光华管理学院
Guanghua School Of Management

信息安全的学术研究情况介绍

李 东

光华宝岛IT战略与创新研究中心

lidong@gsm.pku.edu.cn

2011.9.17

1、信息安全学术研究的整体情况

信息系统安全的重要性

Table 3. Key IS management issues in China

Ranking	2004 Survey	2008 Survey
1	Integration of Information technologies with enterprise business practices	Security & Privacy
2	Improving enterprise information system security	The building of enterprise IS infrastructures
3	Enterprise Information Systems strategies	Applications' adoption and use
4	Making effective use of data resources	Making effective use of the data resources
5	The influence of CIO and IS departments	Enterprise Information Systems strategies
6	Business Process Reengineering	Business Process Management
7	The building of enterprise IS infrastructures	Developing and installing Information System
8	Building a responsive IT infrastructure	Network System building and its management
9	The evaluation of ROI of IS	Business Performance Management
10	Integration of different suppliers' open systems	Knowledge Management

有关学术期刊

2011	信息网络安全
2011	软件导刊
2011 计数	2
2010	信息网络安全
2010	信息网络安全
2010	网络安全技术与应用
2010	现代情报
2010	金融电子化
2010	计算机安全
2010	信息安全与技术
2010 计数	7
2009	工业工程
2009	信息网络安全
2009	情报杂志
2009	计算机工程
2009	信息化建设
2009	会计之友
2009	信息网络安全
2009	北京交通大学学报
2009 计数	8
2008	计算机安全
2008	东北财经大学学报
2008	计算机安全
2008	信息与电脑
2008	网络安全技术与应用
2008	电信技术
2008 计数	6
总计数	23

2008 计数	6
2007	中国标准化
2007	微计算机信息
2007	信息安全与通信保密
2007	计算机与信息技术
2007	科技决策
2007 计数	5
2006	信息网络安全
2006	信息网络安全
2006	信息网络安全
2006	信息安全与通信保密
2006	计算机应用
2006	信息网络安全
2006	信息网络安全
2006	电信科学
2006 计数	8
2005	网络安全技术与应用
2005	程序员
2005	情报杂志
2005	计算机工程与科学
2005	计算机工程与设计
2005	计算机应用研究
2005	信息安全与通信保密
2005	计算机工程
2005	信息化建设
2005	信息网络安全
2005 计数	10

文献检索结果

分类 \ 时间	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	总计
安全措施的组织		1					1	1		1	4		1	9
持续性规划			1	1		2	2	1	1	2	1			11
应用和基础设施				1	2	2			1					6
访问控制		1			1	2	4		1		1			10
计算机和网络管理	1	1	2			2	1				1	1		9
规则遵守				1	1	1	1	3			1	3		11
人力资源相关			1		2		1		1					5
IT 的物理安全性								1		1		1		3
设备分类和管理				1	2			2	1	1				7
安全政策标准				1	2	1				1		2	1	8
总计	1	3	4	5	10	10	10	8	5	6	8	7	2	79

2、信息安全部分研究课题介绍

1、信息安全的政策和标准

- 美国标准
  - 美国国家技术与标准局（NIST）：联邦信息处理标准(FIPS) 、《联邦信息安全管理法案》（FISMA)、《联邦信息系统认证认可指南》
  - 美国国家标准学会(ANSI)：负责金融安全的小组是ASG X9和X12
  - 信息技术治理研究所（ ITGI）为ISACA的一个下属机构，发布了COBIT 。
  - 美国总统信息化顾问委员会(PITAC)：发布有关报告。
- 欧盟标准
  - 欧洲网络与信息安全署（ＥＮＩＳＡ）：提出数据保护法（Data Protection Directives）、电子商务法(Electronic Commerce Directives)、网络与信息安全提案(Network and Information Security: Proposal for A European Policy Approach)等
  - BS7799是英国信息安全管理的标准，也是在全球影响最广的信息安全管理标准之一，其标准的第一部分《信息安全管理实施细则》目前已成为国际标准ISO/IEC27001:2005，该标准包括了11个安全控制域和39个主要的安全条目。

