# 基于产教融合的网络安全评价体系研究

张蕾
西安电子科技大学，陕西 西安 710126
DOI: 10.61369/TACS.2025080018

**摘　　要：** 随着数字经济时代的快速发展，网络安全问题日益严峻，而相关专业人才短缺则是制约网络安全建设的重要因素之一。本文即以产教融合建设为视角，针对现有网络安全评价体系中暴露出的评价标准多元且不统一、企业内生动力不足及评价体系滞后于技术发展等问题，提出构建政府、高校、企业、行业组织等多元主体参与，安全治理与合规、技术防护与控制、安全运营与韧性、业务影响与价值等多维指标设计，并且通过动态反馈驱动网络安全评价体系的方法与策略，以此推动网络安全人才培养与产业需求的精准对接，提升人才培养质量与效能。

**关 键 词：** 网络安全；产教融合；评价体系；校企协同

## Research on Cybersecurity Evaluation System Based on Industry-Education Integration

Zhang Lei
Xidian University,Xi'an, Shaanxi 710126

**Abstract:** With the rapid development of the digital economy era, cybersecurity issues have become increasingly severe, and the shortage of relevant professional talents is one of the important factors restricting cybersecurity development. From the perspective of industry-education integration construction, this paper addresses problems exposed in the existing cybersecurity evaluation system, such as diverse and inconsistent evaluation standards, insufficient internal motivation of enterprises, and the evaluation system lagging behind technological development. It proposes methods and strategies for constructing a cybersecurity evaluation system that involves multiple subjects (including the government, universities, enterprises, and industry organizations), incorporates multi-dimensional indicators (covering security governance and compliance, technical protection and control, security operation and resilience, and business impact and value), and is driven by dynamic feedback. The aim is to promote the accurate alignment between cybersecurity talent cultivation and industrial demands, and improve the quality and efficiency of talent cultivation.

**Keywords:** cybersecurity; industry-education integration; evaluation system; university-enterprise collaboration

## 引言

网络空间是现代社会视域下的第五空间，其不仅与人们的生活生产息息相关，同时也事关国家安全与社会稳定。现阶段我国仍面临着网络安全人才短缺的突出问题，其中每年人才缺口近百万，而高校培养的人才规模不足3万[1]。与此同时，数字化转型浪潮推动着智慧城市、工业互联网、新媒体平台等新兴领域持续发展，进一步对网络安全提出了更高要求。在此背景下，企业应当承担起人才培养的重要职责，通过产教融合的途径与方式参与到教育活动之中，以此连接教育系统与产业系统，为破解网络安全人才培养与评价困境提供了新路径。

## 一、网络安全评价体系建设现状与问题

### （一）评价标准多元且不统一，缺乏权威共识

当前网络安全评价体系构建呈现出“多元并存，各有侧重”的格局特征，未能建立系统性、广泛性、权威性的标准体系。其多元化特征主要呈现在三个层面：第一，国际标准与国内标准并存。在实际工作中，目前可参考的标准既包括 ISO/IEC 27001（信息安全管理体系）等国际标准，也包括国内的《网络安全等级保护制度》等相关法律法规[2]，因而形成了适配性问题。第二，行业标准各自为政。不同行业对网络安全的要求不同，因此其基于自身业务特性建立了不同的安全标准，尤其在金融、电信、能源等关键基础设施行业，标准之间的差异较大[3]，导致评价体系难以实现跨行业、跨企业的多重应用。第三，企业及第三方机构标准林立。随着网络安全重要性的持续提升，相关企业、测评机构与

 

安全厂商快速崛起，并形成了差异化的评价框架与能力认证，加剧了市场的复杂度。

**（二）监管驱动为主，企业内生动力不足**

现阶段，我国的网络安全评价活动主要依靠外部监管和合规要求驱动，并非企业自身对安全水平的内部要求。具体可以从三个方面分析：第一，评价活动具有强合规性。企业大多为了达成《网络安全法》《数据安全法》等法律法规的强制性要求[4]，因而选择了构建网络安全评价体系，但其评价目标在于通过测评，并没有从根本上建立发现和解决网络安全问题的核心导向。第二，评价呈现“运动式”和“周期性”特征[5]。部分企业在开展网络安全评价工作时，大多选择在定级备案、迎接检查等特定实践阶段，使得其评价目的不纯，并且无法与业务发展、技术迭代和日常运营管理形成良好的协同关系，更无法建立常态化工作机制。第三，成本中心思维占据主导。由于缺乏内生动力，多数企业，尤其是中小型企业将网络安全投入视为成本支出，而非视为价值投资[6]，因而该类企业在满足合规要求之后缺乏持续改进的积极性，难以持续发挥评价体系的功能价值。

