地震信息安全管理现状及策略研究

郝 柽，杨立庭，洪 敏，赵林林，高永国
（甘肃省地震局，甘肃 兰州 730000）

摘要：随着网络和信息技术的发展，信息安全建设已经成为信息化建设的重要组成部分。网络信息安全问题已经上升为一个关系到国家前途的战略高度的问题。信息安全这门处于蓬勃发展中的科学，将会越来越密切地关系到社会的各行各业。本文分析了地震信息安全管理的现状，并着重讨论了加强地震信息安全管理的策略。

关键词：信息安全；安全管理；安全策略
中图分类号：P315－392.2；TP393.08 **文献标志码**：A **文章编号**：1000－0844(2013)增刊－0201－05
DOI:10.3969/j.issn.1000－0844.2013.增刊.0201

The Seismic Information Security Management Status and Strategy Research

HAO Zheng, YANG Li-ting, HONG Ming, ZHAO Lin-lin, GAO Yong-guo
(*Earthquake Administration of Gansu Province, Lanzhou Gansu 730000, China*)

Abstract: With the development of network and information technology, the construction of information security has become an important part of information construction. Network information security has been a strategic problem related with the future of the nation, which should be paid more attention to. As a growing science, information security will be more and more closely related to all sectors of society. In the paper we analyzed the status of information security management and focused on the strategy which could strengthen the security management of seismic information.

Key words: information security; security management; security policy

0 引言

在信息社会中，一方面信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用，另一方面由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出。由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，这样将使组织在业务运作过程中面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞，以及大量存在于组织内外的各种威胁，因此对信息系统需要加以严格管理和妥善保护，信息安全管理也随之产生。

1 国外信息安全管理现状

(1) 制订信息安全发展战略和计划

制订发展战略和计划是发达国家一贯的作法。美、俄、日国家都已经或正在制订自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。2000年初，美国出台了电脑空间安全计划，旨在加强关键基础设施、计算机系统和网络免受威胁的防御能力。2000年9月12日，俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措

收稿日期：2013-10-20
基金项目：2013年度甘肃省地震局政策研究课题(zy2013001)
作者简介：郝 柽(1971－)，男，高级工程师，主要从事地震信息网络维护工作. E－mail:good@gssb.gov.cn

施[1]。

(2) 加强信息安全立法,实现统一和规范管理

以法律的形式规定和规范信息安全工作是有效实施安全措施的最有力保证。制订网络信息安全规则的先锋是各大门户网站,美国的雅虎和美国在线等网站都在实践中形成了一套自己的信息安全管理办法。2000 年 10 月 1 日,美国的电子签名法案正式生效。2000 年 10 月 5 日美参议院通过了《互联网网络完备性及关键设备保护法案》[2]。2000 年 9 月,俄罗斯实施了关于网络信息安全的法律。

(3) 标准化与系统化管理

在 20 世纪 90 年代之前,信息安全主要依靠安全技术手段与不成体系的管理规章来实现。随着 20 世纪 80 年代 ISO9000 质量管理标准的出现及随后在全世界的推广应用,信息安全管理也同样在 20 世纪 90 年代步入了标准化与系统化管理的时代。1995 年英国率先推出了 BS7799 信息安全管理标准,该标准于 2000 年被国际标准化组织认可为国际标准 ISO/IEC17799。现在该标准已引起许多国家与地区的重视,在一些国家已经被推广与应用;组织贯彻实施该标准可以对信息安全风险进行全面系统的管理,从而实现组织信息安全。与此同时,其他国家以及组织也提出了很多与信息安全管理相关的标准。

2 中国信息安全管理现状

(1) 初步建成了国家信息安全组织保障体系

国务院信息办专门成立了网络与信息安全领导小组,成员有信息产业部、公安部、国家保密局、国家密码管理会员会、国家安全部等强力部门,各省、市、自治州也设立了相应的管理机构。2003 年 7 月成立了国家计算机网络应急技术处理协调中心(简称 CNCERT/CC)。

