院的人员、处方、诊疗行为、患者隐私保护和信息安全等内容。



这一文件也对互联网医院的信息化建设与管理提出要求。如在病历资料管理方面，要求互联网医院为患者建立电子病历，并按照规定做好病历的保管、借阅与复制、封存与启封、保存。

互联网医院开展互联网诊疗服务过程中所产生的文字、符号、图表、图形、数据、音频、视频等数字化信息，应按照电子病历要求管理，资料传输、保存时应做好加密处理。患者可以在线查询检查检验结果和资料、诊断治疗方案、处方和医嘱等病历资料。（来源：网信上海）

- **《上海市互联网医院管理办法》**
- **全文：**http://wsjkw.sh.gov.cn/yzgl3/20190812/64913.html

五、本期重要漏洞实例

➢ 关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告

发布日期：2019-08-14
更新日期：2019-08-14
受影响系统：
Windows 10 for 32-bit Systems、Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems、Windows 10 Version 1607 for x64-basedSystems
Windows 10 Version 1703 for 32-bit Systems、Windows 10 Version 1703 for x64-basedSystems
Windows 10 Version 1709 for 32-bit Systems、Windows 10 Version 1709 for 64-basedSystems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems、Windows 10 Version 1803 for ARM64-basedSystems
Windows 10 Version 1803 for x64-basedSystems、Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-basedSystems、Windows 10 Version 1809 for x64-basedSystems、Windows 10 Version 1903 for 32-bit Systems、Windows 10 Version 1903 for ARM64-basedSystems、Windows 10 Version 1903 for x64-basedSystems
Windows 7 for 32-bit Systems Service Pack 1、Windows 7 for x64-based Systems ServicePack 1
Windows 8.1 for 32-bit systems、Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 R2 for tanium-BasedSystems Service Pack 1、Windows Server 2008 R2 for x64-basedSystems Service Pack 1、Windows Server 2008 R2 for x64-basedSystems Service Pack 1 (Server Core installation)
Windows Server 2012、Windows Server 2012 (Server Coreinstallation)
Windows Server 2012 R2、Windows Server 2012 R2 (Server Coreinstallation)
Windows Server 2016、Windows Server 2016 (Server Coreinstallation)
Windows Server 2019、Windows Server 2019 (Server Coreinstallation)
Windows Server, version 1803 (Server CoreInstallation)、Windows Server, version 1903 (Server Coreinstallation)
Windows 10 Version 1803 for 32-bit Systems、Windows 10 Version 1803 for ARM64-basedSystems
Windows 10 Version 1803 for x64-basedSystems、Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-basedSystems、Windows 10 Version 1809 for x64-basedSystems、Windows 10 Version 1903 for 32-bit Systems、Windows 10 Version 1903 for ARM64-basedSystems、Windows 10 Version 1903 for x64-basedSystems
Windows Server 2019、Windows Server 2019 (Server Coreinstallation)、Windows Server, version 1803 (Server CoreInstallation)、Windows Server, version 1903 (Server Coreinstallation)
描述：

CNTA-2019-0028
2019 年 8 月 14 日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft 远程桌面服务远程代码执行

漏洞（CNVD-2019-27323 、CNVD-2019-27324、 CNVD-2019-27325 、CNVD-2019-27326）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节虽未公开，但已引起社会高度关注，微软公司已发布官方补丁。

Microsoft Windows 是美国微软公司发布的视窗操作系统。远程桌面连接是微软从 Windows 2000 Server 开始提供的组件。2019 年 8 月 13 日，微软发布了安全更新补丁，其中修复了 4 个远程桌面服务远程代码执行漏洞，CVE 编号分别为：CVE-2019-1181、CVE-2019-1182、CVE-2019-1222、CVE-2019-1226。未经身份验证的攻击者利用该漏洞，向目标服务端口发送恶意构造请求，可以在目标系统上执行任意代码。该漏洞的利用无需进行用户交互操作，存在被不法分子利用进行蠕虫攻击的可能。

CNVD 对该漏洞的综合评级为“高危”。

建议：

厂商补丁：

目前，微软官方已发布补丁修复此漏洞，CNVD 建议用户立即升级至最新版本：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

