文章编号：1005-8451（2015）02-0001-04

铁路行业信息安全管理面临的挑战及对策探讨

史天运
（中国铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：随着铁路行业信息化程度不断提高，信息安全风险日益成为影响行业核心业务的重要因素。本文从铁路行业安全管理现状入手，分析行业信息安全管理面临的挑战，探讨如何通过管理机构及多维管理制度的建设，结合信息安全综合管理平台，制定符合铁路行业的信息安全风险防范措施和管理办法。

关键词：铁路信息化；信息安全；安全管理；综合管理平台
中图分类号：U29-39 **文献标识码：**A

Challenges and countermeasures of railway information security management

SHI Tianyun
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: As the informatization constantly improved, information security risk was increasingly becoming an important factor affecting the key business of railway. On the basis of the current situation of railway information security management, the paper analyzed the challenges of information security management, discussed prevention measures and management methods of railway information security risk by means of constructing regulatory agency and institution, combined with integrated management platform of information security.

Key words: railway informatization; information security; security management; integrated management platform

随着信息系统在铁路应用范围的不断扩大、功能的不断强大、网络覆盖的不断延伸、开放性与互联性的不断增强以及技术复杂性的不断提升，信息网络和信息系统自身的缺陷、脆弱性以及来自内外部的安全威胁等所带来的信息安全风险日益凸显，并且日趋多样化和复杂化，传统的安全管理方式已不适应信息安全保障要求，必须采取先进的管理理念和科学的管理方法。

铁路信息安全管理是运用科学的理论和方法制定有效管控和处置措施，加强安全风险过程控制，强化应急处置，使安全风险可能造成的后果降低到可以接受的程度。实施铁路行业信息安全管理既是系统安全稳定运行的内在需要，也是保障铁路运输安全和正常秩序的必然要求。

1 铁路信息安全管理面临的挑战

1.1 行业信息安全等级保护标准体系缺乏

信息安全等级保护制度是我国信息安全保障工作的基本制度，开展信息安全等级保护工作是保护我国信息化健康发展、维护基础信息网络与重要信息系统安全的根本保障。目前，铁路信息系统安全建设和管理的目标不明确；信息安全保障工作的重点不突出；信息安全监督管理缺乏依据和标准，监管体系尚待完善。如何在信息安全等级保护相关国家标准的基础上，研究适合铁路信息系统安全等级保护的行业标准，提出一套完整的等级保护行业标准体系是铁路行业信息安全管理工作面临的重要挑战。

1.2 信息安全运行维护管理体系不健全

铁路信息安全事故绝大多数由管理手段缺失或执行不到位导致，因此信息系统的安全运维管理是铁路安全生产的重要环节。铁路行业系统的运营及生产安全的管理思想比较落后，与铁路信息化建设和发展速度严重脱节，管理手段还主要依靠人员意识和单纯的手工式作业，缺乏行之有效的安全运行维护管理体系。主要表现在：维护人员操作无依据、执行不到位；应急预案可操作性差，应急演练欠缺，应急处置效果不佳；系统运行监测监控手段缺乏，网

收稿日期：2014-10-08
作者简介：史天运，研究员。

络监管不够。

1.3 安全管理措施缺乏有效执行力

铁路行业系统日趋商业化，面临的信息安全风险和挑战更加严峻，信息系统的网络边界防护及准入控制等措施是否完备且有效执行，是行业面临的重要挑战。对已发布的规章制度的执行力不强，对各类存储介质或外部接入设备的管理和准入控制措施执行不到位，如出口准入控制、客户端准入控制、服务器准入控制、网络准入控制方面规章制度不完善；另外，系统网络边界防护措施、系统之间安全隔离措施、互联网接入安全防护措施、重要数据传输及存储的安全管理措施不够具体，缺乏实效性。

