信息安全管理

课程简介

课程目的

- 理解信息安全风险评估技术、理论与应用
- 熟知信息安全标准体系、信息安全法规体系
- 掌握信息安全服务、信息安全建设方案设计能力

先修课程

- 信息安全导论、密码学

教材&参考文献

- 《信息安全管理》，徐国爱，北京邮电大学出版社

课程考核

课程成绩

- 平时(40%)：考勤、课堂表现、作业、（案例）分析与讨论，
- 考试(60%)：结课论文

课程内容安排

Ch. 1 概述（3学时）

Ch. 2 信息安全风险评估（7学时）

Ch. 3 物理安全（2学时）

Ch. 4 信息系统安全审计（2学时）

Ch. 5 灾难恢复与业务连续性（4学时）

Ch. 6 信息安全标准与法规（4学时）

- 创新实践与讨论（10学时）
  - 案例分析
  - 信安热点、前沿与趋势

第一章　概述

本章提纲

§1 信息安全威胁

§2 信息安全概念

§3 信息安全技术

§4 信息安全管理

§5 信息安全发展

§1 信息安全威胁

§1.1 信息安全事件统计

§1.2 信息安全威胁分类

§1.3 信息安全威胁的根源

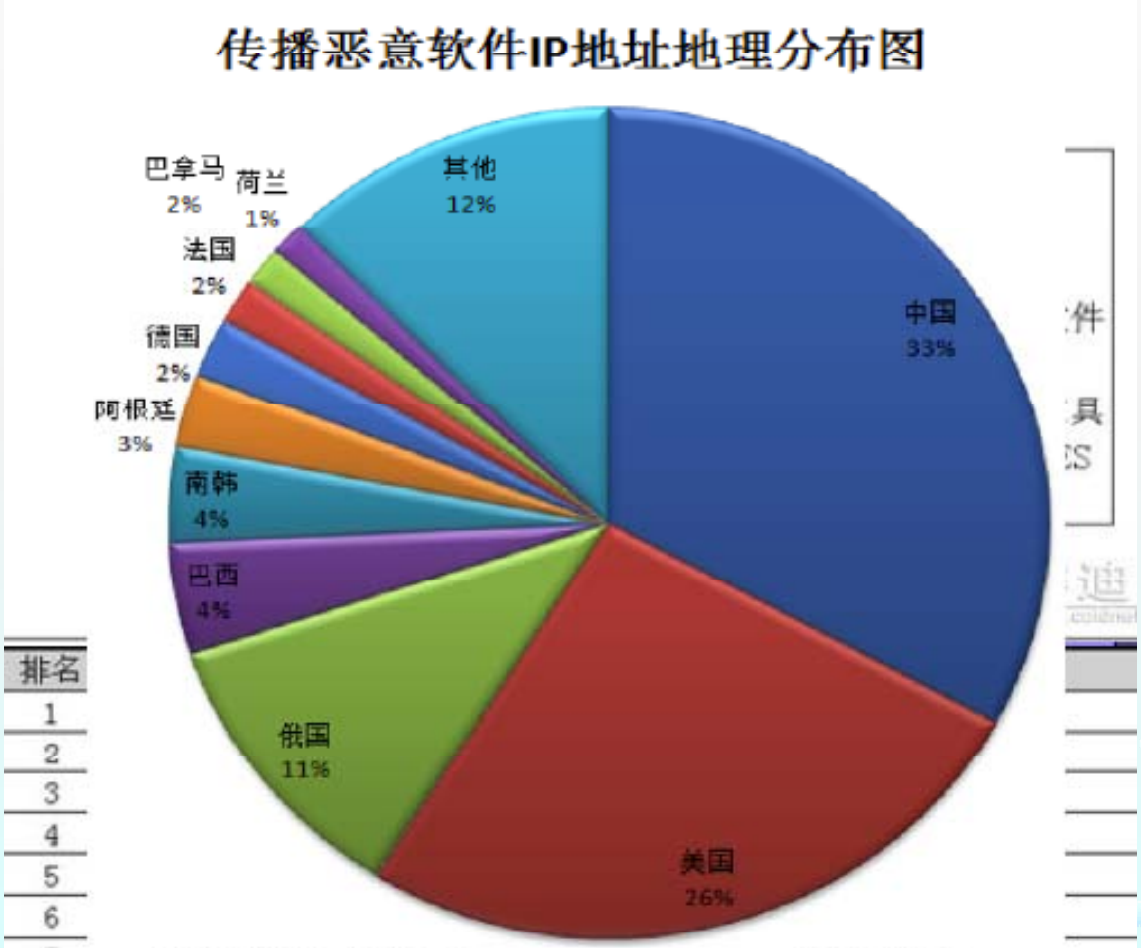
§1.4 信息安全威胁趋势

§1.1 信息安全事件统计

- 第一个蠕虫诞生：莫里斯蠕虫
  - 1988年11月2日，设计者为康奈尔大学的研究生罗伯特.莫里斯(22岁)，目的是验证网络中自动传播程序的可行性
  - 感染6000台计算机，使Internet不能正常运行，造成的经济损失达1亿美元
- CIH病毒
  - 1998年6月2日开始出现相关报道，台湾大学生陈盈豪编写。设计者动机是“为自己设计病毒”
  - 1998年4月26日首次发作，可损坏主板/硬盘，变种版本极多
  - 2001年4月26：CIH 第三次大范围爆发。仅北京就有超过六千台电脑遭CIH破坏，瑞星修复硬盘数量当天接近400块

§1.1 信息安全事件统计

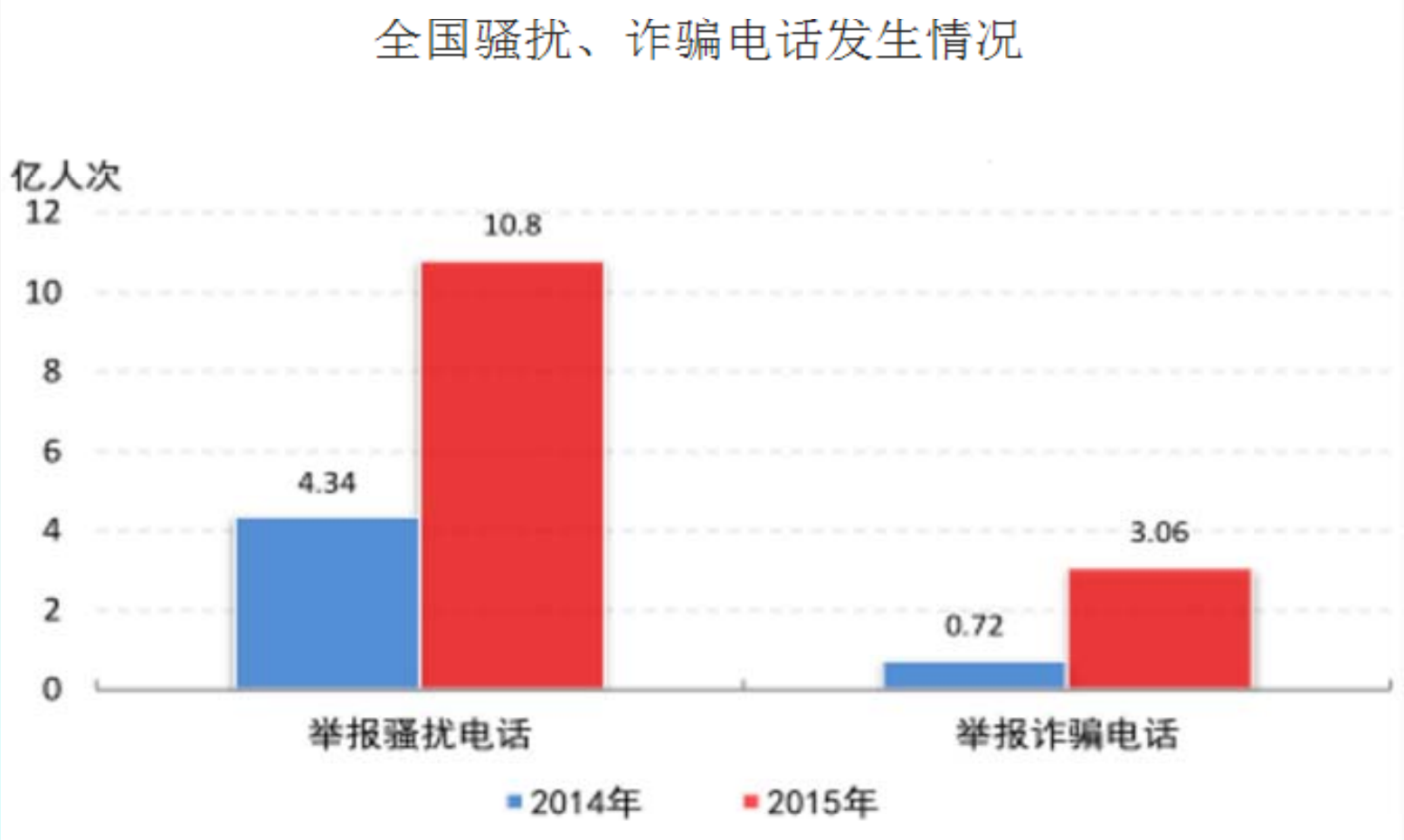
- 信息安全问题突出



排名		
1		
2		
3		
4		
5		
6		
7	Worm.Win32.AutoKun	U盘病毒生成
8	Trojan. Win32.Agent	木马代理
9	Trojan-Dropper.Win32.Agent	木马辅助工具
10	Trojan-PSW.Win32.Nilage	AV终结者

