网络安全创新大会
Cyber Security Innovation Summit

金融行业骚扰电话防治和敏感数据保护

广发证券　周轶伦

推荐股票的骚扰电话，你遇到过吗？

你好，我是XX证券客服，我们创建了一个免费股票交流群……

你好，我是XX证券老师，请加我微信，免费推荐即将拉升的股票……

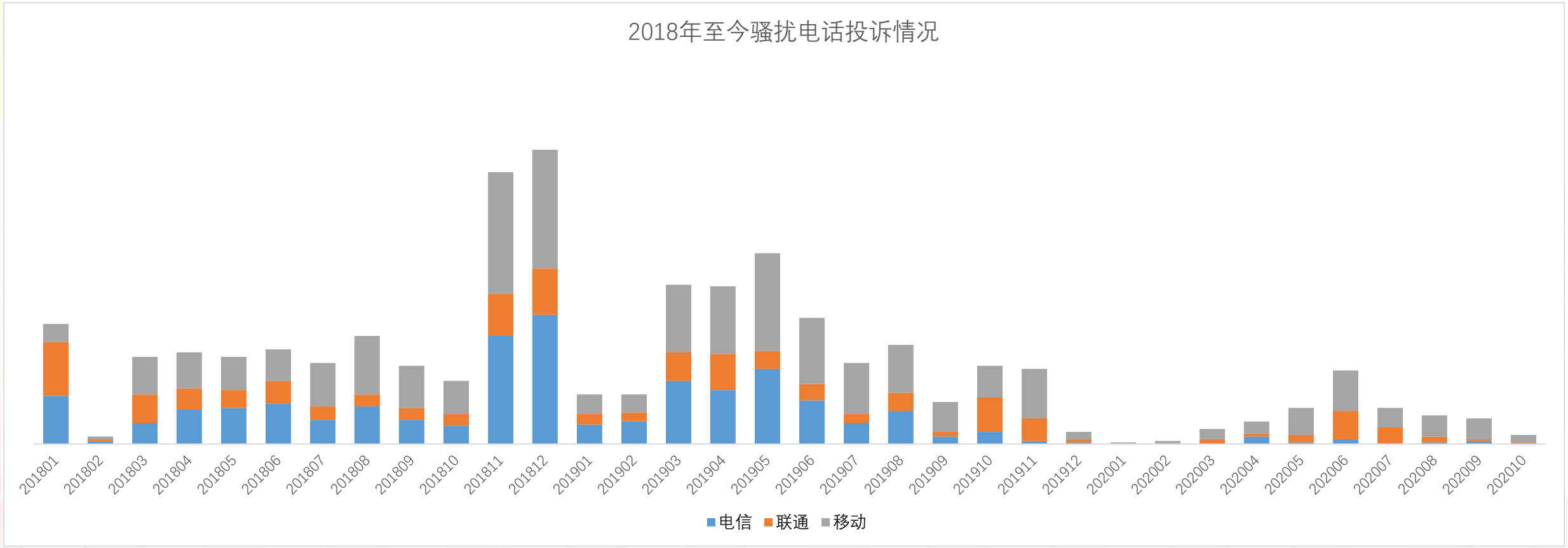
01 骚扰电话防治

投诉情况、调查情况、破案情况、泄露源头分析

骚扰电话，愈演愈烈

网络安全创新大会
Cyber Security Innovation Summit

- 2016年开始，广发证券接到投资者投诉接到骚扰电话的情况屡有发生



这头刚开户，那头就来电？

- 骚扰电话冒充广发证券工作人员，要求客户加群荐股，甚至以调整佣金的名义诱骗客户加微信。
- 骚扰电话多出现在开户、手机证券绑定账户等需要接收短信验证码等环节之后。

客户营业部	投诉反馈信息
天津XXX营业部	多次有非广发官方电话骚扰客户对客户造成困扰。自称广发证券客服人员，试图诱骗客户加入股票交流群。
重庆XXX营业部	客户表示第一天开户，第二天就有说广发证券的工作人员来让加群。骚扰电话速度这么快，客户异常生气。
天津XXXX营业部	本人为公司员工，3个月前新办理的手机号码 155****7373。2020年6月5号，也就是3天前刚刚报备完后绑定的自己手机易淘金 和 账户。今天6月9号早晨就接到诈骗电话自称广发证券，希望添加微信，拉进股票群。

