闪捷信息
SECSMART

2019年度数据泄漏态势分析报告

闪捷信息安全与战略研究中心

2020年4月

免责声明

本分析报告中的数据来源于闪捷信息安全研究中心、合作伙伴、互联网。由于样本收集范围所限，未必能够反映事件的全貌，特此说明。

闪捷信息根据可获得的数据发布该分析报告，并不保证所有数据的精确和完整，报告中所包含的信息具有一定的概括性，并不能用来解决特定的安全问题。意见和结论只是在报告发布时间得出，后续的变更将不会特别通知。任何人在使用报告中的信息时，责任自负。

目录 CONTENTS

背景

数据安全关系国家安全、社会公共利益，以及公民、法人和其他组织在网络空间的合法权益，一直受到社会各界的重视。特别是在近几年，与数据安全相关的法律法规，行业规范密集出台，反映了国家层面对数据安全高度重视，力度空前。

2017年实施《网络安全法》，2018年实施《个人信息安全规范》，2019年发布《等保2.0》，并起草了《数据安全管理办法（征求意见稿）》，2020年的立法计划中包含了《个人信息保护法》。期间还有各个行业的标准规范大量发布，例如《信息安全技术 大数据安全管理指南》、《公安大数据安全总体技术框架》、《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》和2020年2月发布的《个人金融信息保护技术规范》等。

数据安全对企业的业务发展意义重大，数据资产的泄漏、破坏都会导致企业的业务遭受损失。全球数字化进程中，合规性要求越来越严格，更多的企业组织以数据为核心资产，与此相关的数据安全将成为关注焦点。

摘要

本报告通过统计分析2019年国内所发生的数据安全事件，尽力为读者呈现2019年国内数据安全的态势全景。

数据分析章节里，主要根据收集的数据，进行了统计图表展现和描述，包括了趋势、比例和排名等形式，并根据统计图表展现的内容，结合掌握的其它情报信息，进行原因分析和说明；建议章节里，是根据分析的原因对企业组织提出降低数据安全风险的建议和措施。

整体态势

回顾整个2019年，国内数据安全态势可以用“两增两新”概括。“两增”指数据安全事件数量增加，同时危害程度增强，“两新”指数据泄漏内容出现了个人的生物特征信息，并且勒索攻击和数据泄漏合并。

2019年的数据安全事件数量同比整体增加接近15%，其中仍然以数据泄漏和勒

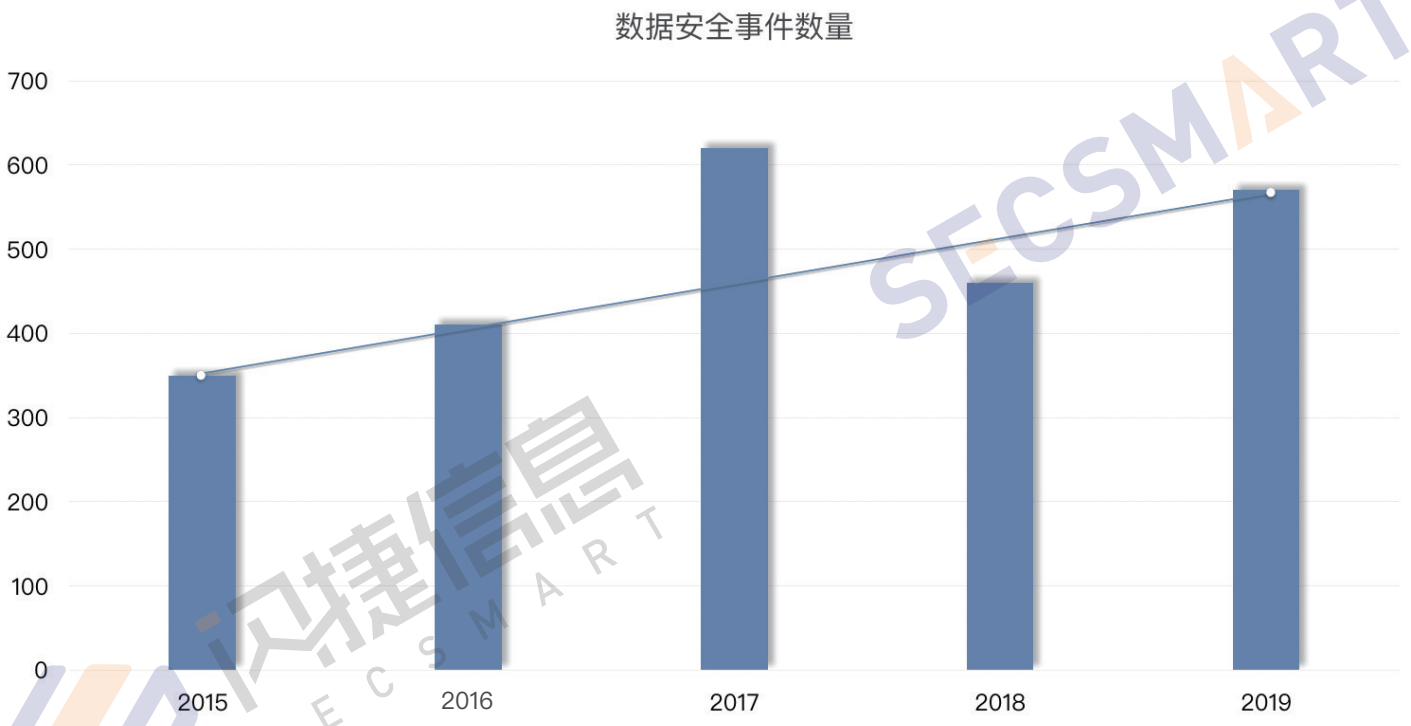
索攻击为主。危害程度是指数据安全事件影响的范围，近年来发生的数据安全事件频频刷新人们对数据安全的认知，泄漏的数据越来越多，造成的不良影响越来越广。以个人信息为例，2019年上半年两起个人简历泄漏事件中，共计5.7亿份简历被曝毫无防护地处于互联网上，由此衍生的后续危害可以说难以估量。

生物特征信息被泄漏，意味着数据安全进入了一个新的时代。生物特征不可更改，不可能像口令一样可以重新设置，一旦泄漏，会对个人造成终身影响。如何使用生物特征，如何保护生物特征数据，是数据安全行业当前需要思考的问题之一。

勒索攻击和数据泄漏通常是不同的数据安全事件，但是2019年开始，个别勒索攻击伴随着数据泄漏。攻击方除了以加密方式勒索受害者之外，还会以泄漏机密数据来要挟受害者，由于这种方式变现更直接，因此很可能会成为未来数据安全事件的主要形式。

