

金融科技中数据安全的挑战与对策

朱建明, 杨鸿瑞

(中央财经大学信息学院, 北京 102206)

摘要: 金融科技为金融业带来机遇的同时带来了新的挑战, 金融业务数字化、网络化、智能化引发的数据爆发式增长, 对数据安全治理提出了更高的要求。因此, 在对金融科技发展现状及其金融数据安全分析的基础上, 针对金融数据特点, 提出了金融数据安全“果壳”模型: 其内部是确保数据保密性、完整性、可用性的安全目标; 外部是可能存在的数据被泄露、篡改、破坏等各种威胁; 中间是各种应对策略, 包括访问策略、防控策略、检测或感知策略等。以此模型为基础, 对金融科技中的数据安全治理提出了相关建议和对策。

关键词: 金融科技; 大数据; 数据安全; 数据治理; 安全模型

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019044

Data security challenges and countermeasures in financial technology

ZHU Jianming, YANG Hongrui

School of Information, Central University of Finance and Economics, Beijing 102206, China

Abstract: While financial technology brings opportunities to the financial industry, it also brings new challenges. With the rapid development of financial technology, the big data explosion caused by the digitalization, networking and intelligence of financial services has put forward new and greater requirements for data security governance. Based on the analysis of the status quo of financial technology development and financial data security, a financial data security “shell” model for the characteristics of financial data was proposed: the internal is the security goals of ensuring data confidentiality, integrity, and availability; the external is a variety of threats including data leaking, tampering and destroying etc; the middle is various coping strategies, including access strategies, prevention and control strategies, detection strategies, perceived strategies and etc. According to this model, relevant suggestions and countermeasures for data security governance in financial technology are proposed.

Key words: financial technology, big data, data security, data governance, security model

收稿日期: 2019-07-10; 修回日期: 2019-08-02

通信作者: 杨鸿瑞, yhrbjsy@163.com

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB1400700)

Foundation Item: The National Key R&D Program of China (No. 2017YFB1400700)

论文引用格式: 朱建明, 杨鸿瑞. 金融科技中数据安全的挑战与对策[J]. 网络与信息安全学报, 2019, 5(4): 71-79.

ZHU J M, YANG H R. Data security challenges and countermeasures in financial technology[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 71-79.

1 引言

以云计算、大数据、移动互联、人工智能、区块链等新一代信息技术与银行、证券、保险、信托、租赁等现代金融业的跨界融合为典型特征,金融科技(FinTech)发展开启了新模式,推动金融业进入了科技革命的崭新阶段,这将深刻改变金融业的生产方式、产品形式、服务模式和竞争格局,金融业正孕育着百年未有之大变局。

全球数据积累存量已达到引爆新一轮行业变革的规模和水平,全球数据正以每年40%左右的速度快速增长,2017年全球的数据总量为21.6 ZB,金融数据在其中占比很高,此外金融市场天然拥有海量标准化大数据,适合前沿科技落地生根^[1]。PwC(price waterhouse coopers consulting)通过调查认为,科技带来的便利,某种程度上放大了金融风险,并且让风险的积聚、扩散和传播更迅速,杀伤力更大,近十年来,网络安全、数据保护逐渐成为金融行业的当务之急^[2]。

2019年5月,美国Verizon公司发布《Verizon 2019年数据泄露调查报告》,对73个组织的41686起安全事件样本和2013起数据泄露样本进行了统计和分析,结果显示:68%的数据泄露事件以勒索钱财为目的;69%的网络攻击来自外部人员、34%涉及内部人员的窃取、2%涉及合作伙伴;超过一半的违规行为需要数月或更长时间才能发现^[3]。

金融业发生数据安全事件屡见不鲜。例如,2011年4月12日下午,韩国四大银行之一的韩国农协银行的计算机网络出现故障,导致客户无法提款、转账、使用信用卡和取贷款(系统故障一直持续到4月15日才恢复部分服务)。调查显示,外部人员恶意删除服务器上的文件(包括数十万客户信息)是直接原因。

