网络安全实践研讨会

——大数据营销及数据安全

内容提要

- 形势严峻
- 知彼知己
- 天网恢恢
- 任重道远

形势严峻

网络安全法：

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理。

- 第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。
- 第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

刑法第二百五十三条之一：

“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

“违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

形势严峻

最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

第五条非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的**“情节严重”**：

（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；

（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

（三）**非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的**；

（四）**非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的**；

（五）**非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的**；

（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；

（七）违法所得五千元以上的；

（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；

（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；

（十）其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的**“情节特别严重”**：

（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

（二）造成重大经济损失或者恶劣社会影响的；

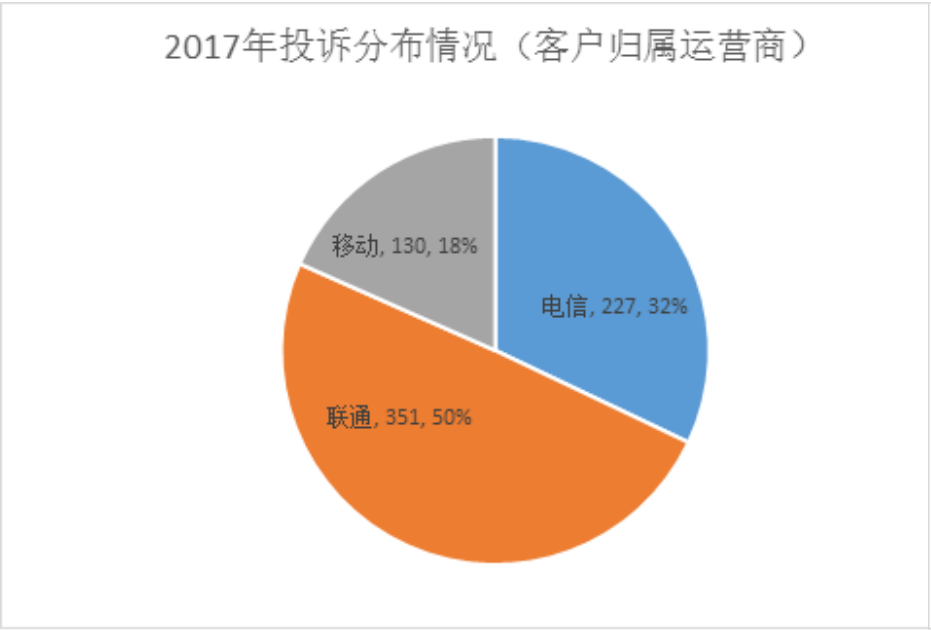
（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；

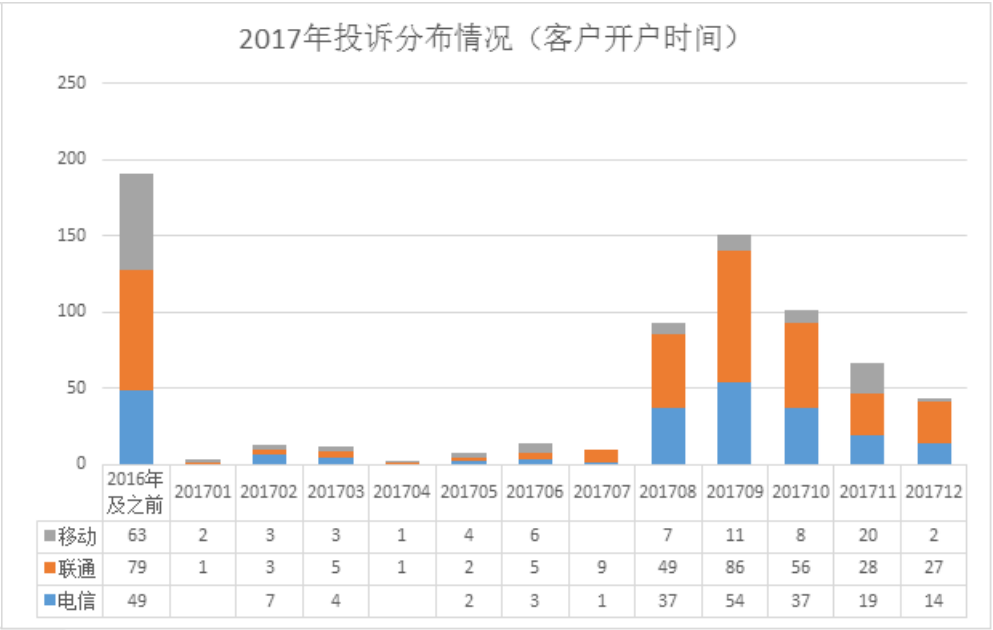
（四）其他情节特别严重的情形。

形势严峻

猜想1：客户信息泄露与运营商相关？

- 电话骚扰投诉中，联通和电信客户占比大：联通占比50%，电信占比32%。
- 我司移动客户占比约70%，假设出现数据泄露源头在我司内部，移动客户应该占比更大，假设与实际不符。





