2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE

西湖论剑·网络安全线上峰会

之江实验室 ZHEJIANG LAB

数治安全 智理未来

DIGITALLY GOVERNED SECURITY INTELLIGENTLY MANAGED FUTURE

2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE
西湖论剑·网络安全线上峰会

之江实验室 ZHEJIANG LAB

新形势下个人金融信息保护的挑战与思考

主讲人：廖敏飞　资深总经理

单位：建信金融科技有限责任公司

2020年6月

Contents 目录

个人金融信息保护

一.个人金融信息保护的现实意义

1.数据泄露频频发生

金融行业

近年来，以大数据、云计算和人工智能等为代表的金融科技正在改变和推动着商业银行向着数字化、智能化的BANK4.0演进，但与之伴随而来的是金融信息问题层出不穷。

2015年
某银行
账户文件泄露

银行账户约3万个账户被曝光，相关账户总计持有约1200亿美元资产。

2018年
中国互联网网络安全权威报告

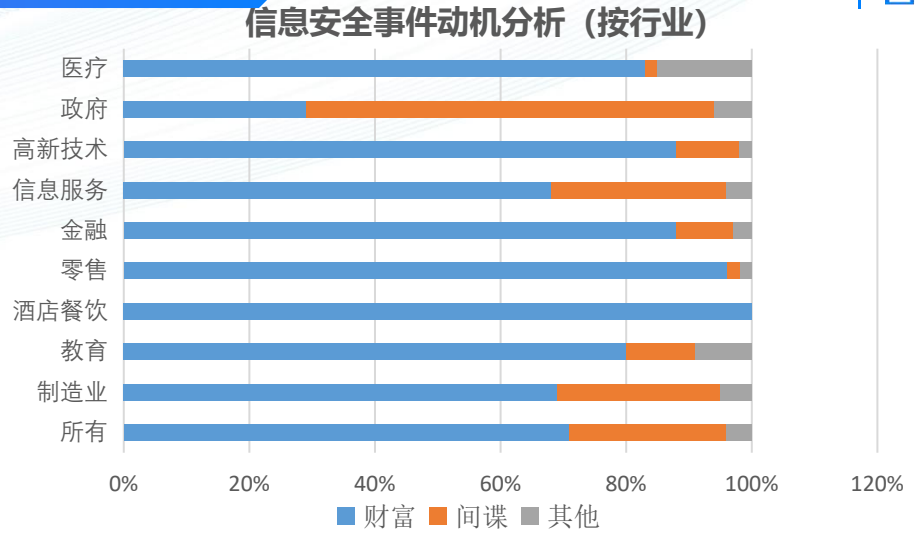
国家互联网应急中心发布：中国互联网金融网站及其APP经检查漏洞有1700个，其中782个是最高危跨站脚本类型漏洞。

2019年
App个人信息违规使用专项治理活动

以四部门全国范围组织开展App违法违规收集使用个人信息专项治理活动为代表，监管部门专项治理活动日趋增多。

一.个人金融信息保护的现实意义

1.数据泄露频频发生



非金融行业

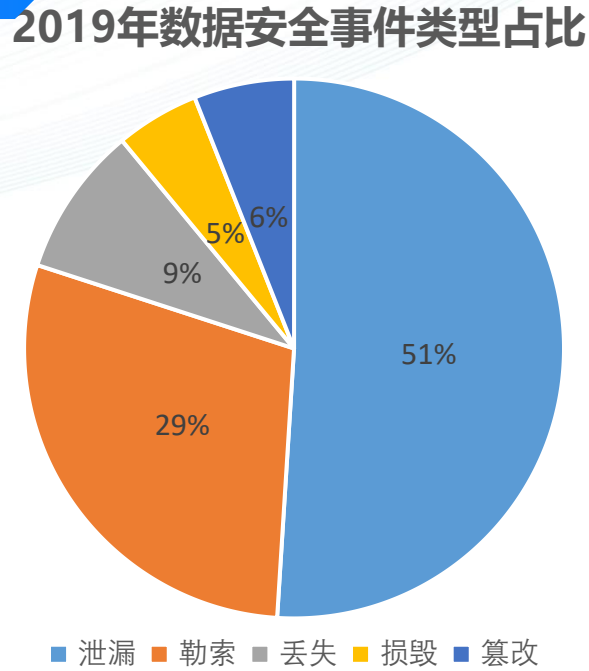
当今互联网已然成为现代社会中人们日常生活不可或缺的重要组成部分，而一旦安全保护不力，就容易产生资料外泄的状况。同时.各行各业数据泄露的原因大致可归为谋求财富、间谍行为和其他。