- ISO标准
  - 国际标准化组织ISO，国际电信联盟ITU和国际信息系统审计和控制协会ISACA等，在全球信息化进程中扮演着日益重要的角色。

面向对产品和计算机系统实施评测的ISO/IEC15408:信息技术安全评价通用准则（CC）；

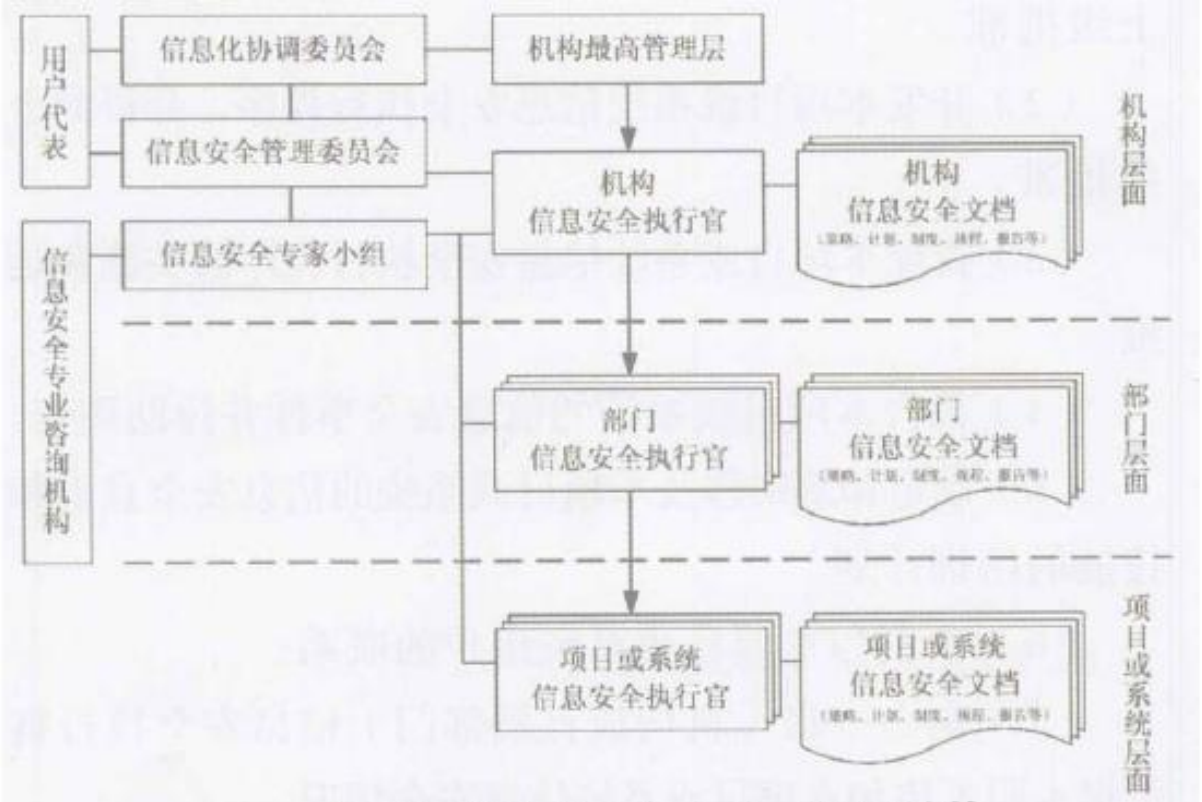
面向工程的ISO/IEC21827:2002（SSE－CMM）：信息安全工程能力成熟度模型；

