关于医院计算机网络安全管理工作的维护策略分析

游庆光，王艳慧[通讯作者]，刘　鹏

（郑州大学第三附属医院，河南 郑州 450000）

摘要：在当前信息技术高速发展的时代背景下，计算机网络技术具有强大的数据交互功能与信息处理能力，能够实现高效的数据存储与管理，被广泛应用于医院、企业等组织。医院临床治疗、医学研究等各项活动的开展过程中均运用了计算机网络技术与设备，实现了大量信息的采集、处理与分析。在这一过程中，必须加强计算机网络数据的安全管理。本文介绍了医院计算机网络安全的内涵及影响要素，并提出医院计算机网络安全的维护策略。

关键词：医院计算机；网络安全管理；维护策略；数据加密系统

中图分类号：TP393　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2023.03.035

医院在运行过程中会实时产生大量的数据信息，包括人事信息、设备采购信息、技术信息、医学研究成果以及患者信息等，这些信息对保证医院的正常运行起着重要的作用。在使用计算机网络技术的过程中，必须保障数据信息安全，一旦出现资料损坏或信息泄露现象，将会给医院带来巨大的损失。因此医院信息管理的重中之重是网络安全管理，要结合影响网络安全的相关因素，制定科学的维护策略，增强网络安全管理效率。

1 医院计算机网络安全的内涵

医院计算机网络安全指的是医院计算机软硬件设备以及数据具有安全性与完整性，能保持数据平稳、连续及有序运行，不受外部系统威胁的一种综合性状态。在当前医疗改革的背景下，很多医院顺应信息时代的发展趋势，建立了独立的计算机网络系统，以管理医院业务运行过程中产生的数据信息，实现对大量数据信息的存储、查找与使用，为医院正常运转提供信息支持。因此，医院信息的安全性成为医院运营管理中的重要内容之一，要求医院不断加强计算机网络的安全管理[1]。

医院计算机网络安全包括物理安全与逻辑安全两个层面。物理安全指的是医院计算机网络设备、设施的安全性与完整性；逻辑安全则体现为计算机软件运行层面的安全性。医院计算机网络安全管理内容较为复杂，包括计算机硬件设备、软件运行、人员配置等多项内容，是一项复杂的综合性体系。在医院计算机网络安全管理中，要综合考虑影响网络安全运行的各项因素，并采取必要的维护策略。

2 医院计算机网络安全的影响因素

为了优化医院计算机网络安全管理，要分析影响网络安全运行的各项因素，提升网络维护工作的针对性与有效性。

2.1 硬件因素

第一，服务器。医院计算机网络架构的核心是服务器，其性能对医院计算机网络运行效果及安全性具有直接影响。服务器能控制上层数据库及连接的计算机终端的使用情况，是保障医院计算机网络安全的基础。

第二，网络布线。网络连接及布置情况是影响网络安全的直接因素。在网络运行过程中，若网络线路出现交叉、断裂、破损等物理损伤，将直接影响计算机网络安全，不利于保持网络信号的稳定性，严重时甚至会导致网络系统瘫痪。

第三，中控机房。计算机网络设备的集中管理场所是机房，所以机房是网络控制管理的中心。中控机房的运行环境是影响网络安全的重要因素之一。在当前医疗改革的背景下，医院计算机的运行强度不断提升，给中控机房带来了较大的工作量。为了保证中控机房安全运行，要加强对机房运行环境的管理，例如避免出现机房环境温度过高的现象，否则容易影响计算机网络运行的安全性。机房运行温度出现剧烈波动的情况下，网络数据容易出现一定的偏离；若机房环境湿度较高，机房设备容易锈蚀；若机房灰尘较大，则容易影响计算机主机运行，导致设备出现噪音或者线路接触不良、短路等问题[2]。

2.2 软件因素

软件也是影响医院计算机运行安全性的重要因素之一，包括内部与外部两个层面。从内部层面分析，医院计算机网络发展历史较为短暂，在软件管理与优化层面存在着一些安全漏洞，给了不良分子可乘之机；从外部层面分析，黑客入侵以及病毒侵袭等因素给计算机网络的安全运行带来了一定隐患，若防护不足，容易出现数据损毁、丢失、系统瘫痪等问题，所以必须引起重视并加强软件维护[3]。医院计算机网络信息安全风险评估指标如表1。

