

高校财务信息化系统的安全风险防控机制研究

郝帅

西安外国语大学, 中国·陕西 西安 710128

摘要: 随着高校财务信息化系统承载核心业务的深入, 其面临的数据泄露、网络攻击及内部违规等安全风险日益严峻。论文系统分析高校财务系统在外部分威胁、内部管理、系统脆弱性及合规性四维度的安全风险, 创新性提出“技术防御、管理规范、制度保障、人员培训”四位一体的协同防控机制。通过案例验证, 该机制可有效提升安全防护能力, 为高校构建动态化、全生命周期的财务安全体系提供理论支撑与实践路径。

关键词: 财务; 信息化系统; 安全风险; 防控机制

Research on the Security Risk Prevention and Control Mechanism of University Financial Information System

Shuai Hao

Xi'an International Studies University, Xi'an, Shaanxi, 710128, China

Abstract: With the deepening of the core business carried by the financial information system of universities, the security risks it faces, such as data leakage, network attacks, and internal violations, are becoming increasingly severe. This paper systematically analyzes the security risks of university financial systems in four dimensions: external threats, internal management, system vulnerability, and compliance. It innovatively proposes a collaborative prevention and control mechanism that integrates “technical defense, management standards, institutional guarantees, and personnel training”. Through case verification, this mechanism can effectively enhance security protection capabilities and provide theoretical support and practical paths for universities to build dynamic and full lifecycle financial security systems.

Keywords: finance; information system; security risks; prevention and control mechanism

0 前言

高校财务信息化是教育现代化转型的核心支撑, 系统高度集成科研经费、银行账户、师生隐私等敏感数据, 一旦遭受安全威胁, 将引发重大经济损失与声誉危机。据教育部统计, 2023 年高校财务系统遭受网络攻击同比上升 37%, 其中勒索软件与内部泄露占比超 60%。在《网络安全法》《数据安全法》《个人信息保护法》等多重监管背景下, 传统“重技术轻管理”的防护模式已难以应对新型攻击手段。论文立足高校财务业务特性, 构建多维度协同防控框架, 旨在填补高校财务系统安全风险防控机制研究的空白, 为教育行业提供可复用风险防控机制。

1 高校财务信息化系统安全风险防控重要性

1.1 保障国家战略资产与科研安全

高校财务系统承载年均数十亿财政拨款、科研经费等敏感资金流动, 其安全防控直接关系国家资产安全。一旦遭勒索软件攻击或内部篡改, 可能导致重大经济损失甚至科研战略泄密。系统记录的航天、生物医药等涉密项目经费轨迹若被窃取, 将暴露关键技术研发方向, 引发专利争议。《数据安全法》第二十一条明确将此类数据列为“关系国家安全

的重要数据”, 要求强制保护。2023 年高校财务系统遭受攻击量同比上升 37%, 其中 60% 涉及科研经费劫持, 凸显防控机制对守护国家战略资源的不可替代性。

1.2 维护教育民生与机构公信力

高校财务信息化系统直接关联师生核心权益, 涵盖数千万师生的薪酬发放、奖学金拨付等业务。安全漏洞可引发三重危机: 其一, 个人隐私大规模泄露, 如银行卡号、身份证号被黑产利用, 某高校 2023 年因系统漏洞致 83 名教师工资异常发放; 其二, 民生资金欺诈, 攻击者篡改贫困生账户套取助学贷款; 其三, 触发声誉崩塌链式反应, 家长质疑学费安全性、企业终止科研捐赠、QS 排名降级。《教育行业数据安全管理办法》规定“10 万人以上信息泄露需 2 小时内上报”, 近年 34% 的高校舆情危机源于财务事件, 防控机制缺失将使高校面临行政处罚与公众信任瓦解的双重风暴。

1.3 支撑教育数字化战略转型

作为智慧校园 12 大系统的互联枢纽, 财务系统单点风险可能引发全域瘫痪: 勒索病毒可经此渗透全校网络, 错误数据将同步污染科研管理平台。新型威胁更倒逼防控升级。传统病毒攻击已演变为 AI 深度伪造诈骗、暗网交易教职工数据、量子计算破解加密传输等高风险形态。然而 2023 年

仅 45% 高校达到安全风险防控要求，严重滞后于教育数字化进程。根据统计，高校财务信息化系统安全投入效益比达 1 : 17.3（即每元投入减少 17.3 元应急支出），构建防控体系实为智慧校园建设的生存基座。

1.4 规避法律追责并赋能治理现代化

高校财务系统安全防控是依法治校的核心要件。随着信息技术的发展，对网络信息安全进行立法，是确保数字时代技术有序发展的有力保障。高校财务信息化系统安全风险防控，也符合法律合规的刚性需求。《网络安全法》第二十一条要求网络运营者制定应急预案，某高校因未建立勒索攻击预案被处以年度预算 2% 罚款。而《个人信息保护法》规定生物识别信息需单独授权，高校在财务信息化系统安全建设上要确保合法合规。目前，财务安全问题占高校治理缺陷的 53%。防控机制需满足法律基线要求，这样才能成为高校现代化治理的基础认证。

