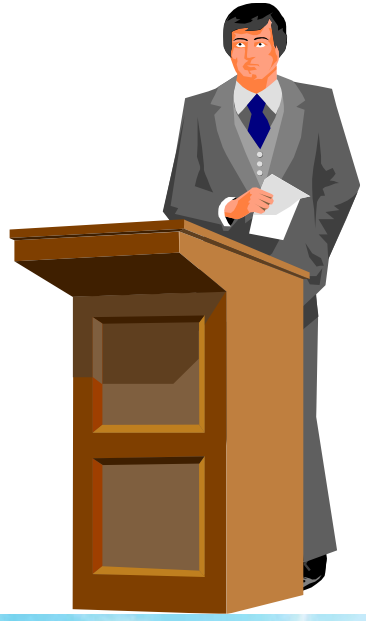
第1章 概述

信息安全管理

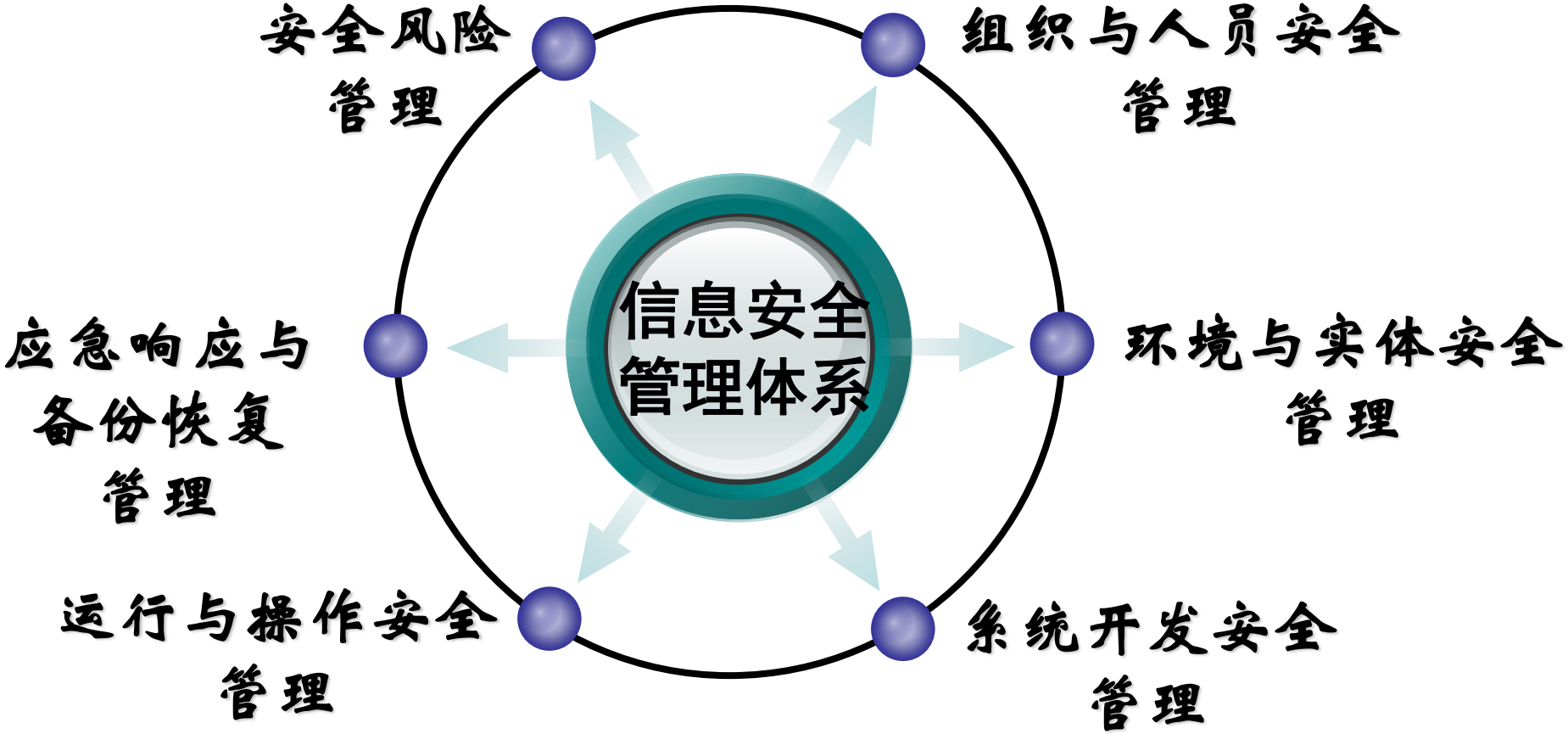


主讲 李章兵

课程介绍

- 本课程主要讨论信息安全管理体系、信息安全管理的相关标准及实施方法。
- 教学目标
  - 掌握信息资产识别与价值评估；
  - 掌握信息安全风险分析方法和测评技术；
  - 掌握信息安全管理的内涵、体系、内容和实施过程；
  - 掌握信息安全管理的基本理论和手段；
  - 全面了解信息安全管理体系，理解信息安全管理体系的构建过程；
  - 树立信息安全管理意识，形成良好的安全观念