附：参考链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

➢ IBM Financial Transaction Manager 信息泄露漏洞

发布日期：2019-08-13

更新日期：2019-08-13

受影响系统：

IBM Financial Transaction Manager for CPS 3.2.1.0

IBM Financial Transaction Manager for Digital Payments 3.2.1.0

描述：

BUGTRAQ ID: 106733

CVE(CAN) ID: CVE-2018-2026

IBM Financial Transaction Manager 是美国 IBM 公司的一种面向服务的体系结构（SOA）行业软件产品，可用于创建管理，协调和监控财务事务的集成应用程序。用于数字支付的 IBM Financial Transaction Manager 3.2.1 版本中存在信息泄露漏洞。经过验证的攻击者可利用该漏洞获取内部产品文件的目录列表。

<*来源：IBM （ncsupp@ca.ibm.com）

链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10795544
https://www-01.ibm.com/support/docview.wss?uid=ibm10795536

建议：

厂商补丁：
IBM
IBM 已经为此发布了一个安全公告（155552）以及相应补丁：
155552：Security Bulletin: Financial Transaction Manager for Corporate Payment Services is affected by a potential directory listing of internal product files vulnerability (CVE-2018-2026)
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10795544

➢ 多款 Zoho ManageEngine 产品本地权限提升漏洞

发布日期：2019-08-06
更新日期：2019-08-06
受影响系统：
zoho Corporation ManageEngine DesktopCentral 10.0.380
zoho ManageEngine ADSelfService Plus 5.7
zoho ManageEngine ADManager Plus 6.6.5
描述：

BUGTRAQ ID: 109298
CVE(CAN) ID: CVE-2019-12876
ZOHO ManageEngine ADSelfService Plus 是美国卓豪公司的一套基于 Web 的终端用户密码管理软件。ZOHO ManageEngine ADManager Plus 是美国卓豪公司开发的一套为使用 Windows 域的企业用户设计的微软活动目录管理软件。Desktop Central（DC）是美国卓豪公司的一套桌面管理解决方案。
ZOHO ManageEngine ADManager Plus 6.6.5，ADSelfService Plus 5.7 和 DesktopCentral 10.0.380 版本中存在不安全权限。本地攻击者可利用该漏洞在受影响系统的上下文中获得提升的权限。
<*来源：Chase Dardaman a?? Adversarial Engineer | SECTION8, CRITICALSTART Quentin Rhoads-Herrera a?? Offensi
链接：https://www.criticalstart.com/2019/07/manageengine-privilege-escalation/
建议：

厂商补丁：
CriticalStart
CriticalStart 已经为此发布了一个安全公告（CVE-2019-12876）以及相应补丁：
CVE-2019-12876：MANAGEENGINE PRIVILEGE ESCALATION
链接：https://www.criticalstart.com/2019/07/manageengine-privilege-escalation/

➢ Cisco IOS Access Points Software 拒绝服务漏洞

发布日期：2019-08-06
更新日期：2019-08-06
受影响系统：
Cisco IOS Access Points Software 8.7

Cisco IOS Access Points Software 8.6
Cisco IOS Access Points Software 8.5
Cisco IOS Access Points Software 8.4
Cisco IOS Access Points Software 8.3
Cisco IOS Access Points Software 8.2
Cisco IOS Access Points Software 8.1
Cisco IOS Access Points Software 8.0
Cisco Aironet 3700 Series Access Points

不受影响系统：

Cisco IOS Access Points Software 8.9
Cisco IOS Access Points Software 8.8.100.0
Cisco IOS Access Points Software 8.8
Cisco IOS Access Points Software 8.5.131.0
Cisco IOS Access Points Software 8.3.150.0
Cisco IOS Access Points Software 8.2.170.0

描述：

BUGTRAQ ID: 109312
CVE(CAN) ID: CVE-2019-1920
Cisco IOS Access Points Software 是美国思科公司的一套专用于 Cisco 无线接入点设备的软件。
Cisco IOS Access Points Software 的 802.11r 快速过渡（FT）实施中存在拒绝服务漏洞，该漏洞源于发送到为快速过渡（FT）配置目标接口的客户端验证请求缺少完整的错误处理条件。未经验证的相邻攻击者可通过向目标接口发送特制的身份验证请求流量来利用此漏洞，从而导致设备意外重启。
<*来源：Cisco
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-aironet-dos

