聚知刊出版社
JZK publishing

网络安全风险评估与可持续发展策略探讨

兰皓

赣南卫生健康职业学院,江西省赣州市,341000;

摘要：随着网络技术的创新发展和互联网的广泛普及，网络安全问题日益凸显，成为各单位必须重视的工作。本研究旨在构建全面的网络安全风险评估模型，通过量化方式，深入分析网络安全风险。该模型包括风险识别、风险分析和风险评估三个核心环节，考虑了网络攻击发生的可能性及其潜在损失，从而实现了对网络安全风险的全方位评估。在此基础上，进一步提出以预防为主的网络安全风险可持续发展策略，该策略强调对风险的提前识别与防范，通过实证案例分析验证，能够有效降低网络安全风险和增强网络防护能力。为制定网络安全策略提供理论基础和实践指导，有助于推动网络安全的可持续发展。

关键词：网络安全风险评估；可持续发展策略；防御性措施

DOI：10.69979/3029-2735.25.1.063

引言

随着互联网和信息技术的蓬勃发展，社会迈向了新的步伐。然而，网络安全问题也日益严重，对个人和单位的信息安全形成了威胁。在这样的背景下，应当重视网络安全风险评估的重要性，预防网络安全事件，建立安全保障系统的基础环节。本研究旨在构建全面的网络安全风险评估模型，配合预防为主的网络安全可持续发展策略，全方位评估网络安全风险，精准掌握安全形势，深入分析和实证研究，证明了所提出策略实用价值，为各单位和团体制定网络安全策略提供参考依据。

1 网络安全及其风险概念的介绍

1.1 网络安全定义及其重要性

网络安全是保护计算机系统、网络及其数据免受攻击、损坏或未经授权访问的措施和技术。其重要性随信息技术和互联网普及而日益凸显，关乎信息保密性、完整性、可用性，以及用户隐私、经济利益等方面。社会高度依赖网络，网络安全缺失可能导致数据泄露、篡改乃至业务中断和法律责任。网络安全是社会基石，关乎国家安全、经济稳定和社会发展。面对技术更新快、攻击多样化的威胁，需持续完善防护措施，通过有效风险管理和技术创新，确保网络生态健康发展。

1.2 网络安全风险的类型和特点

网络安全风险可以根据其来源和性质划分为多种类型。常见的网络安全风险包括恶意软件攻击、网络钓鱼、分布式拒绝服务攻击(DDoS)、数据泄露和内部威胁等。恶意软件攻击通过病毒、蠕虫和特洛伊木马的传播，对系统的完整性和保密性构成威胁。网络钓鱼则是一种欺诈行为，通过假冒合法实体的方式来获取用户的敏感信息，其攻击特性具有极强的隐蔽性和欺诈性。DDoS攻击则是一种对资源极度消耗的攻击方式，通过大量的伪造请求来达到使服务中断的目的。当敏感数据遭到未经授权的访问时，数据泄露的风险就会产生，这可能引发极其严重的隐私问题。而内部威胁则是来自员工或内部人员的攻击，其具有强大的隐蔽性和破坏性。这些风险的共同特点是复杂、多变且难以预测，这要求我们必须采取分级的管理和防范策略。

1.3 现有网络安全风险评估方法及其局限性

现有网络安全风险评估方法主要包括定性分析、定量分析和综合分析。定性分析依赖于专家判断，可能导致主观偏差。定量分析虽具数据支持，但适用性受限于模型的复杂性和数据获取难度。综合分析力求两者结合，但复杂度增加，难以实现实时响应。这些方法的局限性在于无法全面、动态地评估快速变化的网络安全环境中的风险。

2 网络安全风险评估模型的建立

2.1 网络安全风险评估模型的必要性

网络安全风险评估模型的必要性在于，它能够全面识别和评估潜在的安全威胁，合理分配资源，优先处理高风险问题，从而有效预防网络安全事件，保障信息资产安全，提高整体信息安全防护水平。传统的网络安全风险管理方式大多依赖经验判断，缺乏系统性和科学性，难以应对瞬息万变的网络威胁形势。网络安全风险评估模型在此背景下显得尤为重要。通过系统识别、分析和评估各类风险，为决策者提供量化的数据支持，使其可以更精准地了解和预测风险状况。这不仅有助于在发生攻击前做好充分的防护准备，还能在攻击发生后快速响