一、同业交流

- 2016年8月和2018年1月，广发证券与华泰、安信、长江、中投、广州等多家券商，就客户信息泄露及骚扰电话问题进行了两次同业交流会议。华泰证券、长江证券等券商反馈存在同样的问题。

二、内部测试

- 内部系统排查梳理、风险评估、更换短信服务商、改造外呼系统均没有明显效果。
- 2017年8月底，通过短信网关向18个测试号码发送开户验证码短信，发送时未经过任何内部应用系统。发送后第2天，3个号码被骚扰，骚扰方在微信上推荐同一只股票。因测试手机号码未经过任何内部应用系统，测试结果显示客户信息泄露大概率出在运营商或短信服务商环节。
- 2017年10月，广发证券向公安机关报案。

三、公安报案，如何取证?

- 电话取证：广发证券员工仿冒受骚扰客户，回拨骚扰电话（选择广州本地电话，以便公安抓捕），录音留存证据。

喂，你好，刚才哪位找我?

我们是广发证券的，我们最近有一些免费的牛股可以做推荐，想问一下你股票做得怎么样?

广发证券？我刚刚开户啊。你们是哪里?

我们是广州这边的，**我们跟广发证券合作的**，这边老师都是从广发证券请过来的。所以我们指导客户做都是老师亲自带着操盘做的，包括我们自己公司有一些私募基金在跟着做，就是私募大资金去操盘。

三、公安报案，如何取证?

- 微信取证：让骗子提供其盈利模式（收费荐股）、银行账号等信息，并留存微信证据

四、顺藤摸瓜，抓捕数据泄露源头

- 经调查，数据源头来自于某电信运营商话费结算系统承建公司员工郭某，郭某利用其系统维护管理权限结合黑客技术，大量调取证券公司客服电话的呼叫记录（即股民电话号码信息）后贩卖。

注：引自广东省公安厅网站： http://gdga.gd.gov.cn/jwzx/jwyw/content/post_1090397.html

四、顺藤摸瓜，抓捕数据泄露源头

- 案件经营成熟后，在广东省公安厅网警总队的指导下，广州市公安在北京、湛江、深圳、珠海等地同步实施收网行动，对该两个犯罪团伙实施全链条打击，共抓获犯罪嫌疑人40余人，源头“内鬼”2人，缴获公民个人信息230G，现场查获电脑、手机、银行卡等涉案物品一批。案件于2018年6月公开。

注：引自广东省公安厅网站： http://gdga.gd.gov.cn/jwzx/jwyw/content/post_1090397.html

数据泄露，追查溯源

- 2018年6月，深圳媒体报道，“深圳市云宽科技有限公司”抓取基站客户信息，可抓取网页、APP和400号码的用户信息，用于精准营销。其中明确提及广发证券的手机软件APP。

注：引自深广电《第一现场》：https://mp.weixin.qq.com/s/ld8KiUiW9dQFjNTAUqqoMA

数据泄露，追查溯源

- 2018年7月8日，新华社报道：涉嫌侵犯数百亿条公民个人信息，大数据行业知名企业“数据堂”被查（新三板上市公司）。泄露源头来自电信运营商。

注：引自新华网微博：https://www.secrss.com/articles/3799、 http://zjnews.china.com.cn/yuanchuan/2018-07-25/143020.html

数据泄露，追查溯源

- 2020年1月3日，南方都市报报道：号百公司（中国电信股份有限公司的全资子公司）中层陈亚华从号百公司数据库获取区分不同行业、地区的手机号码信息，向他人提供并在网络上销售获利累计2000余万元，涉及个人信息2亿余条。这也意味着上述被告人是从电信系统内的数据库获取用户个人信息以出售牟利。

陈德武、陈亚华、姜福乾等侵犯公民个人信息罪二审刑事裁定书

发布日期：2019-12-25　　浏览：62次

浙江省台州市中级人民法院
刑 事 裁 定 书

（[redacted]

原公诉机关温岭市人民检察院。

上诉人（原审被告人）陈德武，男，1973年2月11日出生于江苏省射阳县，汉族，硕士研究生文化，居民，住上海市徐汇区。2016年9月27日因涉嫌侵犯公民个人信息罪被台州市公安局椒江分局刑事拘留，同年11月3日被台州市公安局椒江分局逮捕，2017年7月6日被台州市椒江区人民检察院决定取保候审。2018年3月17日因涉嫌对非国家工作人员行贿罪被台州市公安局刑事拘留，2018年4月23日被依法逮捕。现羁押于温岭市看守所。