(2) 制定和引进了一批重要的信息安全管理标准

为了更好地推进我国信息安全管理工作,公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17895－1999《计算机信息系统安全保护等级划分准则》,并引进了国际上著名的《ISO 17799:2000:信息安全管理实施准则》、《BS 7799－2:2002:信息安全管理体系实施规范》、《ISO/IEC 15408:1999(GB/T 18336:2001)－信息技术安全性评估准则 》、《SSE－CMM:系统安全工程能力成熟度模型》等信息安全管理标准[3]。

(3) 制定了一系列必须的信息安全管理的法律法规

从上世纪 90 年代初起,为配合信息安全管理的需要,国家、相关部门、行业和地方政府相继制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《商用密码管理条例》、《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《中华人民共和国计算机信息系统安全保护条例》《计算机病毒防治管理办法》、《互联网电子公告服务管理规定》、《软件产品管理办法》、《电信网间互联管理暂行规定》、《电子签名法》等有关信息安全管理的法律法规文件。

3 地震行业信息安全管理现状

地震信息网络从地震监测运行的一个业务支撑系统已经逐步发展成为具有一定规模的行业信息基础系统,建成了全国地震行业网络系统、数据系统、信息服务系统、地震现场卫星通信系统、政务系统和网络监控管理系统等业务子系统,初步完成了覆盖全国的从国家－区域－大中城市－县级－台站的层次化的中国地震行业网络系统。实现了网络通信、网络服务、数据存储、应用服务、政务办公、网络安全等功能,以及“网络到台站,IP 到仪器”的目标。为地震监测、地震预测、科研、地震应急响应、地震灾害评估等多种应用搭建一个先进的、功能强大的技术支撑平台。地震信息网络已成为地震行业各业务系统正常运转的必要保障,是防震减灾事业发展的关键环节。

(1) 安全管理规章制度和技术方案

目前地震行业信息网络的建设与发展,已经与防震减灾三大工作体系的建设、地震科学研究及科技创新工作的关系日趋紧密,地震业务工作对信息网络的依赖性日趋增强。地震信息网络不仅为防震减灾工作提供了网络、通讯、数据、信息、计算等技术支撑,而且在推进地震行业的全面网络化、信息化进程中具有极其重要的作用和地位。地震行业内也相继出台了《地震信息网络管理暂行规定》、《地震信息网络运行管理办法》、《中国地震局信息安全等级保护建设方案》、《中国地震信息服务系统技术规范》等一系列的信息网络安全管理规章制度和技术方案。

(2) 地震信息网络安全防护薄弱

随着地震信息网络规模的逐步扩大,承载业务量和依存度快速增加。一旦发生网络中断和服务停滞,就会出现地震监测数据传输、交换与服务中断、

地震预警信息汇集停顿、应急指挥系统陷入混乱、紧急救援行动延缓等场景,其后果将十分严重。在"5·12"汶川地震后陕西和广西地震局网站被黑客攻击,黑客甚至在陕西地震信息网主页上发布了"23时30分陕西等地会有强烈地震发生"的虚假信息,产生了不良的社会影响。汶川特大地震发生后中国地震信息网站(CSI)受公网带宽限制,因访问过多导致约2个小时的瘫痪,直到13日CDN提供服务后才完全正常地提供信息服务,但仍存在响应速度慢的现象。显然,对地震信息网站在大地震时的舆论作用认识不足,仓促上阵,缺少技术准备和信息资料储备,大震信息服务能力明显不足,没有做好应急预案的准备。

(3) 等级保护定级工作初步完成

根据《国家信息化领导小组关于加强信息安全保障工作的意见》、《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》等文件要求,地震系统已经完成全部信息系统的定级工作。通过系统定级,行业信息系统安全较之国家等保要求有一定差距与不足,需要制定相关方案,对信息系统安全进行全面改建,配合国家完成等保后续系统评审、审批,备案等工作[4]。

(4) 安全管理意识不强

在有需要信息共享时,就开通网络连接,很少考虑安全问题,安全评估不足。已经投入的安全设备大多是在多项目中拼凑而成,没有统一的安全规划。办公网、业务网和互联网互相关联,存在不安全因素。

