信息安全风险评估模型及其优化研究

梁定菲

（广西交科集团有限公司，南宁 530000）

摘　要：信息安全风险评估模型是一种系统化的方法，用于识别、分析和评估信息系统中存在的安全风险。通过对信息系统的全面评估，可以及时发现并解决潜在的安全漏洞，确保信息系统的安全稳定运行。然而，现有风险评估模型在动态性、准确性及全面性方面仍存在不足，需进一步优化以适应日益复杂的信息安全环境。

关键词：信息安全；风险评估；模型优化；算法改进；评估精度

中图分类号：TP393　　**文献标识码：**A

Research on information security risk assessment model and its optimization

LIANG Dingfei

（Guangxi Transportation Science and Technology Group Co., Ltd., Nanning 530000, China）

Abstract: The information security risk assessment model is a systematic approach used to identify, analyze, and evaluate security risks present in information systems. By conducting a comprehensive evaluation of the information system, potential security vulnerabilities can be identified and resolved in a timely manner, ensuring the secure and stable operation of the information system. However, existing risk assessment models still have shortcomings in terms of dynamism, accuracy, and comprehensiveness, and need further optimization to adapt to the increasingly complex information security environment.

Key words: information security, risk assessment, model optimization, algorithm improvement, evaluation accuracy

1　引言

随着信息技术的飞速发展和广泛应用，信息安全问题日益凸显。作为保障信息系统安全的重要手段，信息安全风险评估对识别、分析和控制潜在威胁至关重要。本文旨在探讨信息安全风险评估模型的基本概念、常用方法及优化策略，以期提高信息系统的安全性与可靠性。

2　信息安全风险评估模型概述

2.1　基本概念

信息安全风险评估模型是指一系列用于识别、分析和管理信息系统中的安全风险的方法和工具。这些模型通过系统化的评估过程，有助于组织了解其信息资产面临的潜在威胁和漏洞，并根据这些风险采取相应的控制措施，以确保信息系统的机密性、完整性和可用性。信息安全风险评估模型的基本概念涵盖以下关键步骤。

（1）资产识别和评估。资产包括信息系统中所有有价值的资源，如数据、软件、硬件、网络设施及人员。通过识别这些资产，评估人员可以确定对组织业务至关重要的资源。资产评估涉及评估这些资源的价值以及其在信息系统中的作用，以确定它们受到保护的优先级。这一过程为后续的威胁建模和风险评估奠定了基础。

（2）威胁建模。威胁可能有多种来源，包括外部攻击者、内部人员失误或恶意行为、自然灾害等。通过识别这些威胁及其特征，评估人员可以预测哪些威胁最有可能对系统造成损害。威胁建模为漏洞分析和风险评估提供了依据，确保了风险评估过程的全面性[1]。

（3）漏洞扫描和评估。漏洞是信息系统中的弱点或缺陷，易被威胁利用，从而对系统的安全性构成威胁。漏洞扫描和评估涉及使用自动化工具或手动检查方法来识别系统中的漏洞，并评估其可能带来的风险。评估结果用于确定需要被优先修复或控制的漏洞。

（4）风险评估和分类。风险评估是将资产、威胁和漏洞信息相结合，计算出每种潜在风险的可能性和影响程度。通过评估这些风险的严重性，组织可以将它们分类为高、中、低等级别。这一过程有助于组织优先处理最严重的风险，并制定合理的风险管理策略。

（5）风险处理和控制。风险处理是指针对已识别和评估的风险采取适当的控制措施。常见的风险处理策

略包括风险规避(避免风险的发生)、风险转移(如通过购买保险)、风险减轻(采取技术或管理措施降低风险)和风险接受(在风险较低或控制成本过高时)。通过有效的风险处理和控制,组织可以将信息系统的风险水平降低到可接受范围内。

2.2 常用模型

(1)NIST风险管理指南。NIST(美国国家标准技术研究所)制定的风险管理指南(特别是SP 800-30和SP 800-37)是信息安全风险管理的权威指南之一。NIST风险管理指南强调在信息系统全生命周期内进行持续的风险管理,并通过一套系统化的过程(包括风险评估、风险应对和风险监控)来保障信息系统的安全性。NIST风险管理指南被广泛用于相关部门和私营企业,特别是那些需要遵循联邦法律和法规的组织。该指南为不同规模和复杂度的信息系统提供了可操作的风险管理框架,强调与组织整体风险管理战略的一致性。