	2016年及之前	201701	201702	201703	201704	201705	201706	201707	201708	201709	201710	201711	201712
移动	63	2	3	3	1	4	6		7	11	8	20	2
联通	79	1	3	5	1	2	5	9	49	86	56	28	27
电信	49		7	4		2	3	1	37	54	37	19	14

形势严峻

猜想2：客户信息泄露与第三方短信平台相关？

2017年8月底，我司向18个手机号码发送一条开户验证码短信，发送时未经过我司任何内部应用系统，发送完成后在短信系统删除发送记录。彻底排除内部泄露可能性。

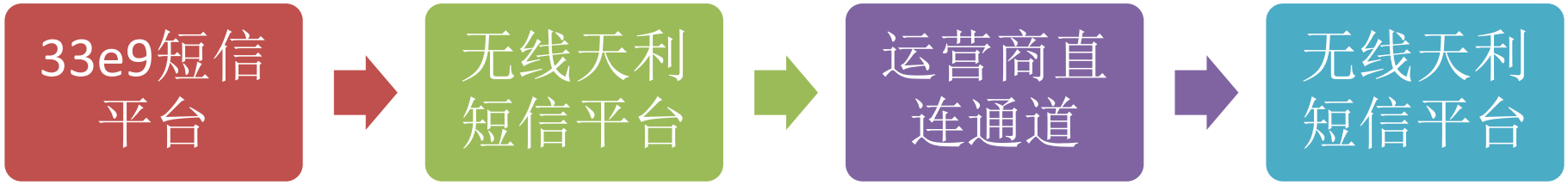
结果：测试手机号码中有三个号码被骚扰（占比16.7%）

- 时间关联：均在测试短信发出后第二天收到骚扰信息。
- 推荐股票关联：骚扰方均在微信上推荐同一只股票（不是偶然现象，而是同一个骚扰团伙所为）。

形势严峻

猜想3：客户信息泄露与第三方短信平台相关？

探索：为了防止第三方短信平台泄露客户信息，我司于2017年至2018年多次切换开户短信发送的平台，但均没有获得明显效果。



猜想4：客户信息泄露与运营商大数据营销相关？

内容提要

- 形势严峻
- 知彼知己
- 天网恢恢
- 任重道远

知彼知己

运营商大数据精准营销

- “运营商广泛聚合大数据源，对逾4亿用户做行为分析、挖掘与画像”