辩护人王正洋、郭真凤，北京市君泽君（上海）律师事务所律师。

注：引自南方都市报：http://m.mp.oeeee.com/a/BAAFRD000020200103245879.html

数据泄露，追查溯源

- 尽管公安机关加大了对电信运营商泄露数据的打击力度，但我们调查发现，仍有“大数据营销”、“精准营销”平台自称使用电信运营商数据实现“精准获客”，贩卖个人信息。

AI天网获客
Skynet wins customers

以下维度，可以支撑

支持类型	需
自定义电话号码类	号码、（主
自定义搜索词类	搜索词、搜
自定义URL类	URL、访问
自定义APP类	指定app、
自定义位置类	位置经纬度、
自定义短信类	号码、（接

您可以
包括但不仅限于，电话
如需其他维度的要

为什么

我能给您提供如此精准的客户数据

因为数据来源权威

所有数据源自中国电信业务三巨头
移动+联通+电信

中国移动 China Mobile
China unicom中国联通 创新·改变世界
中国电信 CHINA TELECOM 世界触手可及

数据泄露，追查溯源

- 暗网交易市场：通过“运营商接口数据”、“运营商大数据匹配”、“端口抓取”等方式获取证券行业客户电话号码
  - 《每日更新一手棋牌QP彩票体育联通运营商数据》——联通数据
  - 《每日更新一手股票股民期货移动运营商数据》——移动数据

商品描述

实时一手股票精准数据运营商接口数据

获取指定网站访客、app登录访客手机号码。

这种数据缺点是不像渗透资源那样类别齐全（基本只包含手机号码、对应的APP）。
因为原理是抓包链接访客，包括主域名、下载、注册、充值。所以访问不一定是后台入库数据。

优点是获取的都是最近登录的访客，而不是几个月前甚至几年前的用户，时效性高，适宜电销运控。
来源广泛，可以指定同行业APP获取，而渗透是不可能做到的。

下单数据不超过T+1天发货，每天15:30 22:00为发货时间。保证提供给你的数据是最新刚出库。

数据泄露，追查溯源

短信劫持接口
针对常规行业（贷款、币、股票、pos等正规行业）推出的稳定接口
要求：应用商店可以搜到的app，并且会发送验证短信
优点：100%活跃、100%真实用户、抓取三网、数据精准
缺点：抓取app有局限性不是所有app都可以抓，要满足上面的要求
适用于电销打粉、微信拉粉等对数据精准度较高的转化方式
181 15:07

【移动电信接口全面升级】
增加新功能运用大数据进行数据二次分析可以添加指定标签（年龄、职业、人生轨迹、有无房车、及婚姻状况等）
私人定制你专属数据！数据的精准性，是你营销推广的第一步

「共赢」运营商精准数据库承接全行业
和大家简单介绍一下抓取实时访客的原理：
三网运营商大数据获客主要是根据用户的终端上网行为，终端通信行为进行用户数据实时抓取。比如用户使用手机终端的蜂窝网络访问了网站，消耗了手机流量，那么这个用户就会被抓取到。再比如用户用手机终端的蜂窝网络使用和浏览了手机APP,消耗了手机流量，这种情况和前者大同小异，我们就是基于这个原理来实现：网站app抓取实时访客的
343 22:09

【三网运营商数据指定抓取直营】BC-体育-...
运营商数据抓取的原理，当访客使用手机4G流量访问网站或者APP的时候会形成一个专属于自己的http报告，访客的手机号、访问了哪些网站、停留了多长时间、都可以进行计算从而最终得出该访客的需求模型。
554 11:28

【三网运营商数据指定抓取直营】BC-体育-...
❤️免费对库测试，骗子勿扰。寻跑量伙伴，工厂价源头直供
❤️免费对库测试，骗子勿扰。寻跑量伙伴，工厂价源头直供

全行业指定抓取，url/app建模实力说话，各类五黑行业/正规行业
棋牌/彩票/网赚/菠菜/体育,股票/教育/医美/兼职/宝妈
充值/访问/注册/客服/下载/登录,自有技术团队，帮助建立各类模型 客服 @shuju20202
641 已编辑 12:03

【三网运营商数据指定抓取直营】BC-体育-...
运营商自营，指定APP端口，网址抓取0.35/条（保15天） 历史数据0.1条，懂得来聊 @shuju20202