针对数据安全治理问题,国内外学者或机构开展了大量研究,提出了解决方案,目前应用较普遍,且最具代表性的是IBM公司的数据治理能力成熟度模型和全生命周期管理模型^[4],IBM公司的数据治理能力成熟度模型在充分借鉴CMM(capability maturity model for software)的基础上,针对数据治理的不同领域进行详细的定义,每个领域都按照CMM的模式进行阶段划分;同时,将数据生命周期管理纳入其数据治理框架的“核心域”,对数据质量和安全隐私进行评估和管理。张明英等^[5]在解读《数据治理白皮书》国际标准研究报告后认为:数据治理以目标和准则为导向,在明确的目标下,考虑重要的关注域和促成因素,并考虑影响促成因素和关注域的流程和活动,最终形成一个从底层活动和流程到关注域和组成要素,再到战略的从底层到高层的业务逻辑。

2 金融科技现状分析

2.1 金融科技

金融科技目前尚无统一定义。2016年3月,全球金融治理的牵头机构——金融稳定理事会发布了《金融科技的描述与分析框架报告》,第一次从国际组织层面对金融科技做出了初步定义,即金融科技是指通过技术手段推动金融创新,形成对金融市场、机构及金融服务产生重大影响的业务模式、技术应用以及流程和产品^[6]。

巴塞尔银行监管委员会将金融科技分为支付结算、存贷款与资本筹集、投资管理、市场设施4类(如表1所示)^[6]。这4类业务在发展规模、市场成熟度等方面存在差异,对现有金融体系的影响程度也有所不同。

2.2 金融科技发展现状及主要问题

在实践中,“金融科技”的含义在不同背景下也存在差异。国内金融科技是以人工智

能、大数据、区块链、移动互联、云计算等新一代信息技术在金融工具、金融服务以及金融管控等领域的深入应用为显著标志。

国内工、农、中、建、交五大行以及部分大型证券、保险公司的金融科技均已覆盖表1业务领域，而且将人工智能、大数据等技术应用于风险控制、客户挖掘、决策管理等领域。

表1 金融科技业务模式分类

支付结算	存贷款与资本筹集	投资管理	市场设施
零售类支付	借贷平台	智能投顾	跨行业通用服务
移动钱包	借贷型众筹	财富管理	客户身份数字认证
点对点汇款	线上贷款平台	电子交易	多维数据归集处理
数字货币	电子商务贷款	线上证券交易	技术基础设施
批发类支付	信用评分	线上货币交易	分布式账户
跨境支付	贷款清收	—	大数据
虚拟价值交换网络	股权融资	—	云计算
	投资型众筹		

金融科技仍处于发展初期，涉及的业务模式尚不稳定，各类业务形态存在不同程度的差异，在不同国家不同金融机构之间的发展也极不均衡。因此，本文重点探讨当前国内主要金融机构在金融科技方面的发展现状。

(1) 人工智能

国内部分大型金融机构已构建企业级的集中式人工智能基础计算框架，实现统一的智能服务，支撑企业各业务领域的AI应用，提供包括人脸识别、语音语义识别、OCR、图形图像处理等诸多功能的感知引擎，以及包括数据建模、智能决策、流程支持等能力的思维引擎，在智能交易、智能客服、精准营销、智能投顾、风险防控、信用评价、智能运维等场景中得到了不同程度的应用^[7]。

人工智能在改变传统金融业务的同时，也存在一些需要关注的问题。当前人工智能还处于初级发展阶段，在处理异常情况和情感类事务时还

远不能与人脑相比拟。人工智能赖以存续的核心算法也可能存在各家金融机构同质化的问题，存在算法集中度的风险。例如，美国股市出现的几次盘中闪崩现象，事后分析师普遍认为是计算机自动交易系统互相踩踏所致，后经人为纠偏调整后快速止跌回升。除此以外，人工智能需要海量的样本数据供机器学习训练，对历史数据依赖性较高，也影响人工智能在金融业的应用场景。

(2) 大数据

银行、证券、保险具有传统的大量客户信息资源和交易数据优势，因此大数据在金融业的应用具有更大的必要性和可行性。大数据是金融科技的源泉和基石，大数据在各行各业的深入应用，为金融科技带来了更多的创新点和想象空间。国内一些金融机构已构建自主可控的大数据平台，率先采用了国际最先进的大数据技术，搭建了基于分布式数据存储的融合架构，国内部分大型商业银行已实现PB级结构化数据处理、EB级非结构化数据处理和毫秒级流计算处理能力，实现了大数据统一解决方案^[8]。在金融机构的财会管理、风险防控、审计监管、客户关系管理、市场营销等经营管理活动中发挥了重要作用。