数据分析

数据安全事件数量



数据安全事件数量的整体趋势是上升的，在2017年出现了最高值，经分析，是由于2017年几款主要的勒索病毒相继爆发导致，例如“WannaCry”、“Petya”、“BadRabbit”等。数据安全事件数量的持续增长，与国内目前信息化程度密切相关，主要体现在四个方面：

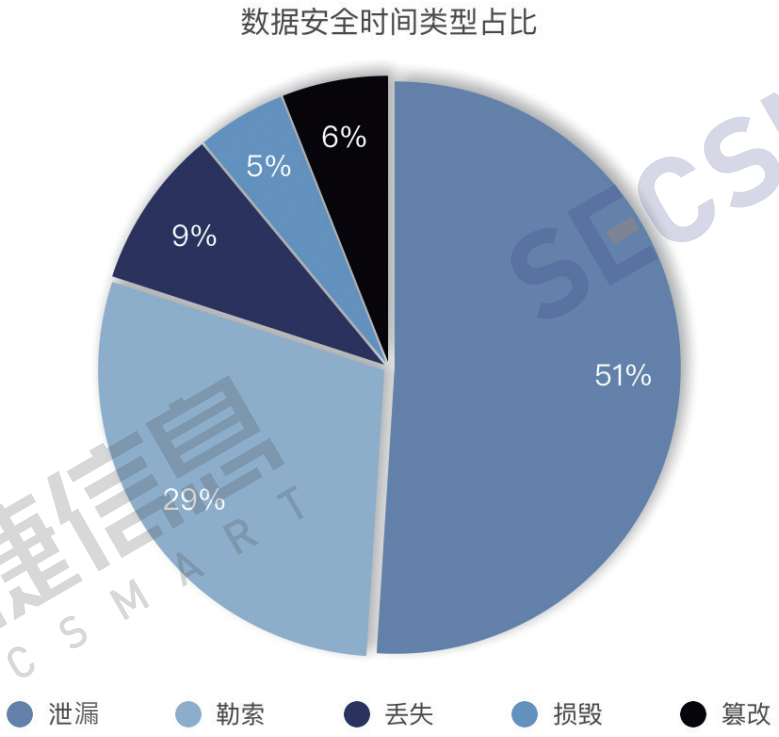
第一，数字化发展迅猛，2019年国内数字经济规模约在38万亿左右，人工智能、大数据、移动互联网、区块链、云计算等新型技术发展迅速，使得攻击目标越来越多；

第二，万物互联，无人机、自动驾驶、摄像头、智能家居等多达上百亿设备与互联网对接，据估计，2020年，联网设备将会达到500亿台，使得攻击的途径越来越多；

第三，数据的价值变得越来越重要，特别是海量数据汇集在一起，蕴含着巨量信息，可以直接反应在商业价值上。因此，以数据为目标的犯罪活动越来越多；

第四，数据安全技术的发展，以及媒体透明度的增加，使得更多的数据安全事件得以发现和曝光。

数据安全时间类型占比



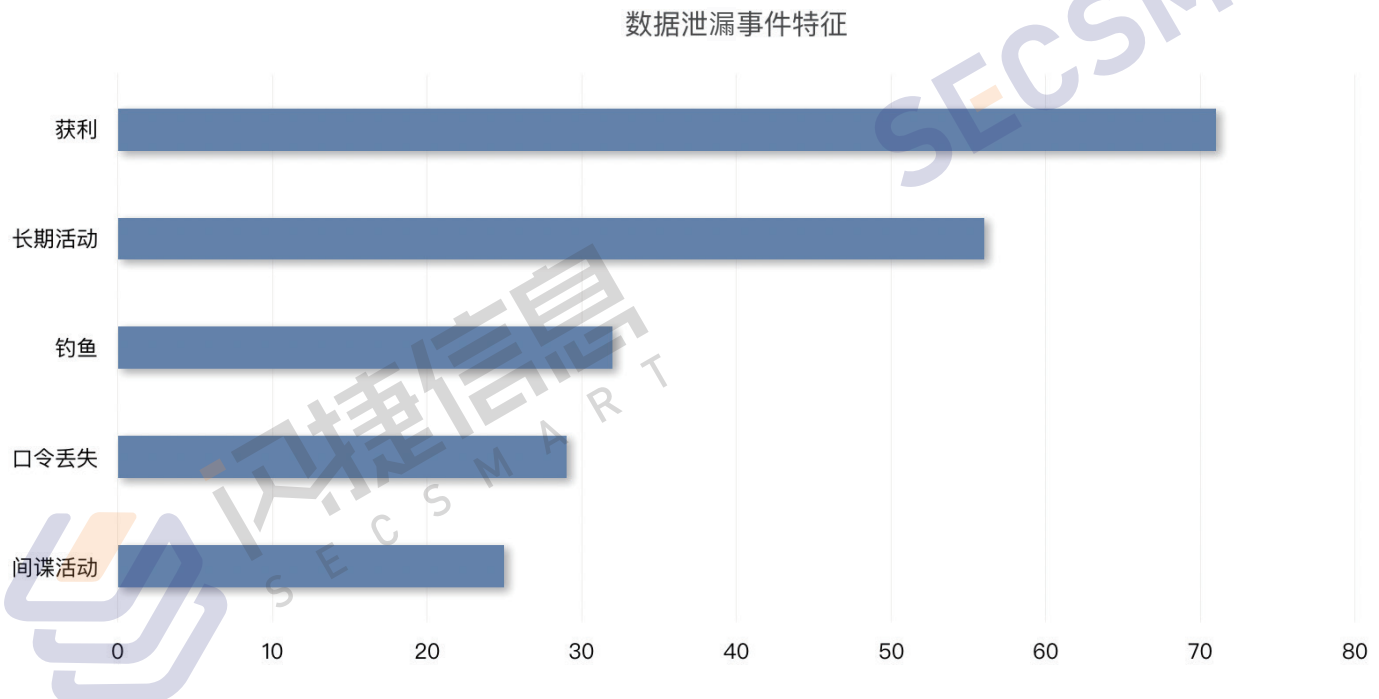
数据安全事件包括数据泄漏、勒索攻击、数据丢失、数据损毁和数据篡改。

2019年，数据泄漏所占比例最高，统计意义上达到了数据安全事件的1/2。数据泄漏事件层出不穷，影响深远。2019年12月4日，国外网络安全研究人员发现一个Elasticsearch数据库泄漏，包括27亿个电子邮件地址，其中10亿个口令都是以简单的明文存储。据悉，大多数被盗邮件域名来自中国邮件提供商，涵盖腾讯、新浪、搜狐和网易等。另外，雅虎、Gmail以及一些俄罗斯的邮件域名也受到影响。伴随着邮件地址和口令同时泄漏，后续的二次危害将难以估量。

