安全+ 沙龙第二十三期之
数据安全

2020年5月20日

浅谈互联网银行数据安全建设

汇报人: 网商银行-河书

目录

正本清源

分析互联网银行的现状，明确数据资产的主要保护范围。

关键问题

在数据安全建设上主要需要思考的问题。

产品制度

针对数据资产，关键问题设计需要的制度及产品。

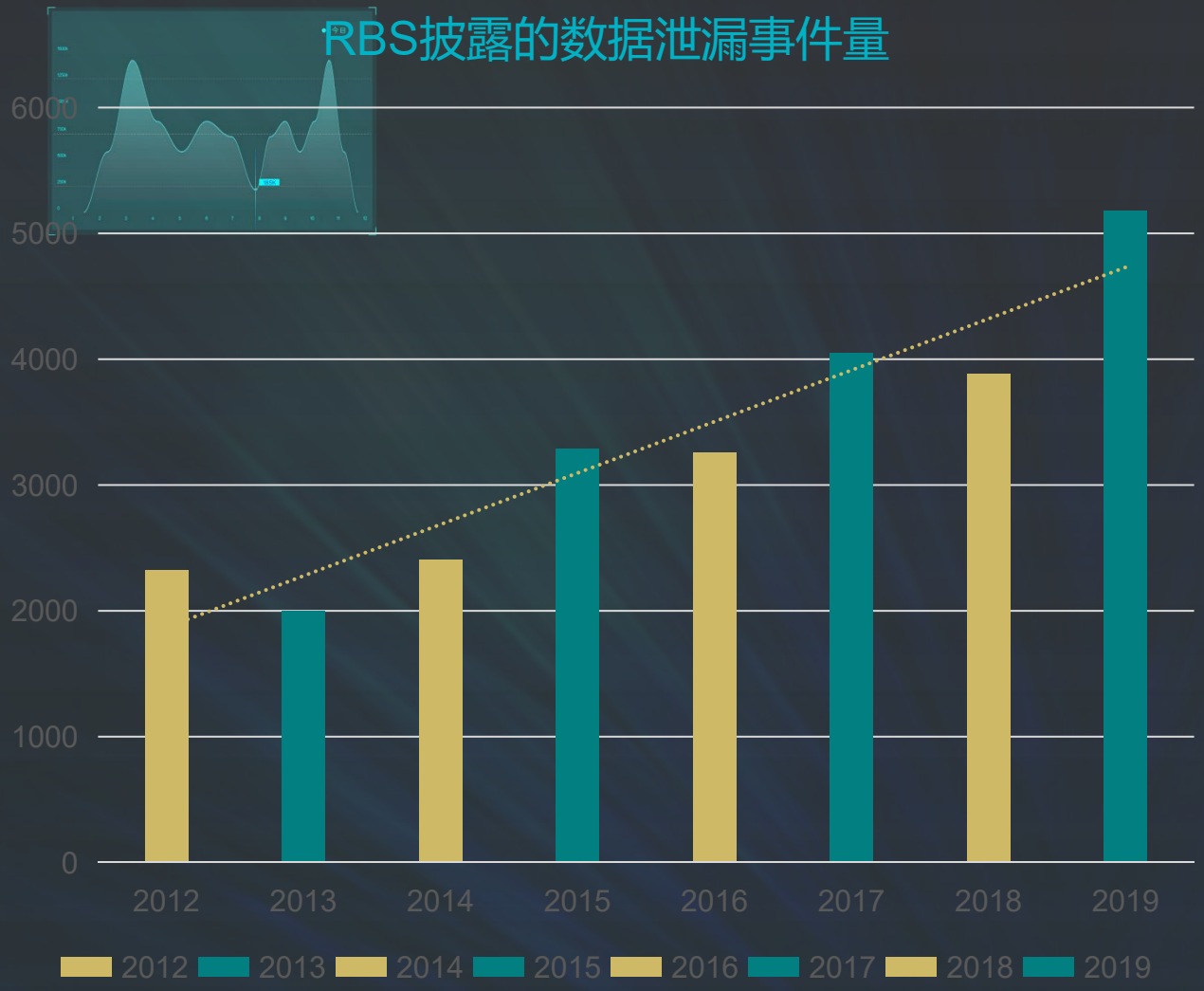
处置运营

针对数据安全事件的处置及运营的策略调整思路，闭环管理。

1

正本清源

正本清源



数据泄漏风险态势

数据安全情报供应商Risk Based Security (RBS) 的2019年Q3季度的报告，2019年1月1日至2019年9月30日，全球披露的数据泄露事件有5183起，泄露的数据量达到了79.95亿条记录！ 为了展示趋势，RBS列举前7年数据泄露情况 （如图所示）。从数据泄露事件数量来看，整体呈现出递增趋势，其中2019年泄露事件（5183）比2018年（3886）上涨33.3%。