1.4 安全检查工作缺乏持续性和针对性

铁路行业信息安全检查工作一直都作为一个常态化的管理机制运行，在一定时间间隔内定期或不定期开展，但大部分单位对检查工作认识不足，需要动用技术力量对系统进行扫描、渗透并部署采集设备时，各单位普遍有畏难情绪，运行维护部门又担心会影响正常的业务使用。总体来看，检查工作本身所能提供的信息有限，从而无法真实并准确反应单位信息系统及信息安全现状，也就无法对系统进行有针对性的信息安全加固及整改。

2 应对措施

建立良好的信息安全管理模式是铁路信息系统安全稳定运行的根本保障，有利于铁路行业信息系统的发展。针对上述铁路信息安全管理面临的挑战，建立铁路行业信息安全管理新模式，结合铁路行业现有组织管理架构，借鉴已有的信息安全管理制度，明确信息安全工作的地位、目标、原则以及策略，从组织管理、制度及应急管理、运行维护管理和等级保护管理几个方面来深入考虑和分析，采用体系化管理方式保障信息系统的安全稳定运行。

2.1 健全组织管理机构

信息安全组织管理方面，建立并逐步健全一套自上而下的安全组织机构，成立铁路信息系统安全管理领导机构，作为系统安全管理的常设组织。同时，采用分层结构，以适应铁路行业铁路总公司、铁路局、站段 3 级管理机制。组织架构如图 1 所示。

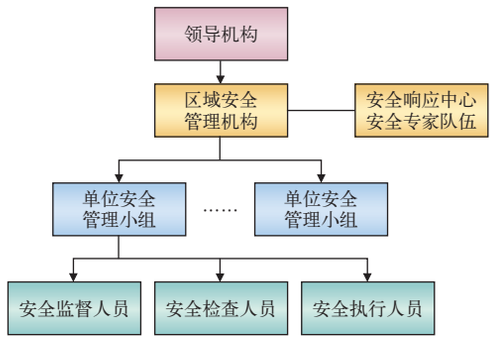

图1 铁路信息系统安全管理组织结构

铁路总公司领导机构作为全路信息系统安全管理的常设领导机构，负责制定全路信息系统安全管理制度及办法，发布铁路信息系统安全防护技术的标准，制定安全管理制度。区域安全管理机构主要职责有：负责各铁路局的信息安全管理中心的日常管理工作，及时与安全专家协商讨论安全执行方案，执行安全响应中心制定的具体安全策略，定期向上级汇报信息安全管理相关工作，下设多个安全管理决策小组和管理执行小组，管理执行小组主要负责监督和协调铁路局下设各车站的信息安全管理执行工作。车站级信息安全执行分组包括安全监督员、安全检查员、安全执行员 3 类安全工作人员。

2.2 强化制度建设及工作流程管理

2.2.1 管理制度

铁路信息系统安全不仅要强化系统建设，更要做好内部安全管理建设，具体要做好以下工作：

（1）建立专门的安全防御组织：针对铁路信息系统整体安全，铁路总公司应成立专门的机构，负责网络的安全管理和应急响应。铁路局、基层站段相应的部门，对铁路基础网实施自顶向下的实时监控与管理。

（2）建立健全安全保密制度：各部门应制定严格的安全保密条例，杜绝不必要的人员接触和了解铁路核心网络设备与技术，防止敏感信息泄露。对有权了解、处理关键信息的内部人员制定更严格、更详细的安全责任制度，明确个人在信息安全方面应该承担的职责以及发生责任事故后的处罚。

（3）建立健全数据安全保护措施：针对铁路核心业务系统的关键数据，需要建立完备的本地和异地备份制度，同时，采用双机备份、物理隔离的技

术方案，定时增量备份。

（4）定期实施漏洞扫描和系统补丁升级：系统管理人员需定期对网络进行扫描，以检测和评估网络漏洞。检测范围包括所有的网络设备和终端设备，同时扫描网络内所有主机系统的配置及安全漏洞。

（5）定期实施计算机安全检查：针对处理关键数据的计算机，应建立完善的日志，记录所有与安全有关的事件。安全日志不仅要完整的记录安全事件，而且需要具备防篡改、抗抵赖功能。