(2)ISACA-Risk-IT模型。ISACA(信息系统审计与控制协会)开发的ISACA-Risk-IT模型专注于信息技术风险管理,特别是在互联网和数字化领域。ISACA-Risk-IT模型基于COBIT(控制目标信息与相关技术)框架,旨在帮助组织识别、评估和管理与IT相关的风险。该模型强调与企业战略目标的紧密结合,以确保IT风险管理支持整体业务目标。ISACA-Risk-IT模型适用于不同规模和类型的组织,从中小企业到跨国公司,特别是在高度依赖信息技术的行业中具有广泛的应用价值。

(3) OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)模型。它由美国卡内基梅隆大学的软件工程研究所(SEI)开发,专注于组织信息系统的整体安全性评估[2~3]。OCTAVE模型强调对组织信息安全环境(包括资产、威胁、漏洞和安全措施)的全面理解,适用于较大型、复杂的组织,特别是那些具有分散IT环境和多种业务流程的企业。该模型强调自我导向的风险评估过程,组织内的各部门和员工共同参与,以确保风险评估结果的全面性和实际性。

(4) EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)模型。它是由法国政府开发的一种信息安全风险评估模型,专注于整个组织的安全性评估。在风险管理过程中,EBIOS模型强调安全需求和目标的明确表达,并据此进行风险识别、分析和控制。该模型适用于各类组织,特别是需要遵守法国或欧洲安全法规的企业和相关部门。EBIOS模型以系统化和详细的风险分析过程著称,强调风险管理的全组织参与和透明度。上述常用模型的主要优势及应用场景如表1所列。

表1 相关模型的主要优势及应用场景

模型/指南	NIST风险管理指南(SP 800-30和SP 800-37)	ISACA-Risk-IT模型	OCTAVE模型	EBIOS模型
主要优势	全生命周期风险管理,系统化过程,与法规紧密关联	专注于IT风险管理,与COBIT集成,支持业务目标	全面理解信息安全环境,自我导向评估	明确安全需求和目标,系统化详细分析
应用场景	相关部门和私营企业,特别是需遵循联邦法规的组织	不同规模和类型的组织,特别是高度依赖信息技术的行业	较大型、复杂的组织,具有分散IT环境和多种业务流程	各类组织,特别是需遵守法国或欧洲安全法规的企业和相关部门

3 信息安全风险评估模型的优化策略

3.1 合理采用样本数据

有效的样本数据不仅能够准确反映信息系统的实际运行状况,还有助于评估人员识别潜在风险,并制定针对性控制措施。因此,建立科学的数据采集和样本选择机制是确保风险评估准确性的重要环节。首先,数据采集应覆盖信息系统的关键组成部分和典型操作场景,以确保所采集的数据具有全面性和代表性。采集涵盖不同时间段、不同使用场景的数据,可以有效避免偏差,确保数据的真实性[4]。采集的数据应包括常规操作数据和异常情况记录,以便识别潜在的安全漏洞和威胁源。其次,样本数据的选择应遵循科学抽样方法(如随机抽样、分层抽样或系统抽样等),以确保样本数据能够反映整个信息系统的整体情况。在大规模信息系统中合理划分系统的不同部分,并在每部分中选择具有代表性的样本,可以提高评估结果的准确性。此外,样本数据的数量应足够大,以确保评估统计的可靠性,但要避免数据量过大带来的处理复杂性和资源浪费。最后,建立样本数据的验证机制,通过与历史数据或外部权威数据进行比对,确保样本数据的有效性和准确性。对数据进行清洗和预处理,去除异常值和噪声,以提高数据质量。同时,定期更新样本数据,及时反映信息系统的变化情况,确保风险评估的时效性和持续性。

3.2 建立合理的评估标准

首先,评估标准应包括对安全风险的分级和分类,以便对不同风险进行有效管理。通过定义风险的严重程度、可能性和影响范围,可以将风险分为高、中、低等级别。这种分级有助于评估人员识别和优先处理最紧迫的风险,从而合理配置资源,确保关键资产的安全性。其次,评估标准应规范风险的筛选和确定过程,确保评估结果的精确性。在风险评估过程中,应结合信息系统的具体情况,考虑各种风险因素,如威胁来源、漏洞性质、影响范围等。通过标准化的评估方法(如定量评估和定性分析),评估人员可以系统分析和评估这些风险因素,从而得出可靠的评估结果。此外,评估标准应是

