



数据价值提升,个人隐私数据泄露事件频发 中国光大银行 CHINA EVERBRIGHT BANK





据IBM Security基于对全球500多个组织数据泄露事件深入分析发布的《2020年数据泄露成本报告》中显示, 2020年数据泄露事件给企业造成的平均成本为386万美元。

国际事件



2020年4月,世界卫生组织疫情期间遭受网络攻击数 量急剧增加,约有450个世卫组织及数千名相关工作 人员信息遭到泄露。



2021年4月,美国社交媒体脸书(Facebook)超5亿用 户的个人数据遭到泄露,包括电话号码、电子邮件等 信息。



2021年4月,据Cyber News报道,LinkedIn信息大 规模泄露,影响5亿用户,目前信息已经被攻击者拿 到网上出售。



2020年12月,富士康遭遇黑客攻击,索要 2.3 亿元 赎金: 1200台服务器被加密, 100GB数据遭窃。

国内事件



2020年初,多地武汉返乡人员配合调查后个 人信息被泄露,包括姓名、家庭住址、电话、 身份证号等, 表格在各个老乡群和小区群里传 播,不少人反映被陌生人通过电话、微信骚扰



2020年8月, 圆通出现多名"内鬼", 40万 人信息被泄露, 一条黑色产业链浮出水面。



2021年3·15晚会,支付7元即获简历,智联 招聘、猎聘、前程无忧上"黑榜"。



2021年3.15晚会曝光科勒卫浴、宝马安装人 脸识别摄像头, 收集海量人脸信息。

国内外加快数据安全保护工作





我国法律法规和监管机构日趋收紧



★ 我国法律法规和监管机构日趋收紧,切实保障国家数据安全

- 加强法律法规、标准规范的统筹规划,重视国家标准、相关领域行业标准的衔接工作;
- 加强关键信息基础设施安全保护,强化国家关键数据资源保护能力,增强数据安全预警和溯源能力。

《网络安全等级保护要求》2.0

《大数据安全管理指南》

《数据安全能力成熟度模型》

《个人信息出境安全评估办法》

《个人信息去标识化指南》

2020年

《个人信息保护法(草案)》

《网络安全法》 <u>《大数据安</u>全服务能力要求》

2018年

2017年

《互联网个人信息安全保护指引》

《个人信息安全规范》

《个人信息影响评估指南》

2019年

《数据安全法(草案)》

《网络安全审查办法》

《金融数据安全 数据安全分级指南》

《个人金融信息保护技术规范》

2021年

新业务生态下的数据安全威胁



数据安全威胁和暴露面随着业务变化而增加



- 利用应用系统的漏洞、网络漏洞进行注入攻击;
- 利用银行移动设备、智能设备、监控设备、无线网络进行渗透;
- 通过病毒、木马、0Day漏洞进行渗透攻击。
- 内部员工有意、无意操作不当造成数据泄露;
- 业务人员使用对内部数据分析,使用数据不当;
- 高权限人员使用特权访问不当;
- 业务人员权控不当, 超权限访问业务数据, 过度访问业务数据;
- 通过邮件、移动存储设备等, 泄露数据。
- 大数据、生物识别、公有云等新技术带来新的数据安全风险;
- 开源社区软件、第三方SDK、开发运维工具带有恶意代码;
- •银行生态中,和第三方合作企业进行的数据交互带来的风险。

业务生态中不平衡数据安全能力带来新威胁 CHINA EVERBRIGHT BANK

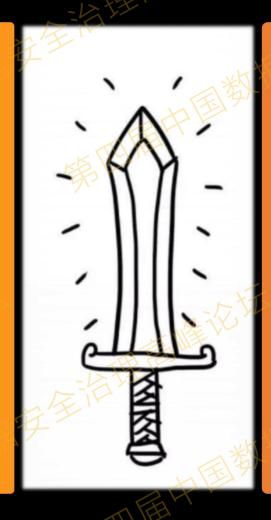






收益

- 生活融入金融生态
- 获客能力提升
- 提升用户DAU MAU
- 降低获客成本





风险

- 生态企业数据安全能力 参差不齐
- 生态企业接入后数据泄 露面增大
- 黑产通过生态企业撞库
- 数据泄露后不可逆

数据安全发展驱动力





数据成为新型生产要素

- 数据辅助决策、数据驱动业务、数据对外变现;
- 数据资源已成为国家基础战略性资源和社会生产的创新要素;

■数据安全风险增加

- 数据类型多、数据量暴增、各类数据的拥有主体多样,处理活动复杂;
- 新技术的兴起,网络趋势变得复杂,传统安全防护已经不能应对新的网络安全形势;
- 数据价值的增加,导致了数据成为重点攻击对象;

■ 个人信息意识崛起

- 网民规模及互联网使用率逐年上升,网民遭遇各类网络安全事件增多;
- 用户维权意识明显提升;
- 知情权、选择权等隐私权益的关注度提升;

■ 监管力度加大

- 数据隐私和数据安全问题频出;数据泄露事件和数据安全罚单增多;
- 国家战略层面催生饿了数据安全需求,国内外数据保护工作;