2019年1月	某招聘网站**2.02亿**份简历854GB数据被公开
2019年3月	某数据库中**7.98亿**电子邮件记录可公开访问
2019年5月	某房地产巨头**8.5亿**份敏感客户财务记录泄露
2019年10月	某社交游戏**2.18亿**用户数据库被黑客入侵

一.个人金融信息保护的现实意义

1.数据泄露频频发生

数据安全事件数量的整体呈现**上升**趋势



数据泄露事件层出不穷，**占比最高**

整体态势：数字化发展迅猛，万物互联，数据的价值变得越来越重要，使得攻击目标越来越多、途径越来越多，以及以数据为目标的犯罪活动越来越多，同时数据安全技术的发展，以及媒体透明度的增加，使更多的数据安全事件得以发现和曝光。

一.个人金融信息保护的现实意义

2.数据黑产暗流涌动

定义

个人信息的获取和买卖其实构成了信息数据**产业链**，有的人专门盯这些漏洞，有的人专门去破解这些数据，然后清洗这些数据，再使用这些数据。

数据的黑产生态从最开始的黑客攻击，然后到后面的拖库、洗库、撞库，再把这些数据卖给一些数据方，这个数据方再提供给下游的需求方，形成了一个非常完整的产业链。在这个产业链中数据的标准格式里各种信息都有，这样的攻击首当其冲的目标是金融行业。

二.个人金融信息保护的发展现状

1.个人金融数据安全保护现状

相关技术规范

安标委

《个人信息安全规范》
(GB/T 35273-2020)

- 2017年12月，2017版正式发布
- 2020年3月，2020版正式发布
- 主要由中国电子技术标准化研究院起草

金标委

《个人金融信息保护技术规范》
(JR/T 0171-2020)

- 2020年2月发布
- 由人民银行科技司起草

二.个人金融信息保护的发展现状

1.个人金融数据安全保护现状

国家主管网络安全相关部委机构

中央网信办、工信部、公安部等多部门，全国信息安全标准化技术委员会、市场监督管理总局标准技术管理司以及行业主管机构。

相关出台管理办法

《数据安全管理办法（征求意见稿）》、《App违法违规收集使用个人信息行为认定方法（征求意见稿）》、《个人信息安全规范（征求意见稿）》、《信息安全技术、移动互联网应用（App）收集个人信息基本规范（草案）》等密集出台。

国家主管网络安全的相关部委机构等正密锣紧鼓展开网络安全及个人隐私保护的相关工作，同时这些法律法规从多方面体系化地完善我国个人信息隐私保护方面的法律法规体系。

二.个人金融信息保护的发展现状

2.个人金融数据安全保护存在问题

问题

1.个人信息范围**边界不清晰**

增加了银行、证券、保险等金融机构的实施难度

民法总则第一百一十一条规定了自然人的个人信息受法律保护，但个人信息范围究竟应该如何确定，未明确提及。

2.目前很多互联网金融、银行、券商、保险上的合作方存在个人信息**监管隐患**

多数情况下获得个人信息的理财所属机构对于消费者个人信息的保管并不在产品营销平台的金融机构监管范围之内。

3.个人信息保存时效**范围尚不完善**

当前法律并没有规定个人信息的保护具体时限

当前法律并没有规定个人信息的保护具体时限。

三.个人金融信息保护新思考

人行科技司牵头组织23家单位共同研究、制定、出台

新形势下个人金融信息保护技术行业规范（JR/T 0171—2020）

中国人民银行 THE PEOPLE'S BANK OF CHINA 科技司 Technology Department

4大领域

- 人行分支机构及直属中心
- 国有商业银行
- 金融业股份制商业集团（公司）
- 金融科技公司

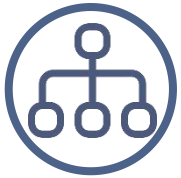
中国人民银行科技司牵头，对我国现行信息保护相关法律、法规和规范性文件进行研读、梳理，各单位信息安全领域的专家、科技人员经过长时间的反复研讨、深入交流，对国内外的网络安全形势和防御机制进行了深入研究和对比分析，于2020年2月制定出台了新形势下的个人金融信息保护技术行业规范。