§1.1 信息安全事件统计

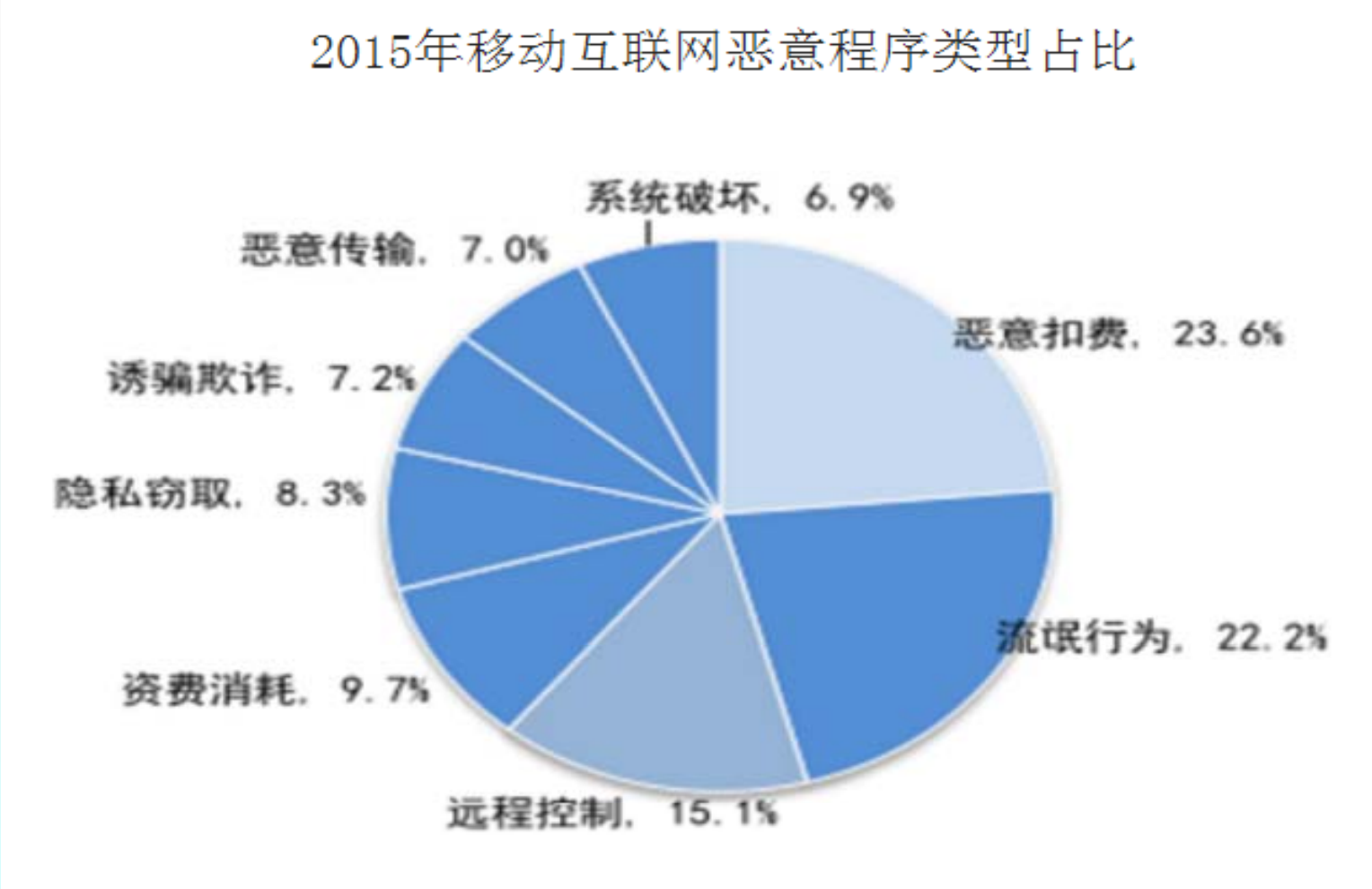
- 信息安全问题突出：2015年中国手机信息安全事件



《2017-2022年中国信息安全行业运营态势及未来发展趋势报告》

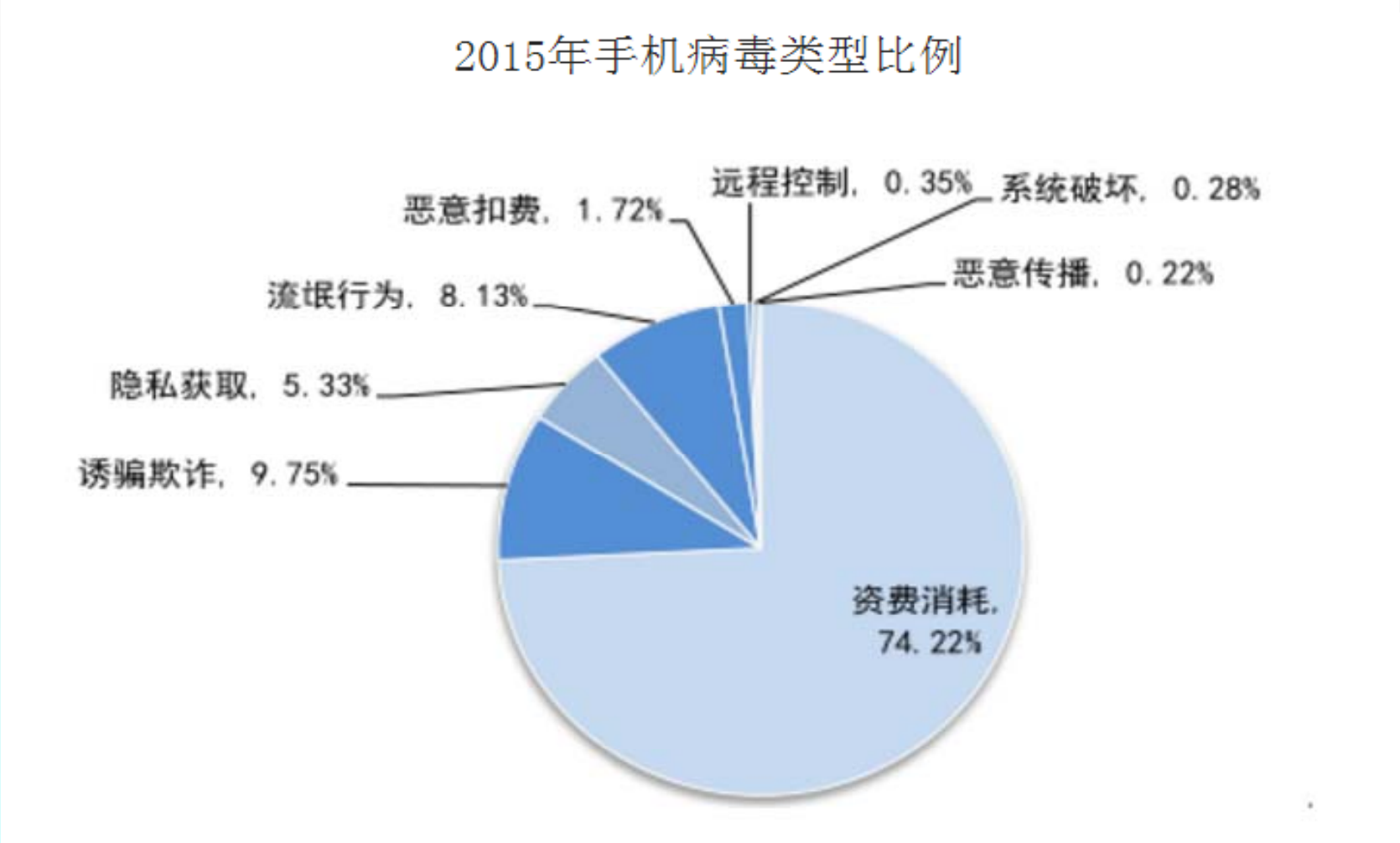
§1.1 信息安全事件统计

- 信息安全问题突出



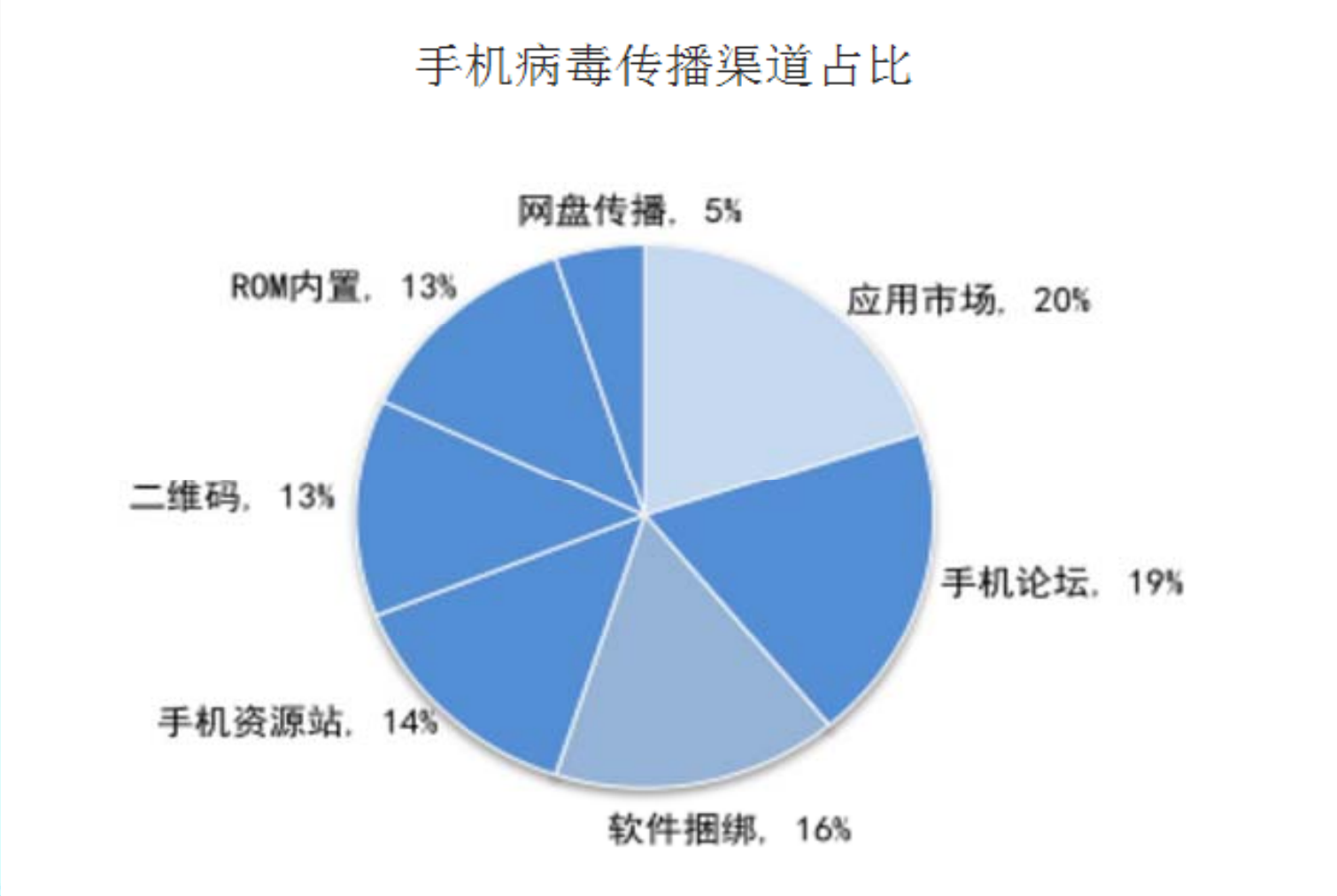
§1.1 信息安全事件统计

- 信息安全问题突出



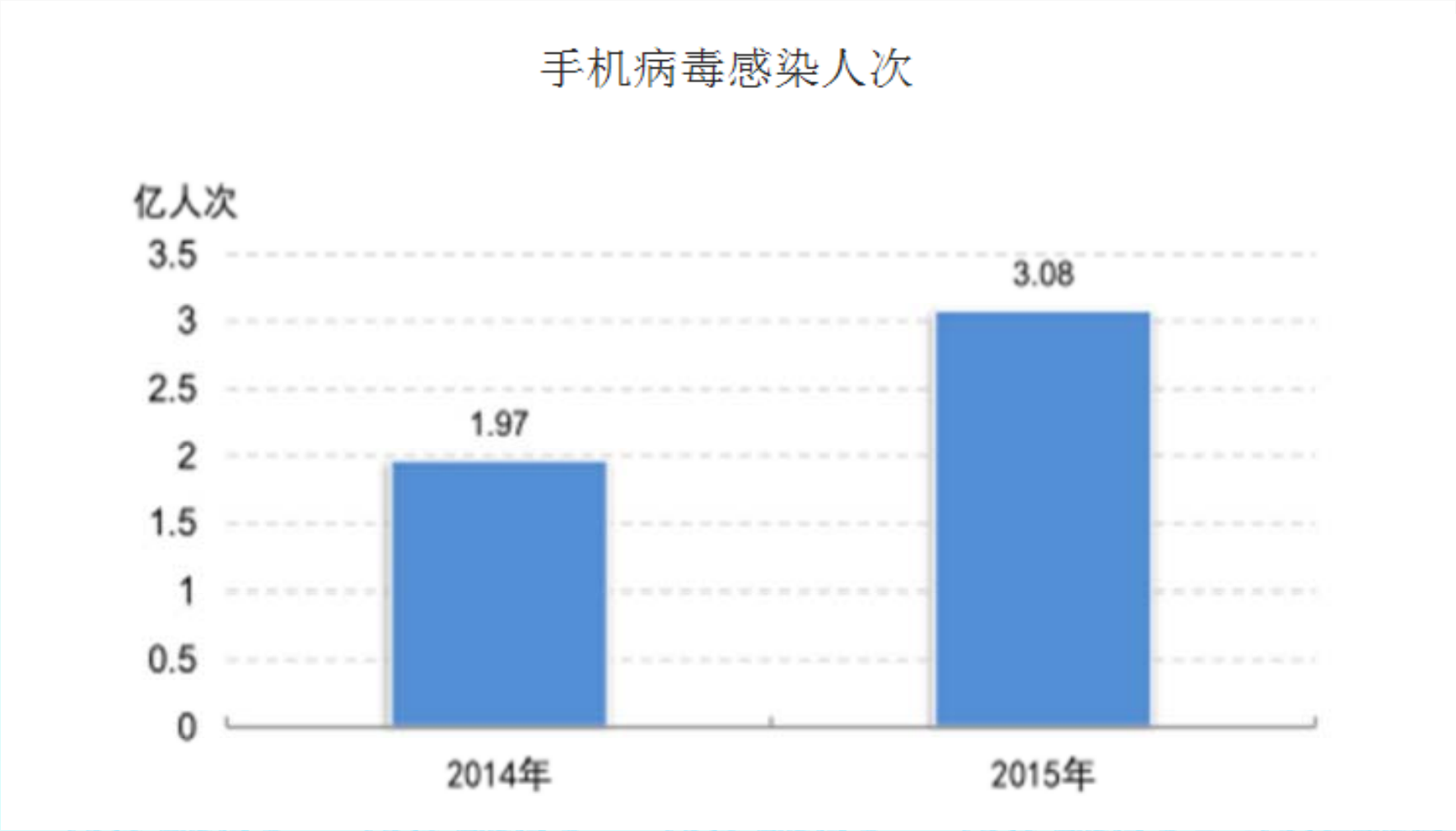
§1.1 信息安全事件统计

- 信息安全问题突出

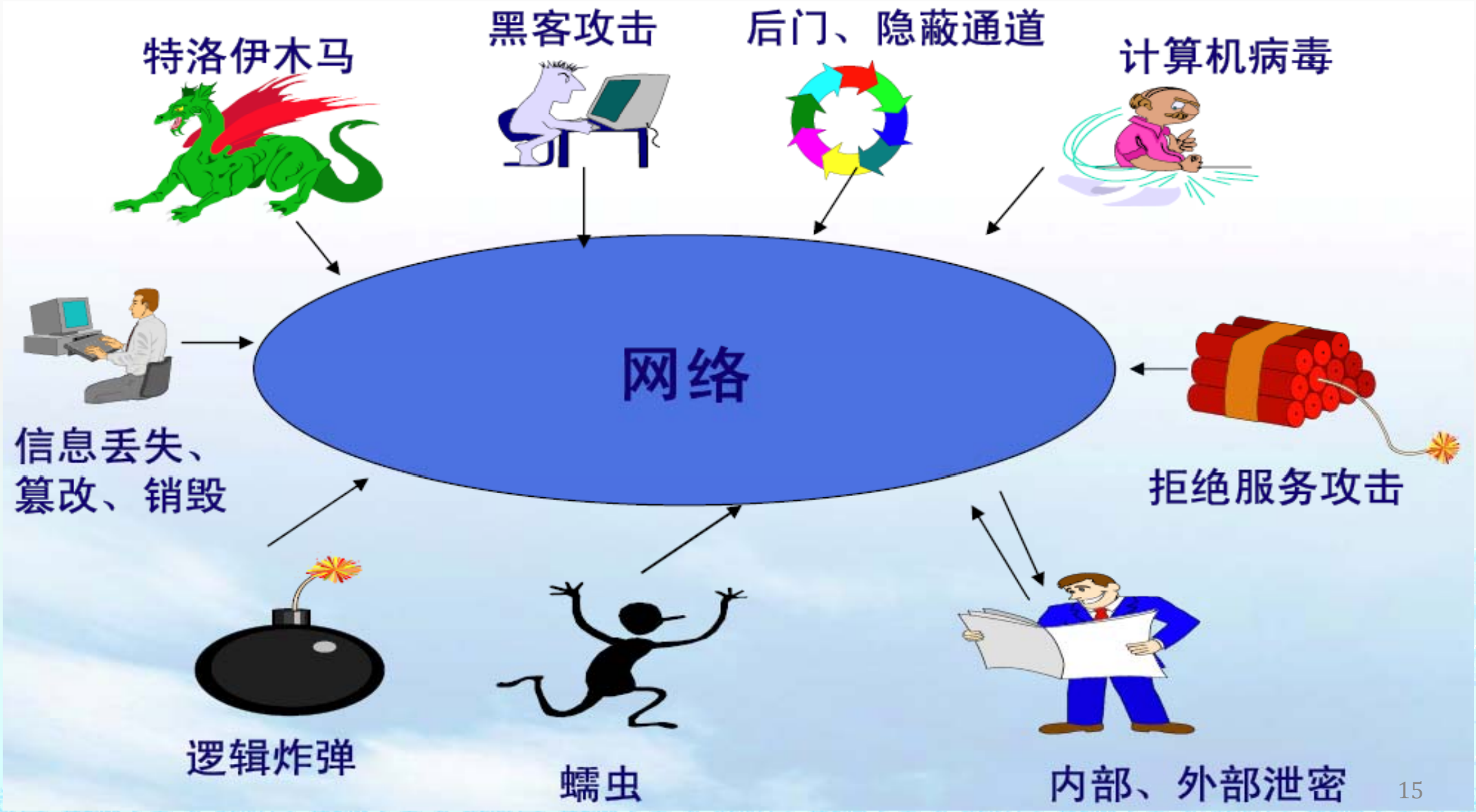


§1.1 信息安全事件统计

- 信息安全问题突出



§1.2 信息安全威胁分类



§1.2 信息安全威胁分类

- 有害程序
  - 计算机病毒：指编制或在程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能自我复制的一组指令或程序代码
  - 蠕虫：指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序