当然，大数据带来的风险隐患也显而易见，近几年一些金融机构客户信息泄露或交易数据被篡改的情况频繁发生。大数据应用中的集中计算处理也给数据的大规模泄密提供了可能。

(3) 区块链

区块链是多种已有技术集成创新的结果，其特点包括去中心化、公开透明、安全可靠和开放共识。如今，区块链已经成为金融科技领域最热门的技术之一。在区块链的创新和应用探索中，金融是最主要的领域，现阶段主要的区块链应用探索和实践，也是围绕金融领域展开的。国内部分大型金融机构在区块链共识、性能、安全等区块链底层关键技术上进行了大量研究探索。例如，

中国工商银行成立了区块链与生物识别实验室，于 2017 年正式推出了自主可控的企业级区块链平台。国内其他大型金融机构也搭建了高安全高可用的区块链技术平台，实现了多节点共享的链式账本、高性能稳健共识机制、可动态升级的智能合约、多级公私钥加密体系、隐私保护及数据失效恢复等功能。

区块链技术也已在电商供应链金融、精准扶贫、跨境支付、可信凭证、票据贴现等领域实现应用^[9]。同时，区块链作为一项新兴技术，存在一些待解决的问题，主要表现在法律体系建设有待完善、技术研发不够成熟、金融监管滞后等^[10]。

由于上述原因，以及区块链技术在国内外缺乏大规模商业应用，其安全性、可靠性等还需要实践检验。各大金融机构也在审慎性考虑，区块链的应用方面还是处于探索试验阶段。因此，区块链在金融业的应用同其他新技术应用一样，存在不确定性风险。

（4）移动互联

随着移动互联网的兴盛和移动技术的快速发展，移动终端已成为移动支付和金融交易的重要工具。移动互联时代下，条码、NFC、5G 等技术的发展，有力推动了金融业务模式的创新。移动支付作为移动互联网领域和金融领域的革命性创新和代表应用，在促进电子商务及零售市场的发展、满足消费者多样化支付需求方面正发挥着越来越重要的作用。国内大多数金融机构推出了各自的移动金融产品，将生物识别、人工智能等技术与掌银认证功能进行结合，提升客户的操作体验。

相比于传统互联网金融，移动互联金融面临更复杂的应用场景和技术路线。在系统保护方面，移动设备硬件、软件多种多样，容易出现系统漏洞风险；在移动金融敏感信息保护方面，商家和用户在公网上传输的敏感信息易被他人窃取、滥用和非法篡改；在金融产品使用方面，不同客户

群体由于各种异常情况，在存储、传输、分享信息的过程中，容易因操作不当导致自身或利益相关方产生损失。

（5）云计算

云计算引发了软件开发部署模式的创新，是承载各类应用的关键基础设施，也是金融科技创新产品的最佳交付载体。云计算和分布式架构的核心思想是在低成本、标准化的开放硬件和开源软件的基础上，通过分布式处理架构实现系统处理能力的无限扩展。对于金融类企业而言，利用云计算技术的核心诉求是实现金融产品快速创新、业务快速上线，满足市场变化和业务系统对 IT 资源要求的弹性供给等更高要求。与大数据、人工智能等金融科技新技术的融合可有效促进业务模式的探索和创新，促进跨行业合作，实现多方共赢。

目前，国内大型金融机构均建立了企业级私有云，一些小型金融机构以共享互联网企业提供的公有云服务为主^[11]。金融数据的加工与存储通过云端的资源实现，这本身就给传统的数据管理模式带来了全新的挑战。

3 金融科技中的数据安全模型

3.1 金融科技中的数据安全面临的挑战

在金融科技的支撑下，金融机构获取各种数据的能力大大提升，数据已成为金融业的重要资产，其重要性和机密性不言而喻。同时，各金融机构海量的数据也面临着数据不可用、数据被篡改、数据被窃取等安全问题。金融机构面临的数据安全主要有如下几个方面。

3.1.1 新技术带来的挑战

人工智能在金融业得到较快发展，但是由于其核心技术严重依赖于机器学习，而机器学习技术的“不显式编程”^[12]，使机器学习（特别是深度学习）存在输入数据与输出结果之间可解释性

差的黑盒特征。为了确保机器学习的输出结果具备真实性、正确性、可回溯性，金融科技质量保证部门除了对传统的方案、架构、软件代码的审查与管理外，对于机器学习中使用的大量训练数据的审查与管理、训练过程的审查与管理、系统功能与非功能的测试等都带来了新的挑战。

