文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

网络安全管理机制优化研究

闫涛
新疆维吾尔自治区人力资源和社会保障厅
DOI:10.32629/acair.v4i2.20387

[摘　要] 为破解当前网络安全管理中制度缺陷、技术碎片化、应急能力不足及人才短缺等问题,文章以ISO27001 PDCA循环、风险管控等理论为支撑,遵循系统性、风险导向等原则,从制度体系、技术防护、应急管理、人才培育四方面探索优化路径。通过构建闭环制度、协同技术体系、全流程应急机制及多层次人才模式,实现安全管理的动态适配与效能提升。研究结果为各组织应对新型网络威胁、保障数字化转型提供了切实可行的解决方案,对维护网络空间安全具有重要实践价值。
[关键词] 网络安全；管理机制；优化路径；风险管控
中图分类号：G250.72　文献标识码：A

Research on the Optimization of Network Security Management Mechanism

Tao Yan
Xinjiang Uygur Autonomous Region Department of Human Resources and Social Security
[Abstract] To address the problems existing in current network security management, such as institutional defects, fragmented technologies, insufficient emergency response capabilities and shortage of professionals, this paper takes theories including the ISO27001 PDCA cycle and risk management and control as support, follows principles of systematization and risk orientation, and explores optimization paths from four aspects: institutional system, technical protection, emergency management and talent cultivation. By establishing a closed-loop system, a collaborative technical system, a full-process emergency mechanism and a multi-level talent model, dynamic adaptation and efficiency improvement of security management are realized. The research results provide practical solutions for various organizations to cope with new network threats and ensure digital transformation, and have important practical value for safeguarding cybersecurity.
[Key words] network security; management mechanism; optimization path; risk management and control

引言

数字化浪潮推动着各行业加速迈向智能化、网络化,信息网络已成为支撑社会运行、经济发展与公共服务的核心基础设施。然而,网络攻击的专业化、组织化趋势日益明显,勒索软件、APT攻击等安全威胁持续蔓延,数据泄露、系统瘫痪等安全事件频发,给个人权益、企业运营乃至国家安全带来严峻挑战。现有网络安全管理机制在应对复杂多变的安全态势时,暴露出制度执行不到位、技术防护缺乏协同、应急响应效率低下等短板。在此背景下,优化网络安全管理机制,构建全方位、多层次、动态化的安全防护体系,成为破解当前网络安全困境的关键举措,对保障数字化转型顺利推进、维护网络空间秩序具有重要的现实意义。

1 网络安全管理机制的现状与核心问题

1.1制度体系存在结构性缺陷

部分组织的网络安全管理制度缺乏系统性设计,多以合规要求为导向,未能结合自身业务特点与风险状况形成个性化管理规范。制度内容存在交叉重叠或空白遗漏现象,对数据全生命周期、第三方合作等关键环节的安全管控缺乏明确细则。制度执行缺乏有效的监督考核机制,部分条款流于形式,难以落实到实际操作中。同时,制度更新滞后于技术发展与安全形势变化,对云计算、物联网等新技术场景的安全规范缺失,无法应对新型安全风险。

1.2技术防护呈现碎片化特征

现有技术防护措施多为分散部署,缺乏统一的统筹规划与协同联动机制。不同品牌、类型的安全设备各自为战,威胁情报无法有效共享,形成“信息孤岛”。边界防护、终端安全、数据加密等技术手段缺乏有机融合,难以构建立体防控体系。部分组织过度依赖单一防护技术,忽视了安全监测、漏洞修复等基础性工作,导致安全防护存在明显短板。此外,技术防护与管理流程脱节,安全设备的运行状态未能与管理制度有效衔接,影响了技术防护效能的充分发挥。

1.3应急响应能力亟待提升

网络安全应急预案的针对性与可操作性不足,多数预案仅停留在框架层面,对不同类型安全事件的处置流程、责任分工缺乏详细规定。应急保障队伍建设滞后,专业人员数量不足、技能单一,难以应对复杂的安全事件。应急联动机制不健全,组织内部各部门之间、与外部网信、公安等部门之间的沟通协调不畅,导致安全事件发生后响应迟缓、处置不当。同时,应急演练形式化严重,缺乏实战性与复盘总结环节,未能有效提升应急处置的实战能力。

1.4人才供需矛盾日益突出

网络安全人才总量不足,高端应用型、复合型人才尤为稀缺,难以满足各行业数字化转型对安全人才的迫切需求。人才培养体系与市场需求存在脱节,高校课程设置偏重理论知识,实践教学环节薄弱,毕业生缺乏实际操作能力。企业对在职人员的职业继续教育重视不足,缺乏系统的培训机制,导致现有从业人员的技能水平难以跟上技术更新与安全形势变化的节奏。人才激励机制不完善,薪资待遇、职业发展空间等缺乏竞争力,难以吸引和留住优秀人才。