  - 木马程序：指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能
  - 僵尸网络：指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其
  - 网页内嵌恶意代码，其他有害程序

§1.2 信息安全威胁分类

网络攻击

- **拒绝服务攻击**：利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行的攻击行为。
- **后门攻击**：利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击。
- **漏洞攻击**：利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施的攻击。
- **网络扫描窃听**：利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征信息的行为。
- **干扰**：通过技术手段对网络进行干扰，或对广播电视有线或无线传输网进行插播，对卫星广播电视信号非法攻击等。

§1.2 信息安全威胁分类

信息破坏

- **信息篡改**：未经授权将信息系统中的信息更换为攻击者所提供的信息，例如网页篡改。
- **信息假冒**：假冒他人信息系统收发信息。
- **信息泄漏**：因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者。
- **信息窃取**：未经授权用户利用可能的技术手段恶意主动获取信息系统中信息。
- **信息丢失**：因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失。

§1.2 信息安全威胁分类

- 信息内容安全
  - 违法：违反宪法和法律、行政法规的
  - 网络舆情：针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的
  - 组织串连、煽动集会游行的
  - 其他信息内容安全

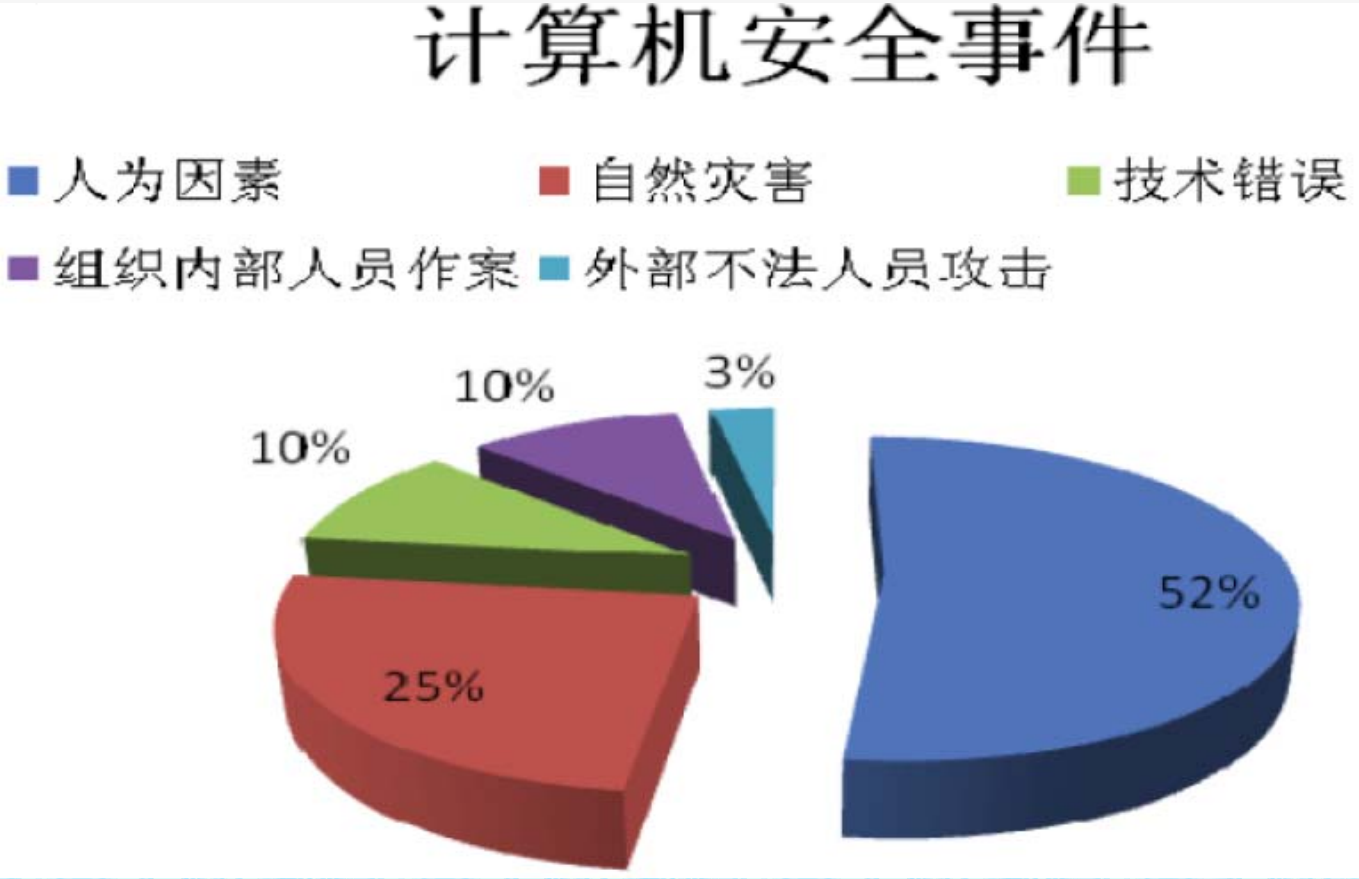
§1.2 信息安全威胁分类

设备设施故障

- 软硬件自身故障：信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等
- 外围保障设施故障：保障信息系统正常运行所必须的外部设施出现故障，例如电力故障、外围网络故障等
- 人为破坏事故：人为蓄意的对保障信息系统正常运行的硬件、软件等实施窃取、破坏等；或由于人为的遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏，影响信息系统正常运行的
- 其他设备设施故障

