# 浅析如何完善高校网络信息安全管理应急处理机制

张明震

（华东政法大学信息化办公室　上海　201620）

【摘　要】随着高校信息化管理的逐步深化，对网络信息安全管理也越来越重视。然而，在网络信息安全管理的过程中，如何应对网络信息安全管理突发事件则是一件值得重视的事情，本文则着重研究如何完善高校信息安全管理应急处理机制。通过健全信息安全应急响应机构、建立健全信息安全突发事件应急预案以及科学处理信息安全突发事件等措施进一步完善高校信息安全应急处理机制，这将对高校信息安全管理工作起到关键性的作用。

【关键词】高校；网络信息安全；管理

中图分类号：C912.6；D035　　文献标识码：A　　文献编号：1009-6833（2014）03-141-02

## Analysis on how to improve the management of university network information security emergency response mechanism

Zhang Mingzhen

Abstract：with the gradual deepening of college information management，and more attention to network information security and management.However，in the process of network information security management，how to deal with the network information security emergency management is one of important things，this paper focuses on how to improve the information security management of university emergency treatment mechanism.The perfect information security emergency response mechanism，establish and improve information security emergency response plan and scientific treatment of information security incidents and other measures to further improve the information security emergency response mechanism，which will be the key role in the information security management.

Keywords：management of university；network information security；incidents

## 0　引言

随着全球信息技术的快速发展，教育信息化建设尤其是高校信息化建设也取得了丰硕的成果。截止目前，我国的大部分地区的高校的网络信息化建设已全部建成，同时对网络信息化的利用也越来越高。如今的校园网络显然已经成为各高校教职工的教学、科研、管理以及学生的日常学习、生活的重要一部分，上海S高校也不例外。作为高校网络的基础设施，如高校的档案管理系统、校园一卡通信息管理系统、人事管理系统、校园数字化管理系统、精品课程的建设、图书馆资源信息等等都是信息化管理的重要部分。高校师生充分利用信息化网络带来的便利，信息资源也得到了极大程度的共享的同时，信息安全问题也悄悄的来临。

## 1　健全信息安全应急响应机构

通过健全和强化高校信息安全突发事件应急响应组织机构，可以有效应对突发事件发生时的及时应对。

根据高校内部情况，可以由学校主要分管领导担任校园信息安全突发事件危机管理小组的组长，而组员可以由学校党办、校办、保卫处、宣传部、信息办、团委、学生处、后勤等有关职能部门的负责人来担任。同时，该小组分别下设办公室、保卫组、宣传组、IT技术组、后勤组等工作小组。为了统一协调日常工作，办公室是学校信息安全应急处理日常办事机构，主任则由党办校办负责人兼任，而各职能部门负责人则兼任各小组的组长。有了应急响应组织机构，一旦发生校网络信息安全突发事件，就可以由指挥中心统一指挥，各个工作小组统一协调，应对突发事件的发生。

## 2　做好信息安全风险评估工作

所谓信息安全风险评估是指政府机关、企事业等单位部门，在信息安全管理过程中，依据国家有关信息安全管理的技术标准，对信息系统及信息的安全属性进行科学评价的过程。信息安全风险评估的任务包括：首先，评估信息系统的脆弱性；其次，评估信息系统面临的攻击威胁，一旦信息系统成为攻击对象，即将面临黑客攻击，这时要对攻击源进行评估，对自己的状态，自己的防御能力进行评估；再次，评估脆弱性被威胁源利用后所产生的实际负面后果，信息系统一旦遭受攻击，要对遭受攻击后的负面结果有一个预判，有多大的负面影响，这样一来，有可能进一步为补救措施做好准备；最后，根据安全事件发生的可能性和因此造成后果的严重程度来识别信息系统的安全风险，从而尽可能采取相应的措施，减少弱点，避免攻击，保护信息系统的资产免受损害。