监管行动，任重道远

- 十三部门《综合整治骚扰电话专项行动方案》重点对商业营销类、恶意骚扰类和违法犯罪类骚扰电话进行整治。

重点工作	牵头部门	具体措施
严控骚扰电话传播渠道	工业和信息化部	1.加强语音线路和码号资源管理。 2.加强电话用户合同约束。 3.全面规范营销外呼业务。 4.全面清理各类骚扰软件。
全面提升技术防范能力	工业和信息化部	1.强化主叫号码鉴权和通话溯源。 2.提升骚扰电话拦截能力。 3.增强骚扰电话提醒和预警能力。 4.增强骚扰电话综合管控能力。
规范重点行业商业营销行为	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	**严格规范金融类等电话营销行为。**
依法惩处违法犯罪	公安部	集中侦破一批利用电话实施诈骗、敲诈勒索、虚假广告宣传等违法犯罪案件。 集中侦破一批**侵犯公民个人信息犯罪案件**。依法严厉打击各行政机关和**电信**、**金融**、医疗、教育、物业、物流、寄递等重点单位工作人员非法出售或者向他人提供公民个人信息的违法犯罪行为。
健全法规制度保障	各部委	略

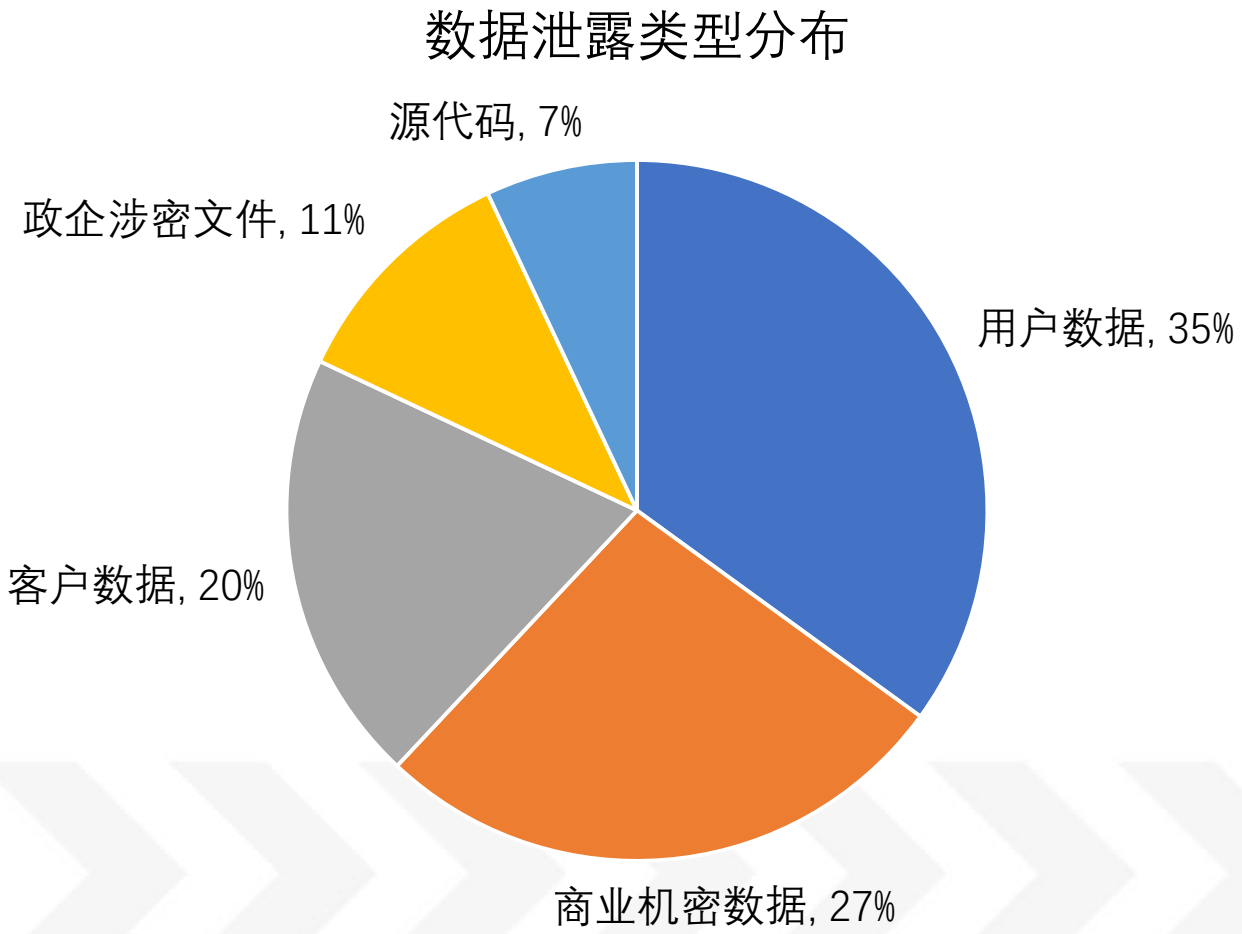
注：工信部网站：http://www.miit.gov.cn/n1146290/n4388791/c6283131/content.html