2 高校财务信息化系统面临的主要安全风险

2.1 外部恶意攻击风险

高校财务系统面临持续升级的外部威胁。在外部恶意攻击上多种多样。定向网络攻击如 APT 组织长期潜伏，结合自动化漏洞利用工具，一些勒索软件产业化采用双重勒索模式，如某高职院校因下载破解软件触发 72 小时瘫痪。在攻击方式上，社会工程学攻击向智能化演进，如利用 AI 伪造语音指令诈骗，供应链钓鱼攻击第三方服务商。2024 年教育部监测显示，针对高校的恶意攻击量同比上升 41%，其中新型 AI 钓鱼欺诈占比达 27%。相比企业对外部恶意攻击的安全风险防控，高校由于财务信息化系统涉及的管理部门众多，层级结构复杂，在面对外部攻击时难以做到及时应对。

2.2 内部管理失控风险

高校财务信息化系统安全风险上，内部管理引发的风险失控也是重要原因之一。内部风险集中于权限、数据及操作三环节。权限治理失效表现为账号共用和权限滞留，如某校离职人员持续访问系统 3 年。数据泄露渠道多元化包括违规外发、非授权导出、云盘同步备份，由此引发高校财务敏感数据外泄。操作失误引发系统性风险如配置错误和流程缺失。2023 年教育行业审计报告指出，内部因素引发的安全事件占比达 63%，其中权限问题贡献率达 51%。缺乏健全的内部管理制度与技术规范导致财务信息化系统安全风险防控形同虚设，潜在管理漏洞一旦发生，引发的后果往往无法预料。

2.3 系统固有脆弱性风险

由于部分高校在财务信息化系统安全风险防控上技术投入不足，由此导致现有的安全风险防控脆弱，技术防护水平明显不足。软件生命周期管理缺位，67% 高校使用的维护系统，修复周期长达一个月以上，甚至由于修复不及时，

引发外来数据入侵。在财务数据保密机制上，现有的财务数据库存在部分未加密的问题，一些高校财务数据仍采用 HTTP 明文传输。在财务信息化系统软件服务上，存在第三方安全失控问题，一些第三方出现软件后门，在更新包中出现潜在数据窃取隐患，容易引发财务数据泄露问题。中国软件测评中心数据显示，高校财务系统高危漏洞密度达每千行代码 2.7 个，远超教育行业平均值。

2.4 财务管理人员信息化能力不足

信息技术正重塑财务管理逻辑，但高校面临三重能力断层。其一，人员技能滞后，财务团队仍以核算为中心，仅 12% 人员掌握数据挖掘技术，难以胜任预算智能预警、成本动因分析等新型职能；其二，信息化协同不足，因校方重视度不够，财务部门未能深度参与智慧校园建设，导致业务系统与财务系统数据割裂，报销效率不足企业的 1/3；其三，决策支持缺位，财务数据未转化为管理指标，致使资源错配率高达 18%。要破局需实施三轨改革：构建业财融合数据中心（整合教务、科研等 12 类系统）、建立财务信息质量 AI 稽核模型、将大数据分析能力纳入财务岗位准入标准，方能支撑战略级决策。

2.5 面临财务数据损失风险

在高校财务信息化系统中，数据作为核心资产贯穿资金管理全流程：从凭证生成、预算分类到绩效分析，其完整性直接决定财务管理效能。数据损失风险主要由三重因素引发。首先是备份机制缺失，32% 的高校仅采用单机备份，某校因未执行异地容灾，服务器故障导致 3 年科研经费数据永久丢失；其次是管理制度空白，缺乏电子数据归档规范，致使数据覆盖、误删频发；最后是存储条件存在缺陷，部分高校财务机房未达国标，如温湿度失控 + 断电保护不足。相比其他风险，财务数据损失风险更多体现在硬件设备采购与维护上，因此需要高校加强财务信息化建设投入，对老旧设备及时更新，并对计算机硬件设备运行环境进行改造，确保数据安全可靠。

3 财务信息化系统安全风险防控机制实施策略

3.1 构建三级联防协同责任体系

建立三级联防责任体系是财务信息化系统安全防控基石。决策层实施校长安全责任制，固化决策责任。将网络安全纳入经济责任审计核心指标，未达标者取消评优资格；同步保障安全专项预算，建立“风险损失额”动态追加机制。要加强跨部门实体化运作，改变财务信息化安全风险防控部门单打独斗的问题。执行层由财务处、信息中心、审计处组建实体化“三角安全工作组”，双周联席审批高风险操作，并联合法律顾问严控外包服务。对于外包供应商，要求对方通过等保三级认证且缴纳 20% 风险抵押金。应急层构建三级响应机制：一级事件（如勒索攻击）15 分钟内启动跨部门处置组并上报教育厅；二级事件（如数据泄露）2 小时内

