TSINGHUA PBCSF 清华五道口 | IFR 金融科技研究院

研究报告

（2021 年 第 5 期 总第 94 期） 2021 年 5 月 10 日

关于金融科技安全的认识与思考

金融安全研究中心

【摘要】金融科技安全是国家安全的重要内容之一，保障金融科技安全发展，对于实施创新驱动发展战略和实现高质量发展发挥着重要作用。随着金融科技从 1.0 阶段发展到 3.0 阶段，金融科技安全 3.0 的内涵也演变成金融生态安全，它是技术安全、客户安全、平台安全、企业安全和金融机构安全五位一体的综合体。这一阶段的金融科技安全面临着三大风险特征：一是受灾广、受灾重， 二是发生风险频次高，三是以网络安全风险和应用安全风险为主。

本文从个人、金融机构与金融行业、社会治理和社会稳定、金融监管、全球化安全以及金融科技自身等六个方面分析了金融科技所带来的挑战，在充分认识金融科技发展与安全的关系的基础上，提出了强化个人金融安全防护、加强金融行业与机构管理、金融科技赋能社会治理、提升金融监管水平、推动国际金融监管合作、提高金融科技核心技术自主创新能力等六个方面的建议。

目录

关于金融科技安全的认识与思考

周道许　张翼飞

（金融安全研究中心）

黎恩银

（中国财政科学研究院 博士研究生）

当前，金融科技已上升到国家发展战略高度，构成了创新发展战略的重要内容之一。央行在《金融科技（FinTech）发展规划（2019-2021 年）》中，将金融科技定义为技术驱动的金融创新，旨在运用现代科技成果改造或创新金融产品、经营模式、业务流程等，推动金融发展提质增效。坚持创新驱动发展，加快金融科技战略部署与安全应用，已成为深化金融供给侧结构性改革、增强金融服务实体经济能力、打好防范化解金融风险攻坚战的内在需要和重要选择。金融科技有望成为推动金融转型升级的新引擎、服务实体经济的新途径、促进普惠金融发展的新机遇、防范化解金融风险的新利器。

在新一轮科技革命和产业变革的背景下，金融科技蓬勃发展，人工智能、区块链、大数据、云计算、物联网等信息技术与金融业务深度融合，为金融发展提供源源不断的创新活力，金融

服务模式与金融产品形态也在发生着深刻的变化，金融科技使得金融服务更加便捷化、智能化的同时，也为金融科技安全赋予了全新的内容，为金融科技安全提出了新的挑战，金融科技安全已经成为金融安全乃至国家安全的重要内容。

一、现阶段金融科技安全的内涵与风险特征

金融科技安全的特征与金融科技的发展阶段相适应。从金融服务模式的变革来看，可以将我国金融科技发展历程划分为三个阶段：

金融科技 1.0 是金融业务电子化阶段，其核心特征是“以账户为中心”的金融服务体系，这一阶段的金融科技实际上是以银行为中心，银行通过账户绑定所有人。

金融科技 2.0 是金融渠道网络化阶段，其核心业务模式是“以客户为中心”的金融服务体系，随着资金和金融产品的过剩，金融机构为了获得更多的资金和更好的客户，金融服务体系的中心开始由“账户”转向“客户”。

金融科技 3.0 是金融与科技深度融合阶段，其核心业务模式是“以场景为中心”的金融服务体系。这一阶段，金融与科技相互交织，金融服务与生产生活场景深度融合，金融机构将金融服务嵌入衣食住行、医疗教育、电子商务等民生领域，人工智能、区块链、大数据、云计算、物联网等新兴技术，在金融场景中扮演了重要角色，成为推动“以客户为中心”向“以场景为中心”

转变的新引擎。

与金融科技发展三个阶段相对应，金融科技安全的内涵也表现出阶段性变化。

金融科技安全 1.0 是传统意义上的技术安全。除了传统风险类型以外，金融安全在技术层面上主要体现在金融机构内部的电子化系统安全保障，如支付清算系统、交易记录数据库、ERP 系统等。

金融科技安全 2.0 是互联网时代的网络安全。互联网出现之后，金融和互联网的融合程度越来越深，联系面越来越宽，建立了网络化的金融服务体系。这个阶段金融科技安全主要关注互联网技术本身及“互联网+”所带来的业态风险，例如，在第三方支付领域存在的风险就包括技术性风险、网络犯罪风险、操作性风险以及互联网金融业务派生的流动性风险等。