2.2.2 标准制度

以信息安全相关管理和技术规范及不同层次的信息安全制度为重点，构建科学严谨、有效适用、系统规范的信息安全管理标准制度体系。制定相应的技术标准、作业办法等，明确工作标准，流程，落实管理责任，规范作业行为。按照信息安全风险管理的要求，对各项管理规章制度进行全面的清理和完善，不断加强铁路信息安全标准制度体系建设，使铁路信息安全风险管理工作制度化、规范化和标准化。

2.2.3 工作流程管理

信息安全管理流程包括信息安全培训工作流程、信息安全运行维护工作流程、信息安全风险控制流程、信息安全应急处置流程、信息安全监督检查与改进流程等各项管理工作流程。应根据工作实际情况，建立健全、持续改进、推广应用先进的信息安全管理工作流程，使铁路信息安全管理和运行维护工作专业化、标准化、规范化。

2.3 建立信息安全运行维护管理体系

2.3.1 安全风险管理

铁路信息系统安全管理中心采用风险评估的方法，分析和评估系统的风险源和安全威胁源，并根据各类信息资产的重要程度和价值，选择适当的控制措施减缓风险。铁路局要组织建立安全风险管理体系，进行信息资产风险评估和风险处理。

从理论上，风险只能降低或减少而不能完全消除。选择控制措施的原则是既能使铁路信息系统受到与其价值和保密等级相符的保护，将其所受的风险降低到可接受的水准，又能使所需要的费用在预算范围之内，使铁路行业能够保持良好的竞争力和成功运作的状态。另外，系统的风险是动态的，风险评估活动应定期进行，特别是在系统的核心功能及技术发生重大变化和内外环境发生重大变化时，风险评估应重新进行。

2.3.2 安全运行维护

铁路信息系统安全运行维护管理依托安全管理中心实现系统的安全运行维护。铁路总公司信息系统安全管理中心运行维护平台可实现对系统中的网络、主机、安全系统、数据库、中间件、存储备份设备和应用系统的可视、可控、可管理，协助运行维护人员监控系统和及时发现问题。各铁路局安全管理部门运行维护人员应通过使用运行维护平台，积极开展运行维护管理工作，实现铁路局安全监管监察部门与铁路总公司安全运行维护工作的有效连接。对各地区安全管理部门能够处理的事件，按照路局区域内管理流程执行，并定时向铁路总公司安全管理中心上报故障情况并提交运行维护处理单。

2.3.3 安全应急响应

铁路信息系统安全应急响应体系的建立应做好以下 5 个阶段工作。

（1）保护阶段：制定应急反应工作流程计划、确定预警和报警的方法、建立备份的体系和流程、建立安全的系统、进行应急反应事件处理的预演。

（2）预警与报警：识别和发现各种安全的紧急事件。在紧急情况发生前，产生安全的预警报告，在紧急情况发生时，产生安全警报给应急反应中心。应急反应中心将根据事件的级别，采取相应措施。

（3）牵制与反馈：在确认紧急事件发生的情况下，应急反应中心将根据预先制定的反应计划，进入应急反应流程。同时，应急反应系统本身将根据预先制定的规则，采取相应的措施，把紧急事件的影响降到最小。

（4）消除阶段：对于系统内部病毒，应该采用最新的病毒专杀工具清除。对于系统的外部入侵和非法授权访问等，应该通过专用的漏洞扫描工具发现系统存在哪些漏洞，然后采用相应的手段消除漏洞安全隐患。对于入侵攻击或超量访问要采用有效的拦截和限量访问措施，使系统资源处于可控范围。

（5）恢复阶段：在数据或者系统被破坏，无法修复的情况下，应进行系统的恢复，且恢复要依据

预先制定的恢复流程严格进行。

2.3.4 安全策略优化

制定有效的安全策略，当原有安全策略无法满足现有系统的安全需求时，要结合实际情况对系统安全管理策略进行调整优化，以适应新的安全管理制度。制定出符合铁路信息系统的安全管理策略，以确保系统的信息安全保密性为主，采用多层次保护、最小授权、综合保护和严格管理等措施。