应与修复。采用这一模型，不仅提升了风险管理的效率和准确性，也为构建更为坚实的网络安全体系奠定了基础，保障网络系统的持续稳定运行[3]。

2.2 网络安全风险识别方法的设计

网络安全风险识别是评估模型中的一个关键环节，直接影响风险分析和评估的准确性。设计有效的风险识别方法需要综合考虑网络环境的复杂性和多变性，充分了解单位或组织的网络架构、信息系统及其相应的安全措施，识别潜在的风险源，包括硬件和软件漏洞、未授权访问以及社会工程攻击等。此外，外部威胁如网络病毒、恶意软件和黑客攻击也应纳入识别范围。通过结合自动化工具与人工分析的方法，可以及时更新和完善风险数据库，以反映最新的安全威胁动态，从而为后续的风险分析和评估提供可靠的依据。这种综合的识别策略能够有效提高网络安全管理的效率和准确性。

2.3 网络安全风险分析与评估方法的构建

在建立网络安全风险分析与评估的方法时，需要综合考虑网络攻击的发生概率及其可能造成的损失，从而构建多层次的综合分析框架，以识别网络系统中的潜在威胁源。在这一过程中，可以借助经验数据和指导意见来估计各种威胁发生的概率。再根据网络资产的重要性，评估可能的经济损失和声誉影响。为了使评估结果更加科学和准确，结合模糊理论和层次分析等多种技术，使得风险分析更加系统化。同时，通过优化模型的参数，提升模型在不断变化的环境中的应变能力，从而为各类单位和机构提供可靠的风险评估工具。

3 可持续发展策略在网络安全管理中的应用

3.1 可持续发展策略的定义与内容

可持续发展策略在网络安全管理中的应用，强调在保护网络安全的同时确保系统的长期稳定性和高效性。其内涵不仅关注当前网络威胁的防御，还着眼于防护措施的长期有效性和成本效益。其核心是将网络安全视为动态过程，要求不断更新和优化安全措施，以应对不断变化的威胁环境。其内容包括以预防为主的风险管理，如定期漏洞扫描和修复，将潜在威胁消除在萌芽状态；强调防御性措施的基础建设，通过多层次的安全体系增强系统抵御攻击的能力。在防范过程中，注重资源的有效配置和使用，以最小化投入获得最大化的安全收益，确保网络安全与经济性发展同步进行。通过这些措施，增强单位和组织面对网络风险时的适应性和灵活性，实现网络安全的可持续发展目标。这种策略的应用不仅可以有效地预防网络安全威胁，而且可以提高网络系统的稳定性和效率，为单位和组织提供更加可靠和安全的网络环境。

3.2 预防为主防御性措施为基础的可持续发展策略的设计

在网络安全管理中，以预防为主、防御性措施为基础的可持续发展策略强调主动识别和缓解潜在风险。通过建立全面的网络安全框架，确保系统在面对可能的安全威胁时具备足够的抵御能力。系统应定期进行漏洞扫描和安全审计，以及时发现和修复安全弱点。此外，引入先进的威胁情报系统可以实现对网络攻击的实时监控和预警。强化员工的安全意识培训，使其掌握基本的安全防护技能至关重要。结合自动化安全工具，提高响应速度和准确性，最大限度地减少网络安全事件的影响。通过这些措施，能够有效提升网络安全管理的整体水平。

3.3 以可持续发展策略提高单位和组织的网络安全防护能力

可持续发展策略在网络安全防护能力的提升中起到了关键作用。通过将可持续发展理念融入到网络安全管理中，单位和组织能够更有效地识别和应对潜在的网络风险。以预防为主的策略强调了提前识别潜在威胁的重要性，能够减少网络攻击发生的可能性。另外，防御性措施为基础的策略通过加强系统的安全性和可靠性，提升了整体的防护能力。这种方法不仅增强了抵御当前威胁的能力，也为应对未来可能出现的安全挑战做好了准备，从而在动态变化的网络环境中持续提供稳定的安全保障。

4 可持续发展策略是否降低了网络安全风险实证分析

4.1 选择样本及数据收集

在进行可持续发展策略是否降低网络安全风险的实证分析过程中，样本的选择至关重要。此研究选取了多个具有代表性的单位和组织作为样本，这些组织横跨息技术、医疗保健、教育机构等不同行业，旨在获得广泛的行业视角。这些样本组织均面临不同程度的网络安全风险，且在管理中已尝试引入可持续发展策略。数据收集方面，采用了访谈、问卷调查和实地观察相结合的方法，获取多元化数据。问卷调查包括对 IT 人员和管理层关于网络安全事件发生频率、损失程度及策略执行效果的评价。访谈则深入探讨各组织实施可持续发展策略的具体过程和遇到的挑战。收集了各组织在策略实施过程中的历史数据，以便于进行对比分析。这种多渠道的数据收集方法确保了数据的全面性和可靠性，为后续的实证分析奠定了坚实基础。

