

安世加

*"Face the challenge, Embrace the best practice"*

# EISS-2020 企业信息安全峰会 之上海站

2020年11月27日



# 后疫情时代券商数据安全体系的实践与展望

中银证券 蒋琮

**安世加**

# 1

## 政策与法规

单位：%

## 中国信息安全数据泄露占比（TOP10）

■ 中国信息安全数据占比



# 最近发生了什么？

会影响企业安全管理者的工作优先级和“职业安全”

01

## 法律：

- 《两高司法解释》
- 《刑法》
- 《个人信息保护法》
- 《数据安全法》
- 《网络安全法》
- 《消费者权益保护法》

02

## 人民银行监管：

- 人民银行执法案例
- 行业标准
- 金融科技风险排查
- 金融数据分级分类
- 司长：基于API模式的开放银行已成为引领商业银行数字化转型升级

03

## 四部委：

- App检测和通报
- App行业备案与认证

04

## 证监会监管：

- 证券法“自证清白”
- 信息技术管理办法
- 证券行业事件报告与调查制度中的自证充分尽职要求

05

## 风险与事件：

- 互联网公司API漏洞泄露事件，涉及2亿数据
- 暗网贩卖
- 开户/签单客户被骚扰和同行恶性竞争
- 电信大数据营销骚扰
- 诈骗、杀猪盘
- 开放银行新挑战：数据、网络和业务风险



# 证券行业信息技术监管指引发展

- 组织架构
- 项目安全管理
- 机房设备管理
- 网络、软件和数据
- 系统事故防范处理

2005.3

证券公司信息技术管理规范

- 备份能力等级
- 备份能力需求
- 备份能力建设管理

2011.4

证券期货经营机构信息系统备份能力标准

- 基础架构管理
- 系统运维
- 网络管理
- 数据安全
- 供应商管理

2012.9

证券期货业信息安全保障管理办法

证监会于2018年12月19日发布了《证券基金经营机构信息技术管理办法》，共7章64条。此次发布的《证券基金经营机构信息技术管理办法》将证券基金经营机构信息技术风险重点归纳至**治理、合规与风险管理、系统安全**三大领域，突出**数据治理**的重要性，也引入了对信息技术服务机构的监管，同时制定了相应的**惩处监管措施**，加大了执行力度，引起行业内外高度重视。

2005

2008

2011

2012

2013

2016

2018

2008.9

证券期货经营机构信息技术治理工作指引

- IT治理目标
- IT治理组织
- IT投入和人力资源
- IT安全和风险控制

2011.12

证券期货业信息系统安全等级保护测评要求

- 物理安全
- 网络安全
- 主机安全
- 应用安全
- 数据安全与备份
- 人员安全
- 系统建设
- 系统运维

2013.1

证券期货业信息系统运维管理规范

- 安全管理
- 供应商管理
- 数据介质管理
- 事件与问题管理
- 网络管理
- 机房管理
- 系统维护
- 应急管理

2016.11

证券期货业信息系统审计指南—证券公司

- 信息技术治理
- 机房网络运维管理
- 信息系统安全等级保护
- 软件正版化管理
- 集中交易系统
- 第三方存管系统
- 网上信息系统
- 重要信息系统
- 营业部管理