4　加强地震信息安全技术和管理策略

面对信息网络存在的各种安全问题,应建立起地震信息网络安全机制、灾难备份体系、快速恢复重建体系;地震信息网络应对突发事件的办法、机制、技术等,保证紧急事件状态下的信息网络接续服务;地震信息数据安全保障和技术措施,建立保密数据和电子政务系统特别安全防护机制;建立完善管理规则和管理体系,保障地震信息网络安全健康稳定运行,保障地震信息网络的可持续发展。要实现上述任务,根据本行业各项业务及其计算机信息系统实际,需要从网络技术和网络管理两个方面加强和完善地震信息的安全策略。

技术安全策略通常与信息系统提供的技术安全机制有关,主要是通过在信息系统中部署软硬件并正确的配置其安全功能来实现;管理类安全策略通常与信息系统中各种角色参与的活动有关,主要是通过控制各种角色的活动,从政策、制度、规范、流程以及记录等方面做出规定来实现。

4.1　网络技术策略

4.1.1　物理安全

旨在保护计算机服务器、数据存贮、系统终端、网络交换等硬件设备免受自然灾害、人为破坏,确保其安全可用。制定物理安全策略,要重点关注存放计算机服务器、数据存贮设备、核心网络交换设备的机房的安全防范。其选址与规划建设要遵循《GB/T 9361－2011 计算机场地安全要求》和《GB2887－2011 计算机场地通用规范》,保证恒温、恒湿,防雷、防水、防火、防鼠、防磁、防静电,加装防盗报警装置,提供良好的接地和供电环境,要为核心设备配置与其功耗相匹配的稳压及UPS不间断电源[5]。

根据计算机信息系统应用需求,要兼顾系统的可靠性和经济性,设计和配备必要的冗余设备。对那些可靠性要求高的系统,可考虑采用服务器主机双机热备、磁盘阵列,配备备用网络,建立异地容灾备份中心。

4.1.2　网络安全

旨在防范和抵御网络资源可能受到的攻击,保证网络资源不被非法使用和访问,保护信息网内各类地震数据安全。

访问控制是维护网络安全、保护网络资源的重要手段,是网络安全核心策略之一。访问控制包括入网访问控制、网络授权控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和节点的安全控制以及防火墙控制。安全检查(身份认证)、内容检查也是保护网络安全的有效措施。

在加强访问控制的同时,可考虑对网络传输的地震数据进行加密。网络加密手段包括链路加密、端点加密和节点加密,链路加密是保护网络节点之间的链路数据安全,端到端加密是对从源端用户到目的端用户之间传输的数据提供保护,节点加密是对源节点到目的节点之间的传输链路提供保护。数字认证在一定程度上保证了网上信息的安全。

4.1.3　数据安全

旨在防止数据被偶然的或故意的非法泄露、变更、破坏,或是被非法识别和控制,以确保数据完整、保密、可用。数据安全包括数据的存储安全和传输安全两个方面。

数据的存储安全系指数据存放状态下的安全,

包括是否会被非法调用等，可借助数据异地容灾备份、密文存储、设置访问权限、身份识别、局部隔离等策略提高安全防范水平。

4.1.4 应用安全

旨在防止由于软件质量缺陷或安全漏洞使信息系统被非法控制，或使之性能下降、拒绝服务、停机。软件安全策略分为系统软件安全策略和应用软件安全策略两类。

系统软件包括操作系统和数据库软件。当前，主流操作系统软件均存在漏洞，在设计信息系统时，选用相对成熟、稳定和安全的系统软件，并通过其官方网站或合法渠道，密切关注其漏洞及补丁发布情况，及时下载补丁软件，弥补不足。

无论是通用的应用软件，还是量身定做的行业应用软件，都存在安全风险。对前者，可参照前款作法，通过加强与软件公司的沟通，及时发现、堵塞安全漏洞。对后者，可考虑优选通过质量控制体系认证、富有行业软件开发的软件公司，加强软件开发质量控制，加强容错设计，安排较长时间的试运行等策略，以规避风险，提高安全防范水平[6]。

4.2 网络管理安全策略

4.2.1 安全管理制度

应制定信息安全工作的总体方针和安全策略，建立安全管理制度和操作规程，形成由安全策略、管理制度、操作规程等构成的全面的地震信息安全管理制度体系；指定或授权专门的部门或人员负责安全管理制度的制定，管理制度应具有统一的格式，对制度进行论证和审定，通过正式、有效的方式发布，并对收发文进行登记。信息安全领导小组应负责定期审定安全管理制度体系，必要时进行修订。

