中国农业银行
AGRICULTURAL BANK OF CHINA

数据安全技术防护体系建设与展望

科技与产品管理局
2023年12月

目录

1.1.1数据安全与隐私保护-国际数据安全法发展趋势

欧盟：2018年《通用数据保护条例》（GDPR）

俄罗斯：2018年《联邦信息、信息化和信息保护法》

美国：2018年《加州消费者隐私法案》

日本：2017年《个人信息保护法》

澳大利亚：2017年《隐私保护法案》修正案

巴西：2018年8月14日颁布《通用数据保护法》

数据安全保护最早成熟于欧洲。最初萌芽于20世纪70年代：

- 1995年欧盟议会首次通过描绘隐私措施的概括指令，提出了5条基本原则；
- 2000年左右，欧盟与美国商务部基于跨境数据流动，首次提出“安全港”七原则；
- 近年，欧盟、美国、日本、澳大利亚、俄罗斯、巴西等先后出台了专项法案。其中以欧盟的《通用数据保护条例》（简称GDPR）最具备通用性。
- 随着我国推动“一带一路”等开放政策，开始引入GDPR。

1.1.2 数据安全与隐私保护-国内数据安全法立法情况

安全上升为国家战略

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。

—2018年4月，习近平总书记在全国网络安全和信息化工作会议讲话

- 成立 **中央网络安全和信息化委员会**
- 出台 **《国家网络空间战略》**

国内数据安全立法迅速推进

2018年5月，国家标准《信息安全技术 个人信息安全规范》实施；

2020年2月，金融行业标准《个人金融信息保护技术规范》发布。

2020年7月，**《数据安全法（草案）》**征求意见。

2020年9月，金融行业标准《金融数据安全 数据安全分级指南》发布。

2020年10月 《个人信息保护法（草案）》征求意见。

2018年

2020年

2017年

2017年1月，银监办发【2017】2号：中国银监会办公厅关于加强网络信息安全与客户信息保护有关事项的通知。

2019年

2017年6月，**《网络安全法》**生效实施。（涉及个人信息；重要数据；跨境传输）

2019年5月，网信办**《数据安全管理办法》**（征求意见稿）发布。

2021年

2021年6月，**《数据安全管理法》**由第十三届全国人大常委会第二十九次会议通过，自9月1日起实施。

1.1.3 数据安全与隐私保护-国内数据安全相关要求

网络安全法

- 将数据安全纳入网络安全范畴。
- 基于网络安全保障的目的为个人信息保护与数据安全的部分重要、核心制度奠定了基础。
- 提出了数据的分类分级，重要数据的保护要求。
- 要求个人数据采集的用户确认、数据采集的频率、数据来源的合法性。

个人信息保护法

- 明确个人信息采集、使用和存储的一般规则和敏感信息处理规则。
- 个人信息跨境管理要求。
- 界定了个人和机构在个人信息搜集和使用过程中的权利与义务。

数据安全法

- 数据安全的基础性法律。
- 明确了数据保护的范围。
- 要求数据开发利用活动应建立在遵循国家相关立法的基础上开展相关工作。
- 明确了数据管理者和运营者的数据保护责任，指明了数据保护的工作方向。


全国人民代表大会
The National People's Congress of the People's Republic of China
首页 | 宪法 | 人大机构 | 委员长 | 代表大会会议 | 常委会会议 | 委员长会议 | 权威发布 | 立法 | 监督 | 代表
对外交往 | 选举任免 | 法律研究 | 理论 | 机关工作 | 地方人大 | 图片 | 视频 | 直播 | 专题 | 资料库 | 国旗 | 国歌 | 国徽
当前位置： 首页
中华人民共和国主席令
来源： 中国人大网 浏览字号： 大 中 小 2021年06月10日 17:42:04
中华人民共和国主席令
第八十四号
《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，现予公布，自2021年9月1日起施行。
中华人民共和国主席 习近平
2021年6月10日

1.2.1 数据安全事件及发展趋势——数据资产受到多方高度重视和觊觎

- 随着数字经济快速发展，数据资产已成为现代经济社会的**重要生产要素**，被视为新时代的“石油”，其价值越来越大，使用面越来越广，与此同时面临的安全风险也越来越高，不法分子窃取敏感信息的事件频发。

万豪国际酒店5亿条用户数据泄露

- 2018年11月，万豪酒店宣布，受2014年发生的安全漏洞影响，有多达**5亿**客人的数据遭到泄露，其中涉及700万名英国居民。

美国第七大商业银行1亿客户信息被盗

- 2019年7月29日，美国第七大商业银行第一资本宣布，大约**1.06亿**客户的个人信息遭黑客窃取。消息宣布后，公司**市值蒸发近27亿美金**。

圆通速递40万条个人信息泄露

- 2020年7月，圆通速递内部员工与外部不法分子勾结，利用**第三方非法工具窃取**运单信息，导致**40万条**个人信息泄露。

英国数据分析公司30TB数据泄露

- 2020年10月，英国数据分析公司Polecat遭受黑客网络攻击，近**30TB敏感数据被盗**，涉及用户名密码、大量行业内部数据。

1.2.2 数据安全事件及发展趋势——网络黑产趋利性攻击成为新常态

- 随着数字化和互联网化的加深，不法分子也在加快向线上化转移，并已发展形成**专业化、规模化、产业化**的网络黑灰产业。同时黑客组织的趋利性攻击越来越明显，**银行机构已成为黑灰产攻击重点。**