§1.2 信息安全威胁分类

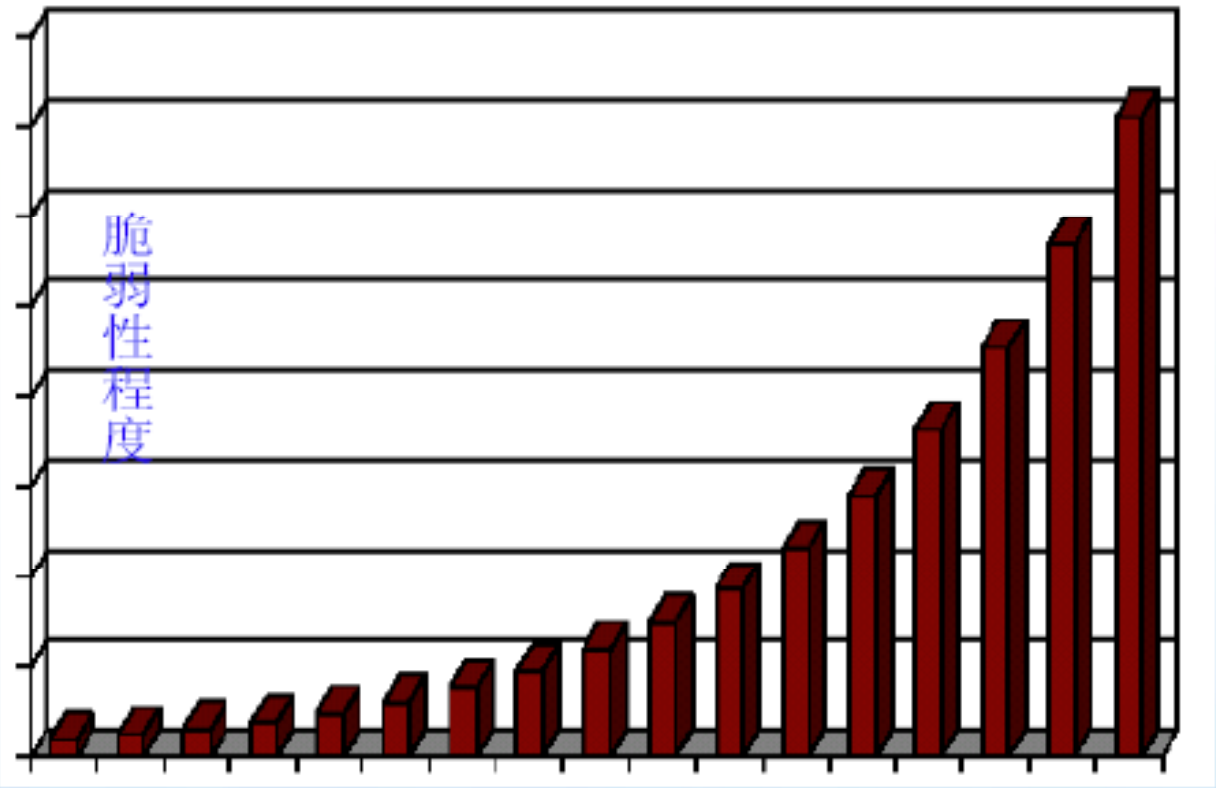
- 环境灾害
  - 包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等
- 其他
  - ……



§1.3 信息安全威胁的根源

§1.3 信息安全威胁的根源

网络系统日益复杂，
安全隐患急剧增加



信息网络系统的复杂性增加

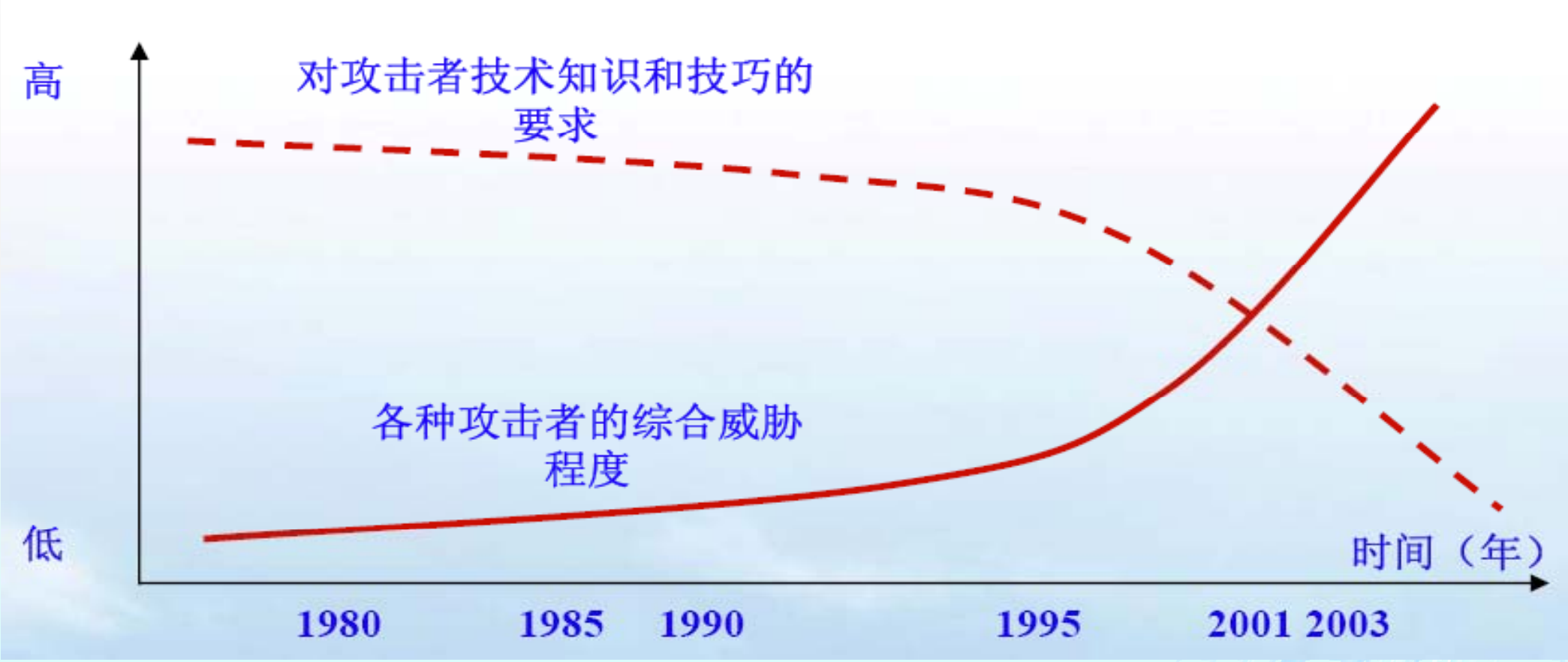
§1.4 信息安全威胁趋势

攻击手段的智能化

- 攻击技术的集成化
  - ✓ 病毒与传统网络攻击手段的融合，病毒技术、攻击技术本身的集成
- 攻击手段的工具化
  - ✓ “一键式”攻击出现
- 间接形式的攻击
  - ✓ 对目标实施攻击的“攻击者”可能本身也是受害者！

§1.4 信息安全威胁趋势

- 黑客攻击越来越容易实现，威胁程度越来越高



§1.4 信息安全威胁趋势

- 针对基础设施、安全设备的攻击
  - 终端、用户系统——基础设施
    - ✓ 危害范围更大、造成损失更大、负面影响更大
  - 主机、服务器——安全设备
    - ✓ 安全设备“后面”往往毫无戒备，用户对安全设备的依赖性更大

§1.4 信息安全威胁趋势

- 来自业务流程、信息内容的安全威胁
  - 垃圾信息（垃圾邮件、垃圾广告、……）
  - 有害信息（反动、色情、暴力、……）
  - 针对业务系统设计漏洞的攻击