表1 医院计算机网络信息安全风险评估指标体系

指标	量化指标	指标属性
计算机设施与设备	计算机网络基础建设能力等	正向
自然威胁条件	漏洞扫描能力、第三方安全指数等	正向
网络防护条件/安全审查	网络安全核查体系完整度等	正向
网络信息内容真实性	信息欺诈安全指数、网络篡改安全指数等	正向
信息可控性	信息共享度、挂马安全系数等	正向
信息隐私性	钓鱼服务器安全指数等	正向
网络资源价值性	攻击状态下价值资源的安全指数	正向
网络脆弱度	计算机中恶性程序的数量、弱口令占比等	逆向
信息对技术保障的依赖性	信息是否属于专利内容、医院计算机网络信息化与智能化水平等	正向
信息管理部门人员素质	从业人员操作计算机网络时的智慧化水平等	正向
信息安全应急响应处理	专项应急预案等工作的完备性等	正向
安全制度完善性	辅助性管理制度的落实程度与执行度等	正向
安全意识	主动防护意识等	正向
安全教育	安全宣传工作落实度等	正向
环境安全性	法律保障水平、法律约束性等	正向

2.3 人为因素

医院计算机系统的运行是在人员操作下进行的，操作人员的计算机操作水平不高给信息安全管理与防护带来了一定的隐患。对当前医院计算机系统运行情况进行实际调研可见，由于人员操作不当导致的数据错误等现象较为普遍，甚至出现了系统运行错误，例如某文档打开之后出现乱码。此外，部分医务人员的信息防护意识不足，出现随意泄露计算机权限账号、密码等现象；对计算机安全管理权限的认知不足，乱插U盘等，给医院计算机安全防护带来了一定的安全隐患，增加了病毒入侵的可能性[4]。

2.4 内部管理

医院计算机网络的安全运行需要相应的内部管理作为支撑。当前，在很多医院的网络安全管理中，内部管理不够完善，使网络运行面临着一定的安全隐患。医院业务的正常运行需要计算机网络技术的支持，为此，要构建完善的内部管理制度，避免医院计算机网络安全管理处于混乱状态。但是当前很多医务人员对计算机网络安全问题的防范意识不足，风险出现时未及时采取必要的安全防范措施，不仅降低了医务工作的效率与质量，同时给不法分子盗窃医院内部信息提供了可乘之机。内部管理不完善，加大了医院计算机网络遭受病毒攻击的可能性，影响了医院业务的正常开展，甚至产生了严重后果。所以要不断优化医院网络运行的安全管理[5]。

3 医院计算机网络安全管理工作的维护策略

要从多个角度加强医院计算机网络安全管理，制定全面的信息安全维护策略，增强安全管理工作效率。

3.1 强化计算机网络安全管理意识

为了更好地落实医院计算机网络安全管理要求，要从思想层面上提升安全防护意识，有效利用医院的人力、物力、资金等资源，发挥技术与管理优势，在医院内部构筑一套完善的计算机网络安全管理组织架构。首先，结合当前计算机网络安全管理现状，从长远发展角度出发，选拔专业人士构建计算机网络安全管理团队，优化安全管理架构设计，明确各个安全管理岗位的具体责任，将安全管理工作落实到个人，确保安全管理措施顺利实施；其次，重点分析当前医院计算机安全管理中的现实问题，构建一套系统的安全防控机制，制定应急管理机制，以更好地处理医院信息安全管理层面的突发事件；最后，医院内部职工强化安全管理意识，不断加强医院人员管理，增强所有人员的网络安全意识，在医院内部开展与网络安全管理相关的演练活动，使医院内部人员从思想层面上重视网络安全管理。

3.2 加强医院计算机病毒防范

为了更好地保障计算机网络安全，要加强医院计算机网络防火墙系统设计与应用，保证防火墙系统的设计对外界尝试性入侵具有极强的反制能力，避免外部人员盗取或者篡改医院信息，同时不断加强对先进信息技术的研究。结合当前最新技术，周期性升级防火墙系统，及时关注并完善当前网络安全隐患防范方案，利用防火墙系统防止医院系统遭受外部入侵，并为医院计算机安全管理人员提示当前面临的风险，根据医院安全管理工作的开展，提升防火墙的安全级别。

3.3 构建医院数据加密系统

为了更好地保证数据安全，可采用数据加密的方式提升医院信息网络安全。加密处理方式指的是在数据传输、存储、读取的过程中，将原有的明码信息转变为需要特定密码才能完成读取的信息处理方式，数据加密系统在计算机网络安全中被广泛运用。接收方在信息获取过程中，要基于特定的程序以及解码口令完成数据读取。数据加密技术能够使医院更安全地完成网络数据的传播与存储，避免数据被其他网络信息系统窃取。当前，很多医院在核心数据的处理层面运用了数据加密系统，有效避免了数据信息被不良分子盗取使用。当前数据加密系统具有多种加密方式，医院可以结合自身对数据安全管理的要求，设置不同的安全保密等级，以更好地保障医院数据信息的安