主要泄漏场景

泄漏场景及原因

根据目前已披露的数据泄漏事件分析目前主要的泄漏场景及原因识别主要风险

内部泄漏
- 数据滥用
- 员工获利
- 误操作

外部泄漏
- 黑客入侵
- 爬虫获取
- 供应链

数据泄漏风险
- 客户损失：个人金融数据泄漏，造成的诈骗风险很高，导致客户的直接利益受损。
- 舆情风险：批量数据泄漏更会引发公司的舆情，使公司信誉受损。
- 合规风险：金融行业监管合规要求比其他行业更严格，产生负面消息时需要面对的监管压力更大。

行业现状

现状分析：

互联网银行目前的现状：1、开放普惠；2、金融数据的敏感性；3、金融监管压力；所以在数据安全中面临最大的问题是

如何在开放的基础上保证敏感数据的安全

？ ？ ？

2

关键问题

明确范围

需要保护的数据是什么

2020年发布了最新的中华人民共和国金融行业标准，其中很重要的一点是明确了个人金融信息的重要性， 针对金融企业的信息进行了数据分类分级的原则指导；各企业需要根据自身的业务，企业情况进行数据的分类分级。

数据分类

客户数据

业务数据

公司数据

数据分级

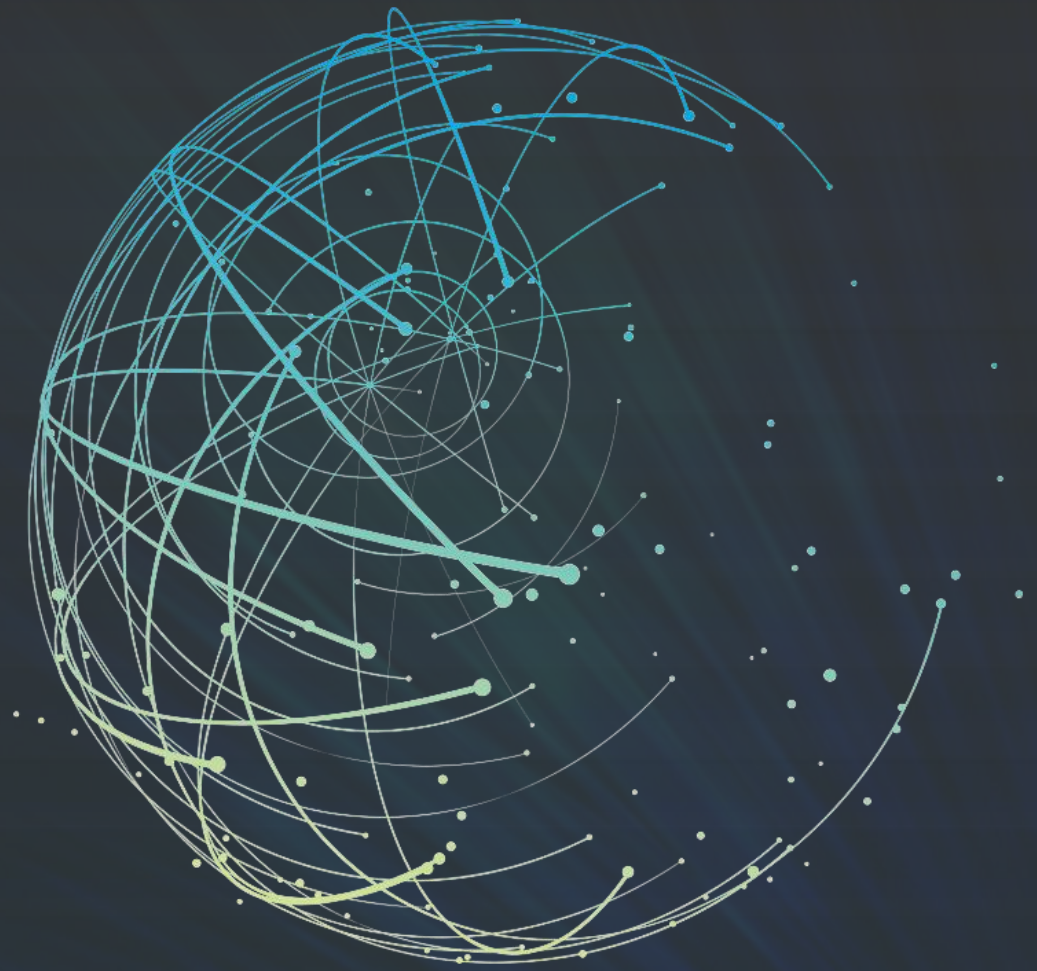
核心数据

敏感数据

内部数据

公开数据

解决策略



及时发现止损

1、如何发现数据泄漏事件；
2、如何有效检测率提升；

发现手段补齐：使用哪些产品技术等手段及时发现问题。

事件响应时间：主动发现率，响应时长，响应流程等。

源头上减少

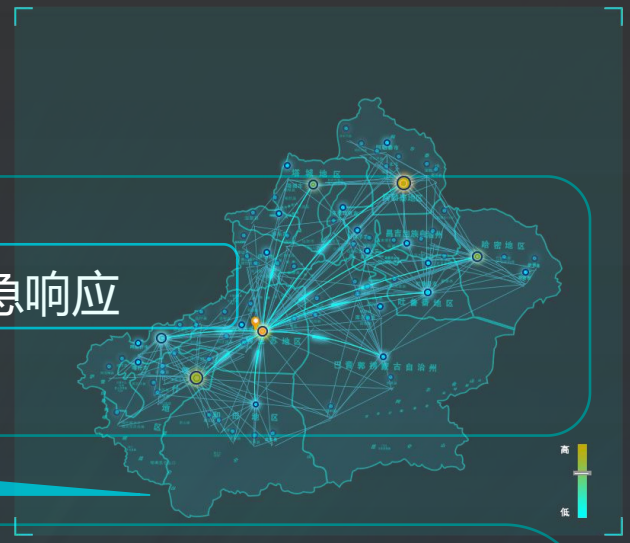
1、如何减少数据风险面；
2、如何减少数据泄漏情况的出现；

数据收口：数据进出口的集中化管理，减少分散点，降低管理成本。
指标收敛：人均数据泄漏量；处置率，场景收敛率等。-完善数据保护能力。

3

产品制度

数据监控系统建设



运营平台

风险大盘

行为审计

制度服务

情报反馈&应急响应

数据展示

策略平台

特征平台

设备指纹

行为链路

人员画像

风险模型

离职审计

违规软件安装

数据外发

权限滥用

数据爬取

关系人信息查询

……

账号盗用/借用

超特权审批操作

数据下载

数据清洗&加工