课程介绍


安全风险管理
组织与人员安全管理
信息安全管理体系
应急响应与备份恢复管理
环境与实体安全管理
运行与操作安全管理
系统开发安全管理

课程介绍

- 第1章 概述……2学时
- 第2章 信息安全管理体系……4学时
- 第3章 合规性与风险评估……4学时
- 第4章 信息安全组织与策略管理……2学时
- 第5章 人员安全与情报……4学时
- 第6章 物理实体与环境安全……4学时
- 第7章 信息系统运维安全……4学时
- 第8章 信息服务与安全事件……4学时
- 第9章 业务连续性管理……4学时
- 第10章 等级保护与测评……4学时

课程介绍

学时与考试

共32学时，28学时讲授，2学时考试（闭卷）。
考试成绩占70%，平时30%。
考勤三次缺课平时成绩为0

第一章 信息安全概述

- 1.1 信息与信息安全
- 1.2 信息安全管理的引入-重要性
- 1.3 信息安全管理的内涵
- 1.4 信息安全管理国内外现状
- 1.5 信息安全管理相关标准
- 1.6 信息安全管理的趋势
- 1.7 信息安全政策
- 1.8 信息安全法律体系

教学目标

- 本章的重点
  - 信息的特点、信息安全定义
  - 信息安全管理定义、内涵
  - 信息安全保障定义
  - 信息安全发展阶段、趋势
  - 信息安全法律体系

1.1 信息与信息安全

- 信息及信息的价值
  - “真相的濒危甚于老虎的濒危”
  - “放映的删节版《色,戒》，剧情不完整，侵犯消费者的公平交易权和知情权 ”
  - “剧情”、“真相”等都是一种信息
- 信息、物质、能量是人类社会赖以生存和发展的三大要素
  - 灾难备份——给银行数据信息上保险
  - 公安部:超过一半单位发生过信息网络安全事件

1.1 信息与信息安全

- 一、信息与信息资产
- （一）信息的定义
  - 广义：事物的运动状态以及运动状态形式的变化，是一种客观存在。（客观存在并不是区分真假信息的依据）
  - 狭义：能被主体感觉到并被理解的东西（客观存在）。
  - 本书的定义：通过在数据上施加某些约定而赋予这些数据的特殊含义。
  - 信息具有价值，是一种资产。

1.1 信息与信息安全

- 信息资产分类
  - 数据：存在于电子媒介的各种数据资料
  - 软件：应用软件、系统软件、开发工具和资源库
  - 硬件：计算机硬件、路由器、交换机、布线等
  - 服务：操作系统、WWW、网络管理和安保等
  - 文档：纸质文件、传真、财务报告、发展计划等
  - 设备：电源、空调、门禁、办公家具等
  - 人员：雇主和各级雇员等
  - 其他：企业形象、客户关系等（软资产）

1.1 信息与信息安全

- （二）信息的特点
  - 感知和理解
    - 信息与接受对象和要达到的目的有关
  - 信息的价值性
    - 信息的价值与接受信息的对象有关
  - 约定的多样性
    - 信息有多种多样的传递手段
  - 可复制性
    - 信息的共享性