2 网络安全管理机制优化的理论基础与核心原则

2.1理论基础支撑

ISO27001信息安全管理体系的PDCA循环模型为制度优化提供了重要理论支撑,通过计划、实施、检查、改进的持续循环,实现管理体系的动态完善与持续提升。网络安全态势感知理论强调对安全威胁的实时监测、分析与预判,为技术防护体系的协同联动与智能化升级提供了理论依据。风险管控理论要求以风险评估为基础,针对不同等级的安全风险采取差异化的管控措施,实现安全资源的合理配置与高效利用。预算管理理论强调根据战略目标与实际需求,科学编制预算、严格执行预算、加强预算监督,确保资金使用的合理性与有效性。这些理论相互补充、有机融合,为网络安全管理机制的全方位优化提供了坚实的理论基础。

2.2核心优化原则

系统性原则要求将网络安全管理视为一个有机整体,统筹制度、技术、人员、应急、预算等各个要素,实现各部分的协调配合、良性互动与闭环管理,避免碎片化与片面化。风险导向原则强调以风险评估为起点,围绕核心风险制定管理策略与防护措施,将有限的资源投入到高风险领域,实现安全效益最大化。动态适配原则要求管理机制能够根据技术发展、业务变化、安全形势与政策调整及时调整优化,持续提升对新型安全威胁的适应能力与应对水平。实战导向原则注重管理机制的可操作性与实效性,以解决实际问题为目标,避免形式化与表面化,确保各项优化措施能够落地见效。协同共治原则强调构建组织内部各部门之间、行业之间、跨部门跨区域之间的协同合作机制,形成网络安全管理的合力,共同应对复杂多变的安全威胁。

3 网络安全管理机制的优化路径

3.1构建系统化的制度管理体系

完善制度框架设计,以《网络安全法》《数据安全法》《个人信息保护法》等法律法规与行业标准为依据,结合组织自身业务特点、风险评估结果与技术发展趋势,建立涵盖管理总则、具体细则、操作流程的三级制度体系。

建立制度动态更新机制,定期开展制度评审与修订工作,结合安全事件案例、技术迭代更新、业务拓展变化与政策调整要求,及时修订完善制度内容,填补新型场景与新兴技术的安全规范空白。

强化制度执行监督,建立量化的考核评价指标体系,将制度执行情况与部门绩效、员工考核、评优评先直接挂钩。定期开展制度执行情况专项检查与审计工作,及时发现并纠正执行过程中的偏差与问题,对违规行为严肃追责问责,确保制度落地见效。

3.2打造协同联动的技术防护体系

优化技术防护架构,以安全态势感知平台为核心,整合边界防护、终端安全、数据加密、漏洞扫描、入侵检测、日志审计等各类安全技术与设备,实现威胁情报的集中采集、统一分析、实时共享与协同处置。

强化关键环节技术防护,针对网络边界建立多层次、立体化的访问控制策略,采用物理隔离与逻辑隔离相结合的方式,严格管控出入网络的信息流,防范外部攻击与非法入侵。加强终端安全管理,实现终端设备的统一准入、漏洞修复、病毒查杀与行为管控,覆盖普通PC终端、云桌面终端、移动终端等各类终端类型,建立终端安全管理分中心,实现与上级管理中心的信息快速共享与协同处置。

推动技术防护与管理流程深度融合,将安全技术的运行状态、监测数据与管理制度、操作规范有效衔接,实现技术防护与管理要求的协同联动。引入自动化、智能化安全技术,如自动化漏洞扫描与修复工具、智能化威胁检测与响应系统等,提升安全防护的效率与准确性,减少人为干预与操作失误。

3.3建立全流程闭环应急管理机制

优化应急预案体系,基于全面的风险评估结果,分类分级制定针对性强、可操作性强的应急预案,明确不同类型、不同等级安全事件的响应流程、责任分工、技术手段、资源保障与处置时限。细化应急处置的操作规范与流程图表,确保应急人员在实战中能够快速上手、规范操作。定期开展应急预案的评审与修订工作,结合安全事件处置经验与安全形势变化,持续优化应急预案内容,提升预案的科学性与适用性。