面向管理的ISO/IEC17799和ISO/IEC27000系列标准：ISO/IEC27004：信息安全管理的评价指标”标准

- 中国的情况
  - 国家信息安全标准化技术委员会：2002年成立，已经正式颁布的信息安全相关国家标准40多项。
  - GB/T22008-2008 《信息技术安全技术信息安全体系要求》是从ISO27000标准转化而来。ISO／IEC 27002：2005是《信息技术安全技术信息安全管理实用规则》， 等同转化为中国国家标准GB／T 2208l一2008，也是ISO／IEC 27000系列最核心的两个标准之一。它从11个方面提出39个控制目标和133个控制措施。

2、信息安全的组织问题

企业或机构中的信息安全的组织问题包括组织策略、组织结构和岗位责任等。根据不同的行业、组织规模和业务需求等又有许多更详细的设计。



《信息安全管理组织体系的建立指南》

认知可靠性和失误分析方法(Cognitive Reliability and Error Analysis Method, CREAM)

表 1 失效模式前因表

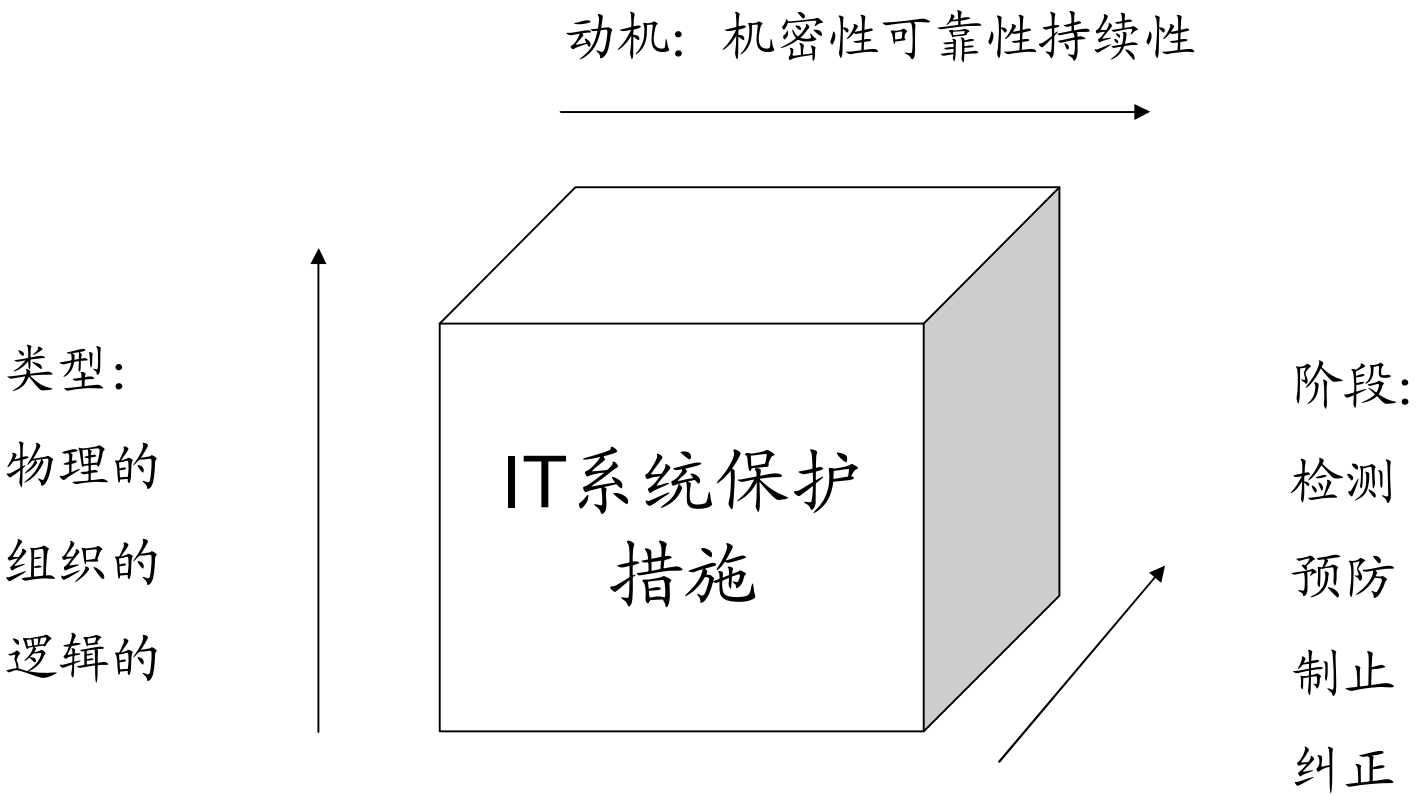
代码	组织管理失误因素	含义或者主要表现
O_1	缺乏信息建设与安全管理专业知识	组织无系统的专业培训, 员工缺乏相关的专业知识和技能
O_2	人事管理制度不严密	组织内部各部门员工流动性大, 人浮于事, 核心人物离职率高
O_3	激励机制不健全	缺乏工作动力和热情
O_4	操作标准与规程不合理	操作流程混乱
O_5	组织文化落后	组织内竞争不激烈, 没有风险意识, 团队协作性差