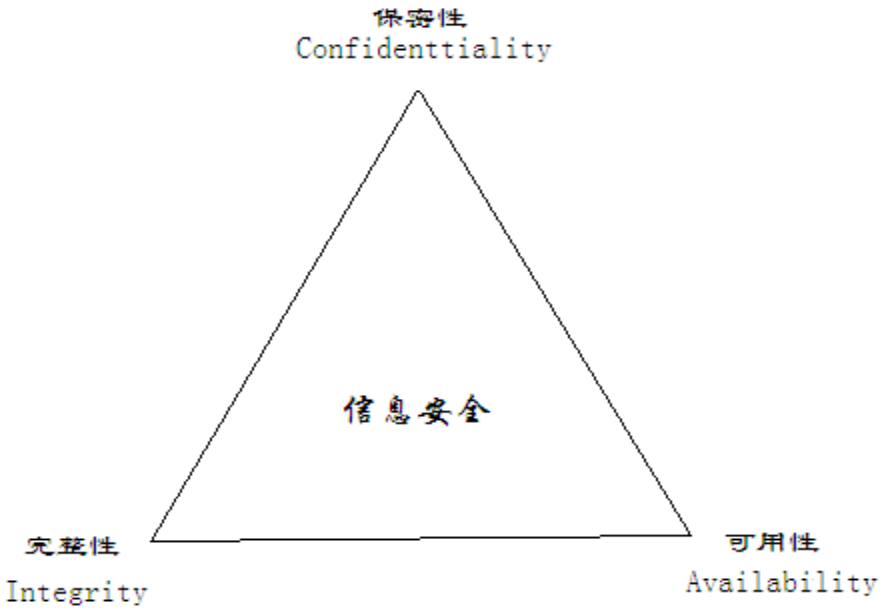
1.1 信息与信息安全

- 二、信息安全
- （一）信息安全的定义
  - ISO：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄漏
- 信息安全的三个主要问题：
  - 1.保护对象：主要是硬件、软件、数据
  - 2.安全目标：保密性、完整性、可用性
  - 3.实现途径：技术和管理

– 3：7

1.1 信息与信息安全

- （二）信息安全三属性的含义（Pass）
  - 保密性
  - 完整性
  - 可用性



1.1 信息与信息安全

- 信息安全表现层面

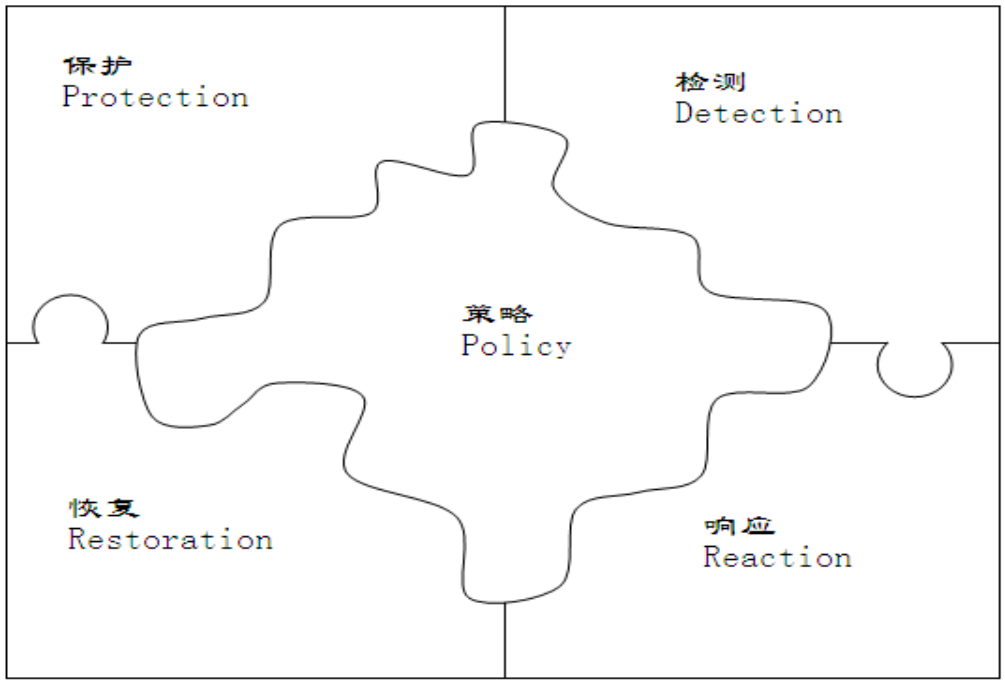
性质	问题	内涵	影响	表现
基础设施	技术安全	信息的完整性、机密性、可用性等	社会经济损失	安全事故
新兴媒体	文化安全、舆论安全	网络信息内容的健康、积极和可控	社会、政治稳定	道德影响、信任危机
社会形态	政治与国家安全、经济和社会安全	网络社会的政治、经济和社会秩序	政权、经济发展和社会稳定	突发事件、社会危机
主权存在	军事安全、国家安全	国家之间的信息对抗与斗争	国家主权、国际利益	军事冲突、信息对抗

1.1 信息与信息安全

- （三）信息安全模型
  - 1.PDR模型
    - Pt(protection)有效保护时间，信息系统的安全措施能够有效发挥保护作用的时间；
    - Dt(detection)检测时间，安全监测机制能够有效发现攻击、破坏行为所需的时间；
    - Rt(reaction)响应时间，安全机制作出反应和处理所需的时间。
  - 安全公式
    - （1）Pt＞Dt+Rt，系统安全 保护时间大于检测时间和响应时间之和；
    - （2）Pt＜Dt+Rt, 系统不安全 信息系统的安全控制措施在检测和响应前就会失效，破坏和后果已经发生。

