计算机安全管理在防范金融科技风险的作用探究

Exploration of the Role of Computer Security Management in Preventing Financial Technology Risks

李君

Jun Li

北京睿智融科控股股份有限公司　中国·北京 100000

Beijing Ruizhi Rongke Holdings Co., Ltd., Beijing, 100000, China

摘　要：为强化计算机安全化管理，降低金融科技风险，促使金融行业的健康、可持续发展，论文介绍计算机安全管理概念和金融科技风险表现形式，并分析了计算机安全管理在防范金融科技风险中的重要性，同时，从强化计算机软件系统管理、强化对计算机硬件管理、加强对计算机网络安全防范等多个方面入手，为实现对计算机安全管理的有效防范提出具有建设性的建议。希望通过这次研究，为相关人员提供有效的借鉴和参考。

Abstract: In order to strengthen computer security management, reduce financial technology risks, and promote the healthy and sustainable development of the financial industry, this article introduces the concept of computer security management and the manifestations of financial technology risks, and analyzes the importance of computer security management in preventing financial technology risks. At the same time, from strengthening computer software system management, strengthening computer hardware management To strengthen the prevention of computer network security and other aspects, constructive suggestions are proposed to achieve effective prevention of computer security management. I hope to provide effective reference and guidance for relevant personnel through this study.

关键词：计算机安全管理；金融科技；风险防范；作用

Keywords: computer security management; financial technology; risk prevention; effect

DOI: 10.12346/csai.v2i1.9107

1 引言

在信息时代背景下，计算机被广泛地应用于金融行业中，促使金融业向金融电子化方向不断发展。但是，计算机相当于一把双刃剑，在给金融行业发展提供一定的便利的同时，还存在一系列金融科技风险，严重危及人们的人身安全和财务安全[1]。而计算机安全管理在金融科技风险防范中发挥出重要作用，通过强化计算机安全管理，不仅可以实现对金融科技的有效保护，降低其安全风险，还能提高金融行业的发展水平。所以，为更好地防范金融科技风险，强化计算机安全管理显得尤为重要。

2 金融科技风险概述

2.1 金融科技风险内涵

金融科技风险主要是指金融行业计算机应用期间，出现的一系列安全风险。这说明金融行业借助计算机网络技术进行金融管理所出现的安全风险。在传统纸质金融时代下，金融机构管理相当严格，外在风险因素无法直接危及金融行业的安全性，这使得传统金融行业具有较高的安全性和可靠性。但是，在电子化金融时代背景下，由于大量应用计算机技术和网络通讯手段，降低金融行业的安全系数。在这样的情况下，金融行业很容易受到外界风险因素破坏，进而引发信息泄露、系统死机瘫痪、网络犯罪等一系列金融科技风险。同时，金融行业在实际发展期间，业务种类越来越丰富，这就增加业务复杂度，此时，金融机构越来越依赖和使用交易系统，为客户提供更加优质的金融服务。

2.2 金融科技风险表现形式

2.2.1 金融机构计算机安全管理意识不强

对于金融机构而言，其计算机安全管理意识相对比较薄

【作者简介】李君（1983-），女，中国深圳人，硕士，工程师，从事计算机和信息研究（金融科技）。

弱，管理方式缺乏一定的严格性，同时，缺乏系统完善的管控制度应用。此外，在金融机构中，拥有计算机安全管理相关专业知识的人才数量少之又少，又加上计算机安全管理技术比较落后，金融科技安全战略还有待更新，难以满足金融业务发展需求 [2]。此外，金融机构缺乏对计算机安全技术人才的培训，导致相关技术人员网络安全意识相对比较薄弱，无法有效地评估和应急处理计算机安全风险。部分金融机构相关业务人员忽视计算机应用安全性，缺乏对账户密码、重要业务数据的有效保护，这为网络病毒、不法分子恶意攻击计算机信息系统提供了可乘之机。

2.2.2 存在不法分子入侵系统和网络诈骗行为

部分非法用户借助病毒，运用网络攻击等技术手段，对金融机构计算机信息系统进行恶意入侵和攻击，从而窃取金融机构用户账户密码、重要业务数据，从而引发一系列金融科技安全隐患问题 [3]。在信息技术的迅猛发展下，目前金融机构为大量客户群体提供多种多样的外部接入模式，极大地提高客户金融服务体验。例如：专线、互联网的接入和使用。同时，在金融机构中，网络黑客通过对外部客户系统进行入侵和攻击，从而达到窃取金融机构计算机系统重要资源的目的 [4]。在移动互联网技术的不断推广和普及下，金融机构应用计算机网络技术，可以提高其服务质量，但是，引发了网络诈骗、网络犯罪等多种金融科技风险。例如：不法分子通过采用植入木马的方式，恶意入侵和窃取金融机构重要客户资源，这为交易所入口管控技术的运用造成严重的影响。