建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-20190717-aironet-dos）以及相应补丁：
cisco-sa-20190717-aironet-dos：Cisco IOS Access Points Software 802.11r Fast Transition Denial of Service Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-aironet-dos

六、本期网络安全事件

➢ 中信银行“断网”事件再敲警钟

2019 年 8 月 9 日，银保监会的一则处罚信息，意外暴露了中信银行的“重要信息系统中断”事件。试想，当你正准备买入一只快速上涨的股票，而突然银行的信息系统出了故障，你只能眼睁睁看着股票上涨而无法成交；当然，你可能还有更重要的业务因为银行信息系统故障而无法办理，给你造成了重大损失……正因为银行信息系统的极端重要性，银行很少出现信息系统故障，而一旦出现故障，要根据情况上报监管部门甚至国务院。

事故发生又隐瞒

2019 年 8 月 9 日，银保监会公布了今年的“天价”罚单，中信银行因十三项违法违规行为，被合计罚没 2223.7 万元，刷新今年以来银保监系统最高罚没金额记录。而且，这个罚单是自去年 12 月 7 日以来，银保监会机关 8 个月内开出的首张罚单。


中国银行保险监督管理委员会
China Banking and Insurance Regulatory Commission
机构概况 新闻资讯 政务信息 在线服务 互动交流
当前位置：首页 > 政务信息 > 行政处罚 > 银保监会机关行政处罚
发布时间：2019-08-09 文章来源：法规部
中国银行保险监督管理委员会行政处罚信息公开表
（银保监罚决字〔2019〕12号）
（中信银行股份有限公司）

行政处罚决定书文号			银保监罚决字〔2019〕12号
被处罚	当	名称	中信银行股份有限公司

罚单信息显示，中信银行“未向监管部门报告重要信息系统运营中断事件”，且认定“信息系统控制存在较大安全漏洞，未做到有效的安全控制”。

银行机构的信息系统中断会对企业造成很大的影响和损失。对于任何金融机构而言，确保业务运行不中断，关键数据得到充分保护，以及在意外发生时，能够实现数据的实时恢复，

这都是业务运营中的重中之重。因此，银行的信息系统会面临着更加严格的国家监管。但是，作为股份制银行第一梯队的中信银行，却在信息系统安全性上“掉链子”，以致遭到银保监会的严厉处罚。

监管严查信息系统风险

信息系统安全运行是商业银行业务正常开展的重要保障和基本前提，关乎商业银行声誉、金融安全和社会稳定。银行服务对象复杂、分布广泛，所提供的金融服务与个人、企业利益乃至国民经济息息相关，一旦发生重大信息科技事件，会引起一系列的连锁反应。（来源：互联网综合整理）

➢ 男子在朋友圈骂人被罚 1000 元 法官:构成名誉侵权

2019 年 8 月 6 日，重庆市合川区人民法院就判决了一起因当事人在朋友圈骂人最终赔偿对方精神损害抚慰金的案子。据悉，柳某与皮某是微信好友。今年 1 月 28 日晚，皮某在微信应用程序中以微信号为“p*****91*”、微信名为“皮××”的个人账号朋友圈中发表言论，称柳某“破坏了别人家庭就该夹起尾巴做人！”“接受了高等教育的人到头来当小三，真是给你祖宗十八代都蒙羞！”“哪个都没屏蔽，随便看，敢做就堵不住让人说！”同时配有柳某照片一张。1 月 30 日，皮某又在其个人账号朋友圈中发表相关文字并配图。

当天，柳某委托律师向皮某发出律师函，要求皮某删除针对柳某的所有不当言论，并在微信平台公开发布道歉信息。皮某收到律师函后，删除了自己于 1 月 28 日在微信朋友圈发