引自中国数据商城网：http://www.chinadatastore.cn/face/spdata.html

知彼知己

- 用户浏览网站，使用APP，搜索关键字——“大数据厂商”了如指掌
- “证券公司客户挖掘” 被当成典型业务场景

✓ 年龄25岁-55　　✓ 地域：西南某省

✓ 网站（3至6个月内高频访问以下网站）

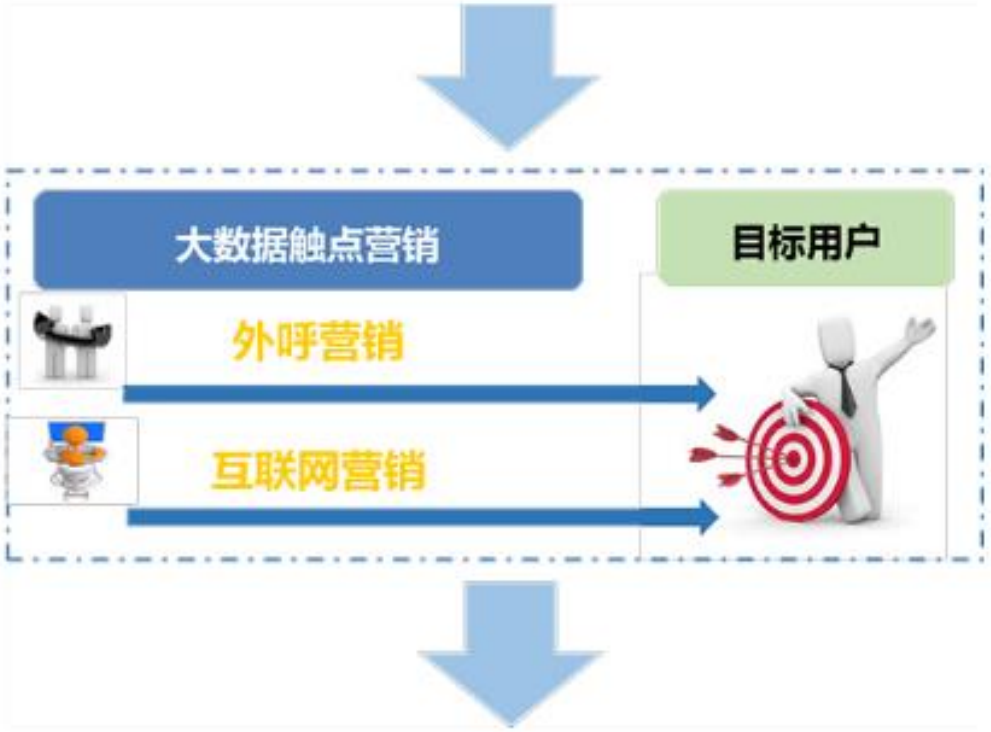
东方财富网 http://www.eastmoney.com/
和讯网 http://stock.hexun.com/
雪球网 http://xueqiu.com/
集思录 http://www.jisilu.cn/
第一财经（股市）：http://www.yicai.com/markets/
第一财经——今日股市 http://www.yicai.com/video/jinrigushi/index.html
新浪网（股市）：http://finance.sina.com.cn/stock/
腾讯网（股市）：http://stock.qq.com/
凤凰财经 http://finance.ifeng.com/stock/
大智慧官网：http://www.gw.com.cn/
同花顺官网：http://www.10jqka.com.cn/
中国财经信息网：http://www.cfi.net.cn/

✓ APP（使用竞品客户端）

大智慧、同花顺、东方财富通、和讯财经、雪球、集思录、第一财经、腾讯新闻

✓ 搜索关键字（3个月搜索过以下关键词，且搜索次数大于1）

1.证券网上开户；2.证券开户哪家佣金低；3.证券万二佣金；4.炒股如何开户；5.炒股网上开户流程；6.炒股入门知识；7.炒股开户手续；8.怎样炒股；9.炒股开户；10.怎么炒股新手入门；11.股票开户最好证券公司；12.股票网上开户；



引自中国数据商城网：http://www.chinadatastore.cn/face/spdata.html

知彼知己

- **只要提供券商URL，就能提取券商开户的客户信息**

知彼知己

- 仅靠我司内部力量，无法解决运营商大数据导致的客户信息泄露。
- 2017年10月，经请示公司领导后，由信息技术部牵头，党群工作部、电子商务部配合，向公安机关报案，并多次向公安补充提交相关证据。

内容提要

- 形势严峻
- 知彼知己
- 天网恢恢
- 任重道远

天网恢恢

公安报案，如何取证？

1、电话取证：

- 信息技术部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），并留存录音证据。
- 回拨后的开场白：喂，你好，刚才哪位找我？

电话对白：

- 员工：喂，你好，刚才哪位找我？
- 骗子：**我们是xx证券的**，因为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？
- 员工：xx证券？我刚刚开户啊。
- 骗子：哦，刚开户是吧？入金量大不大？
- 员工：入金量……你们是哪里？xx证券的你们是？
- 骗子：对对对，**我们是广州这边的**，**我们跟xx证券合作的**，这边老师都是从xx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，就是私募的那些大资金去操盘。