◆ **60%以上来自移动设备。2018年发现移动互联网恶意程序283万余个，同比增长11.7%。**

暗扣话费
恶意移动广告
手机应用分发
… …

→

木马刷量
勒索病毒
“薅羊毛”
… …

移动化

◆ **精准掌握人员身份**
- ◆ 作案针对性强：如针对租房者以中介的身份诈骗，针对企业财务人员以税务或企业高管身份诈骗。
- ◆ 个人信息倒卖猖狂：**百元四大件**（姓名、账号、密码、电话），**千元买全套**（认证介质、住址、亲友关系等）

精准化

产业化

工具开发	信息采集	诈骗实施	分赃销赃
钓鱼编辑	钓鱼零售商	团队经理	财务会计
木马开发	域名贩子	业务员	ATM马仔
盗库黑客	个人信息贩子	话术指导	分赃中间人
	银行卡贩子	短信群发代理	
	电话卡贩子		
	身份证贩子		

技术化

➢ 早期黑产通过**“社攻”、伪造磁条卡等手段**进行盗转盗刷。

➢ 每年银行卡盗刷投诉量就达**7千余**次，经济损失超**1.8亿**元。

→

➢ 二代K宝等技术提升了凭证伪造门槛后，黑产通过**短信嗅探**技术进行资金盗窃。

➢ 2020年央视曝光了一起短信嗅探盗窃案，受害人**未做任何操作银行卡被刷走5万。**

→

➢ 黑产利用**AI技术**伪造来绕过生物认证。

➢ 2020年央视报道，利用AI技术将“**照片活化**”，生成动态视频**骗过人脸识别系统。**

1.2.3 数据安全事件及发展趋势——监管重视程度高，执法越发严格

- 由于网络安全领域涉及的面较广，渗透到信息科技建设的方方面面，同时，相关的技术内容较为复杂。面对新的形势，监管部门也加强监管工作力度，**执法越发严格。**

行政处罚

- GDPR处罚上限：两千万欧元或上一财政年度全球营业总额4%（二者取其高）。以农行营业额估算，上限可达251亿元。
- 《网络安全法》第六十四条，最高行政处罚金额是违法所得的十倍罚款，严重情形下吊销营业执照。

- 2019年7月，美国联邦贸易委员会（FTC）对Facebook罚款50亿美元。
- 英国ICO对英航罚款约2亿欧元。
- 2018年，人民银行针对金融机构违法查询客户数据，开出716万元的处罚。
- 2019年，在公安部开展的APP违法违规采集个人信息集中整治中，包括光大银行在内的100款App被要求下架整改。

刑事处罚

- 《刑法》“侵犯公民个人信息罪”明确：非法获取、出售或者提供公民个人征信信息、财产信息50条以上的，属“情节严重”范畴，处三年以下有期徒刑或者拘役。

- 某大型商业银行西夏支行某员工非法查询并出售储户信息200条，判处有期徒刑三年。

1.3.1 数据泄露事件对金融企业的危害

- 随着数据价值的提高，黑客越来越多的攻击目标转向企业内部存留的用户、员工数据，当企业发生数据泄露时，损失的不仅仅是经济利益，还面临着声誉、资金、合规、网络攻击等风险。