勒索攻击在2017年爆发过之后，国内企业或组织都相继采取了应对措施，包括更新补丁，更新安全策略，部署防范勒索攻击的安全产品。因此，在2019年，勒索攻击所占比例比数据泄漏少约20个百分点，但是由于勒索攻击的变现方式简单直接，后续的勒索攻击数量仍然会增长。关于勒索攻击的变现能力，可以从另一个消息看出，2019年6月，GandCrab勒索软件团队发布官方消息宣布，在一年半的时间里，团队通过勒索软件已赚取超过20亿美金，人均年入账1.5亿美金，所以决定停止更新这个恶意程序，从此风光隐退。也许，整年的勒索攻击事件也与此有关。

数据丢失和损毁的比例偏低，主要是因为近年来数据存储方面的建设过程中，对数据备份容灾等问题考虑得很充分，因此，这一类型的数据安全事件相比较少。

数据泄漏事件特征



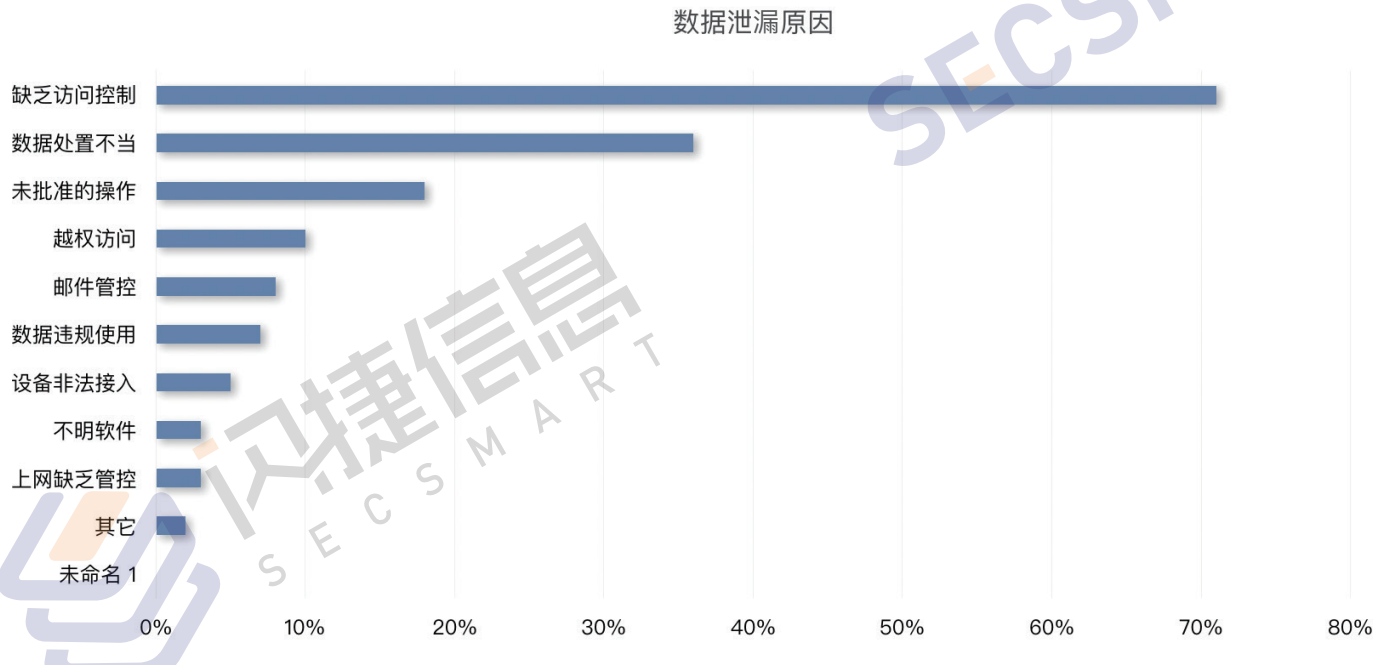
不同的数据泄漏事件，具有不同的表现特征。以获利为目的的数据泄漏事件占所有泄漏事件的70%以上，这说明数据泄漏事件，仍然是利益驱动，背后关系着很庞大的黑产利益链，数据防泄漏将是一个系统工程，任重道远。当然，不以获利为目的数据泄漏事件造成的损失同样令人担忧，例如2019年2月，据荷兰GDI基金会安全研究员发现，国内某人脸识别科技公司的MongoDB数据库未做访问限制，直接被开放在互联网上面，超过250万人的数据可被获取，680万条数据发生泄漏，数据类型包括身份证信息、人脸识别图像及图像拍摄地点等。

排名第二的特征是长期性。统计表明，接近60%的数据泄漏事件具有长期性这一特征，这说明受害企业组织的整个系统缺乏必要的安全审计，使得数据泄露活动能够长期存在。

超过30%的数据泄漏事件与网络钓鱼有关，接近30%的数据泄漏事件是由于被泄露的口令导致，

接近25%的数据泄漏事件属于间谍活动。这类数据泄漏事件同时具有长期性的特点，例如360公司近期确认的美国CIA针对国内11年的网络渗透攻击，我国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等多个单位均遭到不同程度的攻击。