表 2 后果 – 前因链追溯表

代码	后果	一般前因	具体前因
O_1	缺乏信息建设与安全管理专业知识	$O_5O_{12}O_{15}O_{16}$	不重视或者相关资源缺乏
O_2	人事管理制度不严密	$O_3O_5O_6O_7O_{12}$	管理方法不当, 职位设计不合理
O_3	激励机制不健全	$O_4O_6O_7O_{12}O_{15}$	薪酬与工作任务不一致
O_5	组织文化落后	$O_2O_3O_4O_6O_7O_{12}O_{13}O_{15}$	执行力不足

《企业信息安全管理中组织管理失误因素分析》

3、信息安全管理体系的评价



Bautz立方体

Theo Thiadens《IT管理的知识体系》

表 4 构造“资产——威胁 / 脆弱性”矩阵

作用于过程中的威胁/脆弱性组合对	资产 / 过程	C1	C2	C3	C4	C5	C6	C7	…	Cn
$TV_{11}, TV_{21}, TV_{35}$	D11		√		√		√			
TV_{52}，TV_{24}，TV_{34}	D12	√	√							
……	……									
TV_{11}，TV_{23}	D1x	√	√	√						
TV_{71}，TV_{35}	D21		√		√	√				√
TV_{31}，TV_{32}，TV_{45}	D22	√	√	√	√					
……	……									
TV_{33}，TV_{46}	D2y	√		√						
…	…									
TV_{20}，TV_{27}，TV_{56}	Dk1		√		√		√	√		
TV_{27}，TV_{65}	Dk2	√	√			√				
……	……									
TV_{62}，TV_{74}，TV_{375}	Dkm	√		√	√		√			

对资产的安全度和组织业务的重要度如何划分等级？对资产面临威胁的权重和威胁发生时对业务的影响程度如何评估？

《信息安全风险评估方法研究—基于“资产—威胁”评价指数矩阵风险分析方法研究》

4、信息安全人力资源管理

意识教育

技能培训

职责明确

考察评估

访问控制

保密协议

惩戒机制

《信息安全人力资源管理问题探要》

- 美国Purdue大学的信息保障和安全教育研究中心，倡导在信息和信息资源保护技术方面的革新， 并致力于发展和提高信息保障和安全方面的知识。James Madison大学也有这种研究中心—信息系统安全教育研究中心。
- 国外专业组织的培训情况

专业组织	培训对象	有无证书颁发	是否举行学术活动
美国计算机协会（ACM）	IT 专业人员、专业安全审计和控制人员	目前在研究中	是
美国工业安全协会（ASIS）	工业安全管理专业人员	有	是
联邦信息系统安全教育家协会（FISSEA）	联邦信息系统安全教育家	目前在研究中	是
电气与电子工程协会——计算机协会	IEEE—CS 的电气与电子工程师	目前在研究中	是
信息处理国际联盟（IEIP）	IT 专业人员	目前在研究中	是
信息系统审计和控制协会（ISACA）	审计、控制和安全人员	有	是
国际信息系统安全证书协会（ISC）²	信息安全专业人员	有	
信息系统安全协会（ISSA）	信息安全专业人员		是
国家分类管理协会	信息和计算机安全人员		是
国家安全研究所	安全专业人员		是
USENIX 系统管理员协会（SAGE）	系统管理员	目前在研究中	是
SANS 研究所	系统和网络安全管理员		是