**（三）评价体系滞后于技术发展，难以应对新型威胁**

网络安全威胁演化迅速，但网络安全评价体系的更新迭代却相对较慢，由此形成了滞后问题，导致以下三个方面可能存在问题：第一，评价范围出现盲区。传统网络安全评价体系主要针对IT架构和威胁，但其无法适应云计算、工业互联网、线上办公、物联网、人工智能等新技术的应用语境[7]，未能建立成熟且普适性强的评价指标与方法。第二，评价方法被动且呈静态化。现有评价体系大多采用静态配置检查和已知漏洞扫描的方式，属于“事后验证”的评价思路，难以对高级持续性威胁、零日漏洞攻击和复杂社会工程学攻击等形成有效评估[8]，缺失了动态防御能力和实时响应能力。第三，重技术轻管理，重设备轻流程。部分企业更强调网络安全设备的部署程度与先进性，却忽视了安全策略、安全运维管理、人员安全意识等方面的重要性，使得评价体系缺乏客观性。

## 二、基于产教融合的网络安全评价体系构建策略

**（一）构建多元协同的评价主体体系**

在产教融合视域下，网络安全评价体系的构建需突破单一评价主体的局限，充分发挥“校企行政”等多方主体的协同作用，建立多元评价共同体。

高校在该主体中主要负责人才培养与评价，并侧重理论知识与基础素养，考核学生对网络安全基本原理、架构和方法的理解与掌握。与此同时，高校主体应与企业主体建立深度合作关系，尤其在资源与项目方面，应引入企业的真实工作场景与实践工作案例，为网络安全领域提供具备复合型能力与实践素养的优秀人才。

企业一方面应深化人才培养参与度，重点对学生实践技能与岗位适配度进行评价，主要包括真实环境中的技术应用能力、问题解决能力及项目协作能力，由此建立“学习、实训、认证、竞赛、研究”五大核心维度，推动网络安全专业人才发展[9]。另一方面则要建立分层级的治理架构。其中决策层可以建立网络安全与风险管理委员会，通过高层管理者完成审批评价体系框架、设定总体安全目标等工作任务，具备裁定对重大安全投入与风险决策的能力。管理层则可以建立首席信息安全官CISO及安全团队，主要指中层管理人员与技术人员对评价体系的具体设计、实施与日常运营，比如指标制定、数据收集、分析和报告撰写等[10]。执行层由各业务部门与IT运维团队构成，主要在本部门职责范围内执行网络安全管理策略，并将相关数据进行采集与存储。

行业组织则应负责提供行业标准与认证体系，一方面要对网络安全评价的结果进行公证，确保其在行业内具有权威性与工作效力。另一方面可以通过竞赛项目、成果奖项评选等方式，规范网络安全评价的标准与流程。

政府部门应负责政策引导与监管保障，保证评价体系既符合国家网络安全战略与法律法规要求，又能满足企业健康、稳定、安全发展需求，从而为数字经济时代建设创设良好的环境氛围与网络平台。

**（二）设计多维度评价指标**

在产教融合视域下，网络安全评价体系还应建立融合业务目标的多为评价指标，既要发挥高校的教学与科研引导作用，又要确保该体系能够全面反映安全状态，并与业务语言形成对接。具体来说，高校与企业应合作建设多元评价维度，并明确其核心指标与数据来源。具体来说，可以从以下四个层面建立评价维度。

第一，安全治理与合规。其核心指标应包括安全政策覆盖率、员工安全意识培训频率、合规审计通过率、第三方风险管控率等，相关评价数据主要以内部审计文件、人力资源系统以及合规管理平台相关信息为来源[11]，而评价目标为衡量安全管理的成熟度与合规一致性。

第二，技术防护与控制。该评价维度的核心指标主要包括网络边界入侵尝试拦截率、高危漏洞平均修复时间、终端防护安装率、安全配置基线符合率等，数据则以防火墙、终端安全管理系统、IDS/IPS、漏洞扫描平台等提供的信息为基础[12]，以此评估技术防护体系的完备性与有效性。

第三，安全运营与韧性。该评价维度的核心指标主要包括平均检测时间）、平均响应时间、数据备份恢复成功率、安全事件数量与等级、应急演练完成度等，评价数据主要围绕安全运营中心、应急响应团队记录、SIEM系统等信息展开[13]，用于衡量主动发现、快速响应和从灾难中恢复的业务韧性。