信息安全的管理是一个过程管理，随着网络信息系统面临的安全问题越来越严重，所以为了更好的做好应急响应的措施，先对信息安全风险进行评估显得尤为重要。高校信息面临的危险时动态的、不确定性，随着时间的推移或环境的变化，新的危险也将有所增加，因此固定的安全管理模式根本不能够起到预防的效果。而信息安全风险评估将对信息系统及信息的安全属性进行科学的识别和评估，其中信息包括传输中的信息和存储的信息，我们通过科学合理的对信息的完整性、保密性及可用性等的评估，可以预知安全风险是否存在，这对于信息安全的管理工作起到很重要的作用。

首先要明确风险评估的目标。随着高校信息化程度越来越高，对于信息系统的应用和对网络技术的应用会日益增加，从而可能会出现更多的脆弱性，高校组织的网络系统、应用软件、数据库信息都将可能成为严重危险的目标，因此建立信息安全风险评估机制，首先要明确风险评估的目标。其次是要建立适当的组织机构。在进行信息安全风险评估时，要针对风险评估的范围和目标，建立相应的组织机构。由高校的信息化管理人员、相关的专业技术人员组成信息安全评估小组。这样可以从管理和技术两个方面进行工作的开展，保证了信息安全风险评估过程中的决策与沟通，有效完成安全风险评估工作。信息安全风险评估做好了，一旦发生信息安全突发事件，则可以根据安全风险情况制定相应的应急处理措施，有所准备就可以免遭更大的损失。

## 3　建立健全信息安全突发事件的应急预案

（下转第144页）

升。将病毒、非法入侵等现象控制在一定的解决范围之内，对安全系统进行评估工作，加强防火墙、信息防漏技术的提升。国土资源局涉密计算机信息安全管理体系设计与实现是一项具有综合性的发展工程，要经过周密的分析论证，加强相关防护工作以及技术的提升。对选用的安全防护产品要注重相互之间联动性，避免出现孤立的状态，运用安全可靠的产品，形成高效，多种安全方式并且的协调性工作，这样才能够建立起全方位的安全防护体系。参照国家相关的涉密计算机信息系统安全防护标准，信息安全管理体系主要对物理、网络安全、数据、用户等进行全面的防控。并且依据各方面的重点采取相应的技术手段形成独立的安全管理系统。主要涉及到：身份认证、终端安全管理以及病毒防护等方面的内容。

## 3 结束语

在实施的过程中我们可以看出，国土资源局在计算机信息安全管理体系的建设过程中要结合自身的实际需求，在物理安全、网络安全以及安全保密管理等方面建立多层次，全方位的信息安全保障体系，采用多种安全管理产品并存的联动作业动态结合的方式进行管理。这样能够从根本上提升信息安全管理水平，提升监控与防御能力。通过对信息技术的提升，技术与管理要相互结合，安全管理体系要结合自身的实际水平，在实践的过程中对系统中存在的漏洞进行跟踪，调整信息安全管理体系的防护能力，加强技术手段的实行，这样才能实现信息安全管理。

**参考文献：**

[1] Manchester James, Saha Deban jan, Tripathi Satish K.Protection, restoration, and disaster recovery[J].IEEE Network, 2012, 18(2): 3-4.

[2] 曾陈萍.基于多主体信息安全管理系统研究与实现[J].计算机工程与设计，2012.

[3] 刘扬，陈晓鹏，苑新玲.基于企业涉密检测的数据安全解决方案[J].计算机工程与设计，2013，29.

**作者简介：**

王璐（1982—），男，本科学历，工程师，研究方向：网络及终端管理维护、政务信息公开。

（上接第 141 页）

高校信息安全管理过程中时刻要有危机意识，所以在成立信息安全突发事件应急响应组织机构的基础上，要有突发事件发生后的应急预案。

应急预案是经过反复论证后制定的，要能够应对高校网络信息安全突发事件，从而免遭损失扩大的有效的方法和措施。应急预案则包括信息安全事件发生前采取的危机预警和检测以及预防等措施，还要包括信息安全事件发生后而采取的应急处理和恢复措施等。所以健全信息安全突发事件的应急预案将是处理信息安全事件成功的关键。