金融科技安全 3.0 是金融生态安全。它是技术安全、客户安全、平台安全、企业安全和金融机构安全五位一体的综合体。如果不依托系统性、动态的观点和对生产力发展的成熟理解来分析金融安全，就可能产生偏颇，并因此形成巨大的金融风险隐患，所以金融科技安全 3.0 必须从整体的金融生态安全来认识与理解。这一阶段的技术创新发展使得金融科技安全面临的突出风险有四类：一是移动 app 普遍存在安全风险；二是大数据融通的同时带来安全挑战；三是人工智能带来新的安全挑战；四是区块链技术不成熟带来的机制风险。

金融科技安全演化的历程体现出，金融越发展，科技越进步，金融科技安全越重要。3.0 阶段的金融科技面临的风险着有三大突出特征：

第一是金融科技安全领域受灾广、受灾重。根据通信院的研究报告，在 2019 年不同行业发生的重大网络安全事件中，金融行业占比高达 33%，成为网络安全事件发生的重灾区。在金融行业细分领域的网络安全事件分布中，银行业占比高达 28%。主要风险体现在业务安全风险外溢、大数据风险严峻、金融科技安全生态不完善、网络安全风险凸显四方面。

第二是金融科技安全领域发生风险频次高。近年来，针对金融行业的网络攻击行为大幅增长，给各类企业、用户以及金融行业造成的损失每年达数百亿，并有继续快速增长的趋势。根据国际证监会组织与世界交易所联盟做的一项调查报告，近年来针对金融市场和企业的网络犯罪数量会急剧上升，大型企业、金融机构、证券交易所已经成为主要的受攻击目标，有超过一半的受访者表示曾遭遇过网络攻击。以支付宝为例，其每年都在遭受成千上亿万次的黑客攻击，每次每刻都在遭受黑客们的“青睐”，每年有 6000 万次的黑客攻击，平均每天 16 万次，在巅峰时期，支付宝曾经一天内就遭到黑客攻击达到 16 亿次。

第三是金融科技安全突出体现在网络安全风险和应用安全风险上。金融科技网络安全风险表现在信息系统、平台承载的数据规模急剧攀升、数据价值愈加凸显，逐渐成为攻击者发动网络

攻击、进行数据窃取的重点攻击目标，如公网安全（ DDoS、恶意软件、勒索软件等）、App 安全、数据安全等。金融科技的应用风险主要是随着金融科技的快速发展，大数据、人工智能、云计算等新技术的广泛应用使得金融业务彼此融合程度不断加深，业务边界不断削弱，为金融科技安全监管带来了新的挑战，如大数据技术应用安全、人工智能技术应用安全、区块链技术应用安全等。

二、金融科技带来的六大风险挑战

毋庸置疑，金融科技对金融业发展和社会经济产生了深刻的积极作用。从金融服务需求者的角度来讲，它使更多的人群得到了金融服务，金融服务的可获得性得以提升；从金融机构的业务发展来讲，金融科技能有效控制成本，提升服务效率，推动了金融产品创新，提升了金融业务的风险防控能力。从社会治理角度来讲，金融科技促进了社会治理智能化、精细化水平，通过治理工具的改进促进了社会稳定。从监管的角度来讲，金融科技丰富了金融监管手段，提高了金融监管效率。从社会意识来讲，金融科技促进人们形成“互联网思维”，加快了社会向“全样本”思维、“容错”思维、“相关”思维的转变。

与此同时，金融科技的进步意味着底层技术和金融业务的复杂化，金融的内在脆弱性和强外部性的属性更加凸显，给民众、行业发展、监管、社会治理以及全球金融稳定带来了不少挑战。

2.1 金融科技对个人信息安全和生活安全带来风险和挑战

第一是个人数据及信息隐私的泄露。在生活信息层面，社交、购物、信息浏览记录、电话住址等会被采集；在金融信息层面，账户、支付、存取款和金融资产的持有和交易信息会被记录；在生物信息层面，面部识别、指纹、健康监测等信息也会被平台收集。一旦保管不当或遭受网络攻击造成数据泄露，信息持有者稍加分析便可获得客户精准画像，导致大量客户隐私泄露，进而造成重大财产损失和人身安全隐患。

