信息化背景下网络安全运维服务质量管理探析

张兴凡[1,2,3]
1. 中国科学技术大学 安徽 合肥 230026；
2. 中国科学院合肥物质科学研究院 安徽 合肥 230031；
3. 中检集团天帷网络安全技术（合肥）有限公司 安徽 合肥 230061

摘 要 信息化正向各行业领域深度推进与全面融入，自动化和数字化的应用，极大地提升了生产与管理效率，支撑企业开展数据驱动型科学决策。在信息化背景下的网络安全运维服务质量管理中，应该认识到现阶段的网络安全态势，明确存在的风险因素，进而制订科学、合理的质量管理策略。基于此，本文围绕网络安全运维服务质量管理展开讨论，分析信息化背景下面临的突出问题，重点关注质量标准、评价机制、过程管理、能力匹配等方面，提出优化策略并明确其应用路径。通过质量管理优化，网络安全运维服务系统性治理能力可以得到显著提升；健全质量标准体系、构建多维评价机制、强化信息透明度、精准匹配服务能力，是提升运维服务水平的有效措施。

关键词 信息化；网络安全；运维服务；质量管理

Exploring the Quality Management of Cybersecurity Operations and Maintenance Services in the Context of Informatization

Zhang Xingfan[1,2,3]
1. University of Science and Technology of China, Hefei 230026, Anhui Province, China;
2. Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, Anhui Province, China;
3. China Certification & Inspection Group Tianwei Cybersecurity technology (Hefei) Co., Ltd., Hefei 230061, Anhui Province, China

Abstract Informatization is advancing deeply and integrating comprehensively across various industries. The application of automation and digitalization has greatly improved production and management efficiency, supporting enterprises in carrying out data-driven scientific decision-making. In the context of informatization, quality management of cybersecurity operation and maintenance (O&M) services should recognize the current cybersecurity situation, clarify existing risk factors, and thereby formulate scientific and reasonable quality management strategies. Based on this, this paper discusses the quality management of cybersecurity O&M services, analyzes the prominent problems faced under the background of informatization, focuses on aspects such as quality standards, evaluation mechanisms, process management, and capability matching, and proposes optimization strategies while clarifying their application paths. Through quality management optimization, the systematic governance capability of cybersecurity O&M services can be significantly enhanced. Improving the quality standard system, building a multi-dimensional evaluation mechanism, strengthening information transparency, and precisely matching service capabilities are effective measures to elevate the level of O&M services.

Key words Informatization; Cybersecurity; Operations and Maintenance Services; Quality Management

信息化背景下的网络安全形势十分严峻，存在着多种安全威胁，应该重视安全运维，发现漏洞并及时修补，提升自身的应急处置能力。网络安全运维服务的开展过程中，存在着多方面的难点问题，需要加强质量管理，提高风险的可控性，保障服务行为的标准化，优化评价流程并采用动态化的评价方式，并根据安全威胁的演化与业务的变化进行质量持续改进。

1 网络安全运维服务质量管理面临的突出问题

网络安全运维服务的开展过程中，以安全监测与预警、应急响应、漏洞管理为基本工作内容。在信息化背景下，网络安全运维的服务对象变得更加复杂，多个主体相互协同，并将智能化的技术手段运用其中。网络安全运维服务质量管理面临着质量标准模糊、质量评价单一、信息不对称、能力与需求错配等问题，这些问题会使运维服务的质量降低，容易对服务需求做出误判，处理安全问题时，缺少明确的质量责任界定，从而增加安全风险。

1.1 质量标准模糊

在网络安全运维服务质量管理中，存在质量标准模糊的问题，缺少统一、规范化的质量标准对服务质量做出全面、精准的评价。网络安全运维服务的相关规范是以合法、合规作为基本要求，其质量标准具有“多”、“杂”、“乱”的特点，缺少可量化的操作细则，不同组织、不同项目对质量合格的定义并不一致。在网络安全运维服务的具体操作中，并未按照标准化的作业程序进行，服务质量更多是由执行者的专业能力和个人经验决定，服务质量容易在多方面因素的干扰下出现波动。选取某2025年度的网络安全运维服务记录（样本量n=1 110项），统计各项指标的达标情况，结果见表1，反映出后期处置环节的质量控制薄弱。在网络安全新环境下，根据行业需求，需要构建整体联动、持续主动的网络安全防御体系，健全网络安全运维服务质量标准[1]。