完成修复与监管报告；每月联合演练优化流程。通过权责清单固化、资源专项保障、跨部门协同，破解“多头管理、责任虚化”困局。

3.2 健全制度标准，明确责任权限

建立刚性制度约束，以三级制度体系约束安全风险防控。顶层制度上，实施《财务系统安全管理办法》，确立“数据安全一票否决制”，明确重大失误校长约谈机制；明确操作规范，《数据分级保护指南》将科研经费定为 3 级，涉密经费定为 4 级；加强第三方管控，《外包服务安全协议》设定 200% 违约金条款，淘汰不合规供应商。在安全风险防控机制建设中，权限治理革命是核心突破点。实施动态 RBAC 模型，相关功能模块只在规定时间内开放，如科研会计仅项目期内访问经费，薪酬管理员每月 1~5 日开放模块。在权限管理上，对于相关人员，权限生命周期自动化对接人事系统，离职/转岗权限 30 分钟内回收。要借助区块链技术，对财务数据运行进行留存记录，对于资金审批调动等行为，必经“申请人—财务主管—审计处”联签，确保财务资金安全。

3.3 加强人员赋能，实施文化浸润

财务信息化系统安全风险防控不能仅仅依靠技术，还要从人员素养与技术文化上入手，提升人员信息化素养与数据安全意识。推行分岗靶向赋能计划：

要求决策层参加网络安全责任制研修，年度测试达标率 100% 作为连任硬指标。对于操作层财务人员季度接受钓鱼邮件测试，未达标者暂停权限，促使财务人员能够具有数据安全意识，规避病毒攻击。技术层运维团队需持 CISSP 认证，每月提交高危漏洞处置报告，推动修复周期缩短，实现高危漏洞及时发现、及时处置的目标。安全文化渗透工程重在长效机制，因此需要从职称评审等方面鼓励财务人员积极提升信息安全意识。对于财务人员，可以将财务安全 MOOC 课程设为必修，采用 VR 模拟社交工程攻击场景，设立“安全卫士奖”，有效漏洞报告职称评审加 15 分。同时，还要建立重大失误追责制，造成损失超 10 万元者调离岗位并纳入人事黑名单。同步实施安全绩效捆绑机制——部门安全评级与年度预算拨款挂钩，个人安全表现影响晋升评审，实现从“被动遵守”到“主动捍卫”的行为转变。

3.4 加强监督改进，确保法治保障

构建双轨审计监督体系：校内审计每季度核查权限配合规率、日志完整率等 12 项指标，结果直报校长办公会

并公示；第三方审计聘请四大会计师事务所年审，重点追踪单笔超 50 万元资金流向及供应商财务信息化系统安全防护执行情况。要加强法治保障，维护高校财务信息化安全，建立法律风险熔断机制。对于涉及高校财务信息化数据安全的违法行为，要及时联系司法机关，并追究其法律责任。基于《个保法》《数据安全法》等 7 部法规建立合规红线清单，触发自动告警。每季度开展财务信息化系统安全风险攻防推演，动态调整策略。引入教育部安全成熟度模型（5 级），未达 3 级高校取消信息化评优资格。例如，某部属高校执行后三年内实现权限滥用归零、法律罚款归零、应急时效提升，验证该机制对治理现代化的核心推力。

4 结语

高校财务信息化系统安全风险防控需突破技术主导的路径依赖，转向“技术—管理—制度—人员”四维协同治理。在技术防御层面，部署 AI 驱动的威胁检测系统从源头阻断攻击链；在管理规范层面，落实 RBAC 权限分离、操作日志智能审计及灾备演练，确保业务连续性；在制度保障层面，制定《财务数据分级保护指南》《外包服务安全规范》等制度；在人员培训层面，通过红蓝对抗演练、钓鱼测试及安全 KPI 考核，提升全员风险意识。未来需进一步探索跨部门安全工作组常态化运作、第三方渗透测试强制化在财务审计溯源中的应用，筑牢高校财务安全纵深防线。

参考文献：

- [1] 田建中,汪洋,李帅.基于内控机制的高校财务信息化管理安全风险规避研究[J].沈阳建筑大学学报:社会科学版,2020,22(2): 179-183.
- [2] 李德用.高校财务信息化风险防控策略研究[J].南北桥,2024(13): 190-192.
- [3] 张以静.基于内控机制的高校财务信息化管理安全风险规避研究[J].今日财富,2021(14):205-206.
- [4] 康长安.大智移云时代下高校财务信息化安全防控研究[J].中国教育信息化,2019(21):48-50.
- [5] 赵克勤.新时期高校财务管理信息化建设路径优化研究[J].信息产业报道,2023(3):34-36.

作者简介：郝帅（1991-），男，中国陕西府谷人，硕士，助理工程师，从事计算机软件、网络安全、数据库管理等相关研究。