第二是算法歧视和数字鸿沟，严重损害特殊群体利益。一是“大数据杀熟”，用大数据算法的结果来精准掌握每位消费者的最高支付意愿，从而进行歧视性定价，消费者毫不知情或无力反抗。二是数字鸿沟。金融科技对社会公众的技术应用的能力提出了更高要求，但科技知识薄弱、老年人等处于金融科技“雷达”范围之外的群体就只能被迫远离部分金融服务，造成社会不公。

第三是对个人金融消费者进行诱导式、掠夺式放贷，导致“超前消费”。 金融服务提供者过度追求利润、开展掠夺性贷款，通过科技手段利用过度授信和场景诱导等共同刺激超前消费，或以高利贷，或以向低信用人群推销不适合的信贷产品等形式，使得一些低收入人群和年轻人深陷债务陷阱，最终损害消费者权益，甚至给家庭和社会带来危害。

2.2 金融科技对金融机构和金融行业安全带来了风险和挑战

第一是金融科技的迅速发展可能加大金融机构的传统风险。金融科技大大延伸了金融机构开展业务的地域边界和群体边界，增加了金融机构资金运用期限错配、货币错配的可能性，可能会加剧金融机构的流动性风险。基于大数据的信贷业务，在长尾客户的资信水平相对较弱，信用风险评估模型不健全等因素影响下，有可能增加信用风险。金融科技增加了操作性风险的新形式，如数据泄露、欺诈、业务中断和网络攻击等网络事故，内部治理和流程管控风险不健全造成的数据滥用，以及第三方服务商数据泄漏等。

第二是大型金融科技公司的出现容易造成行业垄断和不公平竞争。大型金融企业凭借技术优势占据市场的主要地位，并通过并购不断强化市场垄断力量，造成“赢者通吃”的局面。一旦放松准入门槛，大型企业会迅速占领市场，不利于公平竞争，垄断最终会导致创新动力削弱、经济效率下降和消费者福利的损失。

第三是大型金融科技企业凭借金融科技和网络平台模糊了产品和业务边界，突破地域和业务范围限制，容易造成风险的溢出和蔓延，从而放大了系统性风险。

2.3 金融科技对社会治理和社会稳定带来风险挑战

一是金融科技的兴起为数字金融诈骗提供了新工具。数字金融欺诈呈现出产业化、职业化、精准化、移动化、场景化和技术化的特点，欺诈手段由之前较为简单的盗号、盗刷演变为现在的借助人工智能、大数据等前沿技术，从撒网式向精准化转变，并叠加传销、兼职赚钱、网购退款、金融理财、虚拟货币等更为复杂多样的手法，典型形式主要有高利理财、网络借贷、网络众筹等。根据 2019 年金融科技蓝皮书数据，网络诈骗的“黑色产业”市场规模已高达 1100 亿元，成为我国第三大“黑色产业”，为居民财产安全造成巨大威胁。

二是冲击就业格局，加剧社会财富分化。一方面，机械性或高危险的低技术含量工作很容易被技术替代。麦肯锡预测，到 2030 年机器人将取代 8 亿人的工作，到 2027 年，金融领域 23% 的工作岗位会受到人工智能带来的颠覆性影响。另一方面，金融科技会重新分配社会财富，人工智能等金融科技的兴起和历次工业革命一样，会重新分配社会财富，提高资本受益者的比重，致使受教育程度低、技术含量低、人文含量低的工作从业者面临更为严峻的挑战。

2.4 金融科技对金融监管带来的风险和挑战

第一是金融科技促使金融风险隐蔽化、分散化，对识别和预

警效率提出了挑战。金融科技兼具金融、技术属性，助推了金融市场和产品的跨界，扩大了监管的模糊地带，增加了监管套利风险；伴随金融科技产生的高频交易、海量账目等问题也加大了监管机构风险识别、监测的难度。

第二，金融科技技术风险扩散的过程非常快，增加了监管的处置难度。金融数据通常面临多系统、多环节留存，导致数据流转追踪难、控制难，金融科技所采用的数据驱动、平台支撑、网络协同的业务模式，使得金融科技风险涉及面广，传播速率快，进一步增加风险处置难度。

第三，由于法律规范和行业技术标准不健全，金融科技监管在法律与技术层面的定量和定性工作都很难，比如数据的使用权是否属于用户、分析使用是否触及隐私、用户数据的产权定价权等没有明确的规定。