云计算是传统银行技术转型的重要方向，但是云平台在管理上的各种不确定性，增加了数据安全隐患。2019年上半年，美国 Verizon 公司发布的《Verizon 2019 年数据泄露调查报告》显示，从 2018 年开始云存储配置错误等事件处于上升趋势^[3]。金融机构越来越多地使用各类云服务，除少数大型金融机构建立了自己的私有云平台外，多数中小型金融机构普遍共享互联网公司搭建的公有云服务，第三方对金融机构数据具有很大的操控权限，而金融机构自身对数据的管控能力有限，数据安全问题不容忽视。当前，无论公有云还是私有云，对数据安全管控都带来了新的挑战。

同时，随着移动互联网技术的广泛应用，金融犯罪呈现网络化、高科技化和快速敏捷化特征，金融信息安全受到威胁和挑战^[13]。

3.1.2 新威胁带来的挑战

在新的金融科技形势下，对金融数据的威胁具有许多新特征。一是高发性。金融行业积累了数以亿计的有价值的客户信息大数据，是不法行为者攻击和盗取的重点对象。PwC 关于全球金融犯罪活动的调查报告显示：在金融犯罪活动中，利用互联网实施金融犯罪活动，已经成为犯罪分子实施金融犯罪时所采用的第二大手段，出现的频率越来越高^[14]。二是动态性。网络攻击过程及手段演变迅速，使风险评估更为困难，近年来，网络犯罪分子不断找到一些新的攻击方式，如高水平黑客利用社会工程学等攻击技术和浏览器/服务器模式缺陷（如 XSS 即跨站脚本攻击），让

其钓鱼网站设计看起来更为合理^[15]。三是匿名性。网络的非实名特征使对于网络威胁的识别更为复杂，随着 IT 技术的发展，各种匿名网络攻击手段不断变化，给金融行业的网络安全造成了新的威胁。四是系统性。在金融科技的推动下，金融数据成为数字经济时代经济发展的战略性资产，是金融企业的核心竞争力^[16]，金融数据安全带来的风险具有很强的溢出和传染效应，一旦金融数据存在安全问题，将在机构和市场构成的系统中引起一系列连锁反应，存在连续损失的可能性。

3.1.3 新数据带来的挑战

随着大数据相关技术的飞速发展，一些机构积累了大量的客户行为数据和交易数据，但因其信息系统管理水平和应对网络攻击能力未能同步，其数据安全管控能力不足，存在数据被集中泄露的风险。

传统的数据安全保护基础是依据数据价值实行数据分级，对不同级别的数据实施不同的保护策略。而在大数据背景下，数据采集、处理、分析过程中，数据内容不断发生迭代变化，数据边界变得模糊，传统的基于数据分级的保护策略不再适用于大数据环境下的保护。同时，大数据的访问控制、加密存储等机制变得更为复杂，均面临新的挑战。