2.3.5 安全检查审计

安全检查审计依托安全管理平台，通过对铁路信息系统中相关信息的收集、分析和报告，判定现有系统安全控制手段的有效性，检查系统的误用和滥用行为，统计系统的安全事件，并按照安全事件的影响和危害程度进行等级划分，从而验证当前安全策略的合规性，为以后的归纳总结，安全系统的进一步改善提供依据。安全管理平台根据从专项的日志审计产品、终端审计产品、数据库审计产品和应用审计产品中收集上来的信息进行关联分析，进行审计规则匹配，发现违规行为并进行告警和响应。

通过安全审计与安全管理平台的融合，使得安全审计体系的建设与安全管理平台的建设目标达成了一致，有助于铁路信息系统整体安全体系的形成和完善，并通过对安全事件的分析，把握系统安全威胁的发展趋势，形成日报告或周报告进行定期安全信息通报，为系统的安全策略优化提供决策性指导。

2.4 建立等级保护管理制度

为切实做好信息安全管理工作，铁路行业需要借助等级保护这一安全抓手，将等级保护与信息安全日常管理紧密结合，将信息安全管理全面纳入铁路运输安全生产管理体系，按照“谁主管谁负责、谁运行谁维护”和属地化管理原则，逐级落实信息安全责任，建立地方与总公司信息化发展相适应的信息安全监督管理机制。同时，为了在纵向上实现对等级保护的控制，铁路行业主管部门在国家文件政策指导下，应制定符合本行业安全需求的等级保护行业标准、行业等级保护实施方法等文件，用以指导本行业的等级保护工作，保障铁路运输及生产安全管理。

2.5 建设铁路信息安全综合管理平台

为保证铁路信息安全等级保护工作的有序展开，需要建设信息安全综合管理平台，旨为铁路总公司及下属单位开展与信息安全管理相关工作的综合工作平台，功能将覆盖铁路总公司及其下属单位的信息安全管理工作的主要内容，并支持公安部等级保护管理工作。平台主要提供以下 3 类功能：（1）以信息系统定级、备案、整改、测评和检查等规定步骤为主线，实现等级保护工作任务的下发、执行、进度监控和督办；（2）风险管理、应急管理、安全检查和事故通报等专项管理功能；（3）日常办公的综合管理、培训教育、标准管理等。

3 结束语

铁路行业信息安全问题更多来源于内部，这就不仅要在安全性技术上下功夫，而且更应该从信息安全管理模式和方法上入手。本文从组织管理、制度及应急管理、运行维护管理和等级保护管理几个方面详细探讨了如何健全和强化管理制度，并通过建立信息安全综合管理平台，实现信息安全工作的规范化管理，促进信息安全管理工作的常态化发展，最终实现铁路信息系统统一、规范、监管和完善的信息安全运用。

铁路行业各单位、各部门要进一步提高对铁路信息安全重要性和开展信息安全管理工作必要性的认识，切实增强做好信息安全工作的自觉性和主动性，努力掌握先进的管理方法，准确把握信息安全风险管理的重点和关键，科学推进铁路信息安全管理工作的有序开展。

参考文献：

[1] 祝咏升，张　彦 . 铁路信息系统安全管理中心的设计 [J].中国铁路，2012（10）：24-28.

[2] 铁路总公司 . 关于印发《铁路信息安全风险管理实施意见》的通知（铁信息 62 号）[Z]. 北京：中国铁路总公司，2013.

[3] 王令朝 . 创建铁路信息安全管理及其标准体系的探讨 [J]. 铁道技术监督，2010，38（7）：1-5.

[4] 朱文生，陈　笃 . 浅论银行业信息安全管理面临的挑战及对策 [J]. 中国金融电脑，2014（2）：71-74.

[5] 李益文 . 烟草行业信息安全运维管理体系建设的思考 [J]. 信息网络安全，2009（2）.

责任编辑　方　圆