

浅议商业银行网络安全与数据治理

张海岗

中国农业银行审计局西安分局, 中国·陕西 西安 710002

【摘要】近年来, 信息技术发展迅速, 经济形势愈发复杂, 尤其是新冠疫情爆发后, 金融安全保障的难度加大, 商业银行作为助力经济发展的重要推动力之一, 在网络安全与数据治理方面肩负着重要和不可缺少的使命, 面对新形势、新挑战, 提升商业银行网络安全与治理能力意义重大。

【关键词】商业银行; 网络安全; 数据治理

Discussion on Commercial Bank Network Security and Data Governance

Zhang Haigang

Xi'an Branch of the Agricultural Bureau of Agricultural Bank of China, Xi'an, Shaanxi, China 710002

[Abstract] In recent years, the development of information technology has developed rapidly, and the economic situation has become increasingly complicated. Especially after the outbreak of the new crown epidemic, the difficulty of financial security guarantee has increased. As one of the important driving forces for economic development, commercial banks It shoulders important and indispensable missions. In the face of new situations and new challenges, it is of great significance to enhance the network security and governance capabilities of commercial banks.

[Keywords] commercial banks; network security; data governance

1 商业银行数字化发展趋势

1.1 金融服务数字化是大趋势

商业银行数字化发展是时代赋予的重要选项。首先, 在过去的很多年里, 不管是互联网的发展变化还是时代的不断推进, 消费者消费的习惯和爱好都已经被深刻改变和调整, 绝大多数的消费者已经在潜移默化中慢慢适应了当前生活中的数字化行为, 比如线上使用移动互联网搜索信息以及互动和分享等, 就像当前数字化、信息化的生活方式一样, 消费者可以通过在线服务获得一些日常生活如外卖、购物等的便捷化, 也可以通过在线服务获得更加优质、快捷、有保障的金融服务, 如理财、贷款、保险等。其次, 一些拥有先进技术水平的金融类的科技公司加入互联网数字化大潮, 给予了传统的银行带来无形的竞争压力, 无论是在快速支付、外汇办理、理财服务等较为细分的业务上, 还是在一些传统的服务上面都远超之前的商业模式。再者, 最近几年的新冠疫情的影响, 社会群体的相对疏离更是使商业银行的数字化进程被加速了, 根据一份调研数据的结果显示, 百分之九十以上的商业银行在疫情爆发当年就已加快数字化的速度, 百分之之的银行则是以四倍速向前, 大大缩短了数字化发展的原本进展速度。

1.2 服务: 数字化转型的关键变量

虽然数字化转型及发展是当今时代进步的大趋势, 但是在现实之中, 数字化的转型无论是探索还是实践方面都还是重重困难的, 极其不易。在数字化的发展及其转型的过程之中, 一个重要的认知误区是: 技术越厉害, 转型越容易成功。究其根本, 商业银行的客户最本质上注重的还是高质量的优质服务, 也即是在商业银行所能提供的数字化的服务能够最大程度上满足客户的需求、达到客户的满意之后, 才能够算是真正意义上的实现了数字化的转型。例如, 当前许多的银行都研发的有各自银行的APP, 在软件之内又设置了许多线上的理财产

品, 对于熟悉互联网操作的人群来说, 安装软件和开通银行账户不管是在成本上还是在难度上几乎可以忽略不计的。但是当客户需要更加合适、准确的、符合自身心意的理财产品时, 如果商业银行的数字化能力较强, 能够精准推介好的理财产品, 控制风险, 就能够获得很大的客流量, 并且留住客户。这些能力的重要程度, 会超过前面技术的作用。说到底, 技术是为“服务”而服务, 也从本质上阐释了“数字化”的意义, 只有真正能够让数据运转和流动起来, 在最大程度上辅助客户作出好的决策, 同时又能辅助商业银行开发和拓展自己的内部业务, 让商业银行系统内部的数据真正意义上“活”起来去实现驱动业务的目的, 才是商业银行能够实现数字化转型的本质。