表1 运维服务质量指标达标率统计结果

指标	阈值	总任务数	达标数	达标率
告警响应时间	≤ 5 min	1 110	954	85.95%
事件处置时间	≤ 30 min	1 110	873	78.65%
高危漏洞修复周期	≤ 24h	129	97	75.19%
过程记录完整率	≥ 95%	1 110	901	81.17%

1.2 质量评价单一

网络安全运维服务质量的评价，存在评价方式单一的问题。服务需求方管理人员作为评价主体，其对于运维服务质量的评价具有较强的主观性。信息化背景下的网络安全运维服务，运维平台可以获取全面的数据并进行综合分析，可作为评价运维服务质量的依据，但是存在着数据失真的问题，不能反映真实情况。结合数据进行质量评价时，数据能够反映出运维服务质量下降的相关性因素，但是难以证明其中的因果关系，不能反映真实的质量状态。在网络安全运维服务质量评价中，评价侧重一个或多个局部指标，未能对安全服务进行整体性评价，忽视安全服务的动态变化，导致评价维度窄化。网络安全运维服务的技术层面评价，主要以配置的合规性作为评价标准，将设备指标作为评价依据，通过防火墙的开启、杀毒软件的安装以及漏洞扫描的执行情况来评价服务是否达到高质量标准，但无法验证相关策略是否有效。将监测系统的预警信息作为评价网络安全运维服务质量的依据时，评价过程过多关注预警数量，容易忽视预警信息本身质量。在预警信息质量不高的情况下，难以反映出真实的安全管理情况，安全问题存在较高的误报、漏报风险。修复高危漏洞时，缺少兼容性测试、二次验证等环节，不能将安全风险完全消除。网络安全运维服务质量管理侧重于安全问题的快速响应，追求在尽量短的时间内进行风险识别并发出告警，却未能持续关注安全问题的处置情况，对处置质量不够重视。

1.3 信息不对称

网络安全运维服务的信息不对称，具体表现为服务需求方、供应方在风险可见性、处置能力等方面的不对称。服务需求方不了解网络安全运维服务的生产过程，难以对产出质量进行全面、客观的判断。服务需求方针对网络安全运维服务工作的开展情况进行监控，主要关注运维人员在风险预警、应急决策与上报等方面的行为，但未能对行为进行深层次的分析，并不了解优化策略、应急响应措施的实际应用效果。在网络安全运维服务质量管理中，由于过程记录不完整，无法对相关操作进行追溯，不能进行质量审计，在处置争议问题时，服务需求方、供应方均无可靠的证据。服务需求方、供应方之间的信息不对称，后者具有信息优势。在风险可见性层面，服务的供应方能够根据原始告警日志、系统底层漏洞等信息进行风险识别，具体了解安全问题的发生情况、处置情况。服务的需求方仅掌握安全问题的统计结果，并不了解安全问题处置的具体情况。在处理能力层面，服务的供应方了解自身的风险处置能力，能够针对安全问题采取有效的处理方法。服务的需求方能够知晓安全问题得以解决，但并不能对安全问题处置过程的有效性、专业程度进行判断。服务的供应方通过选择性披露、过度解释复杂性等途径进行信息操作时，虽可在技术层面达到合规要求，但是也会导致服务质量下降。

1.4 能力与需求错配

服务能力难以匹配复杂的系统，知识的更新滞后于技术的升级，会导致网络安全运维服务在面对新型安全风险时，不能及时、精准地进行识别以及采取有效的处置措施。网络安全运维服务岗位对专业人才有着较高的要求，既要熟练掌握专业技术知识，又要具备丰富的工作经验，深入理解业务逻辑。但在实际的工作岗位上，复合型人才的缺失会导致网络安全运维服务质量下降。

2 网络安全运维服务质量管理的优化策略

2.1 健全网络安全运维服务质量标准体系

健全网络安全运维服务质量标准体系，使质量标准更加清晰、明确。制定行业基线标准，要求网络安全运维服务具备监测、响应、漏洞管理、加固、报告等服务能力，并对风险事件响应、高危漏洞修复提出具体的时限，规范记录其过程，形成网络安全运维服务的“合格标准”。考虑到不同行业对网络安全运维