声誉风险

- 客户流失
- 信任度下降
- 公众形象严重受损

资金风险

- 数据财产损失
- 股价下跌
- 客户资金损失导致大额赔偿

合规风险

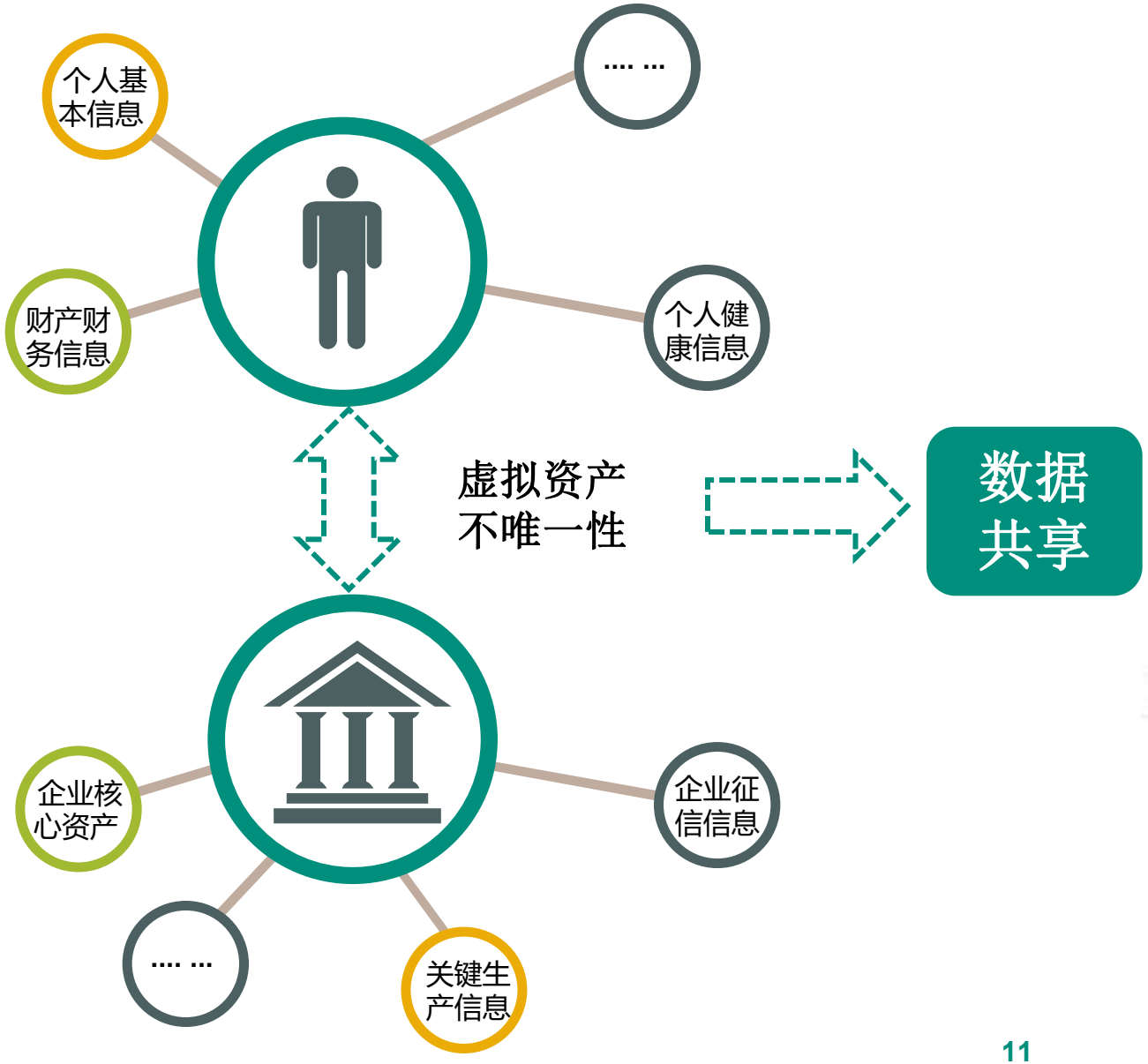
- 监管处罚
- 客户起诉
- 内部审计

网络攻击风险

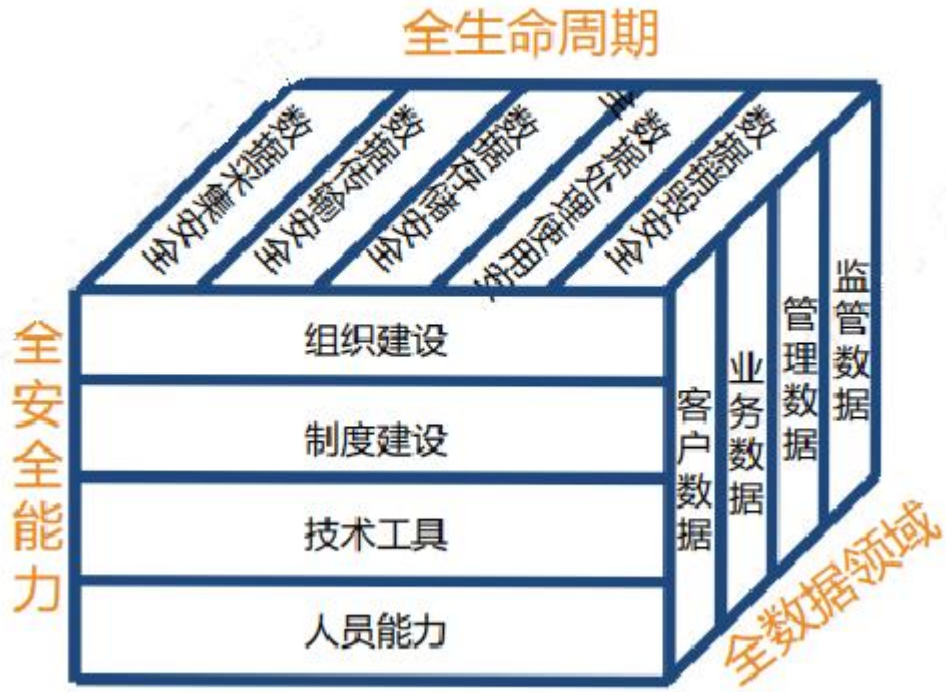
- 引发黑客攻击
- 内部管理疏忽
- 存在安全漏洞

目录

2.1 数据资产的特点



- 数据安全管理与其说是管安全，其本质是保证数据访问过程合理合规，即从全数据领域，按照数据全生命周期，建立管理组织、制度、技术工具以及人员能力，以全面构建数据安全管理能力。



2.2.1 数据安全管理的难点

- 当企业采集了用户信息，一般都作为共享资产，而数据资产的虚拟性特征，使得同一数据应用于不同场景，在企业内部难以确定归属，随着数据增多，**管理责任极难界定。**
- 同一数据资产在多企业中同时存在，一旦泄露，很难界定责任，治理难度大。

- 数据呈现一种生命周期形态，涉及数据产生、传输、存储、使用、共享、交换、销毁等环节，每个环节都面临安全风险。
- 随着数据复制和拷贝过程中数据量不断增长，**风险暴露面越发增大，导致管理成本高，投入较大。**

