医院信息安全管理刍议

于增涛 张 屹

（首都医科大学附属北京妇产医院信息科 北京 100026）

〔摘要〕 结合北京妇产医院实践，从物理安全、网络安全、应用与数据安全、管理与统筹安全、应急处置几方面探讨医院信息安全管理相关问题，认为在医院信息安全管理工作中技术手段与管理体制缺一不可。

〔关键词〕 医院；信息安全；信息技术

Discussion on Hospital Information Safety Management *YU Zeng – tao, ZHANG Yi, Information Department, Beijing Obsterics Gynecology Hospital Afliliated to Capital Medical University, Beijing 100026, China*

〔**Abstract**〕 Combining with practices of Beijing Obstetrics Gynecology Hospital, the paper from safety of facility, network, application and data, management and coordination, response to emergency, discusses information safety management in hospital, believes that technology means and management system are both indispensable parts in hospital information safety management work.

〔**Keywords**〕 Hospital; Information security; Information technology

很长时期里，在传统意识中保障信息安全工作就是注重技术产品的购买、使用、升级换代，正因如此反而忽略了以管理为主体的人为因素的重要性，这样做使得信息安全工作缺乏全面性与完整性[1]。换言之，即使技术层面做得再好，如果管理层面不到位也不足以保障信息安全。据有关数据统计，在计算机安全事件中 70% 以上都是由于管理方面的问题所导致的[2]。所以在平时的工作中应注重技术手段与管理体制缺一不可。从理论上分析，信息安全工作只是保障、防微杜渐，根本不可能做到 100% 安全，“安全只是相对的，不是绝对的”。因此，制定并落实相关的制度，对人及其行为的管理显得更为重要，不仅可以弥补技术上的缺陷，还可以提高信息中心的工作效率。

1 物理安全

1.1 中心机房

机房的选址尤为重要，应避免建在高层、地下室及用水设备的下层级隔壁，与此同时应做好防水、防雷击、防火、防静电、防盗、防破坏等工作。信息中心应制定机房相应管理制度，并由专人管理，做好机房出入登记工作，机房作业人员必须佩戴防静电设备。机房应配备门禁系统，以防止除信息中心工作人员以外的其他人员对机房的盗窃及破坏；配备空调系统（至少双机以防止无人期间设备出现故障）保持相应温度及湿度；配备灭火器及消防自动预警系统；配备双路供电、UPS 系统、稳压器、过电压保护设备以保障电力的供应与安全。

1.2 竖井设备

分布在信息中心外的各配线架竖井关系到各门诊、住院、行政楼是否能正常工作，也应得到足够

〔收稿日期〕 2010 – 10 – 13

〔作者简介〕 于增涛，助理工程师，发表论文 1 篇；通讯作者：张屹，副主任。

重视，同样是信息安全工作的重点。首先，各竖井应安装锁具，钥匙由专人管理，并且定期检查巡视；其次，竖井中配有交换机等电力设施，同样应做好防火防水工作，竖井最好不要建在强电、水管隔层；最后，为了防止电力故障引起的断电对交换机模块的损害，每个竖井应安装 UPS 系统。

1.3 工作站

医生工作站与护士工作站所有的内网终端机器需拆除光驱、软驱类外设，对 USB 端口进行存储设备封闭。这样工作站没有配备光驱和软驱，移动硬盘、U 盘等类似的存储设备不能随意使用，不但可以防止这些存储设备携带病毒，避免人为恶意破坏医疗系统，还能防止相关资料被复制、拷贝。

2 网络安全

2.1 简述

网络安全是指通过采取各种技术和管理措施使网络系统的硬件、软件及其系统中的资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄漏，保证网络系统连续、可靠、正常地运行[3]。计算机网络系统为整个医院资源共享奠定基础，支撑着医院工作正常顺利地展开，提高了工作的效率，并拥有着良好的扩展性。但与此同时应该意识到，网络资源的共享性、扩展性越强，带来的信息安全隐患也就越大，因此从某种意义上讲网络应用的广泛性与网络安全的风险性是对立的。

随着医院规模不断扩大，具有一定规模的医院都拥有内网（业务网）和外网（办公网）两套网络系统，而采取的安全措施多为内、外网物理隔离与连接两种方式。物理隔离的方式，可以有效防止外网对内网的威胁，很大程度上保障了医疗业务的正常进行；内外网络连接的方式，需安装安全隔离网闸以提高网络安全性。

2.2 网络设备防护

医院正常工作的基本条件是网络的正常传输，因此维护网络设备应得到足够的重视。交换机、路由器、集线器、负载均衡器、打印服务器、网络机柜等设备需要定期检测，查看日志，检查指示灯状态是否正常，是否有预警报告。核心交换机需做双机热备，可以保证主交换机一旦损坏在极短的时间内自动切换到另一台交换机。对于工作量较大的医院可考虑加装负载均衡器，平均分配会话以保障服务器的稳定运行。