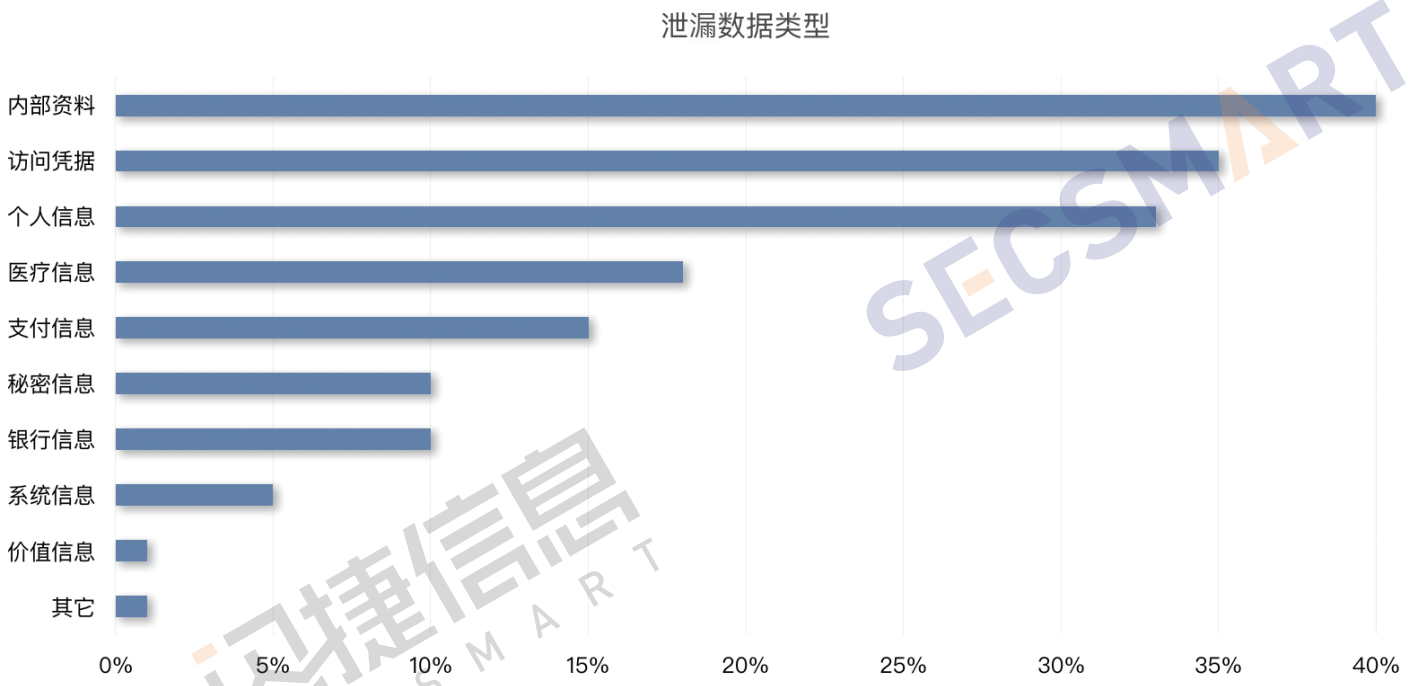
数据泄漏原因



据统计，70%的数据泄漏事件，原因是缺乏对数据的访问控制，包括管理措施和技术措施两方面。访问控制可以根据预先定义的权限和策略对数据访问行为放行或阻断，访问控制的缺失，会使数据完全暴漏，很容易成为窃取对象。例如2019年7月，国内一家经营智能家居设备的管理平台，被曝用户数据库暴漏在互联网上。该数据库无任何密码保护，运行在物联网（IoT）管理平台。暴漏的数据库包含超过20亿条日志，包含了电子邮件地址、密码、帐户重置代码、精确的地理定位、IP地址、用户名等12个维度的个人信息。

排名第二的数据泄漏原因是数据处置不当，例如配置错误，共享数据时没有脱敏，对敏感数据没有加密，以及其它没有按照规范或者标准对数据提供应有的保护。以配置错误为例，2019年多次出现因为JIRA配置错误而导致数据泄漏的事件，由于这一款任务跟踪/项目管理软件服务了全球135000家公司和组织，因此包括NASA、谷歌、雅虎等成千上万的公司因此泄漏了内部的员工信息和项目数据。配置错误说明企业组织在变更管理方面存在漏洞，值得引起重视。

泄漏数据类型

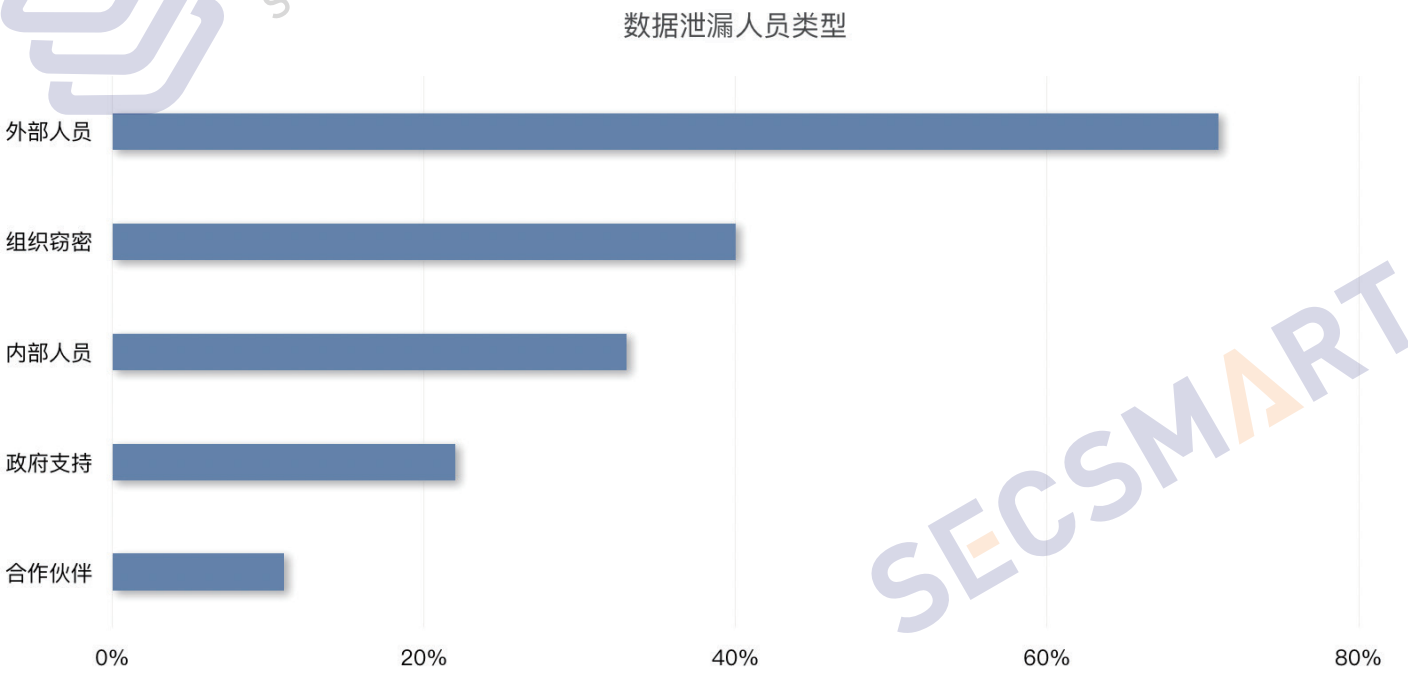


个人信息非常重要，但是在泄漏的数据类型排名中，仅处于第三位。在所有泄漏数据类型中，内部资料泄漏排名第一，约为40%。内部资料包括各种国家机密、

企业商业机密、技术机密、组织机构的秘密信息等。2019年5月，据外媒报道，美国First American金融公司，由于网站缺乏安全措施，任何人无需身份验证即可访问客户数据库，造成大约8.85亿份文件泄露。泄漏的数据高度敏感，如抵押贷款、税务记录、社会保险号、电汇收据、驾照图像、银行账号和对账单等。

排名第二的访问凭据包括口令信息、证书及其它用于证明身份的数据。访问凭据通常会被用在后续的犯罪活动中，黑客通过收集互联网已泄漏的用户账号及密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户，这种被称为“撞库”的攻击又会导致更多的数据泄漏，因此所造成的危害是持续的。

