ISSN 1002- 4956
CN11- 2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第 26 卷 第 5 期 2009 年 5 月
Vol. 26 No. 5 May 2009

世界大学实验室

美国高校信息安全管理情况分析与启示

吴海燕, 苗春雨, 蒋东兴

(清华大学 计算机与信息管理中心, 北京 100084)

摘 要: 信息安全是高校信息化可持续发展的重要保障, 信息安全经历了技术浪潮、管理浪潮、制度浪潮 3 个发展阶段, 以体系化的方式实现信息安全已经得到业界的认可。调研了美国部分知名高校的信息安全管理部门的名称、组织方式、管理内容以及技术措施, 总结了我国高校信息安全管理可以借鉴的几个特点。

关键词: 美国高校; 信息安全管理; 借鉴

中图分类号: G51 文献标志码: B 文章编号: 1002- 4956(2009) 05- 0169- 04

The analysis and inspiration of information security management in U.S. universities

Wu Haiyan, Miao Chunyu, Jiang Dongxing

(Computer and Information Center, Tsinghua University, Beijing 100084, China)

Abstract: Information security is an important guarantee for sustainable development. The information security has experienced in three phases, such as the technology wave, the management wave, and the institutional wave. Gaining information security by means of architectural ways has been recognized by industry. The name, organization, management, content and technical measures of some well-known U.S. university's information security management department are introduced, and several special features, which China's colleges and universities information security managers can use for reference, are summarized.

Key words: U.S. universities; information security management; use for reference

我国高校信息安全工作起步较晚, 目前大部分高校还处于主要通过技术手段保障信息安全的阶段。美国高校因为信息化起步早, 在信息安全方面也处于领先位置, 很多高校已经成立了与传统的信息化建设部门(如 ITS) 平级的、专门的信息安全管理部门, 统筹信息安全相关的管理工作, 逐步建立、完善高校的信息安全体系。本文对 Stanford 大学、Harvard 大学和 Berkeley 大学等美国知名高校的信息安全管理情况进行了调研, 介绍了这些高校信息安全管理部门的名称、组织方式、管理内容以及技术措施等, 国内高校的信息安全管理工作提供参考, 以期促进国内高校信息安全管理工作的发展。

1 信息安全的发展

随着高校信息化建设的不断深入, 信息成为对高校组织业务至关重要的一种资产, 信息安全也受到了越来越大的关注, 如何保障个人隐私和重要数据不被泄漏成为信息管理部门重要的职责。高校由于其业务涉及面广、信息量大、环境复杂、人员变化快等问题, 对信息安全的保护提出了更高的要求。

信息安全工作的目的是保护信息免受各种威胁、损害, 确保业务连续性、业务风险最小化, 投资回报和组织利益最大化。信息安全的目标是保证信息的保密性(confidentiality)、完整性(integrity) 和可用性(availability); 另外也可包括诸如真实性(authenticity)、可核查性(accountability)、不可否认性(non-repudiation) 和可靠性(reliability) 等。

随着人们对信息安全的认识不断深入, 信息安全实践也在不断地发展。Basie von solms 教授将信息安全的发展因 3 个标志性的飞跃划分为 3 个阶段。

第一阶段, 技术浪潮。这个阶段主要通过技术手段保障信息的安全, 例如访问控制、身份鉴别和口令等。这时人们没有认识到管理的重要性, 信息安全策

收稿日期: 2008- 09- 18 修改日期: 2008- 11- 19

作者简介: 吴海燕(1974—), 女, 黑龙江省大庆市人, 博士, 高级工程师, 主要从事教育信息化方向、信息安全方向的研究。

略、信息安全意识等没有被考虑, 相应地, 人们认为信息安全是技术人员的责任, 而不需要全员参与。

第二阶段, 管理浪潮。分布式计算和网络的发展使得高层管理人员开始关注安全问题, 关于信息安全的文件化规定迅速发展起来, 信息安全方针、信息安全经历、信息安全架构等都成了重要的方面。比较技术控制阶段, 这个阶段使得高层管理人员参与到信息安全中来, 很多组织都设置了信息安全经理的职位。

第三阶段, 制度浪潮。随着信息安全的发展, 人们很自然地关心自己的组织比起其他的组织来信息安全活动是否成功, 这就引发了第 3 次浪潮, 即以体系化的方法实现信息安全。其中包括 4 个不同的方面:

(1) 信息安全标准化, 或者遵守国际上信息安全的最佳实践与控制措施集。标准可以解决用户"如何得知在实践中漏掉了哪些方面"。

(2) 信息安全认证。认证可以解决"怎么向合作伙伴证明组织的信息安全"或者"一个什么样的合作伙伴才能接入自己组织的系统"。

(3) 培育组织自己的信息安全文化。信息安全文化可以消除"组织内部用户是组织的最大敌人"的问题。

(4) 应用持续和动态的手段来测量组织的信息安全。测量可以解决"组织的信息安全方针, 程序等执行情况如何"。

2 信息安全管理部门情况

2.1 部门名称

随着对信息安全的重视程度日益提高, 在美国的知名高校中都成立了专门的信息安全管理部门。由于关注重点、管理范围和组成方式的不同, 各个高校的管理部门的命名也不同, 但一般都包括"information"、"security"两个关键词, 有些高校还将"privacy"、"technology"涵盖进了部门名称中, 详细名称参见表 1。

表 1 美国部分高校的信息安全管理部门名称

高校名称	信息安全管理部门名称	在 CIO 体系中的位置(与 ITS 部门的关系)
哈佛大学	建立信息安全和隐私网站(Information Security and Privacy), 在 CIO 体系中没有独立的信息安全管理部门	CIO 办公室制定信息安全策略, ITS 部门负责策略的执行
伯克利大学	最初被称为信息安全委员会(Information Security Committee, CISC), 2006 年 10 月改为信息安全和隐私委员会(Information Security and Privacy Committee, CISPC)	与 ITS 共同隶属于 CIO 办公室, 受 CIO 的直接领导
斯坦福大学	信息安全办公室(Information Security Office, ISO)	与 ITS 共同隶属于 CIO 办公室, 受 CIO 的直接领导
德州大学达拉斯分校	信息安全办公室(Information Security Office, ISO)	与 ITS 共同隶属于 CIO 办公室, 受 CIO 的直接领导
印第安纳大学	信息技术安全办公室(Information Technology Security Office, ITSO)	与 ITS 共同隶属于 CIO 办公室, 受 CIO 的直接领导

2.2 部门隶属关系

美国高校于 20 世纪 90 年代中期开始了首席信息官(chief information office, CIO)体制的实践探索, 1990 年美国克莱蒙特大学的 Kenneth C. Green 教授首次提出了"Campus Computing"(校园信息化)的概念, 并于同年开始了针对美国高校信息化的研究项目: Campus Computing Project(CCP)。该项目至今已持续 18 年, 是目前世界上最有代表性的高校信息化研究项目。CCP2006 年的调查报告显示, 目前有 30%的美国高校建立了基于 CIO 的信息化组织体制。我们此次调研的美国高校都已经建立了比较完善的 CIO 体系, 因此我们将从信息安全管理部门在 CIO 体系中的位置、与传统的信息技术安全(imformation technology security, ITS)部门之间的关系两个角度来分析信息安全管理部门在学校中的隶属关系。

我们分析了 Harvard、Berkeley、The University of Texas at Dallas、印第安纳大学的 CIO 组织体系图, 发现在这几所高校, 信息安全管理部门都是直接向学校的最高管理部门负责, 与 ITS 是平级或者是 ITS 的上级单位, 具体如表 1 所示。例如, 在 Stanford, ISO 通过商业事件执行主席(the Vice President for Business Affairs)或首席财务官(Chief Financial Officer)的办公室直接向学校的高级管理部门汇报。在 Berkeley, CISPC 是由学校的首席信息官发起, 并向学校安全和隐私负责人(campus security and privacy officer)汇报。而在印第安纳大学, ITSO 则是直接向学校的 CIO 和 IT Policy Officer 负责。

2.3 部门组织方式

根据职责的需要, 不同高校的信息安全管理机构的组织方式存在着差异。在大部分高校中, 信息安全管理机构是一个实体, 有固定的组织机构和人员。有些高校的信息安全管理机构还有自己的开发人员和维护人员, 负责相关系统的开发、数据的管理, 以及对引进软件的审核等。图 1 是印第安纳大学的 CIO 体系