2.5 金融科技对全球化安全发展带来的风险

第一是跨国金融科技企业增强了全球金融风险网络的关联度。跨国金融科技企业所提供的跨国别金融产品进一步增强了全球金融市场的关联性，将全球市场绑定在同一风险环境中，全球金融科技风险的传播路径更多，杀伤力更强。特别是“大而不能倒”的跨国金融科技巨头，其系统重要性上升为全球层次，牵动着全球金融系统的神经。这些跨国大型金融科技企业用户规模和交易规模都十分庞大，覆盖了大量金融知识和投资水平相对较弱

的长尾客户，一旦出现风险暴露，引发羊群效应，将造成严重的连锁反应，很可能会引发全球化的系统性风险。

第二是国际资本流动更加复杂和不可控。数字技术促进了跨境支付便捷性的提升和成本的下降，国际资本流动更加频繁，投资性资金更加活跃，这会加剧各国金融市场的波动性，为维护金融市场稳定和有效执行货币政策的带来新的挑战。

第三是加密货币带来的风险。加密货币基于区块链技术开发，具有去中心化特点，绕开了银行在跨境收支中的中介作用和资本账户的监管，这一方面使得跨境支付统计的完整性和真实性面临挑战，削弱一国对国际资本流动的有效管控。另一方面加密货币具有较强的隐私保护和匿名性，已经开始成为恐怖组织、洗钱、非法交易等跨境非法活动利用的新工具，增加了追踪和打击这些非法活动的难度。

2.6 金融科技技术自身带来的风险

人工智能、区块链、云计算、大数据、物联网等在技术上并非是完美的，在空间上也不是绝对安全的。比如在人工智能领域，人工智能学习框架和组件存在安全漏洞风险，一旦被攻击者恶意利用，可能危及人工智能产品和应用的完整性和可用性；逆向攻击可能导致算法模型内部的数据泄露；算法设计或实施有误会产生与预期不符甚至伤害性结果。

在区块链领域面临着共识机制挑战，对于区块链中的共识算

法，是否能实现并保障真正的安全，需要更严格的证明和时间的考验；区块链存在的其他漏洞也会招致攻击，对账户安全造成一定威胁。

云计算领域中，在 IaaS 层存在着来自主机安全、虚拟网络、数据存储等方面的安全威胁；在 Paas 层存着着数据处理、开发环境等安全威胁；在 SaaS 层存在来自 SaaS 提供商、用户以及数据传输的安全威胁。

大数据领域中，大数据平台在开源模式下缺乏整体安全规划，自身安全机制存在局限；大数据平台服务用户众多、场景多样，传统安全机制的性能难以满足需求；大规模分布式存储和计算模式导致安全配置难度成倍增长；针对大数据平台网络攻击呈现新特点，传统安全检测技术暴露不足。

物联网领域中，核心网络具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。此外，现有通信网络的安全架构都是从人通信的角度设计的，并不适用于机器的通信。

三、 要正确认识金融科技发展与安全的关系

3.1 金融科技安全的发展态势取决于国家对金融科技的定位、社会对金融科技的认知程度和监管部门对金融科技风险的驾驭能力

首先，国家对科技的定位较高。官方对金融科技的定位为：推动金融转型升级的新引擎、服务实体经济的新途径、促进普惠金融发展的新机遇、防范化解金融风险的新利器。其次，社会需要平和、理性地认识金融科技。不要说好就是“好的不得了”，说坏就是“洪水猛兽”。实际上，金融科技没有设想的那么好，也不像批评的那么坏，技术用的好就是“天使”，用的不好就是“魔鬼”，技术是中性的；最后，监管部门的作用很重要。监管部门就好比一个骑手，如果驾驭的好，金融科技就会为我们“随心所欲”地使用。如果驾驭的不好，就可能会被“掀翻在地”。综合以上三个方面来看，金融科技安全发展的态势是一个不断强化的过程。

3.2 从长期看，金融科技安全的积极因素和消极因素虽然相互交织博弈，但总体发展态势是金融安全不断增强，并呈螺旋式上升

金融科技安全内部“发展”和“安全”这一对矛盾在相互转化。安全是发展的前提，发展是安全的保障，安全和发展要同步

推进。有时积极因素也会伴随着隐患，而消极因素也会通过改进优化带来进步。所以说金融科技的积极因素和消极因素将长期处于相互融合、相互补充的过程。总体上来看，科技是人类进步的工具，是社会衡量文明的标准，而经济又是科技的外在体现，所以金融科技安全的态势不断增强的。