02 敏感数据保护

数据泄露类型、数据泄露角色、泄露动机和渠道、数据泄露防范

泄露动机及泄露渠道分析

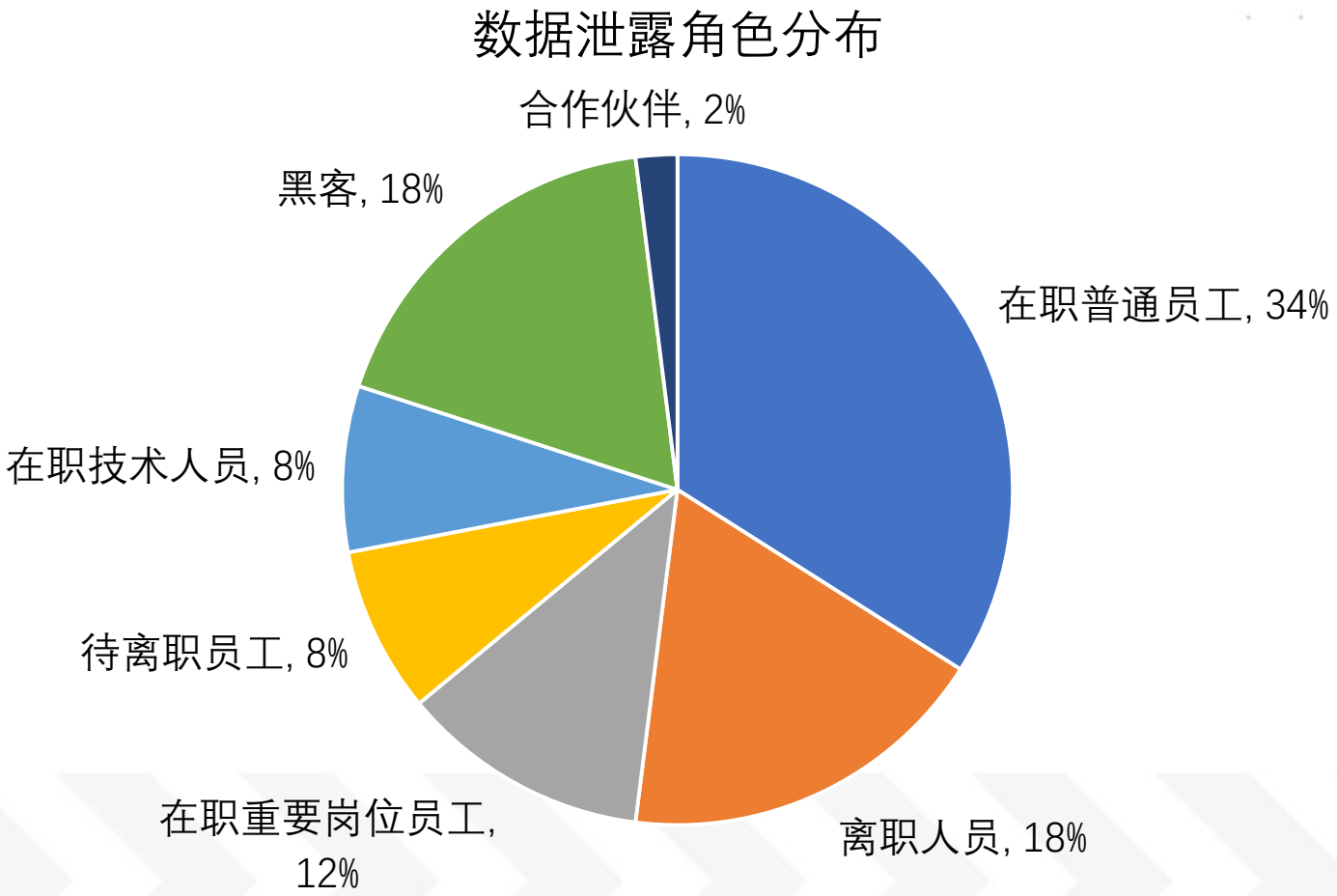
- 中国裁判文书网2011年-2019年10月发布的所有与数据泄露相关的150份裁判文书样本数据，从泄露数据类型、 泄露人身份、 泄露动机和泄露渠道等维度对样本数据进行解读整理还原泄露过程。