数据泄漏人员类型



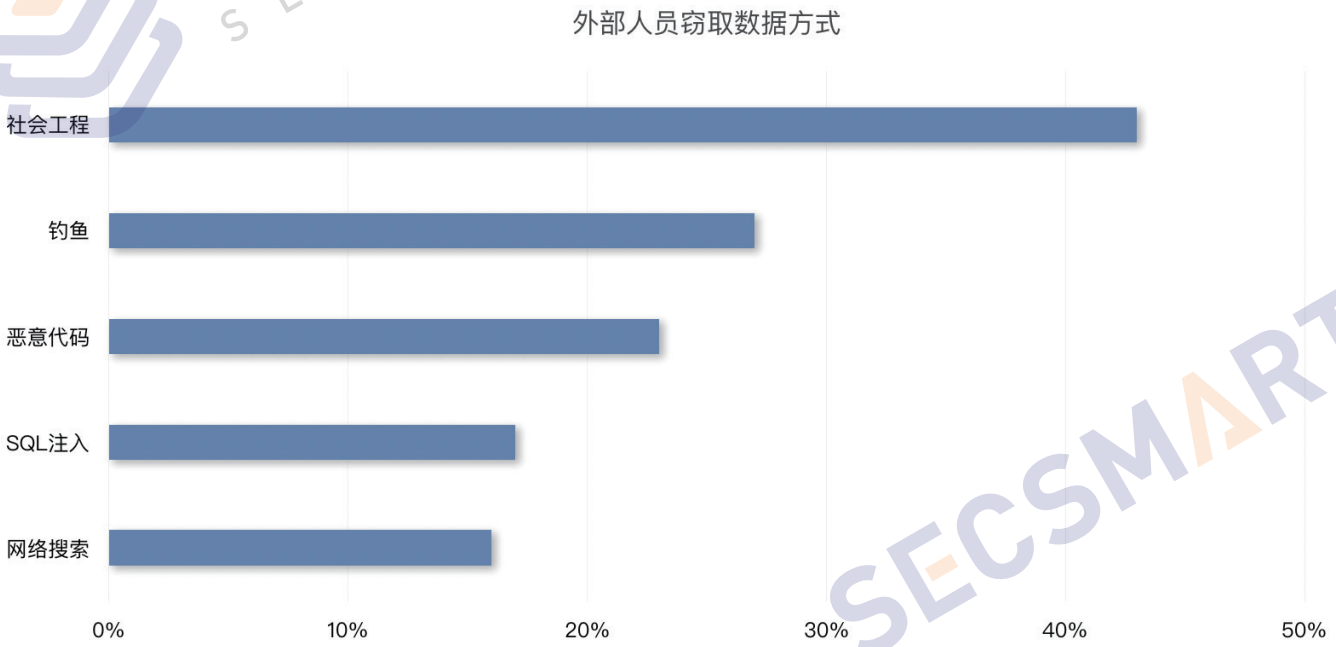
每一个数据泄漏事件背后，都是有实际操作人员的。统计发现，外部人员导致的数据泄漏事件占比达到70%，与其它类型相比，占比显著。外部人员通常采用钓鱼、SQL注入、恶意代码、社会工程等方式窃取数据，也会通过扫描网络，搜索任何人都可以访问的数据库并直接获得数据。

有组织的窃密占数据泄漏事件的40%，以著名的“Anonymous”组织为例，该组织核心成员有数千名，包括一些高级计算机专家以及记者，还包括大量遍布在

世界各地的黑客，他们可以进入大公司和政府部门内部网站，中断他们的服务，删除备份数据，截取电子邮件以及盗取各种文件。

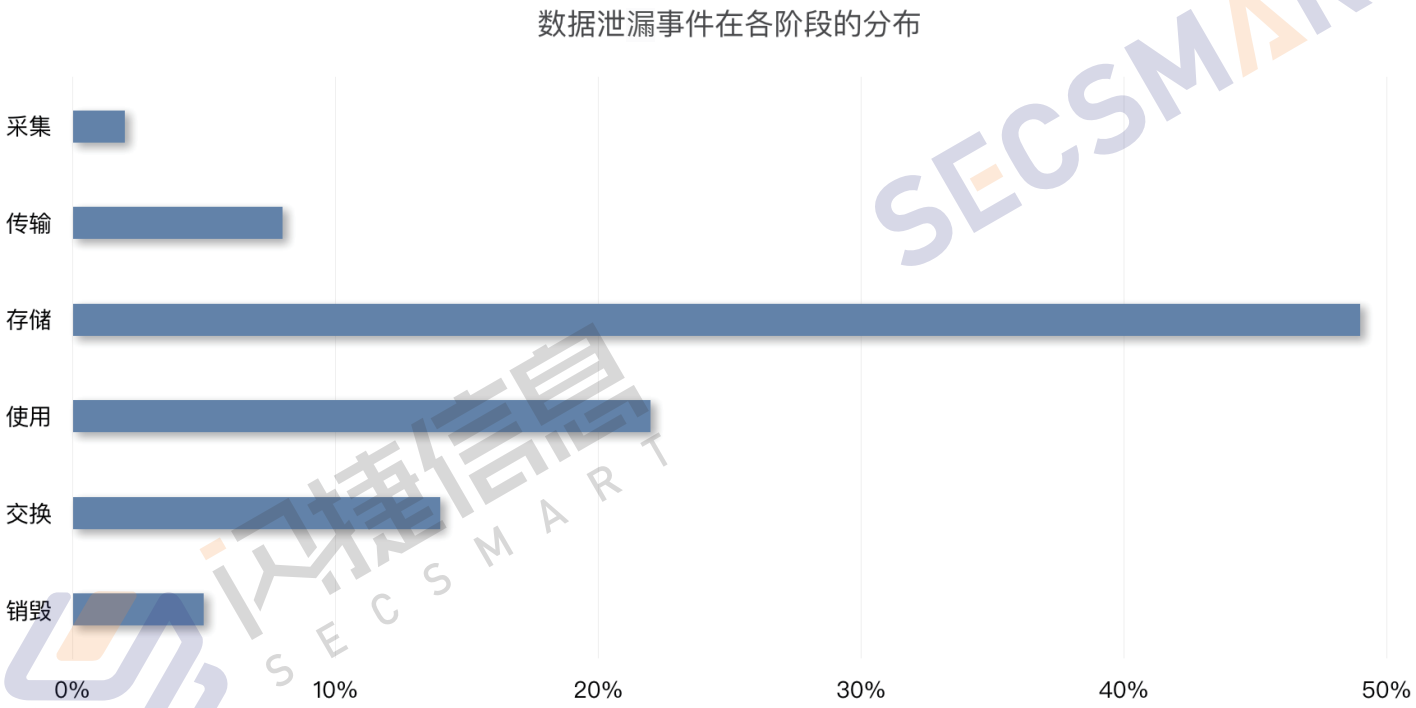
内部人员造成的数据泄漏达到30%以上，包括主动的泄密和由于失误造成的泄密。在主动的泄密类型中，内部人员受利益驱动泄漏数据，或者被外部人员欺骗泄漏，或者对企业有不满情绪而泄漏。失误造成的泄密类型中，由于安全意识或者流程的问题，造成安全策略配置错误，例如访问权限控制缺失、安全管控粒度过大、账号凭据丢失等。