数据安全治理思路



数据安全治理规划

- 国家法律、监管条例梳理;
- •银行业务梳理、使用场景梳理,数据资产梳理,数据分类分级制定;
- 针对具体条款的遵从性建议及落地应对措施建议,遵从性建议可分为"必须 遵守项、可选项、不适用项",应对措施建议可分为技术手段和管理手段, 并制定数据安全能力演进路线;
- 制定数据安全能力建设计划和演进路线图。

数据安全运营体系

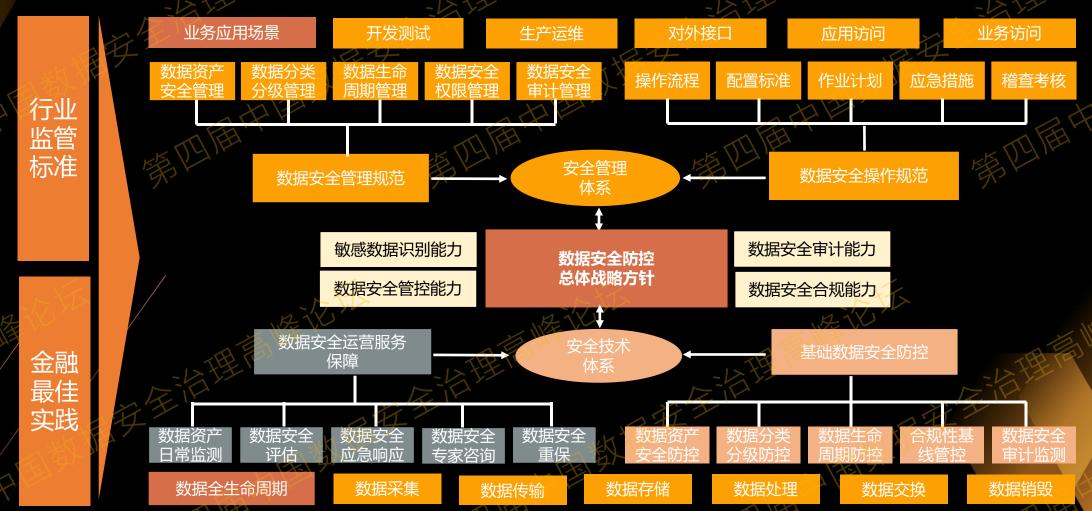
- 构建符合监管合规要求、贴合业务场景的数据安全管控策略;
- 管控策略匹配管理制度、组织架构、流程机制和技术基础设施;
- 信息安全新技术的探索和应用;
- 数据安全KPI考核制度建设;
- 数据安全人才的培养。

数据安全技术体系

- 各业务开发、测试、生产、运维场景中的数据安全能力建设;
- 数据生命周期中,各个阶段的数据安全能力建设;
- 保护个人敏感数据的数据安全能力建设;
- 办公区域等物理场所数据安全能力建设;
- 敏感数据全网流向监测能力建设。

数据安全治理规划





数据安全治理实现



							-12-12					-1> \\			
	安全运营	数据资源安全运营		数据安全策略运营		_ 11	数据安全事件运营			数据安		安全风险	安全风险运营		
		数据资源 稽核	数据地图	标准规范库	安全策略 稽核	・・・ 安全 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	事件 安全事 则 处置	件 }	安全事件 响应	数据流转 视图		风险可视化	风险分析	风险感知	
7	数据安全管控能力			策略管理			风险事件监测					风险分析		运行监控	
		数据特征管理 分类分级 策略		数据加密 策略	策略		业务区域		数据生命周期		接口访问分析		Ш	组件运行状态 监测	数
		数据资源清单	数据资源 发现策略	数据水印 策略		访问数据 内容	、 异常访问 行为		数据采集 过程监测	数据处理过程监测		URL访问分析	-11	安全能力监测	据安
		数据资源备案	製品 製品 製品 製品 製品 製品 製品 製品 製品 製品	数据防护策略		敦感数据 访问	越权访问		数据传输过程监测	数据交换过程监测	18	ין כלנייונאים	-#-	X THO/JIII/N	全
		分类分级管理		任务管理	- H	接口备案	高频访问	╠	数据存储数据销毁	业务用数分		析	平台日志检索	管	
		数据资源统计	-		i i	访问频率	超量访问		过程监测	监测	-18	开发测试分析		安全能力测试	和
	监控分析 引擎	业务引擎										 分析模型			运 营
		流量解析 引擎	风险监控 引擎	规则解析 任务调度 引擎 引擎		数据可视化引 擎	比引 安全流程 引擎		数据流转分析模型		敏感	敏感数据风险分析模型		网络安全 风险分析模型	
15		日志解析	生命周期 资产备案 核查引擎 核查引擎		能力调度 风险可视(引擎 鄭		比引 能力测试 引擎		接口访问数据 风险分析模型		数据生命周期 风险分析模型		URL风险分析模型		
2/11/3	接口层	-/							文件			<u> </u>	=====================================		
4	基础安全能力	2/3/	网络安全				数据	安全	2/5		- 11		终端安全	E	· · · · · · · · · · · · · · · · · · ·
		防火墙	WAF	主机WAF	数	据库审计	传输加密	数据	运维管控	文件水印	#	身份/权限/准	X T	终端DLP	测
		入侵检测	入侵检测 防病毒		网络隔离数		数据库加密		数据库防火墙 屏幕水印		移动存储管理		邮件DLP		和防
		网络审计	防DDOS	日志分析	文化	件保险箱	文件系统加密	数	居库水印	网页水印		敏感数据监控	Ē	终端网络管理	护
		L	-105							77777	<i>Y</i> 2⊤L				