3.3 金融与科技相互靠拢、相互融合是发展的趋势，金融更像科技，科技更像金融

这里存在两个趋势，一个是金融领域的业务和技术更加紧密结合；一个是金融机构和金融科技市场的主体更加多元融合。金融科技内的金融和科技正是“你中有我，我中有你”。尽管金融科技领域里金融和科技具有不同的业态属性，但实际上两者已经相互融合、相互促进，很难再分开。

3.4 随着监管水平的提高，会逐步打破市场垄断，金融科技在促进社会的公平和效率方面会起到更好的平衡器作用

首先，阶层分化、贫富不均是人类社会发展的必然现象，不是金融科技造成的必然结果。但其中技术起了放大的作用，金融科技在主观上和客观上都加剧了社会分化，放大了财富分配的不均。主观来看，科技的门槛比较高，只有少数人才能进行专业挖潜，需要头脑和毅力，再经过有商业才能者之手才能把技术变成商品、把想法变成应用，进而建立一个企业。客观来讲，金融科

技助长了“赢者通吃”，加剧了马太效应。

其次，科技是中性的，用好了它会推动社会的发展和经济的增长，使每一个社会成员都会在做大的“蛋糕”中得到自己的一份；从促进财富增长来看，金融科技有利于社会的公平。

最后，金融科技会有助于对社会财富实行量化管理，有利于对财富进行科学、公平分配。金融科技的技术手段使社会财富的量化管理成为可能，从而为制定更加公平合理的财富分配制度和方案提供科学依据，在程序、公正和效率等方面起到更好的平衡器的作用。

四、 关于进一步做好金融科技安全的建议

4.1 不断强化个人金融安全防护

一是不断加强个人数据安全保护制度建设。加快明确金融科技企业所持有巨量消费者数据的法律属性和产权边界，要以保护个人信息安全为宗旨加强数据管理，完善个人数据的采集、管理和使用监管规则，严格控制数据滥用风险的同时兼顾数据开放、推动数据共享。

二是重视个人信用体系建设。加强个人诚信教育，完善个人信息安全、隐私保护和信用修复机制，完善个人守信激励和失信惩戒机制。

三是警惕针对金融消费者的诱导式、掠夺式贷款。进一步规

范市场主体的借贷范围和行为；加强消费者权益保护，完善第三方调解、仲裁和诉讼等金融纠纷处理机制；警惕消费至上等消费主义思潮带来的不良影响，避免过度消费、超前消费，倡导公众理性消费。

4.2 加强金融行业和金融机构管理，维护市场公平

第一，严格市场准入，坚持金融持牌经营原则和“一致性”原则。金融科技的本质是金融，机构和平台只有获得监管部门准入许可，才能开展金融业务；坚持一致性原则，在现有法律框架下，只要从事相同的金融业务，就要接受同样的管理，以维护公平竞争、防止监管套利。

第二，加快完善相关标准，推动行业有序发展。进一步加大推进金融科技标准化工作力度，完善相关技术和金融业务标准，完善产品服务标准体系建设；有关职能部门要加快制定区块链、大数据等技术标准和风险规则，发挥标准规则和检测认证作用，推动金融科技在行业技术和业务运用上有序合规发展。

第三，加强行业自律，引导从业机构合规审慎经营。通过推行行业基础设施建设，包括统计监测、信息披露、标准规则、投资者保护等工作，引导从业机构合规审慎经营。金融机构自身应该构建起科学有效的内控体系，并在此基础上搭建起完备、安全的金融科技防护体系。

4.3 利用金融科技手段，助力经济社会治理安全

第一，利用大数据的手段防范化解金融欺诈风险。建立起来源广、范围宽、维度多的反欺诈基础数据库；充分利用分布式大数据结构，提高对海量数据的实时处理能力，建立金融交易实时反欺诈监测系统，做到风险的实时监测；利用机器学习深度挖掘海量数据，构建科学合理的反欺诈模型，提高金融反欺诈决策效率与胜率。依托大数据手段，建立起先进的监测预警、分析研判、风险处置与监管协同平台。