4.2 实证方法与分析过程

在实证分析过程中，采取了定量研究的方法，通过收集和分析多个单位和组织实施网络安全可持续发展

策略前后的安全事件数据来评估策略的有效性。采用统计分析工具对收集的数据进行处理，计算和比较在策略实施前后网络安全事件的频率、损失水平和风险指数变化。为了确保数据的可靠性，数据来源于具有代表性和多样性的样本，包括不同行业和规模的组织。分析过程中，特别关注了与策略相关的防御性措施对事件频率和影响程度的作用，并对不同类型和规模组织的数据进行分类比较，揭示出可持续发展策略对降低网络安全风险的显著效果。

4.3 实证结果及其解读

实证分析结果显示，以预防为主、防御性措施为基础的可持续发展策略显著降低了网络安全风险。在选定的样本中，采取该策略的单位和组织，其网络攻击发生率和潜在损失均有明显下降。数据表明，风险识别和评估模型在实际应用中提高了风险预测的准确性，而防御性措施增强了对各种攻击的抵御能力[5]。通过具体案例的演示，证明了策略的实用性与有效性，为风险的长期管理提供了坚实支持，为网络安全策略的优化提供了指导。

5 对网络安全风险评估与可持续发展策略的思考

5.1 这套系统的应用优势与不足

网络安全的风险评估及可持续发展战略体系展现出显著的优势。其风险评估模型全面覆盖，能够精准识别风险，并对潜在损失进行量化，使得评估结果更加直观且具备科学依据。在战略层面，该体系强调预防，短期内有助于单位降低风险，而从长远来看，则能维持高水平的防护。这为决策者提供了明确的方向，支持他们制定有效的安全战略。

然而，这一系统并非没有缺陷。复杂多变的网络威胁可能使模型难以应对，无法及时适应最新变化，因此需要对不同的行业和单位进行大量定制化调整。尽管该系统具备降低风险的潜力，实际应用时仍需根据不同行业和单位的特性进行优化，以确保其广泛有效性。必须持续改进，以适应不断变化的安全环境，从而在更广泛的场景中提供更有效的应用。

5.2 如何进一步提高网络安全风险评估的有效性与网络安全管理的科学性

为了提高网络安全风险评估的有效性和网络安全管理的科学性，需要从多个方面进行深化。一方面，可以引入人工智能和大数据分析技术，以提高风险识别和分析的精确度。这些技术能够处理大量数据，识别潜在威胁和异常行为，提高风险评估的及时性和准确性。另一方面，加强跨行业的信息共享与合作也是不可或缺的方法。通过建立信息共享平台，实现安全威胁情报的共通，从而更全面地预判网络风险。同时，评估模型需要进行动态调整和实时更新，以适应快速变化的网络环境和新兴威胁。网络安全教育和意识培训也需要纳入管理体系，将人员意识提升到与技术措施同等重要的位置。此外，结合技术手段与管理策略的综合应用，能够更加科学有效推进网络安全风险管理的进程。这些措施将有助于提高网络安全风险管理的效率和精确度，提供更加全面和可靠的安全保障。

6 结束语

本研究通过构建全面的网络安全风险评估模型和以防御为主的可持续策略，为网络安全风险管理提供了新的视角，并通过案例验证了模型与策略的实际效果。考虑到网络安全风险管理的复杂性，未来的研究应针对不同的网络环境和威胁，进一步优化模型和策略，以适应技术的快速发展和环境的复杂性。目前的研究局限于现有的网络环境和技术水平，因此需要持续关注最新的威胁，并对模型和策略进行优化和完善。从网络安全人员的经验、最新的检测技术等多个角度深入研究，并考虑网络环境的复杂性、用户行为及潜在威胁等实际情况。积极探索更有效的风险管理模式，以实现网络安全风险的可持续管理。网络安全风险管理是一项长期且复杂的任务，需要在理论与实践中不断进行探索和创新，提供更有效的管理策略和方法。

参考文献

[1]姚洪磊,刘国梁,解辰辉,杨轶杰,牛温佳.AHP 策略下CTCS 网络安全风险评估方法[J].中国铁道科学,2023,44(04):241-250.
[2]闫星臣.林业管理可持续发展策略探讨[J].南方农业,2019,13(32):76-77.
[3]崔光耀.构建网络安全可持续发展良性生态[J].中国信息安全,2019,0(10):3-3.
[4]叶自谦.网络安全风险评估策略设计[J].电子技术与软件工程,2019,(14):207-207.
[5]邓斯.单位可持续发展策略探讨[J].营销界,2019,(47).