5、信息安全标准的实施

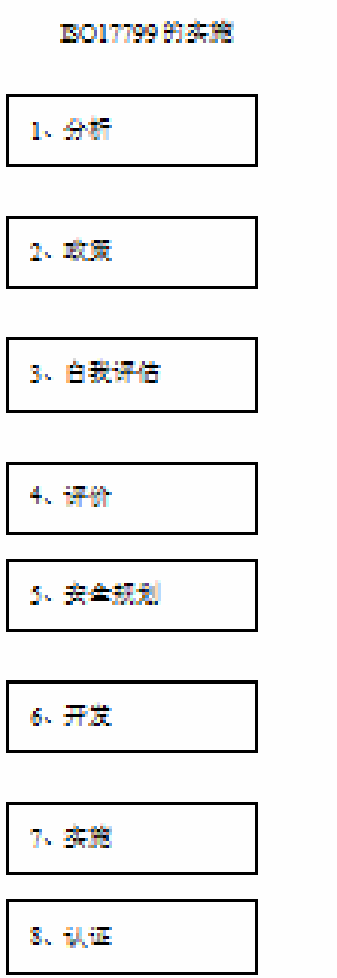
关键措施：
－从法律的观点：
　－防止非法复制
　－保护重要的业务文件
　－保护私人数据
－安全性基础：
　－安全政策的目标
　－责任分配
　－培训和教育
　－报告和解决事故
　－持续性规划

定性分析

被普遍接受的措施(基本集)：
这些是在整个组织内实施的。它是最低限度的安全性。这个基本集是根据以下项目来选择的：
　－对于最重大风险的评估
　－来自合同和法律的协议
　－IT 的相关发展
从这里可以得到：足够的基准：

更深入的对依赖性和脆弱性的分析

具体的深层次措施(例如基础设施的备份)，然后是包含成本、价值、损害和发生概率的扩展性风险分析：
　－准则 f(重要的组织流程)：重要流程，财务影响等等
　－准则 f(自然引起的事故)：环境危险，名誉，质量服务
　－准则 f(事故的损害)：对流程的破坏，破坏 IT，修复成本，生产损失，违约金



6、信息安全保障的技术

- PITAC报告认为：信息技术基础设施的不安全，是因为已有的基础设施是在人们并没有见到大量赛博攻击的较为安全的年代开发出来的。随着无线和嵌入技术及网络连接的增长以及由系统的系统(Systems of Systems)构成的网络其复杂性不断增强，内部与外部已难以区分。打补丁、堵漏洞的办法不能解决根本的安全问题。现在需要的是全新的技术和架构，以解决更大规模基础设施中的安全性问题

- 为保护数据的机密性，有许多相关的技术，需要综合运用。
  - 防盗技术：如实施特定的保密流程和模式，或者对应当保密的文件进行加密。
  - 认证技术：为客户和供应商提供适当形式的访问途径。如身份管理，权限检查等，以保证有关人员适当地控制和管理整个系统。
  - 政策规程：如设置安全政策、建立安全组织，分配角色和责任，定期进行安全审计等。

总结

- 信息安全问题逐渐从计算机技术类的问题向技术和管理结合的角度发展，涉及到许多组织、权限、职责、意识、文化等方面的问题，因此成为商学院所关注的领域。
- IS学术界对此方面的研究目前的成果还比较少，但是在国外作为硕士生教育课程已经开始增加，而且硕士论文的数量近年来不断增加。预期今后将会和实业界的合作越来越多。