由政府支持的窃取数据行为，通常与APT攻击关联，由于潜伏期长，不易发现，因此占比较低。合作伙伴泄漏数据近年来有增长趋势，一般发生在提供运维服务、业务外包等场合，因此在选择合作伙伴时，除了管理制度上的措施外，还应评估合作方在保护数据安全方面的资质和能力。



外部人员使用社会工程的情况非常普遍，占比第一，超过40%，这说明外部人员窃取数据，很大比例上并不需要特别专业的信息技术。通过网络邮件、伪造的网站、电话，甚至是当面沟通，外部人员都可以诱骗内部人员为其服务。网络钓鱼则是社会工程学攻击中的一种，可以直接诱骗受害者提供敏感信息，由于网络钓鱼不易察觉，因此占比靠前。恶意代码方式包括木马、后门等工具，在植入目标网络后，扫描所有有价值的资源，并以隐蔽的方式回传数据。此类泄密方式的特点是隐蔽性强，危害大。

数据泄漏事件各阶段分布



数据泄漏可以发生在其生命周期中的任何一个阶段。据统计，数据泄漏发生在存储阶段的占比最高，接近50%，这说明针对存储阶段的数据安全防护非常关键。据统计，2019年数据泄漏影响前10的数据泄漏事件，其中9件都发生在存储阶段，1件发生在使用阶段。如表格1所示。

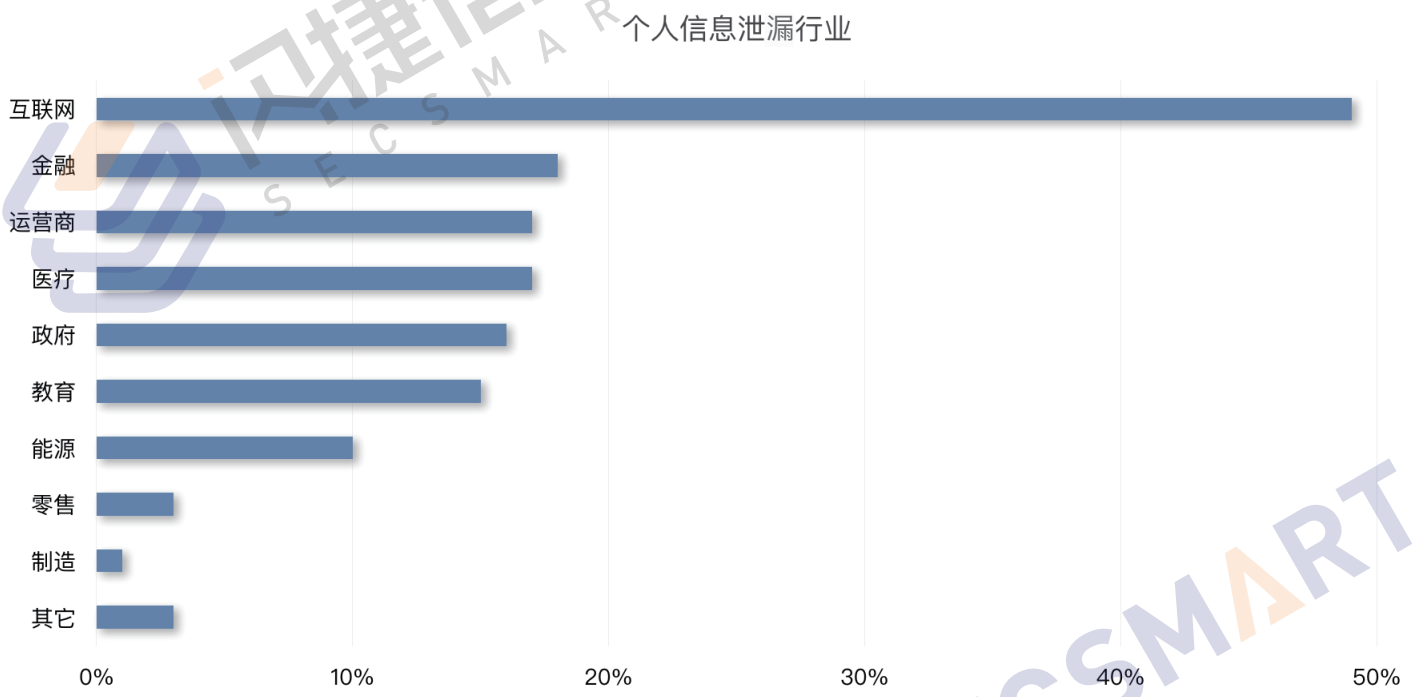
2019年影响前10的数据泄漏事件

行业	报告时间	泄露内容	信息子类	数量	泄露源	泄露阶段
互联网	12月	个人信息	Email地址、登录凭据	27亿	Elasticsearch	存储阶段
科技	7月	个人信息	Email地址	20亿	数据库	存储阶段
科技	4月	个人信息	视频	200亿	摄像头	采集阶段
教育	6月	个人信息	电子邮件元数据	95亿	Elasticsearch	存储阶段
互联网	3月	个人信息	简历	3.9亿	Elasticsearch	存储阶段
互联网	1月	个人信息	简历	2亿	MongoDB	存储阶段
科技	2月	个人信息	人脸图像	680万	MongoDB	存储阶段
互联网	4月	业务数据	源代码		代码仓库	存储阶段
医疗	9月	个人信息	医疗信息	28亿	数据库	存储阶段

使用阶段，占比超过20%，仅次于存储阶段，依然是数据泄漏的高风险阶段。数据在使用阶段的泄漏方式包括肩窥（shoulder surfing）、掠读（skim）、拍照、截屏和打印等。使用阶段泄漏的数据量比存储阶段泄露的少，但是发生得非常频繁。