布的内容，但双方就赔礼道歉、赔偿损失等未达成一致意见。因此，柳某诉至合川法院。

合川法院经审理认为，皮某出于个人情绪和主观推断，擅自在微信平台上公开发布柳某照片，并配上关于柳某隐私及带有侮辱性的文字，导致柳某名誉受到损害。皮某的行为已构成名誉侵权行为，应当依法承担侵权责任。皮某发表言论的范围仅限个人朋友圈，且及时删除 1 月 28 日的评论，对柳某名誉的影响力有限。根据侵权人的过错程度，侵权的手段、场合、行为方式及造成的后果，判决皮某立即删除 1 月 30 日在微信朋友圈中所发布针对柳某的不当言论，并于判决生效后 3 日内赔偿柳某精神损害抚慰金 1000 元，同时在微信朋友圈中发表道歉声明(内容由法院审定)。

所谓名誉权，是指公民或法人保持并维护自己名誉的权利。那么朋友圈发布的言论，达到何种程度，构成侵犯名誉权呢?侵犯名誉权的行为，客观上存在损害他人名誉的事实，传播损害他人名誉的虚假言辞，并为第三人知悉，包括：

(1)以语言或行动，公然损害他人人格、毁坏他人名誉，比如不当的言词评价、贬低和毁损相对人的人格，但不涉及“事实”的真实性问题;

(2)捏造并散布虚假事实，破坏他人名誉;

(3)故意披露、散布法律所保护的他人私生活信息。

其次，从主观过错方面来看，行为人存在实际恶意，并在客观上造成他人的社会评价降低。再者，受害者应为特定的人，不管是行为人指名道姓，还是指桑骂槐，只要在特定的环境和条件下，能够确定被侵害对象，同样构成侵害名誉权。最后，侵权行为给受害人名誉造成严重损害，使得受害人精神和心灵遭受创伤，尤其是公众对其社会评价降低，带来的不良影响。

所以即使在朋友圈发布不实消息，哪怕指桑骂槐，若能对应当事人，造成当事人的社会评价降低，依然构成侵犯名誉权，受害人有权诉请法院，责令侵权人停止侵害、恢复名誉、消除影响、赔礼道歉、赔偿损失。

警方提示：随着自媒体平台的普及和应用，个人言论自由的时空范围已被极大地拓展。新媒体在带来诸多便利的同时，也带来了新矛盾、新问题。在自媒体平台上，言论超出应有界限的情况时有发生。这些内容一定不能发！

1、谣言：在不掌握真实情况前，一定不可盲目散布、转发谣言。对未经核实的信息，不要随意转发，更不要故意“杜撰改编”，否则，将承担相应法律责任。对故意传播、散布谣言信息的，公安机关将依法严惩。

2、谩骂：如今，微信朋友圈就像是我们的“日记本”，记录着我们生活中的点点滴滴，

越来越多的人会在微信朋友圈上分享开心的事、吐槽不爽的事…….但如果你在微信朋友圈里骂人，那可是会给自己惹来麻烦的。严重时，甚至构成违法行为。

社交参与者在网络发表言论时，应当遵守国家有关法律法规的规定，文明有度地发表言论，切勿逾越言论自由的界限。（来源：央广网）

➢ 以信息技术操纵非法集会，谷歌公司被俄罗斯警告！

2019 年 8 月 14 日，据俄罗斯塔斯社报道，俄罗斯方面近日再度发布消息指出，有境外势力通过视频分享、信息推送等计算机信息技术手段，操纵俄罗斯公民参与非法集会，怂恿他们违反法律。

俄公民收到网站推送 教唆市民从事违法活动

俄罗斯联邦委员会也就是议会上院捍卫国家主权和防止干涉内政临时委员会主席、外事委员会副主席安德烈·克利莫夫 11 日表示，根据已经掌握的有效情报，有境外势力通过计算机信息技术手段，操纵俄罗斯公民参与非法集会，鼓动他们违反法律。

克利莫夫指出，俄罗斯公民近日突然收到部分网站推送的信息，教唆市民走上街头从事违法活动，而这些市民从未订阅这些网站和频道。克利莫夫指出，没有某些西方组织和网络公司所有者的帮助，这些技术是无法使用的，俄罗斯不会置之不理。