§1.4 信息安全威胁趋势

- 攻击手段与传统犯罪手段的结合
  - 各种形式的信息盗取
  - 各种形式的网络欺诈
  - 各种形式的网络敲诈

§1.4 信息安全威胁趋势

- 攻击组织的战争倾向
  - 黑客组织为集团服务
  - 黑客攻击用于战争
  - 黑客组织行为用户煽动民众情绪
  - 分发式攻击

§2 信息安全概念

§2.1 信息安全的属性

§2.2 信息安全范畴

§2.3 信息安全的特点

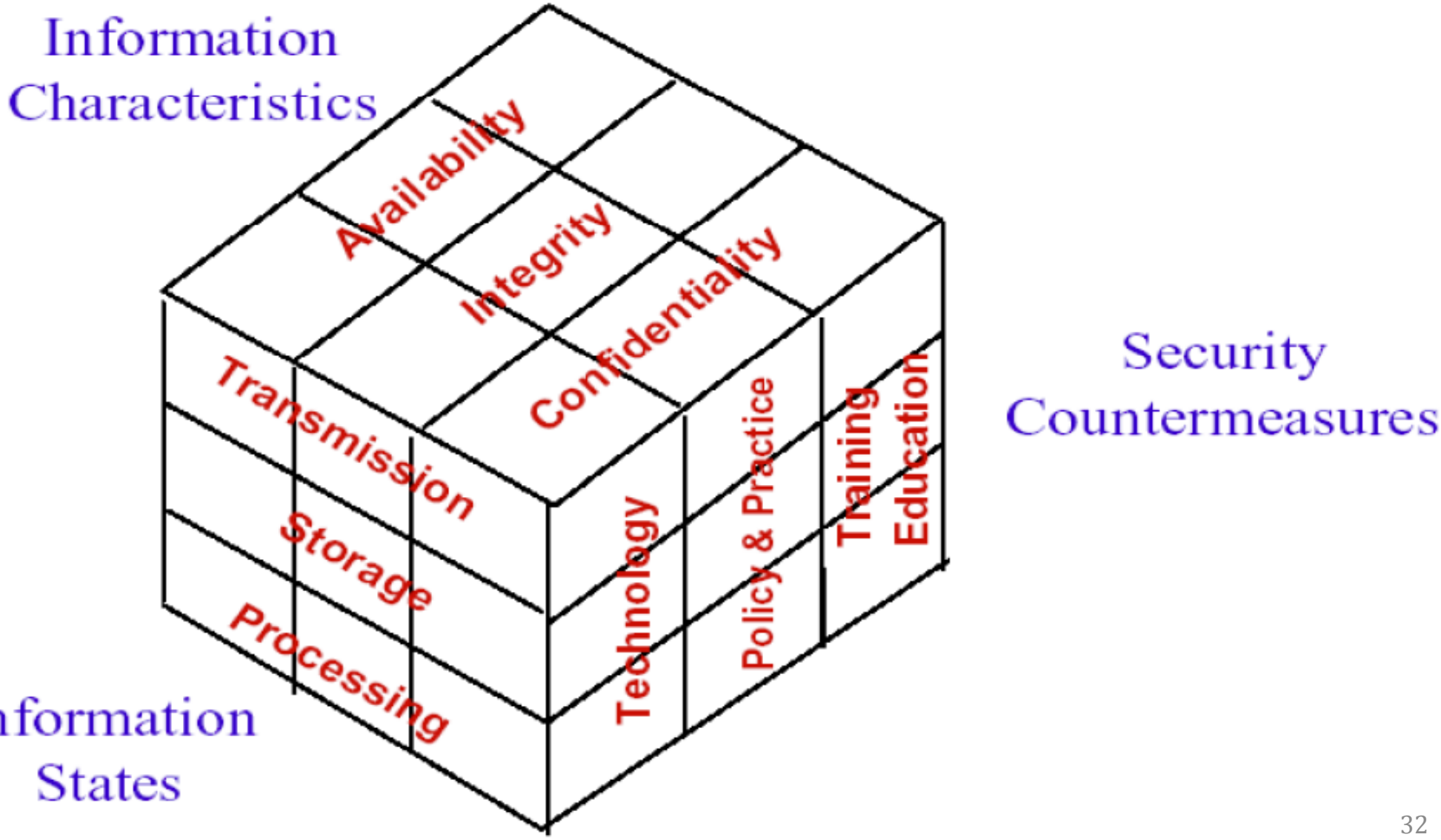
§2.4 信息安全的重要性

§2.1 信息安全的属性

信息安全的六个方面

- 保密性：信息不泄漏给非授权的用户、实体或者过程的特性
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性
- 可用性：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息
- 可控性：对信息的传播及内容具有控制能力，访问控制即属于可控性
- 可靠性：系统可靠性（不可抵赖性？）
- 真实性：内容的真实性（完整性？）

§2.2 信息安全范畴


Information Characteristics
Availability
Integrity
Confidentiality
Transmission
Storage
Processing
Technology
Policy & Practice
Training
Education
Security Countermeasures
Information States

§2.3 信息安全的特点

信息安全的特点

§2.3 信息安全的特点

信息安全的特性

- 攻防特性：攻防技术交替改进
- 相对性：信息安全总是相对的，（够用就行？）
- 配角特性：信息安全总是陪衬角色，不能为了安全而安全，安全的应用是先导
- 动态性：信息安全是持续过程

§2.4 信息安全的重要性

- 信息安全与政治有关
  - 1999年1月份左右，美国黑客组织“美国地下军团”联合了波兰的、英国的黑客组织，世界上各个国家的一些黑客组织，有组织地对我们国家的政府网站进行了攻击
  - 1999年7月份，台湾李登辉提出了两国论
  - 2000年5月8号，美国轰炸我国驻南联盟大使馆后
  - 2001年4月到5月，美机撞毁王伟战机侵入我海南机场

§2.4 信息安全的重要性

- 信息安全与经济犯罪有关
  - 我国计算机犯罪的增长速度超过了传统的犯罪： 97年20几起，98年142起，99年908起，2000年上半年1420起
  - 利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务
  - 近几年已经破获和掌握100多起，涉及的金额几个亿

§2.4 信息安全的重要性

- 信息安全与社会稳定有关
  - 互连网上散布一些虚假信息、有害信息对社会管理秩序造成的危害，要比现实社会中一个造谣要大的多
    - ✓ 1999年4月，河南商都热线一个BBS，一张说“交通银行郑州支行行长协巨款外逃”的帖子，造成了社会的动荡，三天十万人上街排队，挤提了十个亿
  - 针对社会公共信息基础设施的攻击严重扰乱了社会管理秩序
    - ✓ 2001年2月8日正是春节，新浪网遭受攻击，电子邮件服务器瘫痪了18个小时。造成了几百万的用户无法正常的联络

§3 信息安全技术

§3.1 密码、访问控制和鉴权

§3.2 物理安全技术

§3.3 网络安全技术

§3.4 容灾与数据备份

§3.1 密码、访问控制和鉴权

- 密码技术（信息安全的核心）
- 两类密码体制
- 鉴权认证相关：口令、密码、生物认证
- 访问控制：身份认证

§ 3.2 物理安全技术

狭义物理安全

- 包括环境安全、设备安全和介质安全，主要解决由于设备、设施、介质的硬件条件所引发的信息系统物理安全威胁问题。

广义物理安全

- 应包含由软件、硬件、操作人员组成的整体信息系统物理安全，即包括系统物理安全。其应确保信息系统的保密性、可用性、完整性。

§ 3.2 物理安全技术

- 机房安全级别要求

安 全 项 目	C类	B类	A类
场地选择	—	⊕	⊕
防火	⊕	⊕	⊕
内部装修	—	⊕	⊕
供配电系统	⊕	⊕	⊕
空调系统	⊕	⊕	⊕
火灾报警及消防设施	⊕	⊕	⊕
防水	—	⊕	⊕
防静电	—	⊕	⊕
防雷击	—	⊕	⊕
防鼠害	—	⊕	⊕
电磁波的防护	—	⊕	⊕

§ 3.3 网络安全技术

- 防火墙技术
- 虚拟专用网络(VPN)技术
- 入侵检测系统(IDS)技术
- …

§3.4 容灾与数据备份

- 依据备份的数据量分类
  - 完全备份(full backup)
  - 增量备份(incremental backup)
  - 差分备份(differential backup)
  - 综合型完全备份（Synthetic full backup）
- 依据备份形式分类
  - 物理备份
  - 逻辑备份
- 冷备份和热备份
  - 冷备份（脱机备份）
  - 热备份（联机备份）

§4 信息安全管理

§4.1 信息安全管理的概念

§4.2 信息安全管理要素关联

§4.3 信息安全管理体系

§4.4 信息安全法规

§ 4.1 信息安全管理的概念

信息安全的“木桶原理”

- **信息安全的建设过程**是一个系统工程，它需要对信息系统的各个环节进行统一的综合考虑、规划和架构，并需要兼顾组织内外不断发生的变化，任何环节上的安全缺陷都会对系统构成威胁。
- 一个组织的信息安全水平将由与信息安全有关的所有环节中最薄弱的环节决定。一个组织必须使构成安全防范体系的这只“木桶”的所有木板都要达到一定的长度。
- 成熟的标准和实践是信息安全工作的重要依据