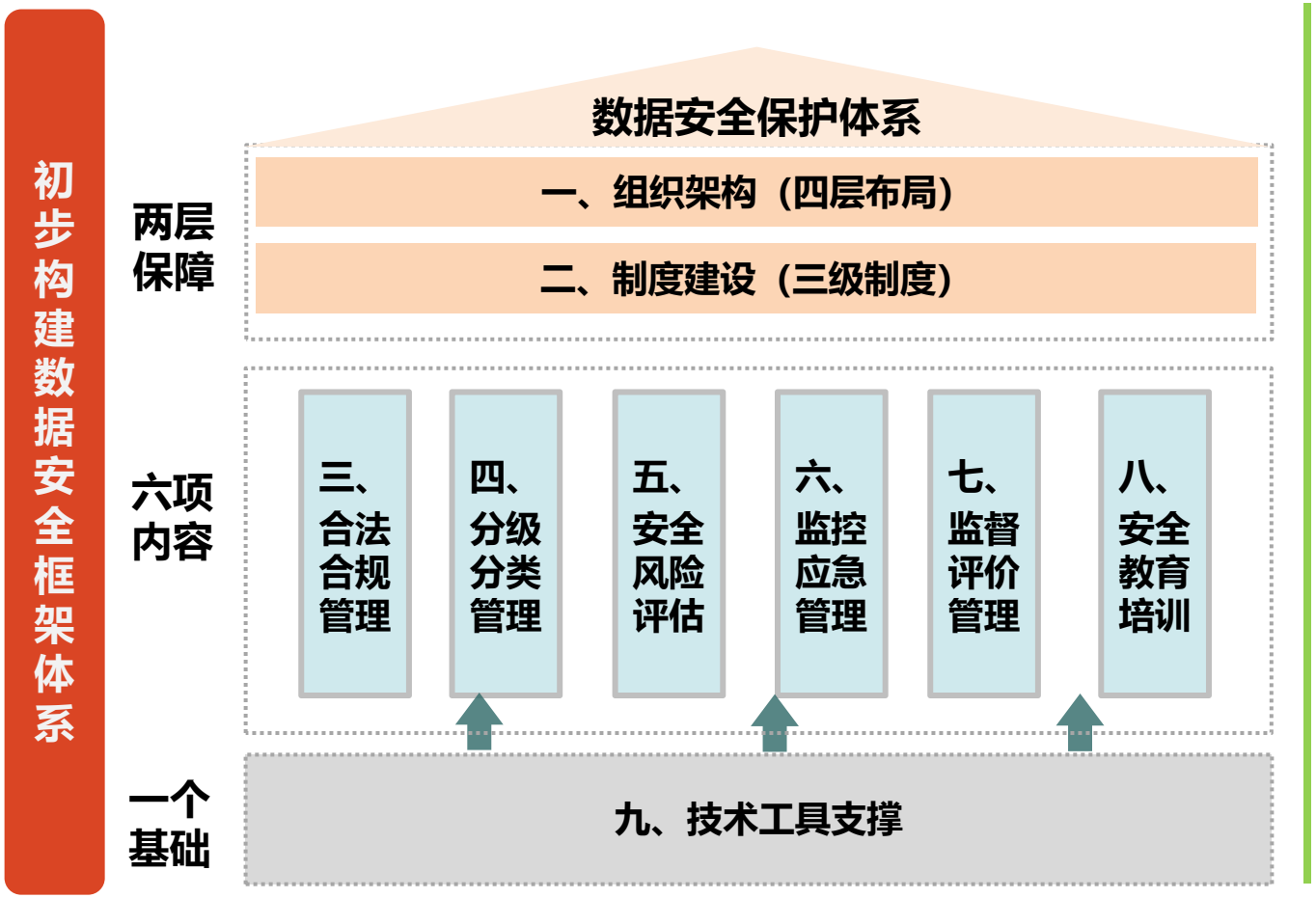
- 数据资产存在形式：数据库、文件、流量等。
- 数据在共享和传递过程中，数据资产的形式不断变化，使用场景多样化，**导致数据所面临的风险面也越来越多**，需要采取的保护措施和权限管理就更困难。

- 一些数据如个人生物信息、客户身份证件号等能唯一标识用户身份的信息具有唯一性，一旦发生泄露，**无法采取补偿措施，给企业造成难以挽回的损失。**

目录

3.1 数据安全防护体系——制度和文化系统建设

- 2020年，着力健全数据安全管理体系，在可比同业中率先发布数据安全管理办法，明确了数据安全管理责任和管理要求。数据分级分类、数据活动审核等工作取得突破，客户信息保护的精准管理、深入落地方面得到改善。



- **人人有责，齐抓共管，提升员工数据安全意识和能力。**

初步建立数据安全法规跟踪机制，按季发布监测简报；并举办专题讲座，组织条线培训；发布《网络与数据安全白皮书》，建立系统化的数据安全知识库。

- **密切沟通，强化落实，压实各级责任。**

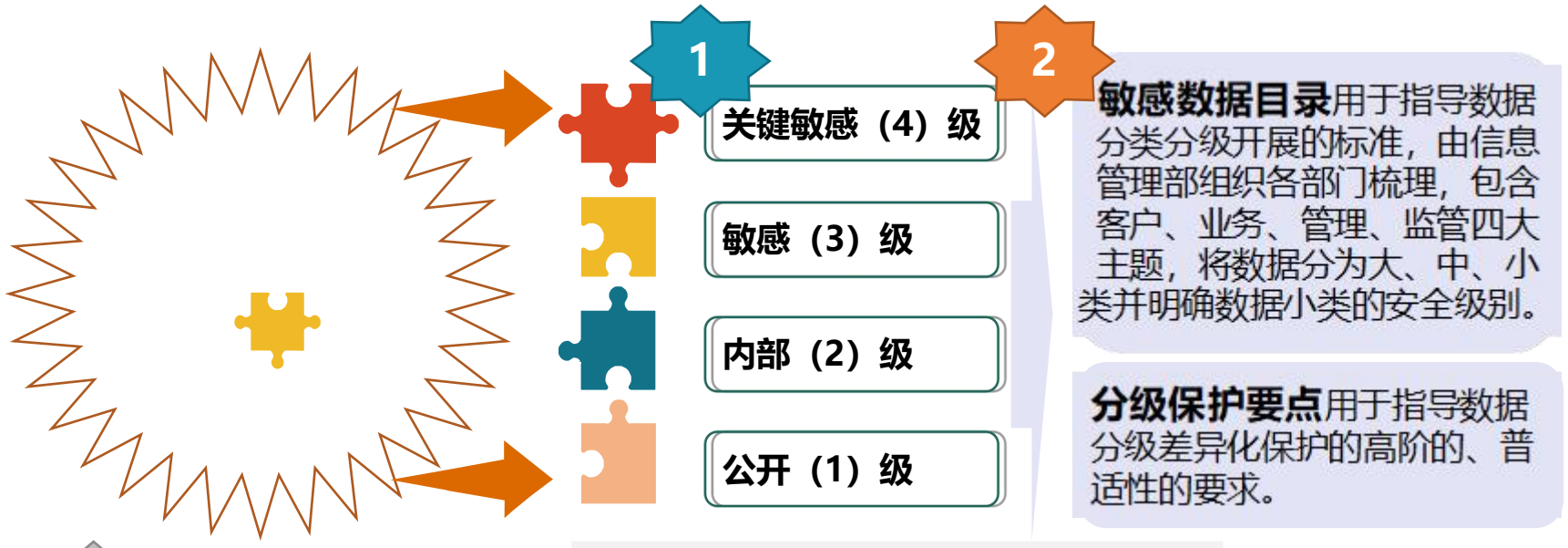
纵向上，各一级分行确定数据安全牵头部门并指定具体负责人员；横向上，总行各部门确定数据安全牵头处室，将安全职责融入各业务部门。