三.个人金融信息保护新思考

分类分级管理

根据信息的重要性和敏感程度进行**分类分级管理**

全生命周期动态管理



采用**灵活的级别界定模式**对个人金融信息全生命周期进行动态管理

整体防护框架

提出企业级的个人金融信息的**整体防护框架**

个人金融信息保护工作的3点思考和建议：

1、提出个人金融信息分类分级管理的思想，根据信息的重要性和敏感程度进行不同级别的保护和管理；

2、采用灵活的级别界定模式对个人金融信息全生命周期进行动态管理，随具体场景界定信息级别，做到因数据而异、因场景制宜；

3、提出企业级的个人金融信息的整体防护框架，辅助金融机构提升个人金融信息管理水平和风险防范能力。

三.个人金融信息保护新思考

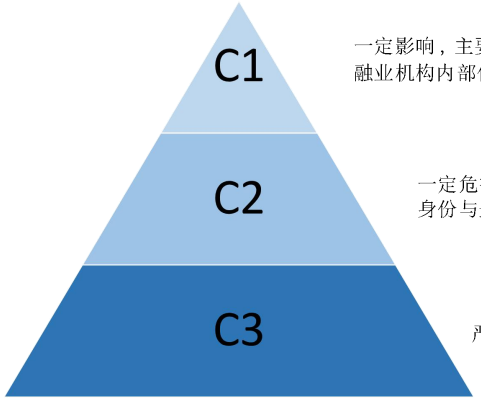
1.个人金融信息分类分级处理

七大类

1. 身份鉴别信息
2. 金融交易信息
3. 个人身份信息
4. 账户信息
5. 财产信息
6. 借贷信息
7. 其他信息

对各类金融信息进行**差异化、精准化**治理和使用

三大级别



C1：一定影响，主要为机构内部的信息资产，主要为金融业机构内部使用的个人金融信息。

C2：一定危害，主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息。

C3：严重危害，主要为用户鉴别信息。

对不同等级的信息内容做**不同程度的规范和约束**，实现信息使用效率最大化。

三.个人金融信息保护新思考

2.个人金融全生命周期动态管理

全生命周期包含六个环节：信息级别动态管理

信息级别动态可变

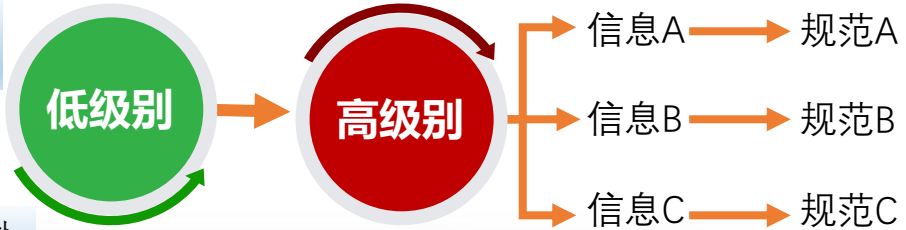
低级别信息经组合关联会转化为高级别信息

例如，C2级短信验证码与C2级账户（手机号）组合便可用于用户身份鉴别，成为C3级别信息。

同级别信息细分规范

同级别中的不同信息，其规范要求不同

例如C2级别“用户鉴别辅助信息”，规定不能委托第三方机构处理，但是C2级别的其他信息可以采取去标识化脱敏进行委托处理。



三.个人金融信息保护新思考

3.个人金融整体防护框架

制度体系

全方位建立

从开发建设、生产运行、安全风险三个方面建立**完整**的个人金融信息保护**制度体系**。

安全准则

七大安全准则

1. 权责一致
2. 目的明确
3. 选择同意
4. 最少够用
5. 公开透明
6. 确保安全
7. 主体参与

技术体系

全生命周期

建立涵盖**全生命周期**所有环节的完备的**技术体系**，指导系统的开发建设、运行监测。

四.个人金融信息保护落实举措

建信金科成立个人金融信息检查整改专项工作组。

组织《规范》专项学习，各领域团队集体学习和成员自主学习相结合，并进行全员知识测验。

根据检查表，结合访谈、资料调阅及技术检测多种技术手段，对所辖系统开展全面检查分析工作。

组织学习培训	试点摸查	全面排查	整改完善

选取重点系统参与试点检查，不断完善检查表项的设置，积累排查经验。

根据排查结果及业务实际情况，制定详细具体的整改计划，并跟踪督促落实。

四.个人金融信息保护落实举措

A

全局观

领导牵头成立个人金融信息检查整改**专项工作组**，引起**全员重视**。

B

高效率

采用**自动化扫描工具**和**人工排查**相结合的方式，提升排查**效率**。

C

全面性

先选取**重点系统**进行**试点检查**，积累排查**经验**，而后开展**全面排查**。

D

时效性

发现潜在隐患**立即**制定整改计划，**避免**发生**安全风险事件**。

五.个人金融信息保护愿景

稳定、安全的金融市场环境需要参与金融市场的所有机构与个人共同遵守个人金融信息保护领域的法律、法规和相关规范，合理、规范地收集、传输、存储、使用数据。

谢谢！