注：引自奇安信《数据泄露典型判例分析报告》： https://www.qianxin.com/threat/reportdetail?report_id=37

泄露动机及泄露渠道分析

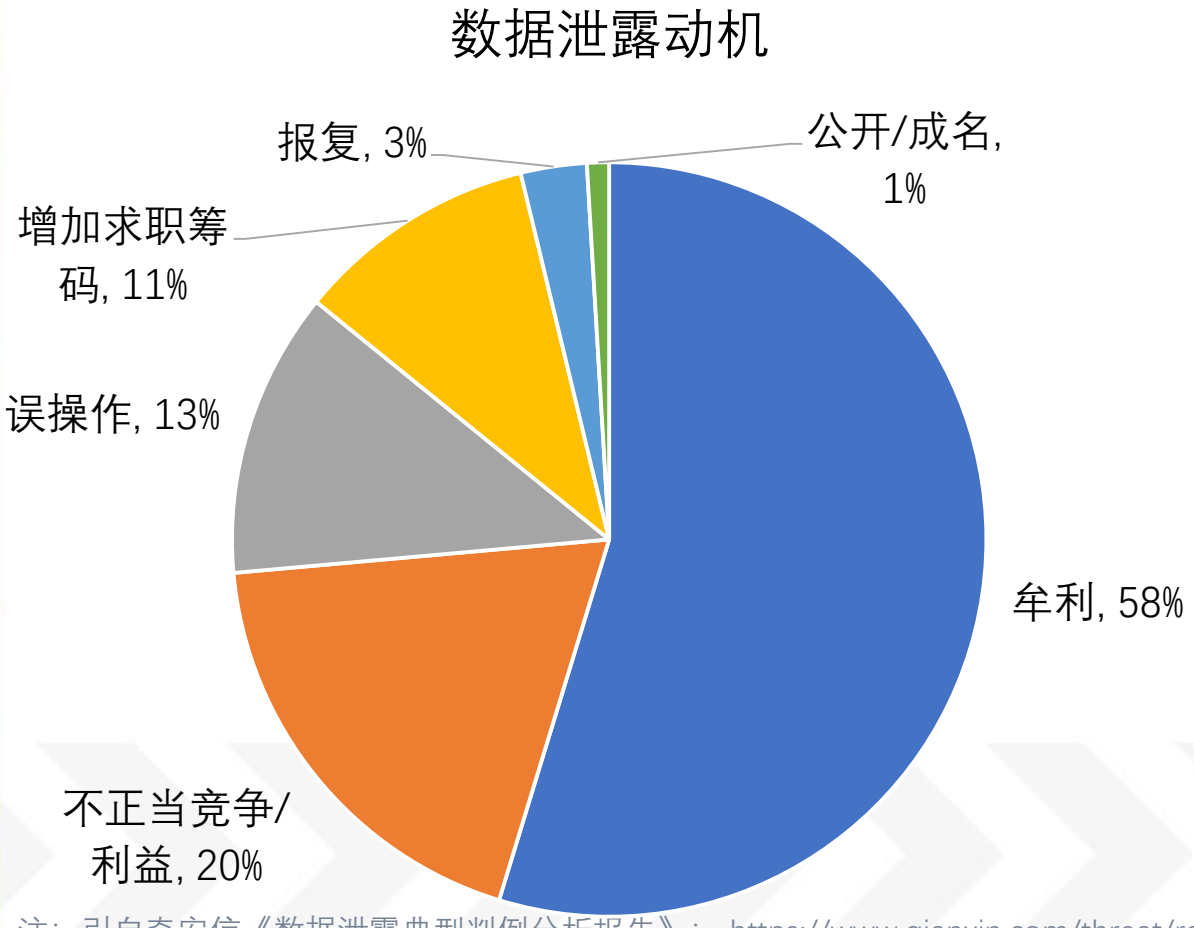
- 数据泄露源头80%来自内部人员，包括在职员工、离职人员、待离职员工等；黑客利用网络攻击窃取数据占比18%。