2.3 病毒防护

计算机病毒对信息系统的威胁不言而喻。对于病毒的防护，一方面，信息中心配备专用服务器，对所有终端安装正版杀毒软件和防火墙并定期及时升级，使得核心设备及终端病毒库得到及时更新；另一方面，需要及时对服务器等设备做系统程序更新工作，并定期安装补丁程序，防止恶意程序的攻击。

2.4 安装网络实时监控系统

对每台终端进行 24 小时的监控并记录其行为，监控绑定至 Mac 地址，防止非法入侵并破坏系统。此外安装网络实时监控系统还可以加强全院计算机管理，对不同部门的终端进行分类管理以便提高统筹管理的能力。

2.5 VLAN 的划分

虚拟局域网[4]（Virtual Local Area Network，VLAN）可以把一个局域网逻辑地划分成不同的广播域，每个 VLAN 号对应一个逻辑的广播域，同一 VLAN 内部的数据必须经过 3 层路由才可以转发到其他 VLAN 中，从而有助于流量的控制，简化网络管理、提高安全性和灵活性。在 HIS 系统中，方便了相关业务用户数据传输，同时避免不同业务用户数据包的干扰。

3 应用与数据安全

3.1 用户权限设置

对操作系统和数据库系统配置高强度用户名和口令（密码长度应该保持在 8 位以上，必须包含数

字与特殊字符），启用登录失败处理、传输加密等措施。不同服务器、数据库设置不同用户名与口令，避免同一用户名与口令可访问多台服务器，甚至医院整个信息系统。可根据具体业务的安全等级划分不同用户。对于核心保密性数据的访问与管理只允许医院主管院长或者信息中心领导掌握超级用户权限。对于其他管理员用户，应定期更换密码并对用户操作历史情况进行跟踪与记录，以形成良好的管理制度。

3.2 数据库服务器保障

廉价磁盘冗余阵列（Redundant Array of Inexpensive Disks，RAID）是一种使用磁盘驱动器的方法，它将一组磁盘驱动器用某种逻辑方式联系起来，作为逻辑上的一个磁盘驱动器来使用，使 RAID 一般是在 SCSI 磁盘驱动器上实现的[5]。对于数据库服务器来说，通常采用双机热备加 RAID5 磁盘阵列。双机热备可以保证服务器硬件一旦损坏，另一台硬件将会在极短的时间内自动切换到工作状态。RAID 是一种把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能并提供数据备份技术。采用 RAID5 不仅可以充分发挥出多块硬盘的优势，实现远远超出任何一块单独硬盘的速度和吞吐量，还可以提供良好的容错能力，在任何一块硬盘出现问题的情况下都可以继续工作，不会受到损坏硬盘的影响[6]。如条件允许应设置异地镜像服务器，建立异地存储应急机制，一旦主数据中心发生地震、火灾等特殊情况造成数据瘫痪，可由异地镜像服务器有效接管所有业务，以最大程度地减少损失。

4 管理与统筹安全

4.1 沟通与协调

一所现代化大型医院拥有几十个科室，上千名医务工作者，每天接待患者几千人次，信息中心面对的问题、困难、需求是各种各样的。因此具备一定的协调能力，应用适度的沟通技巧，让院领导、其他科室的同事及患者能够尽快明白自己要表达的意愿，得到他们的支持，这对工作的顺利开展与完成将起到事半功倍的效果。信息中心作为医院的一个职能部门，很多工作还需要与临床部门共同完成，单凭信息中心的努力是远远不够的，怎样发挥“1 +1 >2”的效应，取决于信息中心怎样与其他科室协调与合作。应时刻牢记自己代表的不仅仅是个人，而是所在科室，一言一行应对科室负责，对全院负责，真正懂得“责任胜于能力，态度决定一切”的内涵。

4.2 管理与保障制度

大型医院每天门诊量几千人次，以北京妇产医院为例（北京市属三级甲等专科医院），全院日平均门诊就诊数量 3 500 人次左右，也就意味着每时每刻都有大量患者就医，一旦发生人为不可抗拒因素导致医院信息系统出现重大问题，造成的社会影响与损失是不言而喻的，因此制定一套可行可用的应急管理办法迫在眉睫。秉承“又好又快”[7]的原则，针对不同情况拟定不同方案，把最值得信赖的同志放在最关键的应急岗位，使损失降到最低，影响程度降到最小。与此同时应定期开展应急方案的演练，从理论出发，到实践中探索，发现问题并加以改进。针对挂号室、收费处等关键部门安装医院信息系统单机版软件，平时维护中应定期对单机版升级，确保出现问题时能及时切换并正常使用。此外手工操作的各项物资应储备充足，手工处方、化验单、领药单等应安放在固定地方，保证应急响应中能够第一时间获取。