交换阶段的数据泄漏占比为14%，在与合作伙伴进行数据共享交换，容易发生数据泄漏。

个人信息泄露行业分布

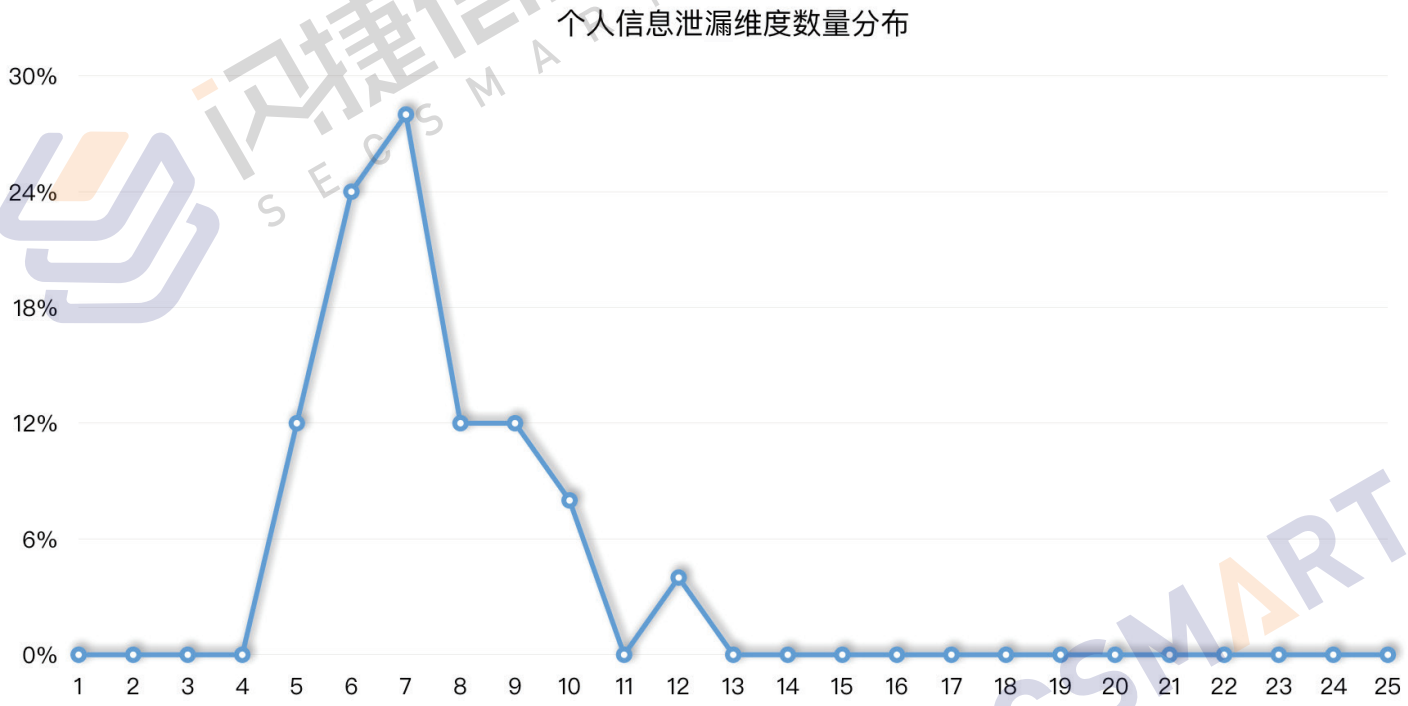


个人信息泄漏最严重的是互联网行业，除了涉及社交网站、在线招聘网站、数字营销公司、约会网站、电商网站等，还包括以互联网形式运作的教育、金融等企业和组织机构。互联网行业内部，各企业对数据安全的态度差异明显，并且只有少数头部企业能够在数据安全方面有实质性的投入。由于互联网行业的特殊性，该行业既是个人信息泄漏的受害者，同时（其中个别企业）也在一定程度上加剧了数据泄露。

金融、运营商、医疗、政府和教育五个行业，在统计意义上，数据泄漏的情况接近，比剩下的行业明显严重。金融行业的个人信息，特别是信用卡号码，是黑产追逐的对象，国外单条信用卡信息在地下市场价格可以达到45美元。运营商行业的

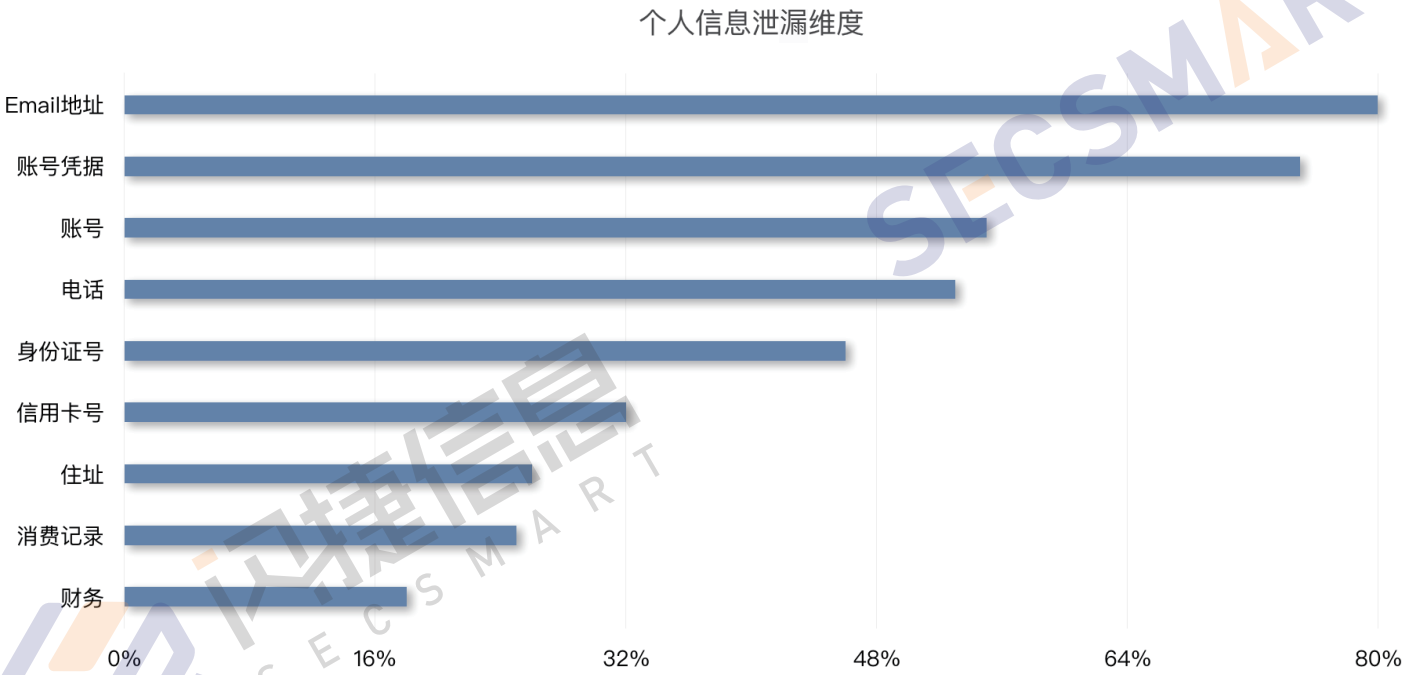
个人信息包含上网记录，是很多企业做精准营销的重要数据来源，也是犯罪分子实施诈骗的基础信息，因此个人信息泄漏将是运营商行业的长期挑战。医疗行业中，个人信息泄漏更加系统化，在所有行业的数据泄漏事件中，医疗行业内部人员参与的比例最高。“统方”信息可以带来直接的利益，这也是医疗行业个人信息泄漏排名比较靠前的原因。教育行业，由于学生社会阅历不丰富，思想简单，因此学生信息也被诈骗分子觊觎，成为数据泄漏频发的行业之一。