- **体制机制建设，客户信息保护的精准落地。**

制定了**1部办法、2部规范文档**，包括《数据安全管理办法》、《客户数据分级规范》、《客户敏感数据目录》等，修订了客户信息保护管理办法及细则；完成第二版《隐私政策》更新发布。

3.2 数据安全防护体系——数据目录和资产梳理

- 厘清数据资产量，将数据资产划分为不同的数据类别，进而确定其安全级别并采取差异化保护措施。数据类别共分为四个层次，分别是主题、大类、中类、小类。按照数据安全级别的不同，并结合收集、处理使用、存储、传输、删除销毁等数据活动或阶段，制定和发布客户数据分级保护要点。旨在通过对数据资产敏感程度和内在价值的划分，开展数据分级分类并实施差异化保护，实现数据安全精准化管理。



敏感数据保护要点共计61条

3

系统敏感数据清单

根据敏感数据目录，明确系统、业务中数据项的分级分类，形成敏感数据清单。

敏感数据保护措施

根据数据分级分类，结合场景，提出敏感数据保护的具体措施。

3.3 数据安全防护体系——数据生命周期安全管理

- 加强数据安全全生命周期管控，从数据收集、存储、使用和传输至数据销毁，有效识别数据流转过程的安全风险，在每个环节使用管理和技术手段结合，有效防范数据泄露风险。

全生命周期：数据收集 → 数据传输 → 数据存储 → 数据使用 → 数据清除

◆ 数据存储是将数据进行持久保存的过程，包括磁盘、磁带、云存储服务、网络存储设备等载体存储数据。

泄露风险　篡改风险　丢失风险　不可用风险

需加密	高敏等级	姓名、身份证号码、护照号码、个人电话、身份鉴别信息、SPII
无需加密	敏感等级	其他的个人数据字段

数据存储风险

◆ 数据使用是在提供金融产品和服务、开展经营管理活动中，进行数据的访问、导出、加工、展示、开发测试、汇聚融合、公开披露、数据转让、委托处理、数据共享等活动。

非授权访问　窃取风险

1-数据使用需求 → 2-属主审批授权 → 3-数据安全传输 → 4-使用后清除

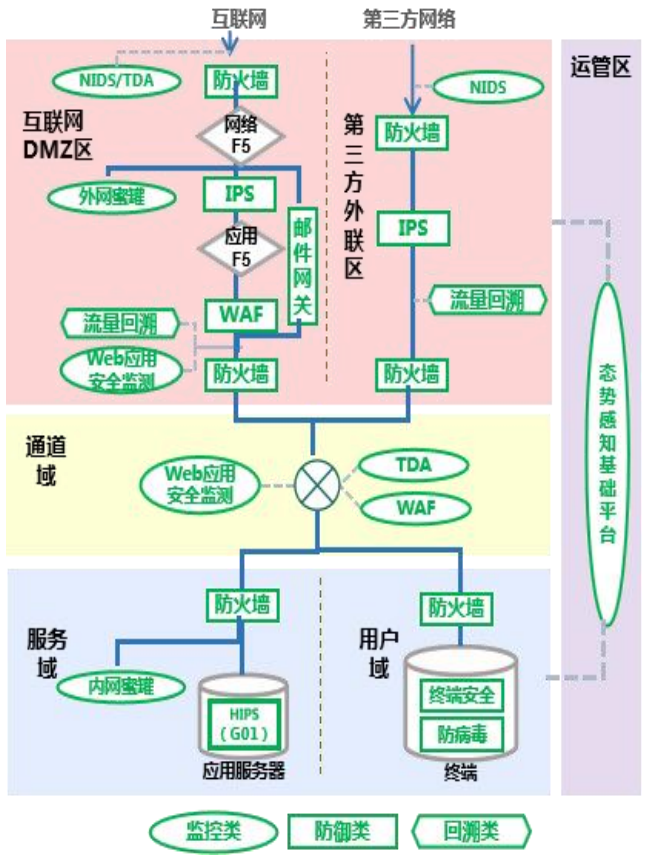
周期	处置策略
临时方案	人工审阅并监控相关操作日志
短期方案	系统自动化监控，但不阻断高危操作，只报告
长期方案	系统自动化监控及阻断高危操作