加强应急保障队伍建设,选拔具备网络安全专业技能、应急处置经验与协同协作能力的骨干人员,组建专业化应急保障队伍。定期组织应急保障队伍参与专题培训、技术研讨与实战演练,提升队伍的应急处置技能、跨部门协同能力与心理抗压能力。建立应急专家库,邀请行业专家、技术骨干与科研院校学者组成专家团队,为应急处置提供技术支持、决策咨询与指导服务。

健全应急联动机制,建立组织内部各部门之间、与上级主管

单位、网信部门、公安部门、安全服务商、电信运营商等相关单位之间的常态化沟通协调与信息共享渠道。明确应急联动的启动条件、沟通流程、信息传递方式与责任分工，确保安全事件发生后能够快速响应、协同处置。加强跨区域、跨行业应急联动演练，提升不同单位、不同部门之间的协同作战能力，形成应急处置的合力。

强化应急演练与复盘总结，定期组织实战化应急演练，模拟各类典型安全事件场景，检验应急预案的可行性、应急队伍的实战能力与应急联动机制的有效性。演练结束后，及时开展复盘总结，全面分析演练过程中存在的问题与不足，深入剖析原因，制定针对性的改进措施，持续优化应急预案与应急管理机制。建立应急处置案例库，将典型安全事件的处置过程、经验教训进行整理归档，为后续应急处置提供参考。

3.4完善多层次人才培育模式

为扩充网络安全人才储备，需从多方面发力。首先在人才培养规模上，要给予高校支持，推动其增设网络安全相关专业，扩大招生数量，同时优化课程安排，加大实践教学占比。高校还应加强与企业、科研机构的合作，建设实训基地，切实提升学生实际操作能力，增强其岗位适应性。另外，要鼓励职业院校开展网络安全技能培训，着重培养一线应用型和技能型人才，以填补中低层人才的空缺。

推进校企协同育人是重要举措。政府应出台政策，激励高校与网络安全企业、关键信息基础设施运营单位合作，联合开设网络安全专业，共同建设网络安全学院与实训基地，实施“订单式”人才培养模式。企业可挑选技术骨干出任产业导师，将实际项目案例及实践经验融入教学环节，提高学生实践能力与职业素养。同时，建立校企人才交流机制，鼓励高校教师到企业挂职锻炼，企业技术人员到高校兼职授课，实现师资共享，优势互补。

加强在职人员培训也不容忽视。要构建常态化的职业继续教育与技能培训机制，依据不同岗位的安全需求，开展专项技能培训、职业认证培训以及应急处置演练。鼓励员工积极参与行业交流、技术研讨和技能竞赛，使其及时掌握最新技术动态与安全趋势，提升专业技能水平。

优化人才激励机制同样关键。提高网络安全人才的薪资与福利待遇，构建与技能水平、工作业绩、职业风险相匹配的薪酬体系。完善职业发展通道，为网络安全人才提供明确的晋升路径与广阔的发展空间。设立网络安全专项奖励，对在安全工作中表现优异、贡献突出的个人与团队进行表彰奖励，增强网络安全人才的职业认同感与归属感。

4 结语

数字化转型背景下，网络安全威胁的复杂性与严峻性持续升级，传统管理机制已难以适应新形势需求。本文基于现状问题与理论支撑，提出制度、技术、应急、人才多维度优化策略，旨在构建全方位、动态化的安全防护体系。未来，网络安全管理需持续紧跟技术发展与安全形势变化，深化协同共治理念，推动管理机制的迭代升级。唯有不断完善安全保障体系，才能有效抵御各类安全风险，为社会运行、经济发展及国家安全筑牢网络安全屏障，助力数字化转型行稳致远。

[参考文献]

[1]段利军,古意瑾,欧虹伶,等.市级气象部门网络安全管理机制建设要点分析[J].网络空间安全,2024,15(4):340-343.

[2]赵腾.计算机信息管理技术在网络安全应用中的应用研究[J].信息系统工程,2025(5):83-86.

[3]王志强,韩寓,刘峰.基于ISO27001的企业管理信息化系统网络安全机制研究[J].铁路计算机应用,2024,33(10):23-28.

[4]李雪莹.优化网络安全预算管理机制,推进网络安全人才培养[J].中国信息安全,2023(4):52-54.

[5]李卫东,覃亚林.数字组织网络安全的威胁分析和保障机制[J].新媒体与社会,2023(2):203-216.

作者简介：

闫涛(1984--),男,汉族,新疆乌鲁木齐人,副高级,毕业于武汉科技大学计算机科学与技术专业,现任职于新疆维吾尔自治区人力资源和社会保障厅,担任政策咨询服务中心(社保卡管理中心)高级工程师,研究专业：计算机科学与技术。