5 应急处置

医院信息系统支撑着全院医疗工作的顺利展开，无论门诊还是住院，医院信息系统几乎涉及到所有的部门，毫不夸张地说，系统一旦瘫痪短时间内所有医疗工作都将无法开展，因此做好应急处置预案是信息安全工作的重中之重。针对不同方面制定好各自的应急流程颇为重要，基本分为数据库问题、服务器问题、网络问题 3 大类。同时 3 大类的

应急流程又应该统一起来，这样才能在应急过程中把握大局。北京妇产医院应急流程，见图 1。

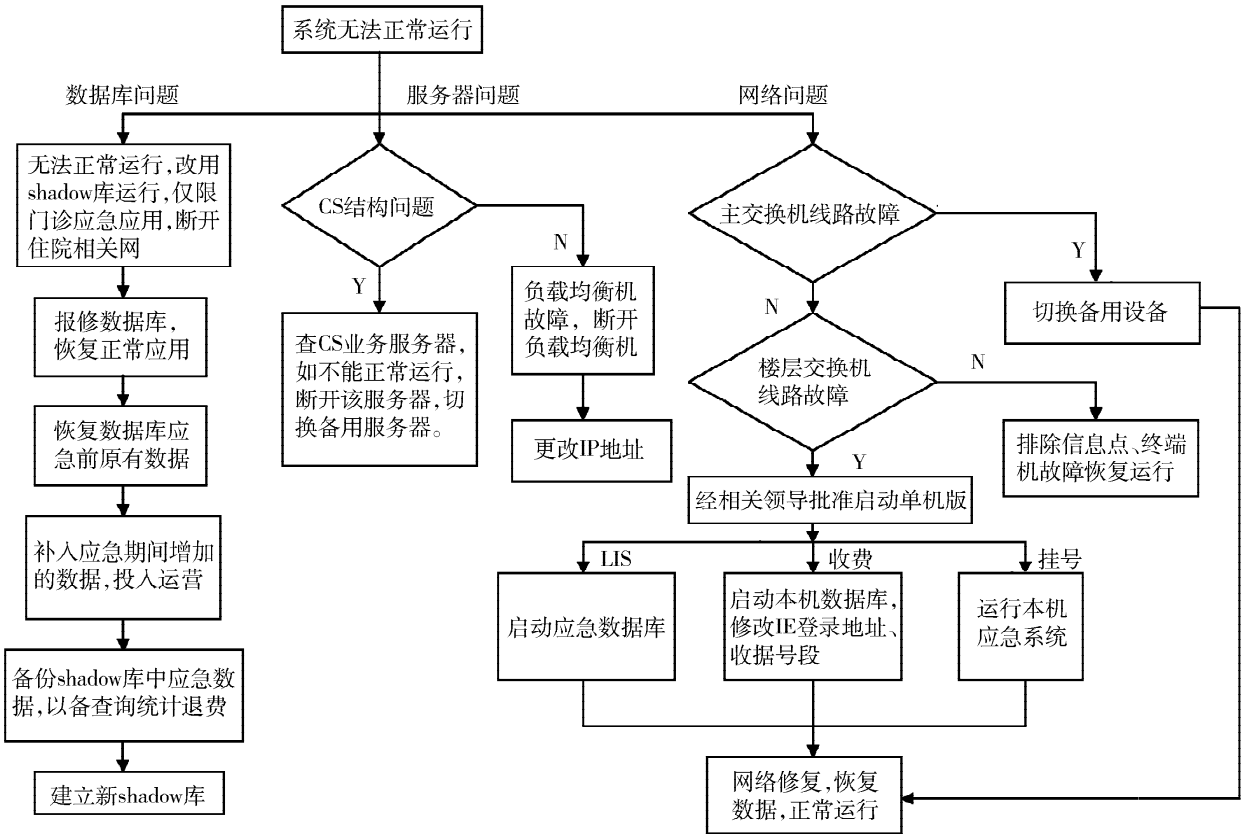

图 1 北京妇产医院应急流程

6 结语

医院的信息安全工作是一项庞大而系统的工程，就如同大海中展开的一道防鲨网，任何一点都不能有漏洞。做好信息安全工作需要每一位同志在平时的工作中一点一滴的积累与努力，正所谓“不积跬步，无以至千里；不积小流，无以成江海”。

参考文献

1 王晖. 信息安全与通信保密〔J〕. 2008, （增刊）：1 - 30.
2 张心明. 信息安全管理体系及其构架〔J〕. 现代情报，2004，（4）：204 - 205.
3 黄惠烽. 网络安全与管理〔J〕. 内江科技，2008，29（7）：142 - 143.
4 骆正云. 医院虚拟局域网规划与实现〔J〕. 医疗设备信息，2005，20（11）：10 - 11.
5 王崇霞. 数据库双机热备份系统解决方案. 微机发展，2003，13（6）：80 - 85.
6 张红，倪皖东. 我院主机系统设计方案〔J〕. 中华医院管理杂志，2001，17（5）：292 - 294.
7 王小元. 从又快又好到又好又快看科学发展观〔J〕. 生态经济，2008，（12）：95 - 98.