2.2.3 金融机构计算机安全管控系统不够完善

现阶段，金融机构在进行计算机安全管理期间，过度依赖相关人员的技术能力和安全意识，缺乏对计算机安全管控系统的运用，这就增加金融科技风险。此外，金融机构在研发和引进计算机电子业务系统期间，由于过于追求业务系统上线高效化，忽视对系统代码的调试和查看，没有做好对计算机的安全控制，同时，没有实时管控外包服务流程，导致外包服务存在一定的安全风险，这样一来，所开发的计算机信息系统难免会出现各种各样的安全漏洞问题，严重危及了金融机构客户财产的安全性 [5]。

3 计算机安全管理在防范金融科技风险中的重要性

3.1 金融电子化所涉及到的金融客户数量多

在进行金融电子化发展期间，通常会涉及到大量的金融客户，一旦出现金融科技风险，海量金融客户相关资料信息因被网络病毒、黑客、不法分子恶意攻击和入侵而出现丢失。泄露等风险，严重危及金融客户的财产安全，致使金融市场变得愈加混乱。而交易所通常涉及到大量的会员信息，一旦会员信息因保管不当会出现泄露、丢失等风险，不利于会员单位相关业务的有效开展 [6]。

3.2 金融行业向来就是不法分子攻击目标

在金融电子化时代背景下，由于计算机信息系统过于脆弱，很容易被网络病毒、不法分子恶意入侵和破坏，导致金融相关信息出现丢失、泄露等风险。交易所接入和使用大量的计算机信息系统，很容易遭到不法分子入侵和攻击 [7]。目前，黑客入侵技术变得越来越先进和高明，出现大量的高级持续性威胁（Advanced Persistent Threat，APT），这给金融科技造成一定的安全风险。

3.3 计算机犯罪已经成为一种趋势

在众多犯罪中，计算机犯罪所赚取的财富更多。因此，不法分子面对这种极大的诱惑，很容易借助计算机信息系统，对金融行业相关信息进行攻击和窃取。在这样的背景下，强化对金融行业计算机的保护，防范和监控金融行业计算机犯罪显得尤为重要。结合国内各大威胁情报相关记载内容，不难发现我国所遭受的网络攻击来自国内外不法分子。交易所作为一种庞大的金融机构，在实际管理和经营期间，同样面临计算机信息系统被恶意攻击风险。因此，强化计算机安全管理，降低金融科技风险相当重要 [8]。

3.4 金融电子化发展是国家信息安全建设的重要保障

金融行业在国家经济发展占据着举足轻重的地位，一旦金融行业出现一系列安全漏洞，不仅会降低整个金融行业经营水平，还会对国家经济发展产生一定的阻碍，甚至还会对国家政局的发展产生不良影响。交易所通过国务院正式批准后，借助中国人民银行力量进行建设，我国主要从事黄金交易量最近几年位居全球首位。所以，强化交易所计算机安全化管理，在促使国家金融市场的健康、可持续发展方面发挥出重要作用。

4 计算机安全管理在金融科技风险中的防范措施

4.1 强化计算机软件系统管理

使用安全可靠的软件系统，可以实现对银行、客户资金的有效保护。对于银行而言，在进行开发或者采购计算机软件时，首先，要保证计算机软件安全系数。同时，还要使用加密技术，提高系统数据的完整性和安全性。在银行计算机系统中，数据是安全防范的关键和核心，所以，严格设置数据库各个级别访问权限，并强化对等级管理制度的实施，同时，还要定期修改密码 [9]。此外，还要强化对操作系统级别的防范处理。由专业人员对其进行系统化管理，避免不法分子恶意攻击和入侵操作系统，从而实现对重要数据的有效保护，特别是在进行应用终端操作时，要重视对相关权限的设置。最后，还要定期查杀和处理计算机软件，防止计算机因被网络病毒、黑客恶意入侵而出现系统死机、崩溃等现象。同时，还要强化对杀毒软件和相关技术的创新，不断地优化和完善病毒检测方案，最大限度地提高计算机软件系统运行的可靠性和安全性。