第四，业务影响与价值。该评价维度的核心指标主要包括因安全事件导致的业务停机时长、安全项目投资回报率、潜在数据泄露造成的财务损失估算等，评价主要参考业务系统日志、财务数据、风险量化模型等数据[14]，以此将安全风险与绩效转化为业务语言，支撑管理决策。

**（三）实施动态与量化的评价方法**

产教融合的深度发展也为网络安全评价体系构建提供了更专业与科学的方法论平台，可以为评价结果的准确性与行动指导性提供参考依据。对此，企业可以采用定量与定性融合、过程与结

 

果兼顾的先进评价方法。

第一，构建量化评估模型。企业可以与高校数学、信息技术、网络安全等相关院系进行深度合作，并基于理论研究引入“风险量化” 与 “成熟度模型” 两大工具[15]，为网络安全评价体系建设提供技术支撑。其中风险量化主要以信息风险因素分析模型为载体，通过将安全威胁发生的可能性和影响程度，转化为具体的财务数据，由此更直观地与其他经营风险在同一维度对比，从而为企业决策提供支持。“成熟度模型”则立足 CMMI 或 NIST CSF 的成熟度等级进行评估，评估对象包括安全治理能力、安全运营水平等。

第二，融合多源数据与自动化工具。企业可以与高校科研团队建立合作关系，由此将自动化数据采集策略与红蓝对抗实战检验方案引入网络安全评价体系之中。其中自动化数据采集策略主要发挥安全编排和自动化与响应（SOAR）平台的优势，依靠安全信息和事件管理系统进行数据采集，采集对象包括各类安全产品、网络设备和业务系统的日志等。红蓝对抗实战检验方案则采用分组对战的方式，其中 “红队” 模拟攻击方，“蓝队”模拟防御方，通过实战攻防演练验证防护体系的可靠性，达到压力测试的效果。

## 三、结语

综上所述，在产教融合视域下，网络安全评价体系的构建不仅要发挥企业的主观意识，更要挖掘高校的教育与科研服务功能，以此通过多元主体建设、多维度评价指标设计与动态与量化评价方法手段，推动我国网络环境的高质量发展，并更好地应对智慧城市、工业互联网、新媒体平台等新兴领域发展带来的网络安全难题。

*参考文献*

[1] 姜宗伯 . 医疗健康场景下网络信息安全评价体系设计及平台研究 [D]. 重庆大学 ,2024.

[2] 袁晨 , 张月国 , 刘功申 . 高校网络安全实战型人才培养的实践与探索 [J]. 工业信息安全 ,2024,(03):6-13.

[3] 周小平 , 韦信喊 . 计算机网络专业产教融合实训基地建设研究 [J]. 广西开放大学学报 ,2024,35(03):57-60.

[4] 曾文丽 , 陈继鑫 , 石睿 , 黄洪 , 吴亚东 . 产教融合背景下的网络安全综合实验课程教学改革 [J]. 计算机教育 ,2024,(03):144-147+153.

[5] 白杨 , 何林波 , 周益民 . 产教融合背景下网络空间安全专业课程体系改革与探索 [J]. 科教导刊 ,2024,(02):105-107.

[6] 魏彬 , 黄海涛 , 王涛 , 彭思远 . 交通运输行业网络安全评价指数体系模型 [J]. 综合运输 ,2023,45(11):43-48+53.

[7] 徐守志 , 杨小梅 , 马凯 . 面向网络安全行业需求的产教融合云实训资源建设与实践 [J]. 计算机教育 ,2023,(S1):124-127+132.

[8] 李鹏飞 , 施一飞 . 基于区块链的计算机通信网络安全评价研究 [J]. 信息记录材料 ,2023,24(10):45-47.

[9] 王法中 , 王磊 , 王曙光 , 许立前 . 基于 GB/T 34680的智慧城市网络安全评价指标体系构建研究 [J]. 中国标准化 ,2023,(07):69-72.

[10] 吴言 , 高卫国 . 高校网络安全综合评价体系研究 [J]. 淮阴工学院学报 ,2022,31(04):99-104.

[11] 雒辛芃 . 新媒体环境下网络安全风险评价与治理 [J]. 科技资讯 ,2021,19(32):115-117.

[12] 姜思佳 , 叶卫华 . 计算机网络安全分层评价防护体系研究 [J]. 长江信息通信 ,2021,34(07):137-139.

[13] 肖跃 . 网络安全服务项目质量评价体系研究 [D]. 北京邮电大学 ,2020.

[14] 曹琰 . 神经网络在计算机网络安全评价中的应用分析 [J]. 质量与市场 ,2020,(14):85-87.

[15] 于灏 . 民航网络安全监管能力评价体系研究 [D]. 中国民航大学 ,2020.

 