的组成结构图。

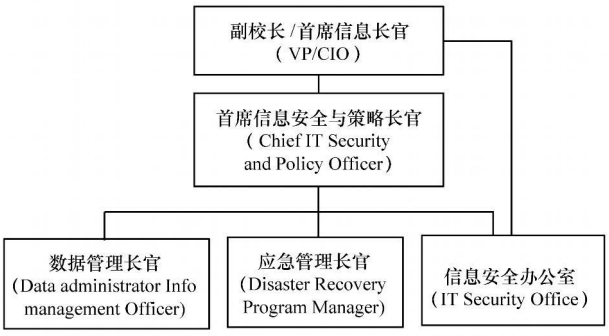

图 1 印第安纳大学的 CIO 体系结构图

(1) IT Security and Policy Officer 向 CIO 汇报, 协调 IT 策略相关问题, 为技术的部署和使用问题提供咨询, 处理事件响应, 推行用于捍卫大学的安全措施, 例如阻断恶意网络流量、隔离不安全的设备等。

(2) Security Officer 向 Policy Officer 和 CIO 汇报, 在技术方面为 CIO 提供建议和意见, 协调安全技术方面资源。

(3) 其他IT 组织也向CIO 汇报, 他们确保其自身的信息安全处于良好的状态, 而且必须准备提供援助, 帮助院系解决安全问题, 甚至提供院系所需的相关备用服务。

也有部分学校, 其信息安全管理部门并没有固定的人员编制, 而是以委员会的方式进行组织。例如在 Berkeley 大学, CISPC 由 CIO 发起, 每个成员的任期为 1 年。在成员中通过投票选出执行主席, 执行主席的任期为 2 年, 但在第 2 年起转为普通成员。所有的决议由成员投票决定, 参加投票的成员必须超过全体成员的 70%, 且需要成员本人参加投票才有效。此外, CISPC 对成员的组成和投票资格都有限制。

3 部门使命和职责

调研中发现, 美国高校信息安全管理部门涉及的范围很广, 从计算机软件、数字媒体的版权到保密数据、重要数据、个人隐私数据(银行账号、社保基金账号、身份信息、电子邮件等) 的保护, 以及不同数据、服务器的分级、分类以及保护策略等。总的说来, 所有的这些信息安全部门的使命都是通过主动的安全分析、风险控制保护学校的计算机和信息资产, 包括重要的理论数据和研究成果以及涉密数据、合同、财务、报酬和个人隐私等数据不被泄漏或违法使用。具体职责各个学校不尽相同, 但一般都包括信息安全体系规划、信息安全策略制定、信息分级保护、安全风险管理、信息安全事件响应、信息安全措施实施协调、信息安全文化培育几个方面。

(1) 信息安全体系规划。建立系统化、程序化和文档化的安全管理体系以及相应的技术措施规划。

(2) 信息安全策略和操作规范制定。建立大学的信息安全策略(关于信息安全的整体强制指导原则), 在信息安全策略的指导下, 制定操作规范。

(3) 安全风险管理。对大学信息和信息处理设施的威胁(threat)、影响(impact) 和薄弱点(vulnerability) 及其发生的可能性的评估, 并进行相应的风险控制。

(4) 信息分级保护。根据信息的保密性、重要性等对信息进行级别划分并提出相应的防护要求, 级别数量各大学各不相同, 但一般划分为 3 级。

(5) 安全事件响应。安全事件的响应、调查和汇报。

(6) 信息安全文化培育。包括对师生的安全教育、培训、讲座等。

一般来说信息安全管理部门会制定大学的信息安全策略, 包括总体策略和一些具体策略, 如 email 安全使用策略等和安全操作规范, 表 2 中, 我们对 UT Dallas 大学和 Harvard 大学的主要安全策略和操作规范进行了比较。

表 2 安全策略和操作规范列表与比较

	UT Dallas 大学	Harvard 大学
信息安全策略	• 计算机软件版权(computer software copyright) • 数字千年版权法案(digital millenium copyright Act) • 加密策略(encryption policy) • 信息资源可接受使用策略(information resources acceptable use policy) • 身份发现(identity finder) • 信息资源使用和安全策略(information resources use and security policy) • 网络连接策略(network connection policy) • 服务器管理策略(server management policy) • 常见问题(SPB-1 frequently asked questions) • 州及联邦法律(state and federal laws) • 大学电子邮件策略(university e-mail policy)	• 大学隐私策略(university privacy policy) 大学安全策略(enterprise security policy) • 信息安全与隐私策略 • 信息保留与归档策略(information retention and archival) • 隐私级别划分策略(privacy levels)

