 DOI: https://doi.org/10.12349/iser.v7i5.10515

Construction and Exploration of a Collaborative “Intelligent Governance” Mechanism for Cybersecurity in Higher Education Institution

Xiaoling Liao[1] Tianshu Chen[2]

1. Guilin Normal University, Guilin, Guangxi, 541119, China
2. Nanning Institute of Technology, Guilin, Guangxi, 541006, China

Abstract

In the process of digital transformation in higher education, cybersecurity governance commonly faces the practical dilemma of disconnect between technology application and management governance. Based on the theory of collaborative governance and starting from frontline management practice, this paper constructs a data-driven, process-linked, and education-supported collaborative "intelligent governance" mechanism for cybersecurity. The study suggests that the current cybersecurity efforts in higher education institutions exhibit a characteristic of "strong in factor input, weak in systematic integration" across the three dimensions of technology, management, and education. The fragmentation among these three aspects is the key bottleneck restricting the improvement of governance effectiveness. The collaborative mechanism proposed in this paper, through three sub-mechanisms-namely, the "data-decision" linkage, "process-education" coordination, and effectiveness evaluation and iteration-establishes a complete management closed-loop that connects risk discovery, responsibility implementation, and capability enhancement. Leveraging the lightweight tool of email workflows, this mechanism is characterized by low cost, replicability, and ease of promotion, offering both theoretical reference and practical pathways for upgrading cybersecurity governance in similar institutions.

Keywords

university cybersecurity; collaborative governance; data-driven; process management; smart campus

高校网络安全协同“智治”机制的构建与探索

廖小玲[1] 陈天树[2]

1.桂林师范学院，中国·广西 桂林 541199
2.南宁理工学院，中国·广西 桂林 541006

摘要

在高校教育数字化转型进程中,网络安全治理普遍面临技术应用与管理治理脱节的现实困境.本文基于协同治理理论,从一线管理实践出发,构建了一套以数据为驱动,以流程为纽带,以教育为支撑的网络安全协同“智治”机制.研究认为,当前高校网络安全工作在技术,管理,教育三个维度上呈现“强于要素投入,弱于体系融合”的特征,三者之间的割裂是制约治理效能提升的关键瓶颈。本文提出的协同机制通过“数据-决策”衔接、“流程-教育”协同、效果评估与迭代三个子机制,打通了从风险发现到责任落实再到能力提升的完整管理闭环.该机制依托邮件工作流这一轻量化工具,具有低成本、可复制、易推广的特点,可为同类院校的网络安全治理升级提供理论参考与实践路径。

关键词

高校网络安全；协同治理；数据驱动；流程管理；智慧校园

【基金项目】2024年中国高校产学研创新基金—新一代信息技术创新项目，项目名称:智慧校园中网络安全体系构建与应用实践–以桂林师范学院为例 项目编号：2024IT272
【作者简介】廖小玲（1991–），女，中国广西桂林人，硕士，信息系统项目管理师，从事通信与网络安全研究。

1 引言

随着国家教育数字化战略行动的深入推进,我国高校信息化建设已全面迈入以数据融合,智能应用为特征的智慧校园新阶段.在这一进程中,校园网络规模持续扩大,信息系统日益复杂,安全风险类型不断翻新,传统的以单一部门为核心的孤立管理模式，越来越难以应对这种动态、复杂的安全环境。

然而,当前安全治理的深层瓶颈,并不在于技术和资金的投入不足,而在于技术,管理,教育三个维度的工作各自为政,平行推进,虽有交集却未能深度融合.技术平台产生的海量数据无法转化为管理决策的依据,管理制度难以嵌入日常业务流程,安全教育与师生实际风险场景严重脱节。三者之间缺乏一个能够真正打通壁垒的协同机制,使得安全治理始终停留在“要素投入”层面,难以形成体系化的治理能力。

基于上述现实问题，本文尝试回答这样一个核心命题:在现有技术条件和组织架构下,如何构建一个能够打通技术,管理与教育壁垒的协同治理机制,实现安全治理从“被动响应,经验驱动”向“主动预警,数据驱动”的根本性转变?围绕这一问题,本文首先系统分析当前高校网络安全治理的现状与短板,进而提出协同“智治”机制的理论框架与核心构成，最后探讨其实施路径与推广价值。

2 高校网络安全治理的现实审视：技术、管理与教育的三重割裂

当前,我国高校网络安全建设在政策驱动与现实需求的双重推动下,已形成明确的发展脉络,但在系统性协同方面仍存在显著短板.整体上可概括为“强于要素投入,弱于体系融合”.以下从技术,管理,教育三个维度分别审视。