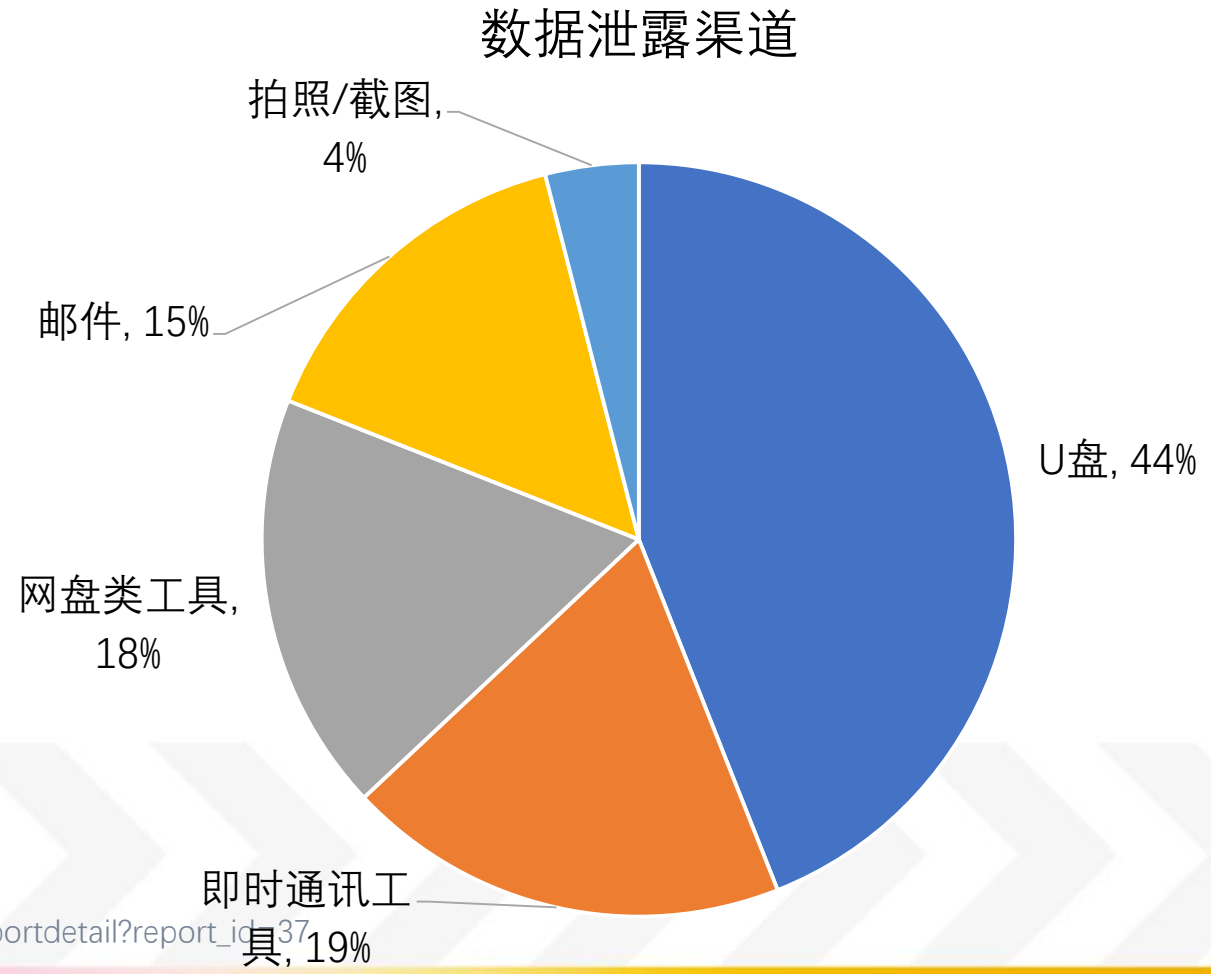


注：引自奇安信《数据泄露典型判例分析报告》： https://www.qianxin.com/threat/reportdetail?report_id=37

泄露动机及泄露渠道分析

- 牟利是数据窃取的最大动机，有利可图才会使人铤而走险。数据泄露渠道之中，移动存储介质占据半壁江山，IM工具、网盘和邮件也常用于泄露数据的外发。





注：引自奇安信《数据泄露典型判例分析报告》： https://www.qianxin.com/threat/reportdetail?report_id=37

证券幽灵（黄金眼）案件

- 辽宁省高级人民法院公开审理了一则新型内幕交易案件。2004年至2016年间，被告人朱某海制作并使用木马病毒非法侵入、控制他人计算机信息系统，非法获取相关计算机存储的数据。