天网恢恢

公安报案，如何取证？

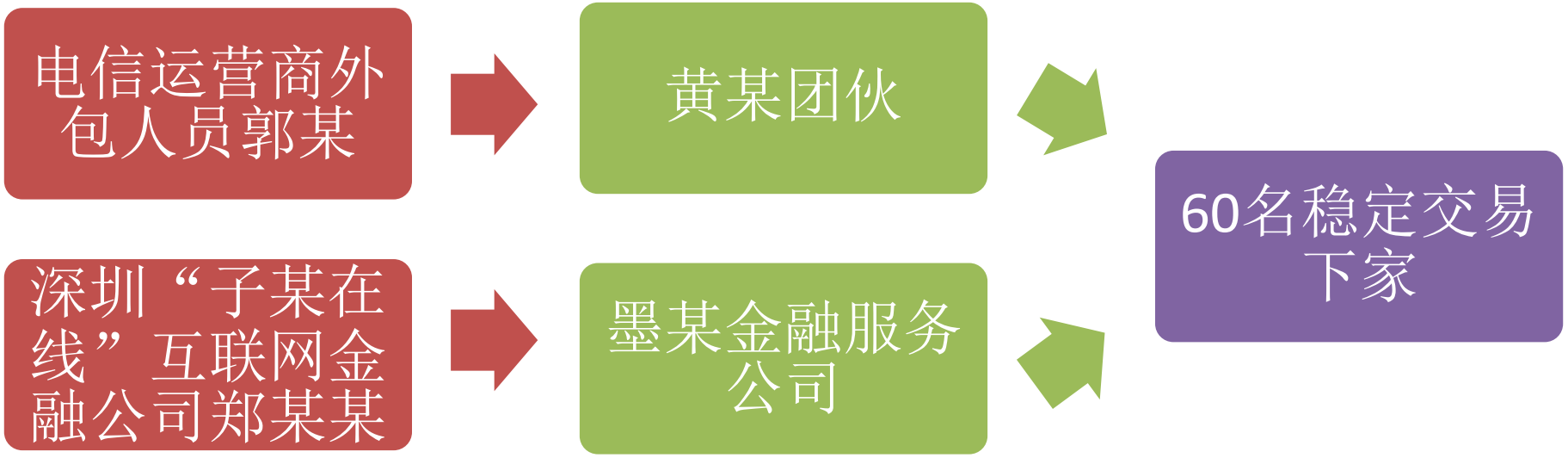
2、微信取证：

- 在对方添加微信后，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

天网恢恢

公安顺藤摸瓜，抓捕数据泄露源头

- 经广东公安进一步深挖，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）后向黄某团伙贩卖。



引自广东省公安厅网站：http://www.gdga.gov.cn/jwzx/jsyw/201806/t20180628_858251.html

天网恢恢

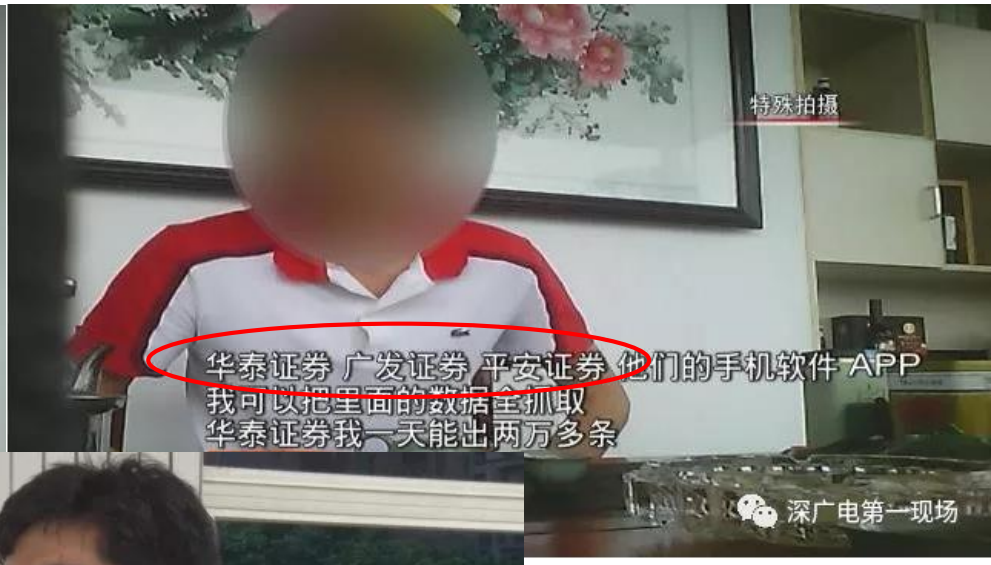
案件告破

- 案件经营成熟后，在省公安厅网警总队的指导下，广州市公安机关在北京、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。