§ 4.1 信息安全管理的概念

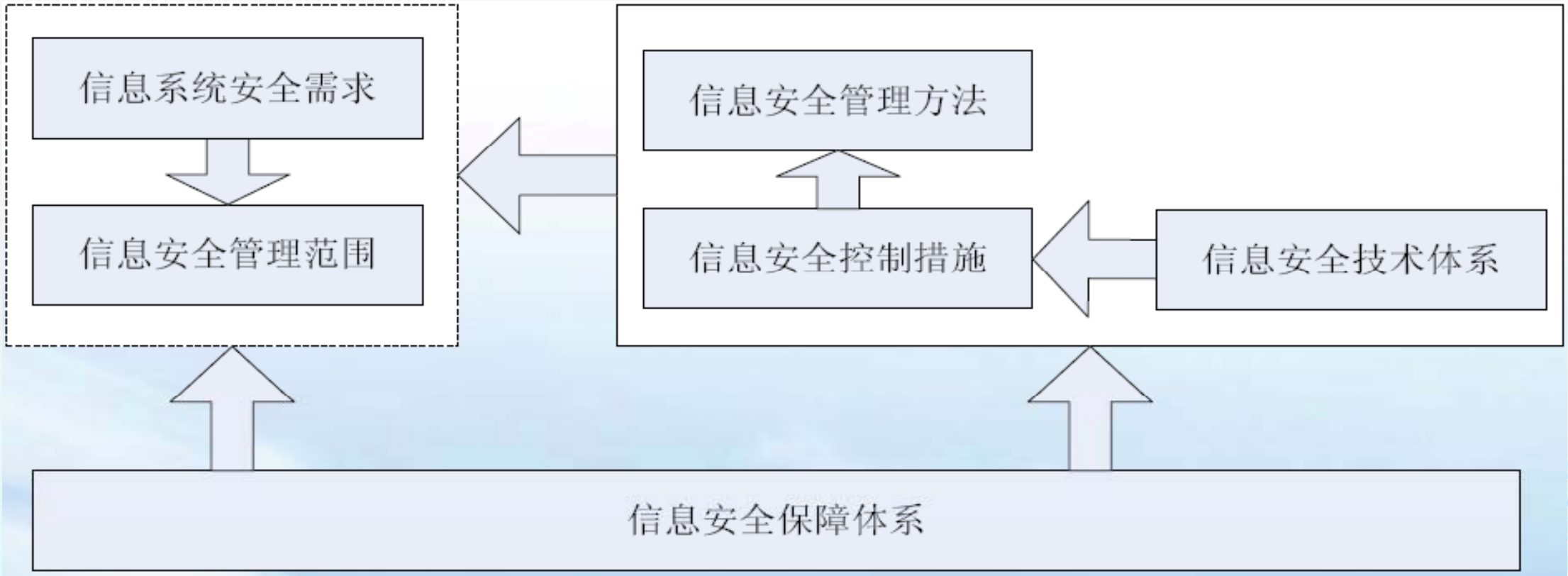
- **管理**是针对特定**对象**、遵循确定**原则**、按照规定**程序**、运用恰当**方法**、为了完成某项**任务**以及实现既定**目标**而进行的计划、组织、指导、协调和控制等活动。对现代企业和组织来说，管理对其正常业务运行起着举足轻重的作用。
- **信息安全管理**是组织为实现信息安全目标而进行的管理活动，是组织完整的管理体系中的一个重要组成部分，是为保护信息资产安全，指导和控制组织的关于信息安全风险的相互协调的活动。**信息安全管理是通过维护信息的机密性、完整性和可用性等，来管理和保护组织所有信息资产的一系列活动。**

§ 4.1 信息安全管理的概念

信息安全管理范围

- 信息安全管理不仅是安全管理部门的事务，而且是**整个组织**必须共同面对的问题。
- 信息安全管理范围涉及**组织安全策略及安全管理制度、人员管理、业务流程、物理安全、操作安全**等多个方面。
- 信息安全管理涉及**全体员工**，包括各级管理人员、技术人员、操作人员等；从业务上看，信息安全管理贯穿到所有与信息及其处理设施有关的**业务流程**当中。

§ 4.2 信息安全管理范畴



§ 4.2 信息安全管理范畴

各相关内容之间关系

- 信息安全需求是信息安全的出发点，它包括机密性需求、完整性需求、可用性需求、抗抵赖性、真实性需求、可控性需求和可靠性需求等。
- 信息安全管理范围是由信息系统安全需求决定的具体信息安全控制点，对这些实施适当的控制措施可确保组织相应环节的信息安全，从而确保组织整体的信息安全水平。
- 信息安全控制措施是指为改善具体信息安全问题而设置技术或管理手段，信息安全控制措施是信息安全管理的基础。

§ 4.2 信息安全管理范畴

各相关内容之间关系（续）

- 对一个特定的组织或信息系统，选择和实施控制措施的方法就是信息安全管理方法，信息安全管理的方法多种多样，信息安全风险评估是其中的主流。除此之外，信息安全事件管理、信息安全测评认证、信息安全工程管理也从不同侧面对信息安全的安全性进行管理。
- 信息安全保障体系则是保障信息安全管理各环节、各对象正常运作的基础，其中包括信息安全法律法规、信息安全标准体系、信息安全基础设施、信息安全产业和信息安全教育体系等方面。

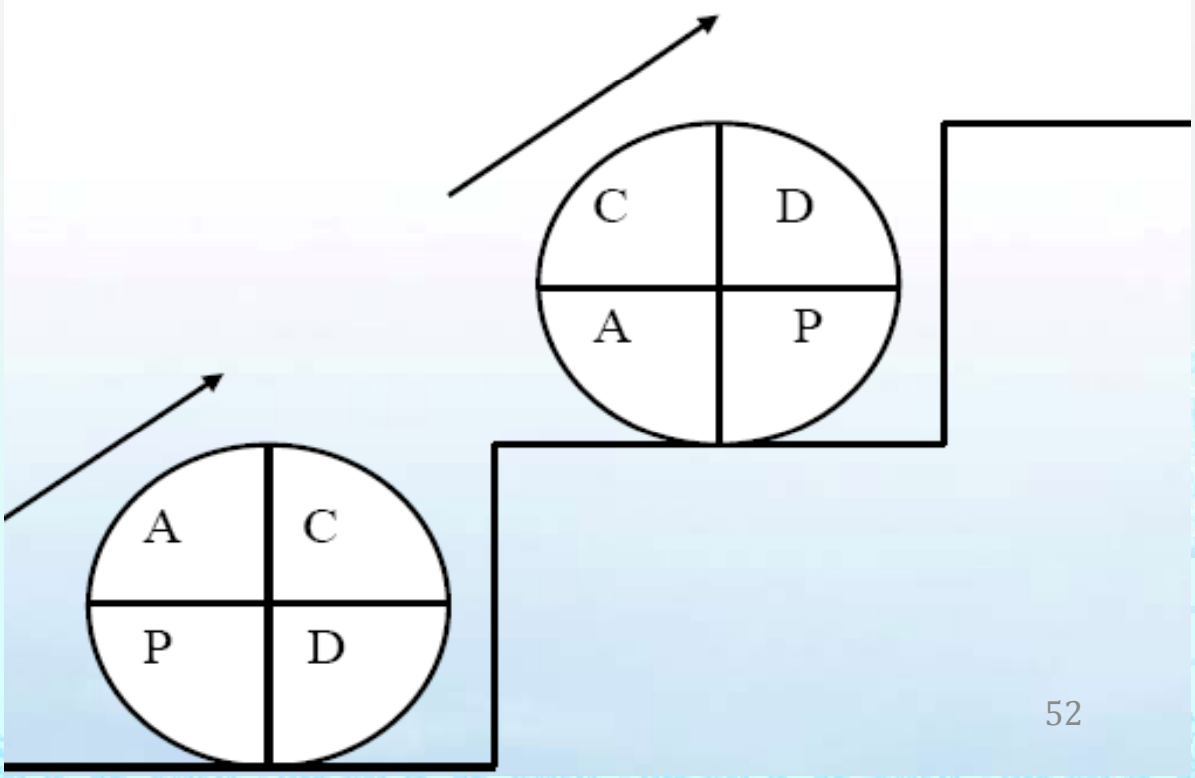
§ 4.3 信息安全管理体系

信息安全管理体系（ISMS：Information Security Management System）

- 是基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进信息安全的一套管理体系，是整个管理体系的一部分，管理体系包括组织结构、方针策略、规划活动、职责、实践、程序、过程和资源。
- ISMS概念的提出源于BS7799-2，也就是后来的ISO/IEC 27001。
- ISO/IEC 27001提出了在组织整体业务活动和所面临风险的环境下建立、实施、运行、监视、评审、保持和改进ISMS的PDCA模型，对PDCA模型的每个阶段的任务及注意事项、ISMS的文件要求、管理职责做了较为详细的说明，并对内部ISMS审核、ISMS管理评审、ISMS改进也分别做了说明。

§ 4.3 信息安全管理体系

- ISMS的PDCA持续改进过程，如下图：
  - P(plan)：计划，确定方针和目标，确定活动计划。
  - D(do)：实施，实现计划中的内容。
  - C(check)：检查，总结执行计划的结果，注意效果，找出问题
  - A(action)：处理总结结果，成功的经验加以肯定、推广和标准化；失败的教训加以总结，避免重现；未解决问题进入下一循环。



§ 4.4 信息安全法规

信息安全法律法规

- 信息安全法律法规泛指用于规范信息系统或与信息系统相关行为的法律法规，信息安全法律法规具有命令性、禁止性和强制性。
- 命令性和禁止性要求法律关系主体应当从事一定行为的规范，其规定的行为规则的内容是确定的，不允许主体一方或双方任意改变或违反，具体强制性。如果不执行，就要受到一定的法律制裁。