俄要求谷歌停止宣传非法集会

同一天，俄罗斯联邦电信、信息技术和大众传媒监督局也在网站上发布公告说，已经致信谷歌公司，要求其停止使用视频分享网站来帮助宣扬非法集会。该机构称，如果谷歌放任这类行为，俄联邦将认为这是在干涉俄罗斯国家主权事务，影响和阻挠俄罗斯的民主选举。俄方将保留充分回应的权利。

俄外交部：美使馆介入非法集会

自今年 7 月 20 日起，俄罗斯首都莫斯科已经连续四个周末出现游行示威活动，其中有 3 起是非法集会。据统计，在上周末的集会活动上，有 130 人被捕。此前，俄外交部发言人扎哈罗娃 4 日曾表示，美国驻俄罗斯大使馆介入了 3 日未经许可的集会活动。（来源：央视新闻）

➢ 黑客花 2 天就成功入侵 F-15 战机系统美军网络安全漏洞百出

2019 年 8 月 16 日，环球时报报道：长期以来注重网络攻击能力的美军，在“以己矛攻己盾”时终于暴露出美军网络安全防御其实“千疮百孔”。美国《星条旗报》14 日披露称，“白帽子”黑客轻易入侵美军 F-15 战机的关键系统。该报道担心，随着美军装备对网络系统的依赖性越来越大，如果网络安全性得不到改善，“未来即便是那些造不出先进战机的国家，只需要键盘入侵也能搞垮美军战机”。

报道称，在美国军方授权下，7 名经过严密审查的“白帽子”黑客大显身手，仅用两天

时间就成功入侵美空军现役主力战机 F-15 的关键飞行支持系统。据介绍，当 F-15 处于飞行状态时，该系统负责从机载摄像头和传感器收集飞行数据。一旦这些后门漏洞被敌人掌握，就可能关闭美军重要的“可信赖飞机信息下载站”。

这些“白帽子”黑客全部来自五角大楼国防数字服务部门的外包商 Synack 网络安全创业公司，尽管这是他们首次获得授权测试入侵 F-15 战机实体系统，但他们去年已在不接触军用设备的情况下，入侵过类似的军用信息系统，事后美国空军试图“亡羊补牢”，却被证明是徒劳无功。

负责采购、技术和后勤的美国空军部长助理威尔·罗珀证实，美军已改变过去的保守思维，放宽“白帽子”黑客测试入侵、攻击军用敏感设备系统漏洞的限制。他表示，“如果不允许本国最优秀黑客搜索发现美军飞机和武器系统的数字漏洞，那么这些后门将被俄罗斯、伊朗和朝鲜等潜在对手国家的顶级黑客率先掌握”。

威尔·罗珀表示，美军所有战机都有数以百万计的代码行数，只要其中一行存在缺陷，就有可能被对手入侵。即便是一个无法制造先进战机的国家，也能通过键盘入侵搞垮美军战机。为此，明年他将把这些黑客送到内利斯空军基地和克里奇空军基地，深入探测军用飞机的每一个网络安全漏洞，搞清楚哪些后门会让黑客得以控制其他系统，乃至有效控制整架战机。此外，他还计划向“白帽子”黑客开放测试一个军用卫星地面控制系统。

信息安全漏洞“千疮百孔”

美国联邦新闻网 14 日证实，美军信息安全的后门漏洞，远远比想象中还要严重。从今年 3 月到 6 月，美国空军与五角大楼国防数字服务部门联合推进“捉虫赏金”计划，让黑客帮助寻找美国空军门户网站的漏洞，并对发现漏洞者给予 13 万美元奖励。在奖金的刺激下，各路黑客先后发现了空军云服务系统的 54 个漏洞。

国防数字服务部门“破解美国空军”项目组成员詹姆斯·托马斯证实，这次悬赏黑客比赛打开了五角大楼无法提供的另一个认知领域，尽管美军编设了专业的内部网络防护团队，开发安装了网络扫描器、入侵检测系统和设备，但军方防御人员并不完全具备黑客入侵的相关知识，黑客们出人意料的攻击也远远超出安防团队的想象。

国防数字服务部门总监布雷特·戈德斯坦认为，信息系统安全是一个持续的过程，不要指望一次测试就能发现所有后门漏洞，美军需要对信息系统安防不断进行重新评估。

美军网络中心战“防不胜防”