数据应用（传输和使用）风险

3.4 数据安全防护体系——安全技术防护体系

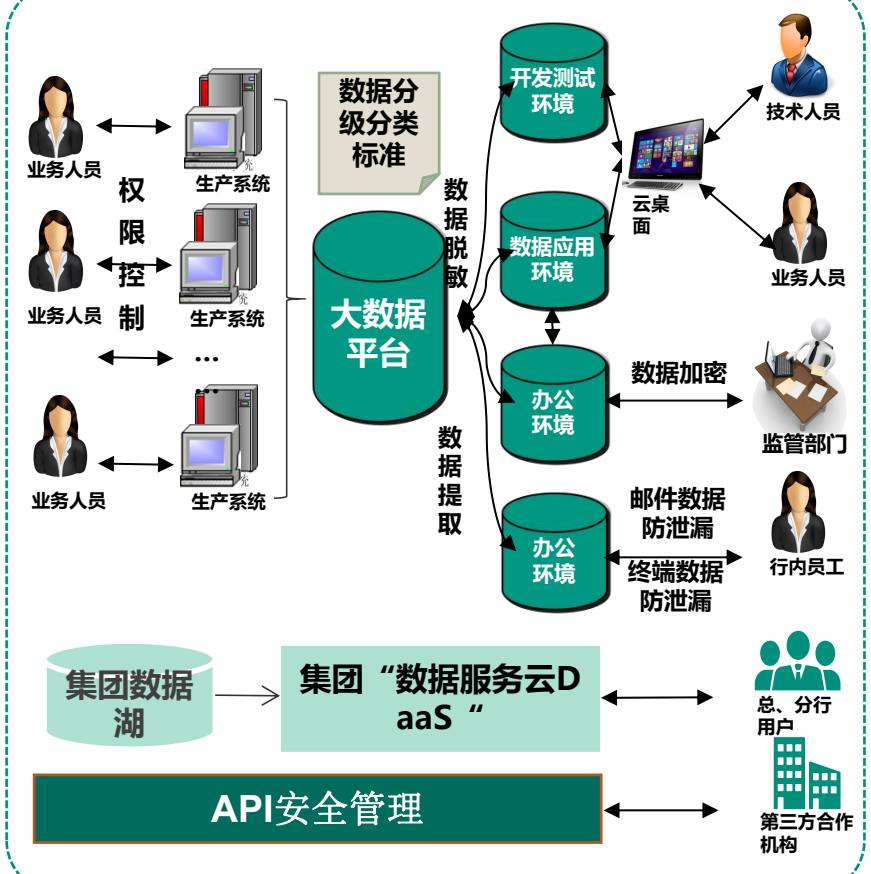
- 通过夯实基础防护体系，完善数据治理体系，强化数据安全机制，通过终端数据防泄漏、邮件数据防泄漏、数据提取等数据安全服务手段，保证安全合规的数据共享。

安全基础防护体系



◆构建了“三横一纵”防护体系，在2019年HW演习中得到了充分检验。2020年，在此基础上，引入**“蜜罐”监测工具**，填补了防御空白，推广**公安部G01主机防护工具**和**终端数据防泄漏DLP工具**，健全防护体系覆盖度，并对**安全设备进行扩容**，进一步夯实现有技术体系。

使用场景安全防护



◆**监管数据报送**：对于需要批量进行数据报送的监管需求，通过数据平台进行自动化提取之后，按照监管要求，采用专线或者专人报送的方式，确保传输过程安全。

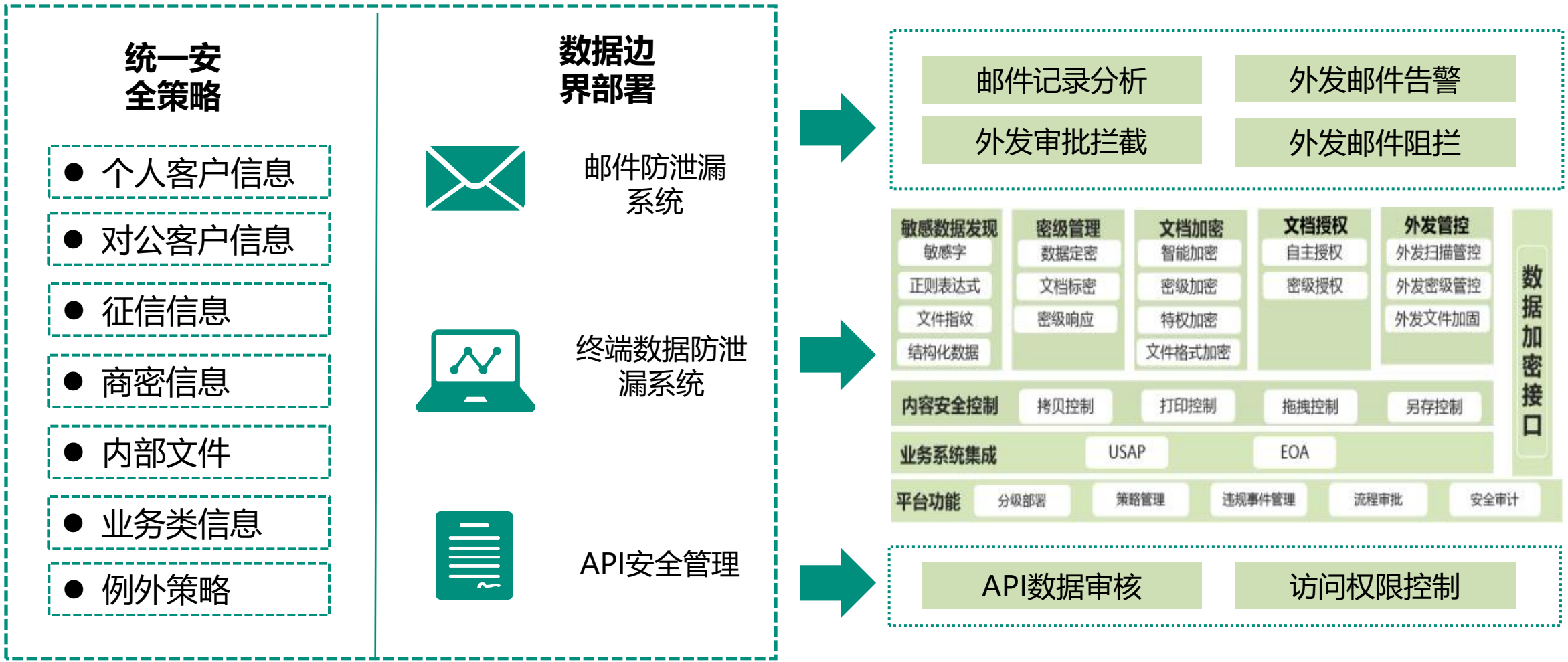
◆**业务部门数据应用**：对于内部业务要求，需要将数据进行下载并在本地设备和终端上进行应用的场景。一是全面推广了终端安全EDR工具，对设备硬件进行防控，确保数据不会被违规拷贝和传输出去；二是推广终端防泄漏DLP工具，对敏感性数据进行自动识别，并分级分类进行加密等安全管控。