§5 信息安全发展

§5.1 新安全技术出现

§5.2 集成化的安全工具

§5.3 管理类的安全工具

§5.4 信息安全管理手段

§ 5.1 新安全技术出现

- 可信计算
- 网格技术
- 数字内容安全
- 隐私保护
- ……

§ 5.2 集成化的安全工具

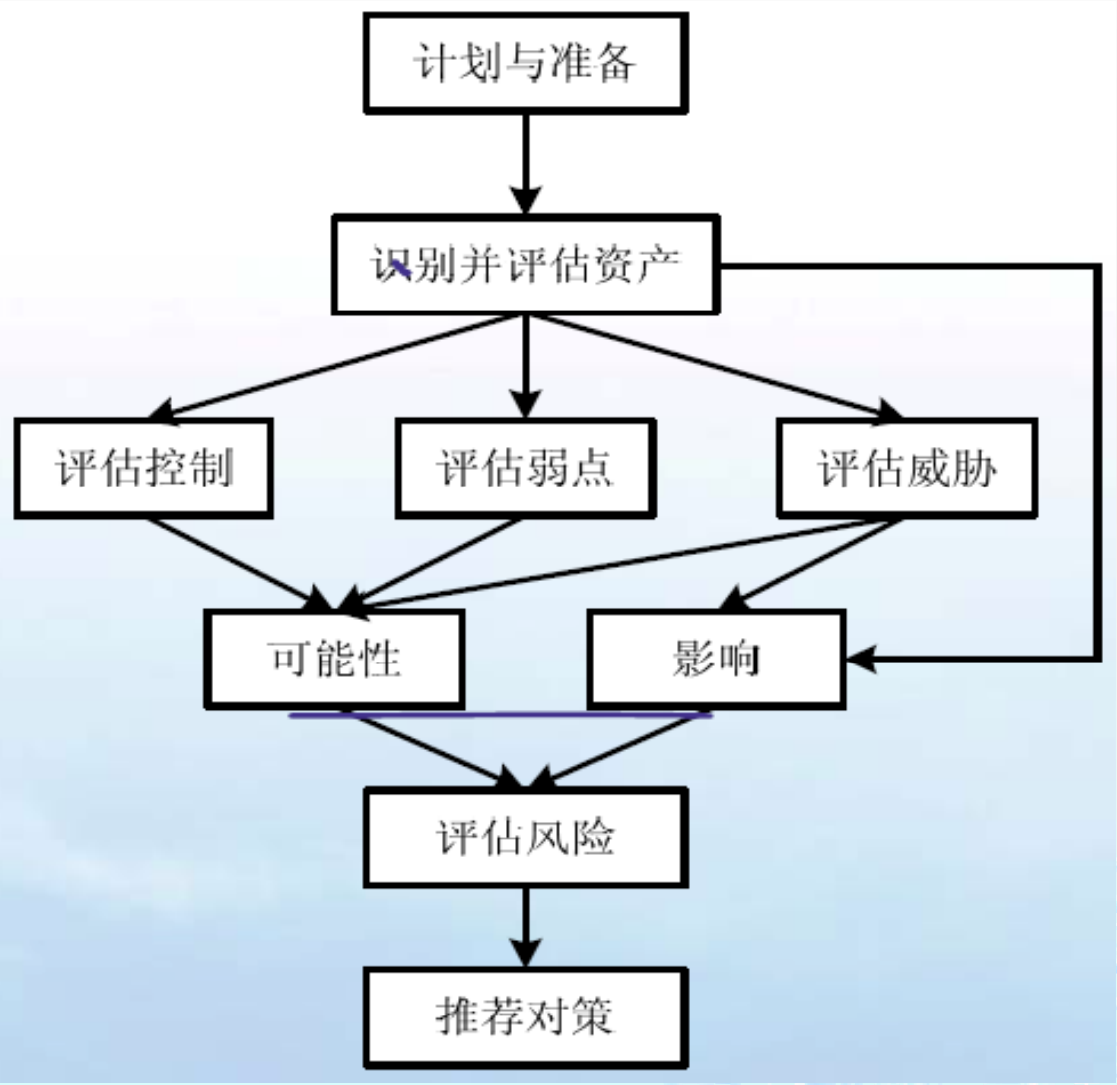
- 防火墙＋防病毒
- 防火墙＋VPN
- 防火墙＋IDS
- 安全网关
- 主机安全防护系统
- 网络监控系统
- ……

§ 5.3 管理类的安全工具

- 安全管理平台
- 统一威胁管理工具
- 日志分析系统
- ……

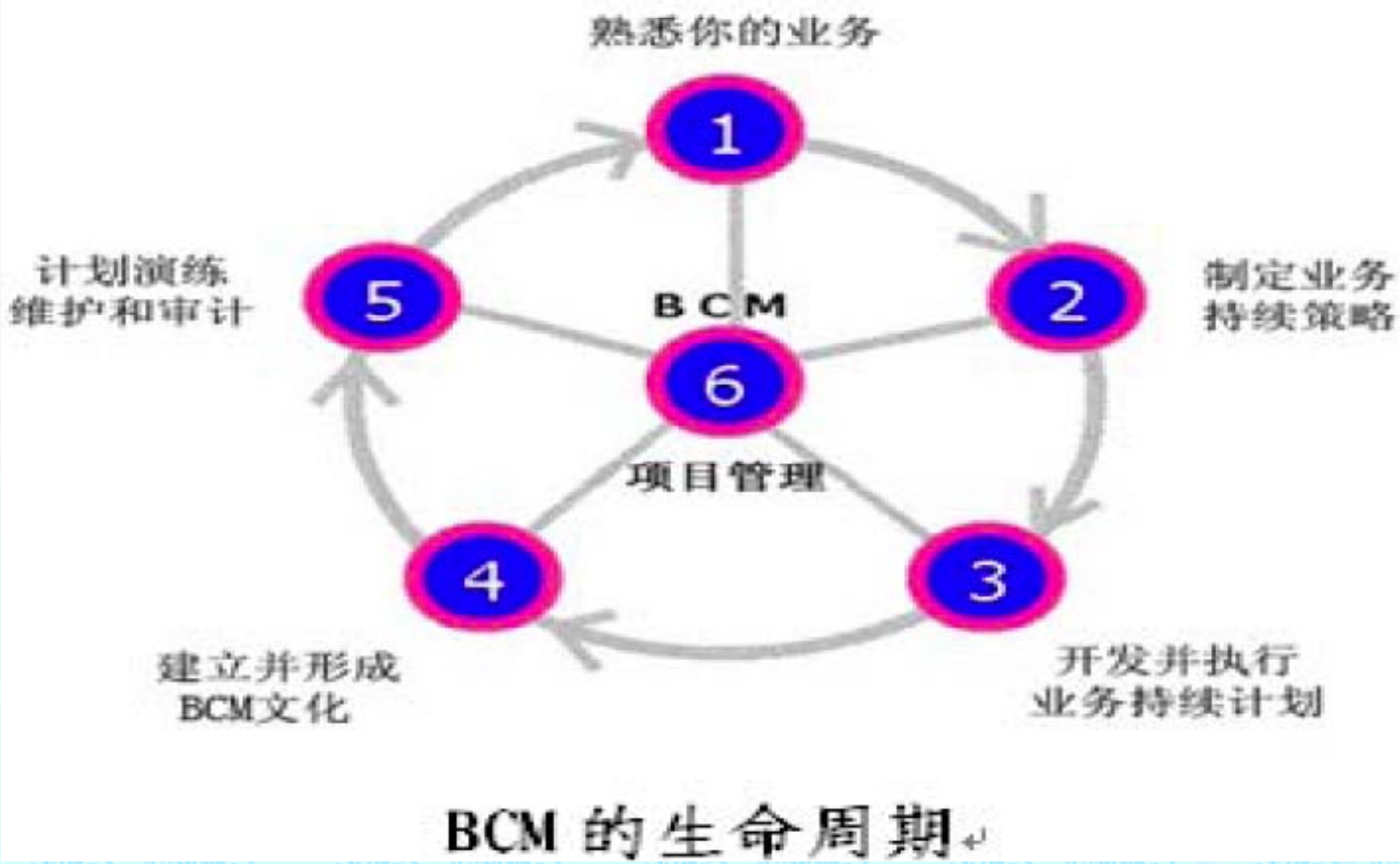
§5.4 信息安全管理手段

- 信息安全风险评估
  - 基本模型
  - 相关标准



§5.4 信息安全管理手段

- 业务连续性计划(BCM)



BCM 的生命周期

本章小结

- 内容小结
  - 信息安全威胁的内容及对策
  - 信息安全、信息安全管理概念
  - 典型信息安全技术

本章小结

- 作业：思考题（下次课前提交手写版）
  - 简述信息安全威胁根源的理解。
  - 简述你对信息安全基本属性的理解。
  - 简述你对信息安全管理涵义与目标的理解。