威尔·罗珀承认，对于美军战机系统被黑客轻易攻破的结果，他并不感到意外。数十年来，美国空军一直将时间、成本和效率列为优先事项，在武器装备研发上忽视网络安全控制。

今天的危险局面正是这种采办惯性的必然结果。一方面，为美空军建造信息系统的公司掌握“后门”钥匙，不愿提供给空军用于测试。另一方面，美空军的传统信息系统落后于时代，即使是最好的技术人员也很难使它们更加安全。

此外，美军的复杂采办体制，让相关改革举步维艰。一位匿名网络安防专家告诉《环球时报》，信息安防是“道高一尺、魔高一丈”的动态对抗过程，随着信息系统软硬件的发展，再安全的系统也难免存在后门，没有绝对安全的信息系统。美军许多武器装备和国防服务大量外包给洛·马等大型军火公司，安防设计又被层层转包给小公司，美军对信息安全很难全程跟踪。F-15 飞行系统被黑客攻破只是问题的冰山一角。作为网络中心战核心的美军新一代战机 F-35，在 2017 年审查时也暴露出网络安全性问题，其已知漏洞没有得到彻底解决，迫使美军追加 2600 万美元让生产商洛·马公司“打补丁”，但这个“补丁”程序有没有漏洞、战时 F-35 会不会被黑、网络中心战会不会断网，美军恐怕心中也没有底（来源：环球时报）

➢ 波音 787 也被爆出安全漏洞 涉及 87 架飞机

2019 年 8 月 8 日，《连线》报道了 IOActive 公司的安全研究员 Ruben Santamarta 对泄漏的波音代码的研究。Santamarta 业余时间用于专研飞机的网络安全。

去年九月，他无意发现波音公司的一台服务器没有任何密码保护，服务器储存了波音

737 和 787 客机的代码。他下载了这些代码。在大约一年之后，Santamarta 声称他从 787 的代码中发现了安全漏洞，可被黑客作为入侵的起点，进一步渗透到飞机的安全敏感系统。他将在拉斯维加斯举行的 Black Hat 安全会议上披露其发现，包括在 Crew Information Service/Maintenance System（CIS/MS）中发现的多个漏洞。CIS/MS 负责维护系统和电子飞行包等应用。

Santamarta 称他在 CIS/MS 中发现了多个内存损害漏洞，可作为入侵飞机安全系统的立足点。波音否认了这一说法，称漏洞不会影响任何关键或必须的飞行系统，它在飞行模式下尝试利用这些漏洞，但没有成功。（来源：金融时代网）

➢ 欧洲央行：其外部托管的下属 BIRD 网站遭黑客攻击

2019 年 8 月 17 日，据俄罗斯卫星通讯社报道，欧洲央行（ECB）8 月 15 日宣布，其网站遭到黑客攻击，481 名用户的数据存在泄露风险。黑客设法破坏了由外部提供商托管的欧洲央行的综合报告辞典（BIRD）网站。

欧洲央行表示：“存在泄露风险的信息包括用户的电子邮件地址、姓名和职位头衔。央行正在与这些用户取得联系”。欧洲央行还强调，BIRD 网站与欧洲央行其他系统是分离的，这可以最大限度地降低其他网站用户信息泄露的风险。BIRD 网站的功能是，向各家银行提供了如何制作统计和监测报告的详细信息。

据彭博社报道，在此前欧洲央行在银行信息安全管理方面有“重大发现”的消息被披露后，相关消息才出现。银行还运行了受控黑客测试，以发现银行系统的弱点。本周早些时候，欧洲央行的银行监管部门发布了一份简报，称未来几个月将对与信息技术风险相关的主题进行一系列现场检查。

值得注意的是，根据彭博社的报道，随着网络威胁越来越频繁，欧洲央行一再呼吁欧盟商业银行使用更安全的信息技术系统，但没料到涉及安全漏洞的事件还是发生了。而这已经不是欧洲央行第一次遭遇黑客攻击。2014 年，欧洲央行公共网站数据库也曾遭到黑客攻击，导致 20000 个电子邮件地址被盗。（来源：俄罗斯卫星通讯社）