全性。

3.4 建立完善的网络安全制度

计算机网络安全运行的重要因素之一是人为安全，因此要加强医院网络安全制度的建立与完善，从制度层面为计算机网络安全提供保障。首先，结合当前计算机安全管理工作的开展要求，对医院内部人员进行网络安全培训，对使用、存储信息的相关人员开展计算机信息安全的专业培训，针对不同的信息数据制定不同的网络安全等级，为相关人员获取数据信息设置一定的管理权限，避免系统外部人员对特定的内部信息进行读取、调用，医院工作人员的操作权限密码不允许外泄，由专业计算机操作人员对医院信息数据进行统一管理，提升医院人员的计算机操作水平；其次，定期对医院计算机设备进行检修与维护，对不同类型的信息进行分类处理，并做好备份管理，避免由于突发事件导致信息流失，从整体保障医院计算机系统的安全性[6]。计算机网络安全量化等级与标准见表2。

表2 计算机网络安全量化等级与标准

序号	计算机网络安全等级	量化标准（γ）	安全状态描述
（1）	一级	γ∈[20，0）	脆弱度极低，网络信息安全性极高
（2）	二级	γ∈[40，20）	脆弱度较低，网络信息安全性较高
（3）	三级	γ∈[60，40）	脆弱度中等，网络信息安全性中等
（4）	四级	γ∈[80，60）	脆弱度较高，网络信息安全性较低
（5）	五级	γ∈[100，80）	脆弱度极高，网络信息安全性极高

3.5 提高医院计算机网络配置的合理性

为了更好地加强医院数据信息的安全管理，要进一步提升医院网络配置的合理性。医院计算机网络安全管理工作内容较为复杂，涉及多个领域，要结合医院数据安全管理的实际要求以及网络运行环境，增强网络配置的科学性，以提升医院网络运行质量与效率，降低网络运行中不必要现象出现的概率。在当前计算机网络技术不断更新的背景下，计算机实际使用过程中容易出现一些客观问题，影响了网络运行的安全性，导致计算机数据信息被泄露。因此要优化医院计算机设备的配置与使用，不断完善医院计算机管理，优化网络管理机制，保证工作人员在使用计算机时严格约束自身的工作行为，坚决不点击来源不明的网站，保证医院设备的正常运行，确保计算机处于安全稳定的运行状态，进一步提升计算机网络安全管理的质量。

3.6 提升计算机网络建设质量

为了进一步提升医院计算机的管理水平，要加强医院计算机网络质量建设，从硬件设备层面进行优化管理。首先，结合医院不同业务的开展需要，设置相应规格与数量的计算机硬件设备，避免大量网线交错缠绕、出现电磁干扰等问题；其次，对网络硬件设备进行定期维护，提升线路的整体使用寿命；再次，加强医院计算机机房的建设工作，医院有大量的医疗设备，机房温度较高，因此要进行必要的设备维护，保障机房内部环境的稳定性，比如安装功率适宜的空调系统，调节机房内部温度，避免机房温度过高，为硬件设备的正常运行提供保障；最后，积极引入当前最新的网络计算机技术，不断提升医院计算机硬件与软件水平，及时更新、采购设备，加快计算机运行软件的更新速度，提升计算机设备的利用效率，进一步保障医院数据信息的安全性。

4 结语

计算机系统的构建为医院各项工作的开展提供了较强的便捷性，同时为数据信息安全管理带来了一定的隐患。医院运行中要严格落实安全管理工作，构筑完善的计算机网络安全管理组织架构、明确安全管理岗位责任、加强计算机网络防火墙系统设计、提升防火墙的安全级别、采用数据加密方式等，提升医院信息网络安全，保证各项数据信息的安全性、稳定性、可靠性，为医院的顺利发展护航。

参考文献：

[1]李根.基于贝叶斯网络的医院计算机网络信息安全风险评估方法[J].电子技术与软件工程，2022,(15)：17-20.

[2]李刚.数字化医院计算机信息网络系统安全及应对策略分析[J].网络安全技术与应用，2022,(01)：119-120.

[3]赵立新.医院信息化建设中计算机网络安全管理维护措施探析[J].信息与电脑（理论版），2020，32(06)：178-180.

[4]陈松斌，赵敏，陈诗唐，等.以“统一外联平台”建设推动医院整体安全管理水平提升[J].中国数字医学，2020，15(02)：95-97.

[5]于金涛，王晓波.基于互联网+医疗健康模式下的医院网络安全与防护工作探究[J].数码世界，2020,(11)：197-198.

[6]张婉.信息技术背景下医院计算机网络安全管理探究[J].信息与电脑（理论版），2020，32(17)：182-184.

作者简介：王艳慧（1986-），女，河南项城人，硕士研究生，主要从事会计研究。