动态的，能够随信息系统的发展变化进行调整和优化。信息技术的发展和业务环境的变化可能会引入新的风险源或改变现有风险的性质。因此，评估标准需要定期审查和更新，以反映最新的安全威胁和技术进展。通过不断完善评估标准，组织可以保持对信息安全风险的敏感性和应对能力，从而更有效地保护其信息资产。

3.3　应用合理的风险评估工具

首先，风险评估工具的选择应与所采用的评估模型相匹配。例如，NIST风险管理框架可能需要使用特定的自动化工具来支持威胁建模、漏洞扫描和风险分类等环节。类似地，使用OCTAVE模型的组织可能更适合选择强调全面性和系统性分析的工具。这些工具能够有效支持模型的各步骤（从资产识别到风险处理），从而为评估人员提供全面而准确的分析结果。其次，评估工具的技术细节是决定其适用性的关键因素。评估人员应深入学习和了解工具的功能、算法原理及操作方法。例如，某些工具可能更擅长处理大规模数据分析，而另一些工具可能在实时监控和动态分析方面表现更好。通过了解这些技术细节，评估人员可以更好地利用工具的优势，确保风险评估过程的准确性和高效性。最后，应根据评估需求的变化和技术的发展趋势，定期审查和更新所使用的评估工具。信息安全领域的发展日新月异，新型工具不断涌现能够提供更高效、精确的风险评估能力。因此，保持对新工具的敏感性和适应性，有助于组织在信息安全风险评估中掌握竞争优势。

3.4　加强动态风险评估能力

随着信息系统环境的高度动态化，传统静态风险评估方法难以应对不断变化的安全威胁。静态评估通常基于固定时间点的数据和假设，而现代信息系统的复杂性和多变性要求人们实时监控和评估安全风险。因此，加强动态风险评估能力成为确保信息系统安全的重要手段。

动态风险评估强调对信息系统运行状态和安全状况的实时监控。通过实时数据采集、分析和反馈，动态风险评估能够及时识别潜在的安全威胁，并根据实时信息调整安全策略。这种评估方式不仅能提供更准确的风险预测，还能在威胁出现时迅速做出反应，降低可能的损害。

为实现动态风险评估，组织需要结合先进的技术手段（如大数据分析、人工智能和机器学习）以自动分析海量实时数据，识别异常行为与潜在威胁。例如，机器学习算法能够根据历史数据和当前状态预测可能的安全事件，并在威胁演变的早期发出警告。同时，动态评估系统可以通过自动化手段实时调整安全策略，确保系统的持续防护能力。组织应建立灵活的安全管理框架，允许根据实时评估结果迅速调整安全策略和措施。此外，动态风险评估应与事件响应计划紧密结合，以便在安全事件发生时能够迅速采取有效行动。定期演练和更新动态评估流程，可以确保评估系统始终处于最佳状态。

4　结束语

建立信息安全风险评估模型是保障信息系统安全的重要手段。通过合理采用样本数据、建立科学的评估标准、应用合适的评估工具、加强动态风险评估能力等措施，可以不断优化信息安全风险评估模型，从而提高信息系统的安全性和可靠性。未来，随着信息技术的不断发展和应用环境的不断变化，信息安全风险评估模型将需要持续被完善和创新，以适应新的挑战。

参考文献：

[1] 陈德泉，林则夫，黄敏. 基于Poisson分布的信息安全风险评估[J]. 中国管理科学，2003，11(1)：168-172.

[2] 陈德泉，林则夫，黄敏. 基于Poisson分布的信息安全风险评估[C]// 中国管理科学. 北京：中国管理科学，2003：168-172.

[3] 桂若柏. 信息安全风险评估模型的研究及其应用[D]. 重庆：重庆大学，2004.

[4] 彭源. 模型与数据相结合的工业信息物理系统信息安全风险评估[D]. 武汉：华中科技大学，2018.

作者简介：

梁定菲（1993—），本科，工程师，研究方向：网络及信息安全、网络工程、运维。