续表

	UT Dallas 大学	Harvard 大学
安全操作规范	• 数据分级标准(data classification standards) • 级别 I 数据扩展列表(extended list of category I data) • 信息资源安全操作手册(information resources security operations manual) • 处理级别 I/II/III 数据的系统的最低安全要求(minimum security standards for systems associated with category I, II or III data) • 安全意外报告流程(security exception reporting process) • 如何为 web 服务器获得一个对外 IP(obtaining an external IP address for a web server)	• 访问控制(controlling access) • 密码策略(passwords) • 数据传输、存储与展示(transporting, storing, and displaying) • 计算机操作(computer operation) • 计算机配置(computer setup)

从表 2 中, 我们可以看到不同高校对安全管理方面的侧重点不同。UT Dallas 大学详细列出了需要保护的内容以及需要遵守的法律、法规, 并就这些需要保护的内容对数据进行分级、分类, 最后落实到不同的规范中; 而 Harvard 大学则通过制定统一的“企业信息安全策略”(enterprise information security policy), 明确了安全保护的措施, 将安全管理落实到具体的内容上, 如计算机的安装、密码保护、需要保护的计算机等。

4 分析与总结

通过对国外高校信息安全管理部门的调研, 可以看到美国高校在信息安全管理方面有如下可以借鉴的特点:

(1) 独立的信息安全管理部门, 该部门向 CIO 或同级别的校级高层领导汇报, 这样有利于信息安全管理措施的执行;

(2) 建立文件化的信息安全管理体系作为高校管理体系的一部分, 基于业务风险方法来建立、实施、运行、监视、评审、保持和改进信息安全。

要想切实保障信息的安全, 除了制定详细的标准和规范, 明确要保护的内容和保护方法外, 还需要将这些标准和规范落到实处, 真正地应用到日常的工作中。在调研中, 我们发现美国高校特别重视以下工作:

(1) 数据的分类和分级。根据数据的重要性进行分类和分级, 根据等级的不同制定适当的规则, 既要确保数据的正常使用, 又要避免资源的浪费。比如对于保密数据、银行账号等信息要采取最高的保护措施, 而对于一些联系方式、电话等信息只限制在校内访问, 禁止对外传播。

(2) 重要数据集中管理。构建一个集中的管理系统, 对重要的数据进行统一的保护。这样既可以减少安全隐患, 又能够对接触数据的人进行有效的监督, 还避免了分别构建保密环境的成本。

(3) 安全规范的推广。要确保接触保密数据的每个学生、教师甚至访客都需要了解并遵守这些标准和规范。要达到这样的目的, 不仅要让所有的人都知道自己有保守秘密的职责, 而且还需要知道怎么做才能够符合要求。比如, 不要使用开放的传真机接受保密文档, 离开时不要把保密文件放在桌子上, 不要把保密数据存放在笔记本电脑上等。

(4) 监督和审计工作。安全管理机构除了要构建一个安全的环境以外, 还需要对使用者进行监督、对使用的过程进行审计, 一方面确保规范被切实地执行, 另一方面当发生事故后也可以做到有据可查。

参考文献(References):

[1] Von Solms, SH. Information Security-The Third Wave[J]. Computers & Security, 2000, 19(7): 615-620.

[2] The Campus Computing project, The 2006 Campus Computing Survey 2006[EB/OL], (2006-10)[2008-6]. http://www.campuscomputing.net/summaries/2006/index.html.

[3] CNCERT. 2006 年上半年网络安全报告[EB/OL]. (2007-1-31)[2007-3-7]. http://www.cert.org.cn/articles/docs/common/2007013163191.shtml.

[4] The University of Texas at Dallas information Security Office. Information Security Policies[EB/OL]. (2007-11)[2008-4]. http://www.utdallas.edu/ir/security/Policies.htm.

[5] 吴海燕, 蒋东兴. 入侵防御系统研究[J]. 计算机工程与设计, 2007, 28(24): 5844-5846.

[6] 吴海燕, 戚丽. 数字校园信息安全保障体系的设计与实现[J]. 实验技术与管理, 2008, 25(8): 1-6.

[7] 赵国栋. 信息时代的大学: 美国高等教育信息化发展及其启示[J]. 现代教育技术, 2003(5): 11-17.