2 商业银行网络安全管理

2.1 持续强化和完善基础安全建设

建立完善覆盖系统涉及到数据信息采集传输、存储、使用、备份等管理内容与数据故障应急恢复、清除丢失数据记录等管理运行环节, 较为全面系统的终端信息安全及风险控制系统架构及信息安全等级保护和决策执行机制, 制定与实施系统终端数据信息的安全风险分级管理及安全保护和管理执行策略, 推进系统终端数据信息防入侵泄漏及预警技术(DLP)等信息安全认证体系项目的标准化建设规范及验证工程, 实现对网络桌面终端信息系统中安全防范信息平台的统一全方位监控集中维护及统一信息安全风险实时管控机制; 对所有的移动互联通讯终端设备系统和全部的移动和互联网APP应用均实施硬件设备安全的升级与加固、对各类涉密移动存储数据介质系统进行信息全面的加密和检测管控、加密信息的集中的传输监测管控、对各类涉密的文件信息进行加密, 集中的信息传输检测管控和信息安全数据存储以及检测管控, 同时集中监测管理监控和过滤。在云网络安全建设方面, 借鉴国内同业思路, 积极探索建设云安全预警监测防御系统, 从云防护、检测、阻断等三个安全层面来构建起多

安全维度、主动型云智能网络的安全与防御体系。

2.2 不断升级优化核心系统

全面更换银行核心业务系统与全面加强商业银行风险管理、资产与负债动态管理、管理会计基础等商业银行更为深层具体的信息化管理及应用需求结合起来。基于今后发展趋势的传统信贷产品科技化创新、集中授信资产规模化运营、移动化科技金融平台搭建等技术,按照未来金融发展需求方向发展提供更为稳定强大、稳定持久的创新业务功能支撑与业务支撑,客户金融化理财的服务产品功能体验感提升和互联网金融风险分析预警、风险防控、风险处理等能力建设,通过系统灵活而便捷高效的新产品模块化开发组合技术设计架构体系和核心软件高度灵活可定制参数化技术设计与配置,确保持续并有效快速的缩短传统金融机构的新业务产品技术架构研发的工作时间周期,提升新一代金融机构业务新架构产品核心技术架构的金融科技能力优势;能够实现很大限度简化金融服务整个智能化系统智能化研发设计操作的管理和流程环节,设计与集成应用系统界面,强化整个金融系统的智能化系统自动与交互与控制,提高传统金融单笔业务信息系统智能化应用处理系统开发应用效率,快速与全面的满足当前金融业与日新月异的发展下的金融多样化的金融产品与持续快速发展转型升级金融服务与金融科技的应用需求。将业务流程要求直接的注入于系统日常操作活动之中,对各项交易数据合法性、准确性逐项进行跟踪检查审核和签章确认,实现对前台业务日常操作控制与前台会计账户核算操作的控制相对完整独立,以全面保障对客户账户资金安全的高安全性,提升系统操作软件的安全易用性,强化了信息系统风险控制。介入到新安全系统整个开发测试流程建设中,在安全系统的正式应用上线或推广运行前全面开展技术合规性全面审查,重点在审查新应用系统设计中涉及各类网络安全威胁的信息泄露与网络传输安全存在的重大风险问题是否及时得到和准确地识别、防范以及各种应对信息安全风险因素的相关控制的措施采取是否正确适当可靠和完整有效。将全面重点加强人民银行对于与我国银行信息、网络管理和系统安全及防范体系相关合规内容相关的内控管理与新制度的出台前的主要业务合规性内容进行审查,从金融机构主要的岗位机构功能设置、人员结构能力配备、授权职责使用权力和权限业务操作审批、沟通交流协作交流与网络信息传输合作、审核和评估风险和内部合规性管理检查及监督工作等各方面内容逐一一对金融机构银行业信息网络架构与金融安全防控网络规划及信息安全的防控相关工作规范要求提出的详细审查规范要求,特别应注意要将所有负责和管理可疑客户信息平台安全的业务相关业务岗位负责人都应视为属于其安全重要责任核心岗位,提出管理内容要求不应涉密相容严格实行各岗位权限职能分离、定期考核调整以及轮岗交流制度执行等相关具体内部管理制度细节要求,确保能按新规范制度流程要求严格规范有效的落实到各项信息安全内部流程控制规范相关标准。