此外，由于网络数据复制的无限性、低成本以及传递的隐蔽性，金融科技领域数据过度采集、数据倒卖等违法违规行为给金融机构如何保护自身权益提出了新的挑战。

3.2 金融科技中的数据安全模型

为便于下文描述，将本文提出的金融数据安全模型取名为“果壳”模型。

“果壳”模型基于信息安全等级保护中的 CIA（保密性、完整性、可用性）原则，设计风险边界和防控措施。“果壳”模型共分 3 层，如图 1 所示。

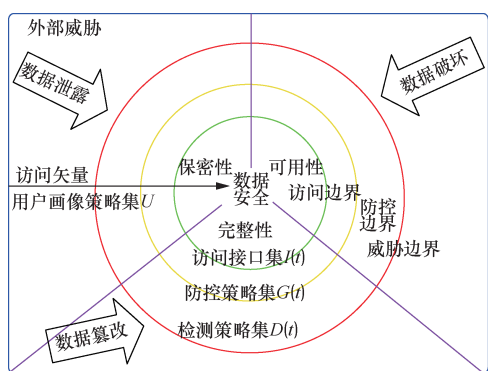


图1 数据安全二维模型

内部（目标或任务）：确保数据安全的目标或任务。

外部（威胁或风险）：数据面临的各种威胁或风险（泄露、篡改、破坏等）。

中间（策略或措施）：通过访问策略、防控策略、检测或感知策略等多种策略或具体措施，实现多层保护。

数据访问视为由外到内突破多层逻辑边界的一条矢量，过程中可能被边界阻断，也可能达到中心。若达到中心，说明通过了认证，获得了访问权限，允许操作。

考虑数据的生命周期，增加时间轴，便构建出“果壳”模型的三维图，如图2所示。

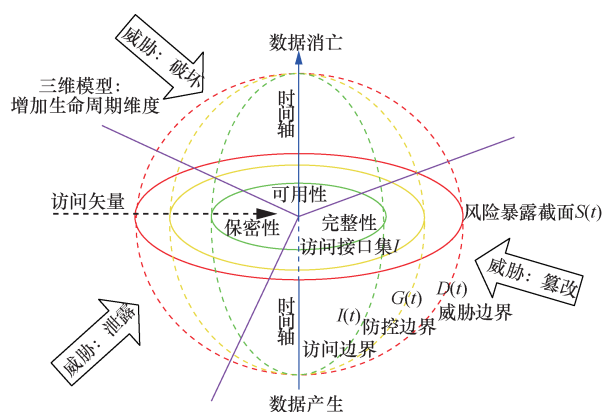


图2 数据安全三维模型

时间轴代表数据生命周期，数据的风险暴露面 $S(t)$ 为时间 t 的函数。随着 t 的增加， $S(t)$ 由小（数据产生）变大（数据存储、传输）再变小（数

据销毁）。在不同的生命周期阶段，风险暴露面大小不同，应该采取的策略也不同。

金融数据生命周期一般包含数据采集（创建）、数据传输（迁移）、数据处理（应用）、数据交换、数据存储（存档）、数据销毁等阶段，再次激活以及退出的整个过程^[17]。

与网络安全的布防方式类似，数据安全也在“边界”处布防，而且布防策略也是时间的函数，在不同生命周期阶段，策略不同。

访问边界：不直接提供数据，而是提供接口。访问接口集 $I(t)=\{\text{接口 1, 接口 2, 接口 3, } \dots\}$ 。

防控边界：对所有接口的访问采取相应的防控手段，对满足条件的访问进行放行，对不满足条件的访问，进行阻断。防控策略集 $G(t)=\{\text{数据脱敏控制, 数据加密控制, 数据权限管理, 防复制管理, 防泄露管理, 数据安全等级控制, } \dots\}$ 。

威胁边界：对数据安全的威胁进行感知、监测、判断，所得到的结论可以用于优化调整 $I(t)$ 和 $G(t)$ ，或根据所得到的情况直接采取应急措施阻止威胁。检测策略集 $D(t)=\{\text{安全态势感知, 威胁情报, 网络安全监控策略, } \dots\}$ 。

访问矢量：包含着用户的行为习惯等信息，可以进行用户画像，区分用户为安全用户还是危险用户。用户画像策略集 $U=\{\text{可信度计算策略, 用户身份判断策略, 用户目的判断策略, 用户习惯判断策略, 访问行为预判策略, } \dots\}$ 。