4.2.2 安全管理机构

应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人、系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责，成立指导和管理信息安全工作的委员会或领导小组，明确职责、分工和技能要求。配备一定数量的系统管理员、网络管理员、专职安全管理员，关键事务岗位应配备多人共同管理。根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等，建立审批程序，定期审查审批事项，记录审批过程并保存审批文档。安全管理员应负责定期进行安全检查，内部人员或上级单位定期进行全面安全检查，制定安全检查表格实施安全检查，制定安全审核和安全检查制度。

4.2.3 人员安全管理

应指定或授权专门的部门或人员负责人员录用，严格规范人员录用过程，签署保密协议，从内部人员中选拔从事关键岗位的人员并签署岗位安全协议。严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，办理严格的调离手续。定期对各个岗位的人员进行安全技能及安全认知的考核，对关键岗位的人员进行全面、严格的安全审查和技能考核，对考核结果进行记录并保存。对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，应对安全责任和惩戒措施进行书面规定并告知相关人员，对定期安全教育和培训进行书面规定，对安全教育和培训的情况和结果进行记录并归档保存。应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案，对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定。

4.2.4 系统建设管理

应明确信息系统的边界和安全保护等级，应确保定级结果经过相关部门的批准。应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施，对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准。应确保安全产品采购和使用符合国家的有关规定。应指定专门的部门或人员负责管理系统定级的相关材料，将系统等级及相关材料报系统主管部门备案。在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。应确保安全服务商的选择符合国家的有关规定。

4.2.5 系统运维管理

应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理，指定部门负责机房安全，并配备机房安全管理人员，建立机房安全管理制度，加强对办公环境的保密性管理。应编制并保存与信息系统相关的资产清单，建立资产安全管理制度，对资产进行标识。应对信息系统相关的各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理，建立设备安全管理制度。应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存，建立安全管理中心。指定

专人对网络进行管理,应建立网络安全管理制度。应根据业务需求和系统安全分析确定系统的访问控制策略,定期进行漏洞扫描,安装系统的最新补丁程序,建立系统安全管理制度。应识别需要定期备份的重要业务信息、系统数据及软件系统等,建立备份与恢复管理相关的安全管理制度,立控制数据备份和恢复过程的程序。应报告所发现的安全弱点和可疑事件,但任何情况下用户均不应尝试验证弱点,制定安全事件报告和处置管理制度,制定安全事件报告和响应处理程序。

5　结语

在地震信息网络安全管理过程中,技术策略从物理安全、网络安全、主机系统安全、数据安全和应用安全几个层面提出安全技术要求;管理策略从安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理几个方面提出安全要求。根据国家有关规定和标准规范要求,按照管理和技术并重的原则,将技术策略和管理策略有机结合,建立地震信息系统综合防护体系,提高地震信息网络系统整体安全保护能力。

技术要求与管理要求是确保地震信息系统安全不可分割的两个部分,两者之间既互相独立,又互相关联,在一些情况下,技术和管理能够发挥它们各自的作用;在另一些情况下,需要同时使用技术和管理两种手段,实现必要的安全控制;只有以有效的信息安全管理体系为基础,完善信息安全管理结构,综合应用信息安全管理策略和信息安全技术策略,才能有效保证地震信息系统的安全可靠稳定运行。

参考文献

[1] 李光文. 计算机网络安全[M]. 武汉:湖北人民出版社,2002.

[2] 孙立立. 美国信息安全战略综述[J]. 信息网络安全,2009,(8):7-10.

[3] 韩永飞. 信息安全与管理[J]. 网络安全技术与应用,2002,(2):33-36.

[4] 计算机信息系统安全保护等级划分准则(GB 17859－1999)[S]. 北京:中国标准出版社,1999.

[5] 中国地震信息服务系统技术规程[M]. 北京:地震出版社,2005.

[6] 毛汗书. 网络技术基础[M]. 北京:人民邮电出版社,2000.