第二，将人工智能贯穿社会治理全过程，提高经济社会治理的效率。加快建设智慧政府，推进人工智能、大数据等技术同教育、社会保障、医疗、基础设施建设等公共服务领域的深度融合，建立起基于数据分析、深度学习的科学决策机制，动态优化政府管理流程、管理措施、管理方法，进一步推动社会治理向智能化、现代化方向发展。

第三，利用区块链，有效保障数据安全，助力经济社会治理的有序推进。打破数据孤岛和数据壁垒，逐步建立安全可信的政务数据融合链，推动政务数据对内部的开发共享和对社会间的有序开放；建立以密钥为加密手段的区块链统一公民身份，使民众能够更好地掌控个人数据使用范围，让个人隐私和数据安全得到真正保护；积极推进区块链在金融领域的应用，加强区块链的数据融合和监管能力，为制定更有效的金融和经济政策提供决策依

据。

4.4 提升金融监管水平，促进金融科技健康有序发展

第一是坚持监管的穿透性、适应性和一致性原则。“穿透性”就是要把资金来源、中间环节与最终投向连接起来，综合全环节信息判断业务性质，执行相应的监管规定；“适应性”就是在金融创新和防范风险之间进行平衡，既不能因为监管过严而遏制创新，也不能过度创新而造成不安全隐患。“一致性”就是要将所有的金融活动纳入监管，并确保实质相同的金融机构和金融业务遵守相同的监管规则，形成公平竞争的环境。

第二要不断优化监管体系建设。一是完善金融科技安全顶层设计，加快制定金融科技安全领域的政策法规、行业标准规范，明确各有关职能部门在金融科技监管中的职能定位。二是完善金融科技安全协同联动机制，建立起工信、网信、公安等部门跟金融监管部门之间的协同联动机制，加强金融科技风险监测、响应与处置的协同性和时效性；针对金融科技前沿安全问题和基础安全瓶颈，开展联合攻关研究，为金融科技安全提供技术支撑。三是要统筹创新与风险监管，持续升级监管手段，探索应用监管沙盒等创新性手段，实现金融科技创新与有效风险防控的双赢局面。四是持续提升穿透式监管能力，不断加强源头监管水平，通过穿透式监管手段强化监管渗透深度、广度和频度，及时化解针对新技术创新过程中出现的风险。

4.5 推动国际金融监管合作，加强全球化治理安全防范

一是进一步加强金融稳定理事会、巴塞尔委员会等国际组织合作交流，积极就金融科技发展、监管等方面开展经验分享以及共同研究，推动形成金融科技发展与监管的共识，探索制定全球通用规则。

二是进一步加强多双边监管合作，积极探索多元化金融监管沟通协调机制，促进跨境监管机构间数据和信息共享，建立共同风险监测机制，完善跨境资本管理政策工具；加强反洗钱、反垄断、数据管理、运营管理、消费者保护等方面的国际合作，确保对金融科技的监管有效、适度，防范跨境监管套利和金融风险跨境传染。

三是完善创新领域金融监管规则，研究建立跨境金融创新的监管“沙盒”。

4.6 提高金融科技核心技术自主创新能力，防范金融科技自身风险

第一，要从国家总体安全观的高度来谋划金融科技自身安全的提升。核心技术受制于人是我们最大的隐患，大量金融科技都在应用国外的基础技术，国产化率并不是很高，从这个意义上讲，没有绝对的安全。因此，要坚定不移实施科技创新战略，加强重大创新领域战略研判和前瞻部署，强化事关国家安全和经济社会

发展全局的重大科技任务的统筹组织，强化国家战略科技力量建设；加快补短板，建立自主创新的制度机制优势，加快推进科研体制改革，激发创新主体活力，构建产学研紧密衔接的创新格局；要加速推动信息领域核心技术突破，加快推进网络信息技术自主创新；加强科技安全体系建设和能力建设，提高创新体系整体效能。

第二，要从技术安全观的角度，形成一系列提高金融科技安全能力的策略。坚持市场化导向，以企业为主体，完善市场机制，激发市场主体活力，引导科技和互联网企业、金融机构在技术安全观的大局之下，构建起科学有效的安全策略，包括网络安全治理、云平台、移动互联、大数据安全、应用程序，以及智能风控等。