2018.12

证券基金经营机构信息技术管理办法

- 信息技术治理
- 信息技术合规与风险管理
- 信息系统安全
- 信息技术服务机构
- 监督管理

## 证券基金经营机构信息技术管理办法重点

信息技术治理

信息技术与合规风险管理

信息技术安全之  
信息系统安全

信息技术安全之  
数据治理

信息技术安全之  
应急管理

信息技术服务机构

监督管理

示例

- ▶ 数据来源合法
- ▶ 数据收集授权

数据收集

- ▶ 数据介质销毁
- ▶ 敏感数据销毁

数据销毁

数据全生命周期  
管理

数据存储

- ▶ 数据备份
- ▶ 数据分类分级
- ▶ 数据存储加密
- ▶ 测试数据脱敏

数据传输

- ▶ 数据传输安全
- ▶ 数据传输合规

数据使用

- ▶ 用户认证
- ▶ 访问控制/日志记录
- ▶ 数据泄漏分析

### 《管理办法》第二十九条：

证券基金经营机构应当结合公司发展战略，建立全面、科学、有效的数据治理组织架构以及**数据全生命周期管理**机制。

2

差距与实践



## | 数据治理相关问题

### 多方参与，明确工作 责任和 workflows

大多数公司没有明确的数据治理架构，不满足《管理办法》的第29条规定。公司管理层对数据治理没有引起足够的重视，数据安全意识薄弱。

### 离线数据管理

公司普遍认为只要数据备份完成就可以，没有后续的保护措施，没有维护记录；对备份介质的管理不严格，机房监控覆盖范围不全面，无法支持对数据泄露、丢失事件进行追责。



### 不能光喊口号，要从 实操抓起

部分基金公司在制度上对数据明确分类分级标准，但在日常管理及实际操作中并未体现；或是制度规定了数据的使用、调阅规范，但没有相应的审批流程留痕。

### 建立完整的个人金融信息 保护体系

存在有公司将个人金融信息视为业务数据的一部分的情况。公司应当引起重视，同时根据个人金融信息的重要性更新相关应急处理流程和预案。

# 数据保护-数据泄露防护体系

## 管理体系

制定数据保护管理制度

制定日常数据安全检查办法

制定数据泄露审计办法

## 责任体系

制定持续性保密意识宣传、培训计划

进行普通员工和高级管理层的信息安全保密意识培训

# 体系、系统化和管理体系

**System** - Set of interrelated or interacting elements

体系 - 一系列相关或相互作用的元素

**Work systematically** – To be effective, things have to be organised in a suitable/practical way and should be done in a certain sequence

系统地工作– 为了有效，事情必须按合适的/实际的方法进行组织，并以一定的顺序完成

**Management system** – system to establish policy and objectives and to achieve those objectives

管理体系—体系是建立方针和目标，并达成这些目标

1

- 传统安全架构
  - 边界清晰，护城河式的管理理念-木桶原理

2

- 零信任安全管理架构
  - 资源的集中管控-基于策略管理
  - 零信任、细粒度权限管理等“正向建设”高度依赖于企业架构成熟度，周期长且需要高层领导力支持，持续地、基于分级分类（固有风险）和实际内、外部威胁的数据访问和泄露事件监控与快速响应，将是安全职能的主营业务之一。

# 威胁在哪？

- **超过85%的安全威胁来自公司内部：**企业员工，驻厂外包人员，实习生，外协方.....
- **信息安全的高危时刻：**如电脑维修或变更、新入职/离职/开除员工、外包人员的进离场之际、新样品...



**泄密的发生往往只在  
不经意的一瞬那！**



**安世加**



# IT外包业的信息安全

- 来自不同客户的特殊要求
- 行业及上市公司的要求
- 客户信息、项目文档、源代码、标书等的机密性
- 重要IT系统的可用性，如邮件服务器、源代码、数据库服务器、配置库服务器等。
- 所有储存重要信息系统服务器的授权访问及权限定期评审，完整性的要求
- 其它如人员、软件版本有效性...