数据安全技术的探索和实践

中国光大银行 CHINA EVERBRIGHT BANK

数据生命周期中,主要安全技术的应用

数据采集	数据传输	数据存储	数据处理	数据交换	数据销毁
指纹识别深度模型 脸部识别深度模型 深度特征学习 身份识别	VPN隧道 数据加密传输 消息队列	文件系统加密 文件加密 数据库加密 存储加密 备份/恢复	机密计算 数据脱敏 联邦学习 差分隐私 K匿名	数据水印溯源 多方安全计算 数据脱敏 文件指纹 身份认证 数据审计	文件粉碎 硬盘扇区清零 磁盘消磁

专项——个人敏感数据识别

通过数据资产分类分级,识别全业务个人敏感数据





数据资产清单

数据分类分级清单

个人敏感数据和业务对应关系

一 个人敏感数据使用告警策略

个人敏感数据使用各项流程

业务人员使用数据权限

结构化数据

非结构化数据

专项——个人敏感数据保护





网络监控

解析协议TCP/UDP内容,发现疑似违反策略的网络流量,产生告警信息,并进行阻断;





URL、API接口监控

解析HTTP/SOCKET等协议,对全行URL,API中交互的个人敏感数据监控,对高频访问、超限访问、非信任客户端访问、非信任的问题,可以通过证据,对高频访问、超限访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户端访问、非信任客户编访问。





数据库监控

解析各类数据库协议,采用应用准入+数据访问行为白名单方式进行监控,对越权访问、高频访问、超限访问、非信任工具访问、非信任时间访问等行为进行告警;





业务人员访问监控

采用业务需要匹配人员权限的方式,对用数人员做最小化数据授权访问;按照需求,对不同的人员使用不同的数据及脱敏操作;对高频访问、超限访问、共享、下载等行为进行监控;





终端和邮件防护

采用身份认证、终端DLP、邮件DLP,文件保险箱,虚拟桌面,文件水印,打印水印,屏幕水印等多种手段,防止重要数据泄露





数据安全治理使用场景



开发测试

数据库开发、测试、运维、生产场景

系统运维人员 运维审批人员 数据 使用 操作审批 数据

动态脱敏 访问控制

拦截防护

语法解析

运维审计 登录准入

数据库运维脱敏

集成OA

操作申请

密码代填

报表统计

行为检索

会话统计分析

应用审计

语法解析

业务人员

数据库安全审计

应用访问

漏洞攻击策略

高危风险策略

风险告警策略

告警方式配置

协议解析

数据脱敏

数据发送

数据抽取

数据发现

数据脱敏

底账 梳理

安全

防护

数据资产分类分级

账户权限梳理

数据资产价值评估

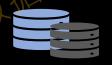
数据库脆弱性评估

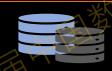
数据库威胁评估

数据 区域



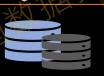
银行核心





网上银行

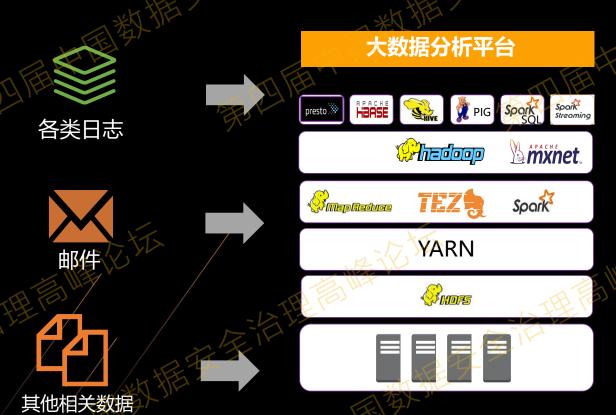




数据安全治理使用场景



数据分析和业务使用场景







数据安全治理使用场景



银行生态使用场景

多方安全计算平台

计算输出1

银行

原始数据1

存证数据1

结果存证1

计算结果1

计算输出2

结果存证2

计算结果2

行内业务

数据异常行为监测

风险行为实时告警

风险分析统计

风险趋势分析

银行生态互联DMZ

敏感信息访问监测

URL

API

URL

API



银行生态服务

餐饮



交通



商城



快递



外卖

运营商

原始数据2





存证数据2

DATA SECURITY GOVERNANCE



安全·服务·创新

THANKS

中国光大银行

୬ 地址:北京市西城区太平桥大街25号中国光大中心

电话: 95595

网址: www.cebbank.com



扫一扫,关注微信号 了解最新安全资讯