2.1 技术层面：从边界防护到主动感知，但数据价值亟待挖掘

国内高校网络安全建设正经历从传统被动防御向主动、动态防御体系的转型.早期研究与实践集中于防火墙,入侵检测等边界防护技术。随着《中华人民共和国网络安全法》、等保2.0的施行，研究重点逐步转向构建覆盖“感知,预警,处置”的网络安全态势感知平台.然而,大量研究也指出,这些平台往往止步于“态势可视化”,其产生的海量告警与资产数据与后续的管理动作,责任归属严重脱节,形成了所谓“数据堰塞湖”.数据如何精准转化为可执行的管理指令,而非仅仅呈现在大屏上,成为技术层面向管理效能转化的关键瓶颈。

2.2 管理层面：从合规导向到责任落实，但制度柔性不足

管理研究高度围绕网络安全等级保护制度展开研究.高校普遍建立了较为完备的静态制度文本,但在动态执行层面问题突出.制度条款往往刚性有余而柔性不足,难以适配高校科研场景中大量临时性,创新性信息系统上线需求，导致“私搭乱建”与“制度规避”并存。

更为关键的是，虽然“网络安全责任制”被反复强调,但由于缺乏将资产,风险与具体责任人动态绑定的有效技术手段和流程,责任常常无法穿透组织层级落实到“末梢”,使得制度悬空,执行力层层衰减.制度文本写得再漂亮,如果责任落不到具体人头,最终就是一纸空文.从国际视野来看,网络安全研究已超越单纯的技术对抗,进入以“人”为核心,以“流程”为关键,以“数据”为燃料的新阶段。

2.3 教育层面：从知识灌输到形式创新，但效果评估薄弱

国内高校网络安全意识教育研究近年来在形式上积极探索.实证研究指出,当前教育内容的同质化问题严重,多聚焦于通用性钓鱼邮件,密码安全等常识,与本校信息化系统,科研数据管理,物联网设备等师生日常接触的具体风险场景严重脱节，导致“学用分离”。

2.4 小结：三个维度的“竖井”特征

综上所述，国内高校网络安全研究呈现明显的“竖井”特征.技术,管理,教育三个领域的研究与实践平行推进,虽有交集但未能深度融合.学者们普遍认识到协同的必要性，但现有成果多停留在理念倡导或宏观框架描述,对于三者之间如何通过具体的,可操作的数字化流程进行信息交换,任务触发与反馈闭环,尚缺乏深入,细致的机理分析与实证模型.这一研究空白,正是本文试图填补的切入点。

3 协同“智治”机制的构建：以数据为驱动、以流程为纽带、以教育为支撑

针对上述“技管教”脱节的现实困境,本文提出并构建一套以数据为驱动,以流程为纽带,以教育为支撑的网络安全协同“智治”机制.该机制的核心在于:将孤立,静态的技术监控数据,转化为驱动组织行动的结构化指令与精准化教育资源,并通过一套标准化的线上流程将其串联,形成从风险发现到责任落实,再到能力提升的完整管理闭环。

3.1“数据－决策”衔接机制：打通技术数据至管理决策的通道

这一子机制旨在解决“技术数据出不了机房”的问题.核心做法是通过数据标准化与研判制度化,将原始安全告警转化为可执行的“管理清单”.具体而言,设计《网络安全风险周报》模板,将专业的技术扫描结果转化为包含归属部门,责任人,风险等级与处置建议的结构化报告,实现技术语言向管理语言的转译.同时,建立定期安全例会制度，明确技术、管理各方在报告审议、风险评估,任务分类与派发中的角色与流程,确保每项风险均能进入规范化处置程序。

这一机制的价值在于：通过“标准化报告+制度化研判”,建立稳定,可靠的转化通道,确保每一次重要的技术发现都能“出机房,上会议,定任务,落人头”,从源头破解数据沉睡与责任虚化的问题.这一步看似简单,实则是打通“技管脱节”的关键——只有把技术发现变成可执行的管理任务,后续的流程才有意义。

3.2“流程－教育”协同机制：将管理流程与安全教育深度融合

这一子机制聚焦于解决“安全教育入不了心”的问题.核心思路是:通过设计智能工作流,使每项管理任务同时成为一次精准的教育干预.具体开发了三类标准化邮件模板：

第一类是“整改通知单”.收到邮件的部门或个人,不仅会看到需要整改什么,何时完成,还会看到具体的修复步骤说明和知识库链接.这意味着收到邮件的同时,也就收到了解决问题的“教程”。

第二类是“风险预警提示”。这类邮件发给全体师生,内容不是笼统的“注意安全”,而是结合近期校内发生的真实案例(脱敏处理),告知师生这个风险具体长什么样,会通过

什么渠道出现,点进去会有什么后果,如果不小心点了该怎么办。

第三类是“制度修订建议”.这类邮件发给管理层,当运行中发现某些制度条款难以执行时,整理成有数据支撑的建议报告,正式提交给决策部门,将管理优化也纳入流程。

这三类邮件的共同点是:它们都是流程的一部分,而不是额外的教育“任务”。收件人不需要专门抽时间学习,在完成日常工作的同时,就已经完成了学习.本文将其概括为“流程即教育，工单即课本”的理念。