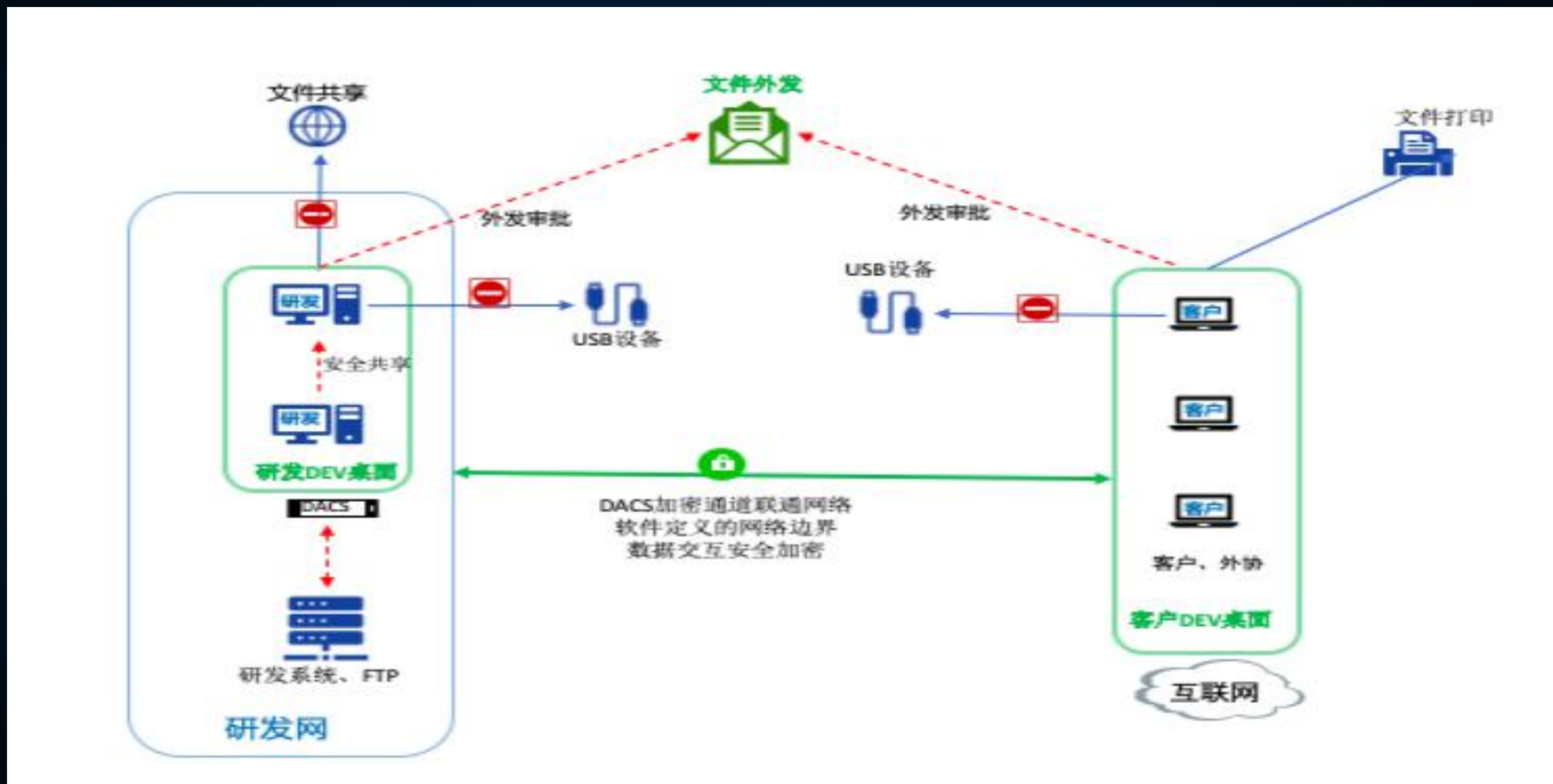
# 零信任应用访问网关模型



# 零信任应用授权流程



# 零信任架构应用场景实践



3

持续与展望



# 体系庞大、挑战很多，采取什么思路应对？

## 6、运营驱动平台效能和战斗力：

打胜仗是原则，既要有装备，更要有常态化战斗力

## 5、项目（群）持续迭代：

确立主线职能和能力方向后，项目群对齐职能能力建设，小步快跑

## 4、治理、组织与团队：

先建职能和团队，再寻找确立组织责任的机会



### 1、识别法律法规依据：

导致入刑、法律义务、行政处罚、影响监管评级、事件后监管措施、法规中实质条款、组织责任、关键控制措施要求以及可被监管措施引用的建议性标准

### 2、确立核心工作逻辑：

先自证合规，再保障结果

### 3、聚焦核心风险：

筛选优先成效和监管  
执法案例领域

# 有效的BCM程序能够实现的益处

- 关键的数据资产被系统性识别并保护
- 有效响应的数据安全事件管理能力
- 可靠可持续的供应链管理
- 保护企业声誉风险
- 有能力管理不被保险的风险
- 纵深缩小后的平衡

留待思考





整体规划、重点突破、分步实施、协调发展

方向的选择： 最急需的  
最重要的  
快速见效的

相辅相成的人员， 流程， 技术  
形成闭环的事前， 事中， 事后

安世加



# 关于我和本次分享

## • 关于我

- 18年信息安全和科技风险管理从业经验，熟悉国内、外银行、证券业大安全环境、生态与实践。
- 国内第一批CISA，DPO。在信息系统安全审计、数据安全实践等方面具备丰富经验。
- 曾任中和软件后台合规性检查系统高级工程师、负责人。
- 中银证券ISG参赛团队论文答辩演讲核心成员。
- 民主建国会上海市委信息工作委员会班子成员。
- 作为在信息科技安全领域长期浸润的女性，既有理工科专业人的严谨理性，也有善于总结思考，坚持推动发展的理想主义情怀。果敢、勇气、执着、从容，持续致力于金融证券行业IT治理与安全管理体系的建设与提升。

## 本次分享

数据安全体系很庞大，法律法规环境持续变化，实现个人信息保护的结果依赖多个领域安全的管理与技术效能、效果

思考和梳理一个职能建设逻辑和优先级

安世加



# 知所从来，思所将往


12/4/2020

为你做更多的事 / 陪你走更远的路



安世加





感谢聆听

安世加

**安世加** 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: <http://anquanjia.net.cn/>

微信公众号: asjeiss



**安世加**