基础数据

上网行为日志

数据库审计日志

终端审计日志

可信设备日志

……

流程管理日志

流量监控

特权操作日志

鉴权认证数据

业务日志

制度沉淀

制度及数据保护能力建设

为了解决关键问题，减少公司数据泄漏风险，针对金融场景下强检管的特点进行制度及流程的建设补齐。

数据分类分级

公司数据分类分级制度是指导数据安全建设的根本。

数据输入输出

通过要求数据输入输出的标准明数据进出口的统一管理，及流程要求。

数据安全行为规范

明确数据安全事件定则的规定，根据数据等级，数据量设定一定的处罚。处罚不是目的，减少风险面才是王道

数据安全响应与流程

针对数据安全事件的应急与响应流程，提出要求，快速反应及应对的基本指南。

应用数据安全规范

明确应用开发过程中的数据保护要求包括但不限于：脱敏、水印，日志，加密，权限、反爬等。借助SDL的卡点，针对应用性质给予水位要求。

数据安全管理办法

设定公司数据安全管理的虚拟组织架构及职责；各部门数据安全责任及划分，明确责任主体，方便自上而下的管理。

权限管理制度

设置权限申请的要求：最小范围，最小事件，最小操作；权限审的要求例如：必要性，最小化，重复性；权限销毁的场景，例如过期回收；离职、转岗权限销毁；无需求权限销毁等。

特权操作申请及流程

某些特定场景的特权操作申请及流程管控。

4

处置运营

处置运营

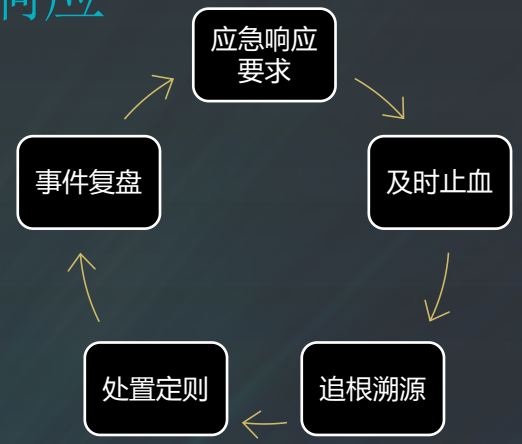
意识培养

意识宣传及相关考试：在大规模企业中，符合价值观的宣导工作，对安全运营的效果非常显著；针对帮助新员工适应环境，了解基本安全水位往往起到奇效。

数据治理

针对响应事件分类聚合，按照项目的形式针对事件进行追溯，从源头解决问题，自上而下进行数据治理。

事件响应



能力沉淀

通过数据治理发现需要沉淀的数据保护能力，针对响应的业务场景沉淀安全能力，平台化，服务化，例如：鉴权服务，水印服务，日志服务等。

谢谢您的观看！

汇报人: 河书

安全+ 专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：www.anquanjia.net.cn

微信公众号：anquanplus