4.2 强化对计算机硬件管理

在信息化社会不断发展下，计算机应运而生。计算机具有精确度高、运行环境配置高等特点。所以，相关管理人员要定期检查计算机硬件设备，一旦发现损坏的零部件，要对其进行及时更换或者维修，降低安全事故出现概率[10]。首先，做好对硬件环境的屏蔽。其屏蔽对象除了涉及到静电外，还涉及到磁屏、电磁。其中，在屏蔽电磁时，由于电磁主要来源于电磁场、电源系统等，其造成危害比较严重。为保证电磁屏蔽效果，所使用的计算机要尽可能地远离电磁场源位置，同时，还要重视对防静电活动底板的铺设和使用。此外，还要重视对双机备份措施的运用。通常情况下，在进行双机备份时，要确保主机型号完全相同、系统控制外设能力相同。在使用通讯控制设备时，要运用电子开关，对其进行自动化切换，确保供电环境的稳定性和安全性，只有这样，才能为计算机硬件运行持续、稳定地供电。最后，重视对计算机硬件环境的科学化配置和优化，从而达到防范金融科技风险的目的。金融机构在日常管理和经营中，要科学地规划计算机硬件配置环境，确保其环境完全满足国家相关标准和要求，只有这样，才能实现对计算机安全化管理，将金融科技风险降到最低，为更好地保障金融行业重要信息资源的安全性和财务的安全性打下坚实的基础。

4.3 加强对计算机网络安全防范

为提高计算机网络安全防范能力，首先，要强化对网络硬件设备保护，降低电磁辐射出现风险。通常情况下，不法分子会采用截取双绞、电磁辐射等方式，恶意盗取数据信息，以达到非法窃听网络传输介质的目的。而计算机光缆转换器和接口位置一旦出现安全漏洞，为不法分子恶意攻击计算机网络提供了可乘之机。所以，当系统数据在传输或者存储期间，要重视对这些数据的加密保护。其次，要强化对网络黑客的关注和控制。计算机系统很容易被网络病毒、网络黑客、不法分子恶意攻击和破坏，这就要求金融机构要实时监管网络信息安全。并严格监控用户登录和操作系统行为，同时，还要采用用户权限设置的方式，有效控制用户的计算机系统，降低网络病毒、网络黑客、不法分子恶意攻击风险。此外，金融机构要运用身份认证等相关技术，管控计算机系统登录操作行为，并采用设置双人操作模式，对重要信息进行保护。最后，还要实时扫描计算机系统漏洞，一旦出现金融科技风险，要对其进行及时修复和处理，只有这样，才能提高计算机网络安全防范能力，将金融科技风险降到最低，促使金融行业安全化、可持续化发展。

4.4 增强内部安全机制控制力度

在金融机构中，要想实现对金融科技风险的有效防范，必须强化对内部安全机制的控制。首先，金融机构要强化对人员的系统化管理，避免非授权人员直接登录和访问计算机系统，同时，还要定期考核相关技术人员的计算机安全管理能力。另外，当金融机构需要更换工作人员时，要及时修改计算机系统登录密码，并实时监督和管控交接工作。其次，增强计算机安全技术管理力度。结合系统软件安全化管理需求，制定系统、完善的安全机制，降低金融科技安全事故出现概率。此外，还要采用职能分离的方式，管控计算机系统运维人员和开发人员，并实时监督和管理外包服务流程，从源头上降低金融科技风险，从而更好地保障金融机构的信息安全和财务安全。

5 结语

综上所述，金融电子化逐渐成为金融行业未来发展趋势，金融机构在使用计算机系统进行金融科技管理时，难免会遇到金融科技风险，所以，要想提高金融机构计算机系统运行的安全性和稳定性，降低金融科技风险，必须强化计算机安全管理工作的有效开展，有效地管理计算机软件系统、计算机硬件，提高计算机网络安全防范能力，增强内部安全机制控制力度，只有这样，才能促使金融行业向安全化、稳定化方向不断发展。

参考文献

[1] 曹心蕊.加强计算机安全管理防范金融科技风险研究[J].南方农机,2019,50(23):285.

[2] 侯建林.计算机安全管理在防范金融科技风险的作用探究[J].新金融世界,2019(7):69-70.

[3] 刘诗懿.商业银行金融科技应用的风险防范措施[J].全国流通经济,2023(5):153-156.

[4] 李勇光.金融科技与金融风险防范探讨[J].中国战略新兴产业,2023(2):23-25.

[5] 夏敏,詹珊珊,张龙健,等.金融科技风险的传播与防范研究——以河南村镇银行为例[J].科技与金融,2023(5):89-92.

[6] 王汝芳.平衡好鼓励发展和防范风险关系,促进金融科技更好服务实体经济[J].民主与科学,2023(1):47-49.

[7] 李秀云.探究金融科技在供应链金融中的风险防范[J].中国科技投资,2023(11):39-41.

[8] 赵霞.网络安全技术在计算机安全管理中的应用分析[J].通讯世界,2023,30(2):49-51.

[9] 郑永奇.计算机安全管理的数据备份和恢复技术应用[J].无线互联科技,2022,19(5):100-101.

[10] 李宁.简析计算机安全管理中云计算技术的应用[J].软件,2022,43(2):160-162.