引自广东省公安厅网站：http://www.gdga.gov.cn/jwzx/jsyw/201806/t20180628_858251.html

天网恢恢

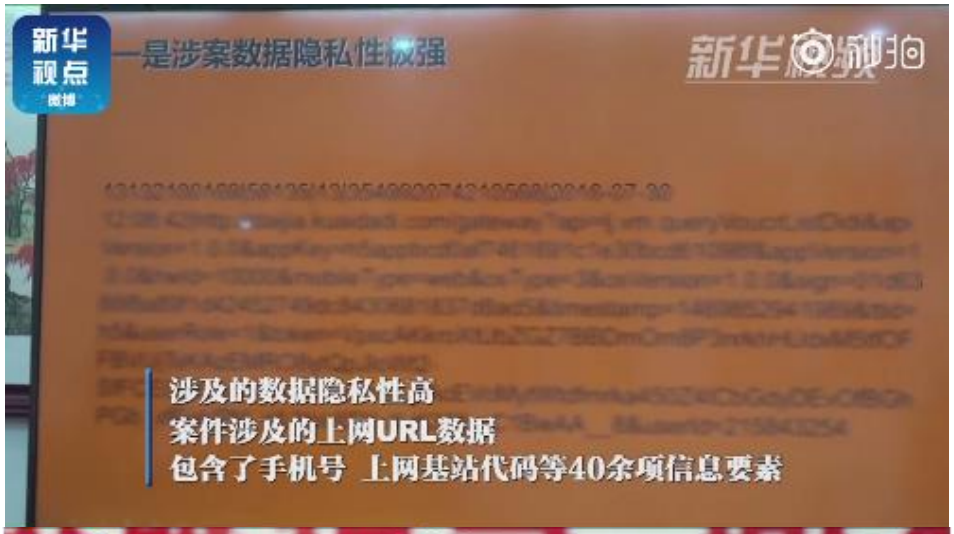
2018年6月，深圳媒体报道，“深圳市云宽科技有限公司”抓取基站客户信息，可抓取网页、APP和400号码的用户信息，用于精准营销。



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

天网恢恢

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被查（新三板某上市公司）



引自新华网微博：https://weibo.com/2810373291/GoZkMotw8?type=comment

内容提要

- 形势严峻
- 知彼知己
- 天网恢恢
- 任重道远

任重道远

两手抓

- 企业内部加强数据安全管理
- 共筑安全防线、联合反击（情报与最佳实践分享，联合向监管部门反馈）

数据因被消费而存在价值。

我们可以考虑面向用户、应用系统数据消费场景，制定数据安全管理体系。

数据消费安全管理基本原则：

1、以接口服务形式提供数据消费功能，并对接口进行统一管理。

2、接口尽量提供数据终态结果，避免原生态敏感数据的输出使用。减少原生态敏感数据的扩散半径。

任重道远

业务人员

1、完善应用系统的数据消费功能（查询、编辑、分享），数据通过应用GUI被用户消费，避免数据直接从后台导出。

2、提供数据消费安全管理平台（用于必须从后台导出数据的场景。后台导出数据只能存放在该平台，平台可提供在线访问、编辑、分享、防下载和拷贝、日志审计等安全控制功能）。

开发测试人员

1、对开发测试用业务数据进行脱敏。

2、通过虚拟桌面环境访问。

运维人员

1、后台访问操作仅提供堡垒机访问方式。

2、对数据库访问操作进行数据库审计。


原则上禁止外包人
员接触敏感数据

应用系统
数据消费

数据消费API接口调用：

1.源数据系统提供数据消费API接口，建立统一网关，调用接口应先注册，再分配ID。

2.接口参数进行严格校验。

3.建立接口调用异常监控规则（如访问频率）。

敏感数据消费管理：

1、敏感数据集中存储+数据消费功能调用接口。

2、提供数据消费的终态结果，避免调用接口输出的数据为中间态且仍带有部分敏感数据信息。

3、临时性非常态消费行为采取数据“阅后即焚”机制，即数据使用完后不做存储，即刻删除。

间谍机构保密管理的启示

单线联系

一个点暴露不影响其他点的安全，且仅限该点信息被泄露。

启示：

1、分层隔离：应用系统+数据服务层+数据库

2、暴露在外的仅为应用系统，应用系统无法接触到源数据，仅对接数据服务层并接收其输出的计算结果。

3、数据服务层读取数据库中的源数据并提供计算服务，输出计算结果给应用系统。

接头暗号

既能提防敌对势力渗入，又能避免误伤友军。

启示：

数据服务接口的授信管理与访问控制。