2.3 打好网络安全“保卫战”

智能实时安全攻击防御系统建立起一个互联网的实时网络安全预警反网络反欺诈攻击预警技术平台,必要时依法作为有效网络攻击活动嫌疑证据,一并集中移送公安至当地公安机关依法调查处理。进一步重点培育提升总体防御网络态势和监测分析感知到各方面情况威胁的应急整体能力,坚决按照公安部“知己知彼、百战不殆”文件部署,主动监测跟踪分析感知到潜在威胁

攻击的源头行为,与维护当前和现有重大网络应急防御和安全防范体系保持紧密有效联动,综合监测跟踪分析在国家各大重要安全层面均可有效监测分析感受到各种潜在威胁的重大网络攻击的威胁行为,自动化阻断潜在的攻击源,并能够对可穿戴监测对象进行主动与反向的实时追踪监测及溯源。提升对现有信息安全网络整体防御能力安全防御和综合防御新技术体系建设运用中的网络安全信息化技术主动性、智能性程度提升和提升网络技术一体化水平。

3 商业银行数据治理构建

3.1 数据治理相关的内部管理架构

内部管理框架的科学与否在很大程度上是决定了一个体系的成功与否,商业银行的数据治理也不例外。商业银行数据致力构建的组织管理框架是其科学高效运转的保障和关键,也是数据治理的的实际的操作和实施体系。包括商业银行数据治理的管理、分工、配合、激励以及约束等环节,主要是通过合理有效的管理架构起到约束和激励的作用,能够在让各个部门、各个环节各司其职的同时,保证数据治理的快速高效。

3.2 数据治理的制度

数据治理的制度是对商业银行数据整体起到约束的行之有效的规范,包括数据资产管理类别和监管数据管理的类别。其中,数据资产管理类别的制度主要涵盖商业银行数据相关的战略、资产策略、知识产权、内部协作机制等,通过制度的科学合理地制定对于商业银行数据整体资产情况以及其价值能够起到更加明确的认知,能够为发现与盘活资产奠定了良好的基础。数据监管类别的制度则主要是商业银行在因对监管机构的监督和检查时需要制定完备的一套制度,虽然与数据资产管理类的制度有相互交叉和重合的地方,但是其侧重点和作用都不同,它的侧重点是发挥监督和管理的作用,作用主要是为了满足监管规范性的需求。

3.3 数据治理的流程体系

商业银行的数据治理流程是商业银行在制度和治理之间发挥关键作用的特殊纽带和关键节点。就数据治理来说,其制度化是从中抽象出来的精炼的内容,是一个整体的内容,而数据治理流程则呈现出细节化、具体化的特征,需要体现出各个部分的内容。商业银行治理的数据治理通过对每一部分流程的规范和约束,让每个环节和流程都能够以一种可以感知和可以视觉化的方式表达和呈现给商业银行的管理层和执行层。在数据化治理的流程之中,具体过程是通过设定信息系统以及文件表格等,分解、优化,将数据治理过程中的权力、责任等在约束和规范、激励和推进的过程中更加具体化,从而得到充分的落实。在商业银行的数据治理过程中可以说制度是目标和手段,但管理流程确实重要的衔接点和关键点。在数据治理的流程之中,数据治理的流程化越是合规,越是精细,最终呈现的结果和效果就越接近完美,商业银行对整体的数据管控能力和掌控力度就越大。随着当前银行等金融机构数字化程度的深入,以及各种网络、数据法律法规的完善,商业银行数据治理的重要性和紧迫性也随之增加,构建好数据治理体系既成为了时代需求也成为了发展需要。

参考文献:

- [1] 金融科技背景下的银行信息安全建设思考与实践[J]. 中国金融电脑, 2017.
- [2] 银行内控合规部门加强信息与网络安全的思考[J]. 金融电子化, 2017.