数据安全保障策略总集合 $A(t)=\{I(t), G(t), D(t), U\}$ ，为随时间变化的函数。

[示例 1] 当 t =数据采集（创建），则 $A=\{\text{数据合规性管理, 数据质量管理, 数据安全等级管理, } \dots\}$ 。

[示例 2] 当 t =数据传输（迁移），则 $A=\{\text{数据加密, 数据脱敏, 防复制管理, 隐私信息保护, } \dots\}$ 。

[示例 3] 当 t =数据处理（应用），则 $A=\{\text{用户画像策略, 数据使用管理, 数据加工安全管理, } \dots\}$ 。

数据脱敏，数据权限管理，数据溯源，...}。

[示例 4] 当 t =数据交换，则 A ={数据导入导出管理，数据共享安全管理，数据监控，数据加密，...}。

[示例 5] 当 t =数据存储（存档），则 A ={数据存储架构，数据归档管理，数据时效管理，数据访问控制，数据安全等级管理，数据灾备备份策略，...}。

[示例 6] 当 t =数据销毁，则 A ={数据介质管理，数据销毁策略，介质销毁处置管理，...}。

在上述示例中，一般还应包含通用安全管理，如机构及人员权责管理、数据资产管理、数据供应链管理规章制度、管理流程、操作规程。

4 金融科技中的数据安全对策

4.1 构建多层次数据安全治理体系

根据上述“果壳”模型，数据安全在不同的应用场景或时间阶段所需要的保护措施不同，金融机构应构建多层次数据安全治理体系。

(1) 构建企业级数据安全战略

金融机构应根据金融科技特点，将数据安全纳入企业战略进行顶层设计和规划，建立涵盖数据生命全周期及业务全流程的制度规范体系，从组织机构、人力资源、资金资源、组织及人员能力等方面予以重点保障，在做好数据保护的基础上开展数据利用，才是金融科技健康长效发展的根本^[18]。同时，要加大宣传教育，将金融科技形势下的数据安全纳入全员教育，成为一种企业文化。

(2) 构建安全技术防护体系

根据数据生命周期的每一个阶段，分别从访问层、防控层、威胁层等层面采取有效的数据安全防控措施，全面的数据安全防控措施一般覆盖 3 个层面，每一个层面要考虑数据的全生命周期。第一是访问层面，是最接近数据的层面，要从系

统建设开始，做好顶层设计，把数据安全治理作为重要需求纳入系统建设的设计内容。例如，通过定义数据访问接口，使数据的访问受限并可控，同时，在新系统投产前，加强对系统的安全性测试。第二是防控层面，可以采用数据加密、数据脱敏、数据泄露防护（DLP）、数据库审计等安全防控手段，防止因内外部不正当操作所引起的数据安全问题。第三是威胁层面，是直接对外暴露的层面，要从金融业务处理的全流程梳理数据的暴露截面，制定业务管理与技术手段相结合的应对措施，技术上可以考虑部署入侵检测、防火墙、安全态势感知等检测工具或平台，主动探测外在威胁，及时采取应对策略。

(3) 构建数据安全治理保障体系

1) 技术保障。金融科技是金融与科技的深度融合，从业机构应该围绕实体经济金融需求和传统金融服务所暴露出来的短板，审慎地选择相对稳定成熟、与业务发展契合度较高的数据治理技术，同时，加大对金融科技相关新技术的跟踪、研究和应用，通过技术手段保障金融数据安全。

2) 建设安全核心能力。成立专职安全团队来推动金融企业的信息安全管理，避免管理缺位；加大 IT 人才培养，要确保需求设计、软件开发、软件测试、生产运维等自主可控。3) 强化职责权限。在数据安全保护方面，要实施风险零容忍的策略；在关键的高风险领域，强化事前、事中的监测和处置，通过行为分析、快速响应来应对数据泄露的威胁；要明确业务管理部门、运营操作部门、系统建设部门、生产运维及数据管理部门的事权划分，确保数据管理、使用、运维等岗位人员职责清晰；严格控制不同层级人员权限，减少具有管理员权限的人员数量^[19]。在数据日常安全管理中，一般应遵循如下原则：集中统一管理原则、责任到位管理原则、最小权限管理原则^[20]。

4.2 引入数据安全能力成熟度评估模型

面对金融科技时代的安全挑战,应该对数据建立一套完整的生命周期管理体系。生命周期管理不仅涉及“硬”的方面,如数据的采集、存储、集成、分析、归档、销毁的安全问题,还包括“软”的方面,如数据与系统资产、组织人员、服务规划、数据供应链和合规性的管理策略。围绕数据的生命周期,根据业务领域,划分数据安全能力维度,建立数据安全能力成熟度模型^[21-22],如图3所示。结合业务的需求以及监管法规的要求,持续不断地提升组织整体的数据安全能力,从而形成以数据为核心的安全框架。

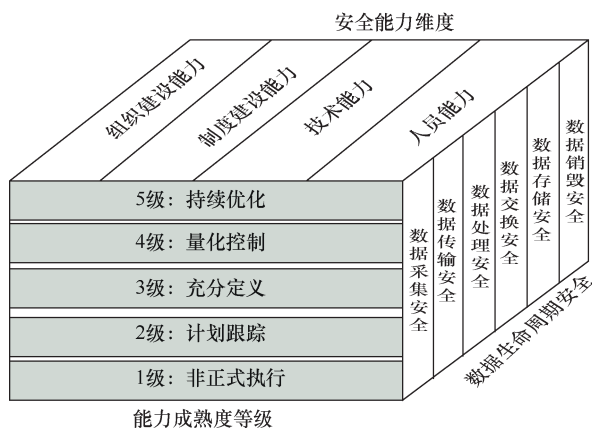


图3 数据安全能力成熟度模型

使用模型时,金融机构应首先明确其数据安全能力的目标成熟度级别。根据各金融机构数据安全战略、对整体的数据安全能力成熟度级别的定义,金融机构可以选择适合自己业务实际情况的短期目标和长期目标。