服务需求的差异性，应该结合各行业的特点，建立场景标准。在具体项目中，服务需求方、供应方基于行业基线标准、场景标准开展网络安全运维服务，还应该共同制订项目标准，并将其写入合同。在合同条款中，加入安全效果指标并约定违约责任。告警响应时间、事件处置时间、漏洞修复周期作为时效性指标，采取分级设定阈值的方式，出现超时的情况时，按要求扣款。依托安全事件复发率、漏洞修复一次通过率等指标进行有效性评价，为各项指标设定底线值，当指标未达标时会触发预警，进而采取整改措施。在月度核查中，依托记录完整率、漏洞修复一次通过率等指标进行完备性评价。在年度评估中，统计安全事件的发生数量，评估各安全事件的严重程度。

2.2 构建三维评价体系

三维评价体系针对效果、过程、感知等维度进行评价。在三维评价体系中，增加安全效果指标的权重，将其作为核心评价指标，针对安全问题进行及时告警响应的同时，能够采取有效的处置措施，进而提高其安全价值。根据高危漏洞的修复、安全事件的根因定位、攻击链路的阻断等情况，进行质量管理效果的评价，进行修复率、定位率、成功率的统计，作为安全结果指标。按照月度、季度、年度对系统整体风险水平进行评估，可根据风险降级情况，对安全质量进行评价。建立多维交叉验证机制，增加网络安全运维服务质量的评价主体，由服务需求方进行过程监督，核查各项量化指标，警惕相关指标的异常波动情况。引入外部安全机构，进行第三方独立评估，对安全防护的有效性、应急响应能力、过程记录的真实性进行验证。在此基础上，服务供应方在提交质量报告时，利用关键操作的原始记录、验证截图作为证据。实施预防性的质量评价，更加积极、主动地进行漏洞管理，在尚未引发安全事件时进行处理。优化检测能力，加强对风险因素的识别并精准预警，尽早予以处置，避免发展为严重的安全问题，减轻其危害性[2]。

2.3 建立过程透明与可追溯机制

在网络安全运维服务中，各项操作均在运维平台上进行并实现自动记录，留下每个关键动作的痕迹。各个运维动作与工单或任务相关联，并留存验证证据以及保留告警处理链路[3]。建立质量透明度机制，确保服务需求方能够具体了解网络安全运维服务的过程，感知真实的服务状态。发生安全事件、变更操作等关键事件时，能够即时向服务需求方通报。引入独立审计，由第三方机构进行随机抽样审计[4]。

2.4 实现服务能力与需求的精准匹配

信息化背景下的信息系统与应用程序、数据与信息资源、网络基础设施与计算资源、终端与边缘节点的复杂度持续提升，对网络安全运维服务质量管理有着更高的要求，需要扩大安全运维服务的覆盖面[5]。采购服务模式的转型，应该以能力为导向，对服务供应方的安全服务能力提出具体要求。针对关键岗位，设置严格的资质门槛，相关工作人员需接受入职验证，并定期进行复测与实战演练[6]。

3 结束语

综上所述，信息化背景下网络安全运维服务质量会受到标准模糊、评价单一、信息不对称与能力错配等问题的影响。健全网络安全运维服务质量标准体系能够为网络安全运维服务的开展提供良好的基础条件。构建多维评价机制，可以获得更加全面、可靠的评价结果。在信息穿透的基础上，强化人才适配，能够从整体上提升安全运维服务的可靠性。

参考文献

[1]陈星,袁明坤,刘蓓.基于网络安全运维新定义的网络安全运维实施指南解析[J].信息技术与标准化,2025(11):54-60.

[2]贾媛媛.“1+X”证书下的网络信息安全专业课程建设研究——以“网络安全运维”课程为例[J].数字通信世界,2025(9):247-249.

[3]田勇,陈平,何刚,等.新能源场站网络安全与运维管理的协同策略[J].水电与新能源,2025,39(5):28-31.

[4]欧阳金福.人工智能视角下数据中心的网络运维与安全防护策略[J].中国宽带,2025,21(6):46-48.

[5]张国庆.基于“互联网+”技术的计算机网络安全智能化运维研究[J].信息与电脑,2024,36(24):54-56.

[6]彭海云,王玉玺.以网络安全监测预警为核心的安全运维服务构建研究[J].电脑知识与技术,2022,18(19):37-39.

（本文编辑 吴文博）