个人信息泄漏维度数量



在本分析报告中，综合统计了个人基本信息、社会信息、隐私信息和网络信息四大类共33个维度。在所有的个人信息泄漏事件中，泄漏包含个人信息维度的数量大部分集中在5-12个之间。其中，泄漏维度6个和7个的占比较高，分别是24%和28%。泄漏的个人信息维度数量越多，说明个人信息暴漏的越严重，对个人造成的损失也就越大。事实上，很多系统在采集个人信息时，根本没有深入考虑所采集的信息维度是否必要，只是习惯性地要求，这种情况的后果就是增加了企业运营的风险，提高了数据安全保护的成本。

个人信息泄漏维度



个人信息包含了很多维度的个人相关数据。在泄漏的个人信息中，Email地址是被泄漏最多的，80%的个人信息泄漏事件中包含了Email地址。Email地址通常会被用来发送钓鱼邮件、或者各种非法广告，对社会造成二次危害。研究数据显示，网络犯罪中，90%以电子邮件的方式开始。根据IC3的估计，电子邮件攻击中只有10%内含恶意软件；攻击者利用办公文件或图片作为邮件附件，趁用户点击浏览时，安装蠕虫、木马、勒索软件、病毒、广告软件等程序。而剩下90%是不含恶意软件的商务电邮诈骗(Business Email Compromise)，包括精准网钓邮件、专门针对CXO的鲸钓（whaling）、CEO诈骗或是退税诈骗等攻击，黑客冒用同事、友人或上级等身份，在信中加入伪造的登录页、恶意链接诱骗收件人点入，或是要求受害者汇款及提供财务、人事或自己的隐私信息。据估计，2019年网钓攻击增加近70%。

75%的数据泄漏事件中包含账号凭据信息。账号凭据用于登录目标系统，因为96%以上的用户会在多个网络系统应用中使用相同的账号凭据，因此登录凭据泄漏，同样会引起一系列连锁反应。

建议

增强数据安全意识

数据安全事故的发生，都和人有关。无论是员工无意的错误配置，还是被诱骗后的操作，或是利益驱使，又或是恶意报复，都是由人实施完成，通过增强数据安全意识，可以降低数据安全事故发生的机率。首先，从公司层面，开展数据安全事故案例分享，使大家认识到数据安全的重要性；其次，普及数据安全相关法律法规，使员工意识到违反数据安全的后果；再次，进行安全知识培训，使大家具备基本的数据安全知识，能够避免一些常见错误操作；最后，就是坚持，任何意识的培养和增强，都是一个长期的过程。

增强数据防泄漏

数据防泄漏需要根据业务场景，综合运用多种技术。首先，应该基于内容识别等技术，自动发现敏感数据并分类分级，并能够记录文档和数据在网络系统中的流转路径；其次，能够在终端和网络环境中对数据的操作和流动进行监控、预警和审计；再次，对外发的数据添加水印，使数据的使用有迹可循，出现泄漏可以溯源追责；最后，具备统一的管理平台，呈现所有的数据安全风险，并能集中管理安全策略。除技术之外，企业也应建设管理制度，培养企业的数据安全意识，做到技术和管理密切配合，提升企业整体数据防泄漏能力。

加强个人信息保护

个人信息保护措施需要覆盖数据的整个生命周期。首先，在个人信息采集阶段，应该按需收集个人信息，过多的个人信息收集会给企业带来合规风险，也会带来防护成本；其次，个人信息的传输和存储，应该加密，防止内部人员或外部人员明文窃取；再次，个人信息的使用和交换过程中，数据应该脱敏，使数据在安全合规的前提下流转；最后，能够响应用户的要求，删除系统中的个人信息，避免数据遗留带来的额外法律风险。

加强访问控制

数据资源联网，需要有访问控制措施保障数据安全。首先，设置访问数据资源的IP地址范围，可以有效防止陌生IP地址发起的非法请求；其次，对数据资源的所有请求，都应该经过身份验证，合法的用户才能请求数据；再次，对用户能够访问的数据内容进行最小权限限制，减少用户越权访问数据的机会；最后，使用三权分立，分别设置审计管理员账号、安全管理员账号和数据库管理员账号，防止权限过于集中而带来的风险。

结论

1、 国内企业的数据安全能力差异较大，各个行业的数据安全能力差距比较明显，虽然个别企业数据安全能力突出，但整体上仍然处于初级阶段。

2、 在利益的驱动下，数据安全问题将会长期存在，并且数据安全所面临的挑战也会越来越严峻。因此，数据安全防护是一项长期的系统工程，需要在不断实践中持续演进。

3、 数据安全无处不在，关系到个人、企业组织和国家的利益。因此，数据安全不仅仅是某个人或某个企业需要考虑的问题，从法律制度的建设、安全意识的提高，到管理流程的实施、技术理念的进步，需要社会各界紧密协作，共同应对。

关于闪捷信息

闪捷信息（Secsmart）是一家专注数据安全的国家级高新技术企业，在业界率先将人工智能、量子加密技术成功应用于数据安全领域，首创“零信任”动态数据安全治理以及“云管端”立体化数据安全解决方案，产品范围涉及数据安全治理、数据库安全、数据防泄漏、大数据安全、云数据安全等，已广泛应用于政府、电力、运营商、金融、教育、医疗等行业。

闪捷信息以“让数据资产更安全”为使命，已拥有40多项发明专利和软件著作权，获国家保密局、国家信息中心、公安部等权威机构认证，在商密、涉密领域均有建树。目前，闪捷已在全国设立2个研发中心和17家分支机构，与国家应急管理部、国家互联网应急中心、国家电网、南方电网、中国移动、中国电信、阿里、腾讯等500多家知名单位持续合作。

闪捷信息由归国留学人员创办，创始团队具备全球数据安全视野和技术实践，秉持“征途路上、你我同行”的企业文化，并荣获“2018年杭州市领军型创新创业团队”。闪捷信息愿与广大客户、合作伙伴共建数据安全生态圈，以先进技术创新推动数据安全行业发展！

闪捷信息科技有限公司
Secsmart Information Technology Co., Ltd.

服务热线：400-811-8806
公司网址：www.secsmart.com
邮箱：sales@secsmart.com
注册地址：杭州市余杭区文一西路998号未来科技城·海创园