- 非法控制计算机信息系统2474台，从XX基金、XX证券等多家机构的计算机系统内非法获取交易指令及内幕信息，进行相关股票交易牟利。一审被判处有期徒刑三年一个月，并处罚金1809.8万元

注：引自证券时报网《惊呆！新型内幕交易曝光，股民用木马窃取基金公司交易指令，12年获利180万…一审判决竟多方不满》：https://finance.sina.com.cn/stock/zqgd/2020-09-23/doc-iivhvpwy8370269.shtml

证券幽灵（黄金眼）案件

- **攻击目标**
  - 在当时国内近 100 家基金管理公司中，至少有 13 家知名公司被监控
  - 另有至少 2 家国内知名的资产管理公司遭入侵控制
  - 证券公司、期货公司等
  - 多个流行的股票交易软件开发公司被入侵和控制
- **攻击方式**
  - 主要攻击Windows，具备免杀能力，通过暴力破解（RDP、Radmin、MSSQL）、抓取Windows密码横向移动
  - 以HTTP、HTTPS、SMTP、P2P等多种方式通信
  - 高度怀疑攻击组织利用为金融机构提供 IT 服务的便利，进行供应链攻击

注：引自奇安信《“黄金眼”行动 - 针对国内金融行业的历史定向攻击活动技术分析》：https://ti.qianxin.com/uploads/2020/09/29/a9e49492211a85d450437607ebd41294.pdf

数据安全模型框架

网络安全创新大会
Cyber Security Innovation Summit

法律合规

1、网络安全法
2、数据安全法（草案）
3、个人信息保护法（草案）
4、App违法违规收集使用个人信息行为认定方法
5、GBT 35273-2020个人信息安全规范
6、GDPR

安全防护

收集	传输	存储	处理	交换	销毁
客户隐私协议	APP全站HTTPS	加密存储	去标识化	数据防泄漏	数据销毁
最小必要	审核认证	开发测试环	数据水印	堡垒机	介质销毁
授权同意	数据加密	境脱敏	蜜表	元数据平台	
数据定级	网络DLP	备份管理	日志留痕	UEBA	
数据识别			数据库审计		
账号安全					

内部管理

1、数据治理管理办法
2、数据管理实施细则
3、数据分类分级实施细则
4、数据标准管理实施细则
5、元数据管理细则
6、员工及合作方保密协议

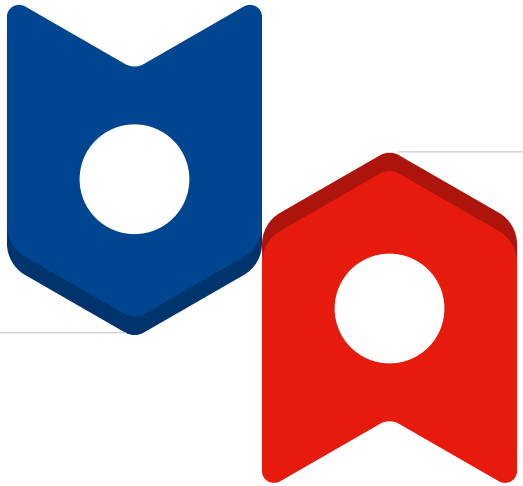
识别 | 保护 | 监控 | 检测 | 响应 | 恢复

法律合规团队 | 网络安全团队 | 数据治理团队

业务部门（数据属主）

纵深防御，加强内部管理

- 外防攻击：WAF+全流量+HIDS+蜜罐、VPN双因素+邮件安全网关、红蓝对抗+SRC+IAST、收敛暴露面
- 内防泄密：堡垒机+文件摆渡、DLP+UEBA、权限控制及模糊化
- 跨部门联动：安全团队、数据治理团队、客服部门、法律合规部门



外部协同，共筑安全防线

- 积极向公安机关提供案件线索
- 积极向工信、证监等监管部门报告破案情况
- 与安全机构联合进行数据安全评估

网络安全创新大会
Cyber Security Innovation Summit

THANKS