高校范围内建立健全信息安全应急预案要遵循科学性和系统性，要在广泛收集理论的基础上制定措施，同时可以跟信息安全风险评估体系进行结合来实施。

在进行信息安全突发事件的应急预案的同时，要考虑到信息安全事件发生时的影响度、和损坏度。这时就要有一个预控措施，要对事件的影响有一个预判，可以有效的预防和控制事件发生时造成的危害。有了预控措施就可以让信息安全突发事件危机管理小组根据预控的影响大小而采取相应的应急措施，可以将安全事件消灭在萌芽状态，从而可以避免事态的进一步扩大。

## 4 科学处理信息安全突发事件

众所周知，信息安全事件一旦发生，其速度飞快，给人们的反应时间非常短，稍有不慎，则会造成极大的损失。高校内发生信息安全事件同样如此。处理信息安全突发事件危机比处理其他危机将更为复杂和困难，因此，为了做好信息安全危机处理工作，应该科学地应对信息安全突发事件。

安全应急处理小组在面对突发事件时要临危不惧，应明确应急处置流程、落实相关处置人员，理清思路，根据信息安全风险评估以及相对应的应急处理预案对号操作，同时迅速组织，根据预案制定相应的应急处理方案处理。在对突发事件进行有效控制的同时，要迅速查找源头，做好预防措施。另外，在处理信息安全突发事件的同时，要兼顾高校校园内正常工作的需要，网络的需求。在控制了校园网络信息安全突发事件后要尽快恢复高校校园网络，不要太影响整个高校的正常办公。

科学的信息安全应急机制是成功处理安全事件的关键一环，可以有效的预防和控制信息安全事件的发生或者进一步扩大，在高校内完善信息安全应急处理机制对于高校信息安全管理工作将起到关键性的作用。

**参考文献：**

[1] 陈红松.网络安全与管理[M].北京：清华大学出版社，2010.

[2] 王海军.网络信息安全管理研究[M].济南：山东大学出版社，2010.

[3] 黄锋.高校校园网信息安全突发事件的研究与对策[J].成都大学学报：社会科学版，2011，(2).

**作者简介：**

张明震（1980—），男，安徽涡阳人，硕士研究生，华东政法大学信息化办公室，助理工程师，主要研究方向：网络信息安全管理。

（上接第 142 页）

补丁程序，有效解决漏洞程序所带来的安全问题。扫描漏洞可以使用专门的漏洞扫描器，比如 COPS、tripwire、tiger 等软件，也可使用 360 安全卫士、瑞星卡卡等防护软件扫描并下载漏洞补丁。

（4）入侵检测和网络监控技术

入侵检测是近年来发展起来的一种防范技术，综合采用了统计技术、规则方法、网络通信技术、人工智能、密码学、推理等技术和方法，其作用是监控网络和计算机系统是否出现被入侵或滥用的征兆。根据采用的分析技术可以分为签名分析法和统计分析法。签名分析法：用来监测对系统的已知弱点进行攻击的行为。人们从攻击模式中归纳出它的签名，编写到 Ds 系统的代码里，签名分析实际上是一种模板匹配操作。统计分析法：以统计学为理论基础，以系统正常使用情况下观察到的动作模式为依据来辨别某个动作是否偏离了正常轨道。

（5）文件加密和数字签名技术

文件加密与数字签名技术是为提高信息系统及数据的安全保密性，防止秘密数据被外部窃取、侦听或破坏所采用的主要技术之一。根据作用不同，文件加密和数字签名技术主要分为数据传输、数据存储、数据完整性的鉴别三种。数据传输加密技术主要用来对传输中的数据流加密，通常有线路加密和端对端加密两种。前者侧重在路线上而不考虑信源与信宿，是对保密信息通过的各线路采用不同的加密密钥提供安全保护。后者则指信息由发送者通过专用的加密软件，采用某种加密技术对所发送文件进行加密，把明文加密成密文，当这些信息到达目的地时，由收件人运用相应的密钥进行解密，使密文恢复成为可读数据明文。

数据存储加密技术的目的是防止在存储环节上的数据失密，可分为密文存储和存取控制两种。前者一般是通过加密法转换、附加密码、加密模块等方式对本地存储的文件进行加密和数字签名。后者则是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据。数据完整性鉴别技术主要是对介入信息的传送、存取、处理的人的身份和相关数据内容进行验证，达到保密的要求，一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。