三级目标适用于所有具备数据安全需求管理的金融机构作为自己的短期目标或长期目标,具备了三级的数据安全能力,则意味着金融机构能够针对数据安全的各方面风险进行有效的控制。能力成熟度等级越高,金融机构的安全防控能力越强。然而,对于业务中尚未高度依赖于大数据等金融科技的金融机构而言,数据仍然倾向于在固有的业务环节中流动,其数据安全需求整体弱于高度依

赖金融科技的金融机构,因此,其短期目标可先定位为二级,待达到二级的目标后再升到三级。

由于各金融机构在业务规模、业务对数据的依赖性等方面的差异,对模型的使用也可以适当调整和裁剪。金融机构基于对成熟度模型内容的理解,识别数据安全能力现状并分析与目标能力等级之间的差异,在此基础上进行数据安全能力的整改提升计划。伴随着金融机构业务的发展变化,金融机构需要定期复核、明确自己的目标成熟度等级,然后开始新一轮目标达成的工作,使用数据安全能力成熟度模型的闭环如图4所示^[22-23]。

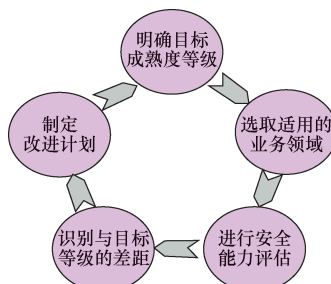


图4 推荐的成熟度模型使用步骤

5 结束语

现阶段,科学技术日新月异、社会经济加速发展,金融科技中的数据安全态势也不断演变,关于数据安全风险的分析方法、治理模型、应对策略等也需要与时俱进、持续研究并实践。

金融科技的发展尚处于一个不断探索和逐步成熟的过程中,金融科技的现状仍面临许多安全挑战。数据安全作为安全建设的关键部分,已经成为金融行业信息化安全建设最核心的一环。

未来金融科技的可持续发展需要更加注重数据安全建设,需要金融机构从企业战略、企业文化、全员安全意识、组织管理、技术能力、人才储备等方面提升整体安全防控能力。只有正确处理金融科技为数据安全带来的机遇与挑战,才能更好地让金融服务实体经济,防范金融风险。

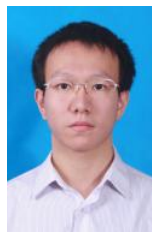
参考文献:

- [1] 尹志超, 余颖丰. 重视金融科技在金融发展中的作用[N]. 光明日报, 理论, 2018-11-20.
YIN Z C, Yu Y F. Pay Attention to the role of financial technology in financial development[N]. Guangming Daily, Theory, 2018-11-20.
- [2] 普华永道. 2018 年中国金融科技调查报告[R]. 2018.
PwC. 2018 China financial technology survey report[R]. 2018.
- [3] Verizon. 2019 data breach investigations report (12th edition)[R]. 2019.
- [4] 吴信东, 董丙冰, 堵新政, 等. 数据治理技术[J]. 软件学报, 2019, 30(9):1-22.
WU X D, DONG B B, DU X Z, et al. Data governance technology[J]. Journal of Software, 2019, 30(9):1-22.
- [5] 张明英, 潘蓉. 《数据治理白皮书》国际标准研究报告要点解读[J]. 信息技术与标准化, 2015(6):54-57.
ZHANG M Y, PAN R. Interpretation of the key points of the international standards research report on data governance white paper[J]. Information Technology & Standardization, 2015(6): 54-57.
- [6] 李文红, 蒋则沈. 金融科技 (FinTech) 发展与监管: 一个监管者的视角[J]. 金融监管研究, 2017(3): 1-13.
LI W H, JIANG Z S. FinTech development and supervision: a regulator's perspective[J]. Financial Supervision Research, 2017(3): 1-13.
- [7] 中国信息通信研究院. 人工智能发展白皮书-产业应用篇 (2018) [R]. 2018.
China Academy of Information and Communications Technology. Artificial intelligence development white paper—industrial application (2018)[R]. 2018.
- [8] 赵维平. 大数据为金融创新插上翅膀[J]. 中国金融, 2019(4):21-22.
ZHAO W P. Big data inserts wings for financial innovation [J]. China Finance, 2019(4): 21-22
- [9] 肖翔, 陈则栋, 战天舒, 等. 我国商业银行金融科技发展现状、问题与建议[J]. 当代金融家, 2018(8): 76-79.
XIAO X, CHEN Z D, ZHAN T S, et al. Status quo, problems and suggestions on the development of financial technology in China's commercial banks[J]. Contemporary Financiers, 2018(8): 76-79.
- [10] 王冠, 张敏. 区块链商业金融的应用层次、问题与对策建议[J]. 商业经济研究, 2018(7): 162-165.
WANG G, ZHANG M. Application levels, problems and countermeasures of blockchain commercial finance[J]. Business Economics Research, 2018(7): 162-165.
- [11] 中国信息通信研究院. 金融行业云计算技术调查报告 (2018)[R]. 2018.
China Academy of Information and Communications Technology. Financial industry cloud computing technology survey report (2018) [R]. 2018.
- [12] 周志华. 机器学习[M]. 北京: 清华大学出版社, 2016.
ZHOU Z H. Machine learning[M]. Beijing: Tsinghua University Press, 2016.
- [13] 李连朋, 罗宏. 国内外金融业信息安全综述[J]. 网络与信息安全学报, 2017, 3(2):9-19.
LI L P, LUO H. Review of domestic and international financial security[J]. Chinese Journal of Network and Information Security, 2017, 3(2):9-19.
- [14] PWC. Global economic crime survey[R]. 2016.
- [15] 朱建明, 高博. 社交金融的信息安全风险与防范[J]. 网络与信息安全学报, 2016, 2(3):46-51.
ZHU J M, GAO B. Social financial information security risk analysis and prevention[J]. Chinese Journal of Network and Information Security, 2016, 2(3): 46-51.
- [16] 石光. 金融科技“双刃剑”[J]. 中国金融, 2019(6): 74-76.
SHI G. Financial technology double-edged sword[J]. China Finance, 2019 (6): 74-76.
- [17] 数据安全治理白皮书 2.0[R]. 北京: 北京安华金和科技有限公司, 2019.
Data security governance white paper 2.0[R]. Beijing: Beijing AnhuaJinhe Technology Co., Ltd., 2019.
- [18] 刘宇. 我国金融科技监管框架完善路径浅析[J]. 中国金融电脑, 2019(7): 35-37.
LIU Y. Analysis on the perfection path of China's financial science and technology supervision framework[J]. China Financial Computer, 2019(7): 35-37.
- [19] KOPP E, KAFFENBERGER L, WILSON C. Cyber risk, market failures, and financial stability[M]. International Monetary Fund, 2017.
- [20] 丁丽媛. 基于数据生命周期的金融数据安全研究[J]. 信息安全研究, 2018(6): 548-554.
DING L Y. Research on financial data security management based on data life cycle[J]. Information Security Research, 2018(6): 548-554.
- [21] GB/T 36073-2018, 数据管理能力成熟度评估模型[S]. 北京: 中国国家标准化管理委员会, 2018.
GB/T 36073-2018, Data management capability maturity assessment model[S]. Beijing: China National Standardization Administration Committee, 2018.
- [22] 朱红儒. 信息安全技术数据安全能力成熟度模型[R]. 北京: 全国信息安全标准化技术委员会, 2018.
ZHU H R. Information security technology data security capability maturity model[R]. Beijing: National Information Security Standardization Technical Committee, 2018.
- [23] 郑斌. 企业数据安全能力框架——数据安全能力成熟度模型的构建及应用[J]. 信息安全与通信保密, 2017(11):70-78.
ZHENG B. Organizational data security capability framework —development and implementation of data security competency maturity model[J]. Information Security and Communication Confidentiality, 2017(11): 70-78.

[作者简介]



朱建明 (1965—), 男, 山西太原人, 博士, 中央财经大学教授、博士生导师, 主要研究方向为信息安全、金融科技与区块链技术。



杨鸿瑞 (1998—), 男, 北京人, 主要研究方向为计算机科学与技术。