3.3 效果评估与迭代机制：驱动治理体系的自我演进

这一子机制旨在解决“制度如何自我完善”的问题.核心做法是建立涵盖效率与效果的双维度关键绩效指标体系.效率指标包括平均修复时间,邮件回复率等;效果指标包括模拟钓鱼测试点击率、制度知晓度等。

通过定期采集与分析数据,识别机制瓶颈,例如针对修复延迟优化教育内容,针对知晓度不足启动专项宣贯流程,形成“监测—评估—优化”的持续迭代循环,推动机制动态完善.这一机制的价值在于:制度不再是僵化的文本,而是通过运行产生的过程与结果数据,作为制度有效性评估的客观依据.通过“制度修订建议”这一标准化流程,将数据化的证据和优化建议正式提交至决策层,从而推动制度从“静态合规”向“动态适配”转变,形成“实践发现问题→数据支撑分析→流程建议→制度优化”的良性闭环。

4 实施路径与可行性分析

4.1 技术路线

本机制的实施以行动研究法为核心方法论,在真实的高校管理场景中开展实践介入.技术路线分为六个阶段:问题诊断与理论构建→机制设计与工具开发→试点运行与过程观察→数据采集与多元验证→效果评估与数据分析→机制优化与知识提炼.这一路线体现了从理论到实践,再从实践提炼理论的完整闭环。

4.2 实施中的关键问题

在实施过程中，需重点关注三个关键问题的解决：

第一,技术数据如何有效转化为可执行的管理任务?通过“标准化报告+制度化研判”建立稳定转化通道，破解数据沉睡与责任虚化。

第二,如何在常规行政流程中实现对不同角色的精准化安全教育?通过将情境化安全指引嵌入管理流程,根据接收者角色与具体事务提供精准、即刻可用的教育内容。

第三,如何建立轻量化的反馈闭环以驱动制度动态完善?通过“制度修订建议”标准化流程,将数据化证据和优化建议提交决策层,推动制度从“静态合规”向“动态适配”转变。

5 发展趋势与理论价值

结合当前研究进展与实际需求,国内高校网络安全治理正呈现出明确的发展趋势.治理模式从“部门孤立”向“流程协同”演进,安全治理不再仅是技术部门的职责,而是需要网络,业务,管理等多方参与,形成联防联控的合力.数据应用从“态势可视”向“流程驱动”深化,数据不再仅是用于展示的“看板”,而是逐步成为驱动管理决策、触发处置流程的关键要素.教育方式从“形式创新”向“精准嵌入”转型，教育将更多融入日常管理流程,通过任务工单,风险提示等方式，实现“流程即教育,处置即学习”.实施路径更加强调“轻量化落地”和“渐进式迭代”,在资源有限条件下,高校将更倾向于采用务实、渐进的建设思路。

本机制的理论价值主要体现在三个方面:第一,揭示了高校网络安全治理中“技管教”三重脱节的深层机理,丰富了教育数字化管理理论中对协同治理的认识;第二,构建了以数据为驱动,以流程为纽带,以教育为支撑的协同“智治”机制,为破解“要素投入强,体系融合弱”的困境提供了理论框架;第三,探索了“数据驱动治理”在高校场景的具体路径,拓展了协同治理理论在教育管理领域的应用边界。

6 结语

高校网络安全治理正走向以流程为中心,以数据为驱动,以教育为支撑的协同发展新阶段.本文提出的协同“智治”机制,针对“技术,管理,教育”三者脱节的深层问题，提供了一个系统性的解决方案.它通过一个具体的,可操作的数字化流程，将数据、流程与教育紧密串联,形成了从风险发现到责任落实,再到能力提升的完整管理闭环。

参考文献

[1] 王伟, 李华, 张明. 面向智慧校园的高校网络安全主动防御体系构建研究[J]. 网络空间安全,2021,12(5):45-51.

[2] 谢波, 王磊, 刘洋. 我国网络安全审查的制度发展、实践逻辑及完善路径[J]. 行政法学研究,2025(2):78-86.

[3] 张蕾, 陈晨, 赵敏. 数智化时代高校网络安全意识教育模式创新研究[J]. 中国教育信息化,2022,28(8):32-38.

[4] 李强, 王伟. 高校网络安全协同治理机制研究[J]. 现代教育技术,2023,33(4):56-63.

[5] Gartner. Hype Cycle for Security Operations, 2022[R]. Stamford: Gartner Inc, 2022.