◆**分支机构数据应用**：建立专门的集团数据湖，采用DAAS数据云架构支持分行和子公司数据应用。分支机构在云端查询和分析数据，数据不可下载和传递，以避免泄露风险。

◆**API数据安全**：对于通过应用接口API进行数据交互的第三方合作机构。一是根据业务场景，开展API审批，逐字段进行敏感性数据审核；二是基于API，建立了数据查询访问限制，例如单笔条数限制等。

3.5 数据安全防护体系——资产加密和数据防泄漏

- 统一数据安全策略，牢守数据外发边界。通过部署邮件防泄漏、终端数据防泄漏系统等技术手段，防止敏感信息外泄，保护数据资产信息。

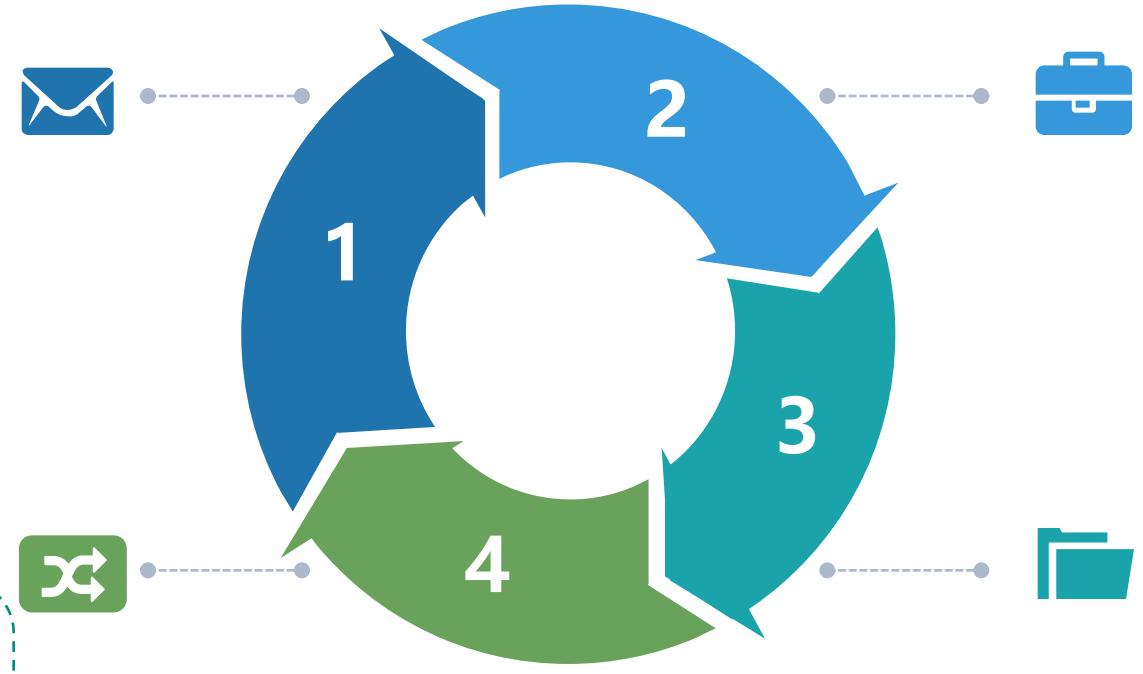


3.6 数据安全防护体系——泄露资产监测、溯源和应急

- 建立客户信息泄露监测机制，在数据流转过程中实施资产监测，发现可疑资产后及时进行数据验真，开展应急处置，实现数据资产安全风险管控，有效控制数据泄露风险。目前，按照该处置流程，已处理**15起**疑似信息泄露事件，未造成影响。

样本采集

- 疑似数据样本采集，主要来源于厂商收集、监管通报等。



数据验真

- 以部分样本数据字段为关键字，在系统中提取相关数据进行比对，以验证数据的真实性。

应急处置

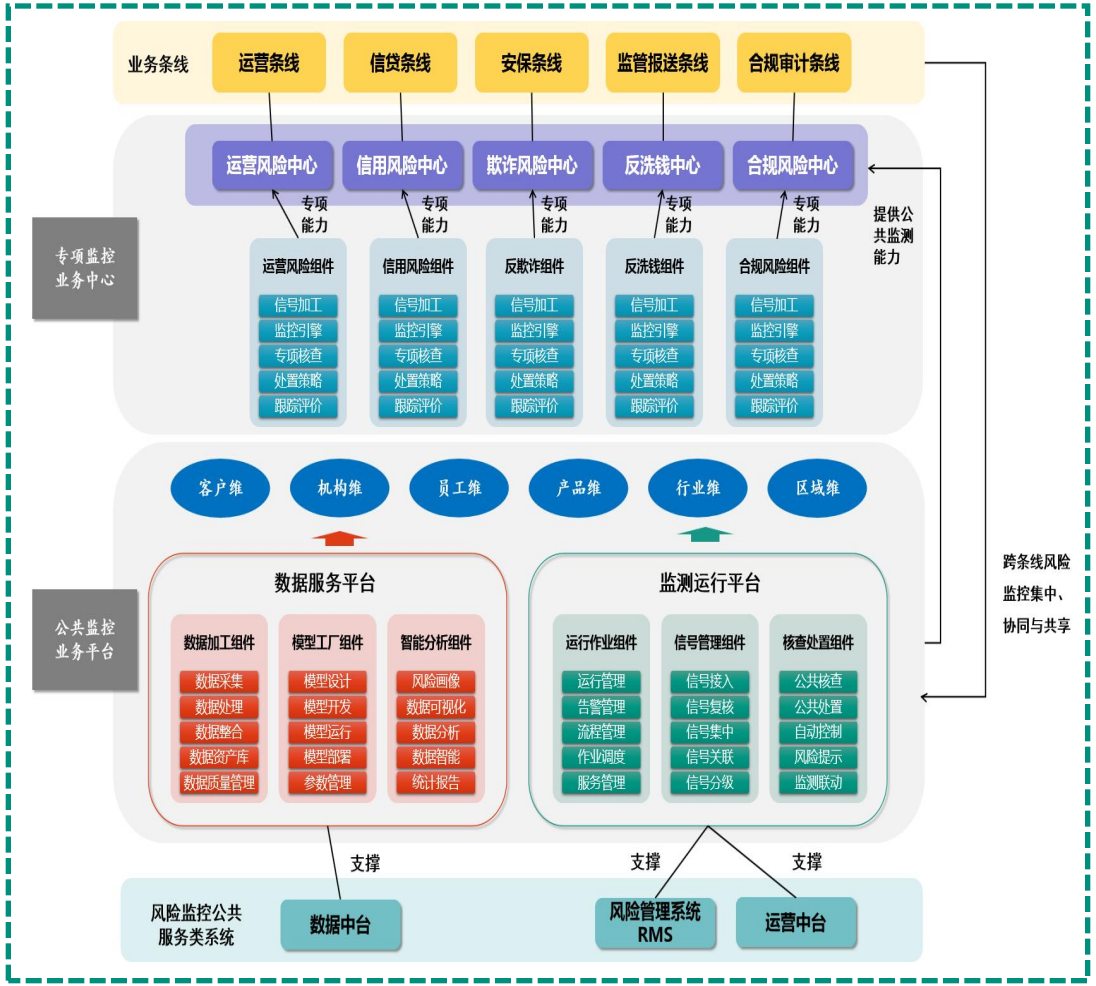
- 对于真实的数据泄露事件进行查漏补缺。
- 对于未造成真实泄露的情况，进行舆论发声，避免造成不必要的舆论风险。

渠道溯源

- 对疑似真实客户数据逐个渠道确认溯源分析，包括用户日志、系统日志、监控日志等。

3.7 数据安全防护体系——数据应用监控和主动防御

- **推动风控系统的整合提升，建立线上、线下一体化的风控体系**，打造数据整合互通、模型智能高效、监测手段多样、风险分类管控、场景全面覆盖的风险防控新架构。



典型案例

- **反洗钱典型案例：**洗钱犯罪手段多样，变化频繁，本质都是通过隐匿资金流转关系，掩饰、隐瞒犯罪所得及收益的来源和性质。通过大额取现或者将大额赃款在多个账户间进行频繁划转；为避免直接转账留下痕迹，将转账拆分为先取现后存款，人为割裂交易链条，利用银行支付结算业务采取多种手段实施洗钱犯罪。
- **反欺诈典型案例：**
  - 开户行为异常，结伴陪同人员全程代答
  - 通过“伪基站”发送木马病毒短信，盗刷事主银行卡资金
  - 老年人集体申请办理借记卡或激活养老助残卡金融功能
  - 信用卡逾期冻结电信诈骗
  - 假冒银行操作失误，利用短信二维码电信诈骗
  - 假冒公安机关电信诈骗
  - ”假信托“电信诈骗
  - ”假冒有权机关“电信诈骗
- **系统防护效果：**
  - 实现用户活动和相关实体信息相连，并定义合法和正常行为，进行多维度上相互比对分析，将异常用户（失陷账号）和用户异常（非法行为）检测出来，从而达到检测业务欺诈、敏感数据泄露、内部恶意用户、有针对性攻击等高级威胁的目的。

目录

4.1 效果

- 按照敏感数据泄露事件应急处置流程，已处理**15起**疑似信息泄露事件，涉及客户数据2万余条，均未造成影响。
- 终端数据防泄漏系统情况：
  - 形成涉及个人敏感信息、对公客户敏感信息、征信敏感信息和商业秘密四类39个策略攻击88条监测规则。
  - 实现了用户自查扫描及离线扫描功能。
  - 启动6个总行处室及3家试点分行的实施，推广客户端100余台。

金科创新社
Fintech Innovation in China

数字金融创新 知识服务平台

关注公众号

查看更多案例

添加金科小助手

网址：http://www.fintechinchina.com/