1.1 信息与信息安全

- **2.PPDRR模型：**
  - 策略、保护、检测、响应、恢复
    - 后四环节在策略的指导下构成相互作用的有机体。



1.1 信息与信息安全

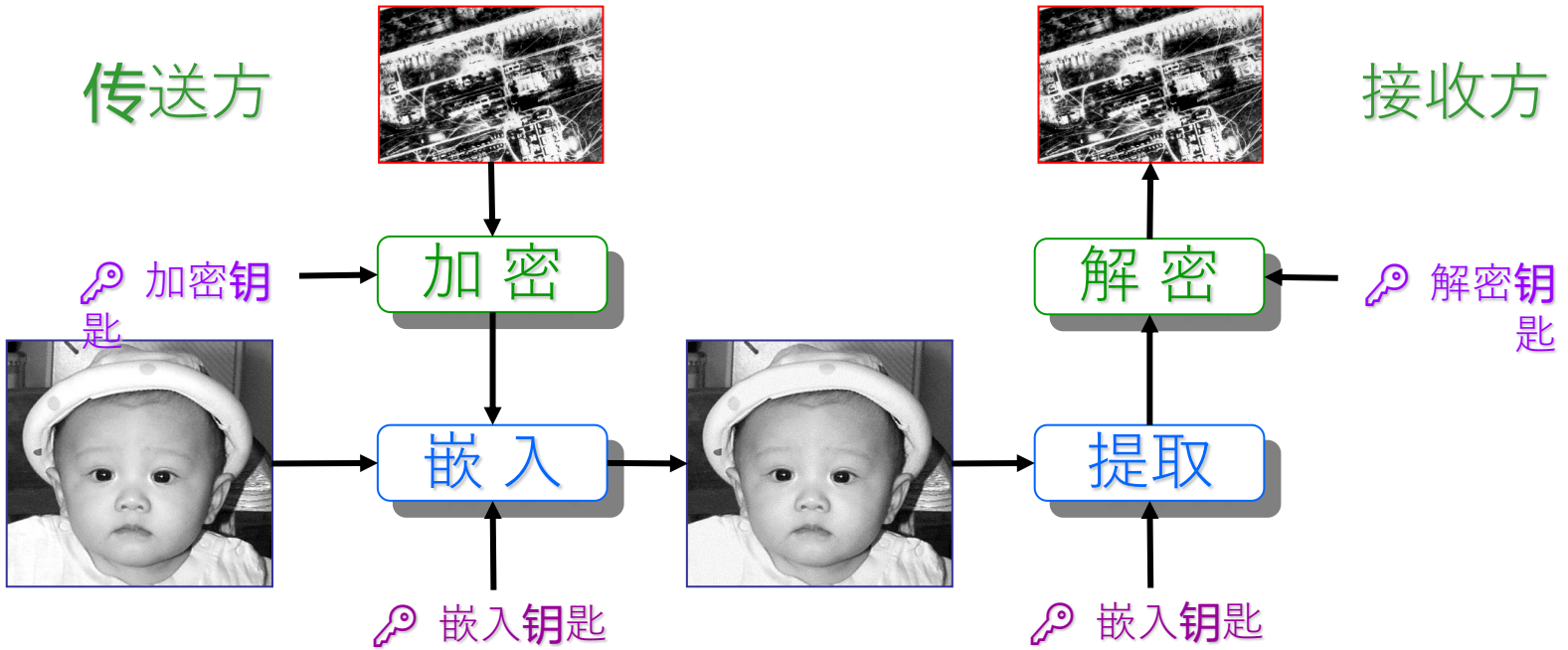
- （四）信息安全的发展三个阶段
  - 三阶段（或四阶段）：
    - 通讯保密阶段：重点是保密（点）
    - 信息安全阶段：关注信息安全的三属性：
      - 保密性 完整性 可用性（线、空间）
      - 本阶段也可分为计算机安全和IT安全2个阶段
    - 安全保障阶段：关注点有空间拓展到时间：
      - 策略、保护、 检测、 响应、恢复（系统）

1.1 信息与信息安全

- 信息安全发展历程
- 第一阶段：通信保密（ComSEC)
  - 上世纪40年代－70年代
    - 重点是通过密码技术解决通信保密问题，保证数据的保密性与完整性
    - 主要安全威胁是搭线窃听、密码学分析
    - 主要保护措施是加密
    - 重要标志
      - 1949年Shannon发表的《保密系统的通信理论》
      - 1977年美国国家标准局公布的数据加密标准（DES）
      - 1976年由Diffie与Hellman在“New Directions in Cryptography”一文中提出了公钥密码体制

1.1 信息与信息安全

- 第一阶段：通信保密
  - 案例分析：**影像加密伪装传输**



1.1 信息与信息安全

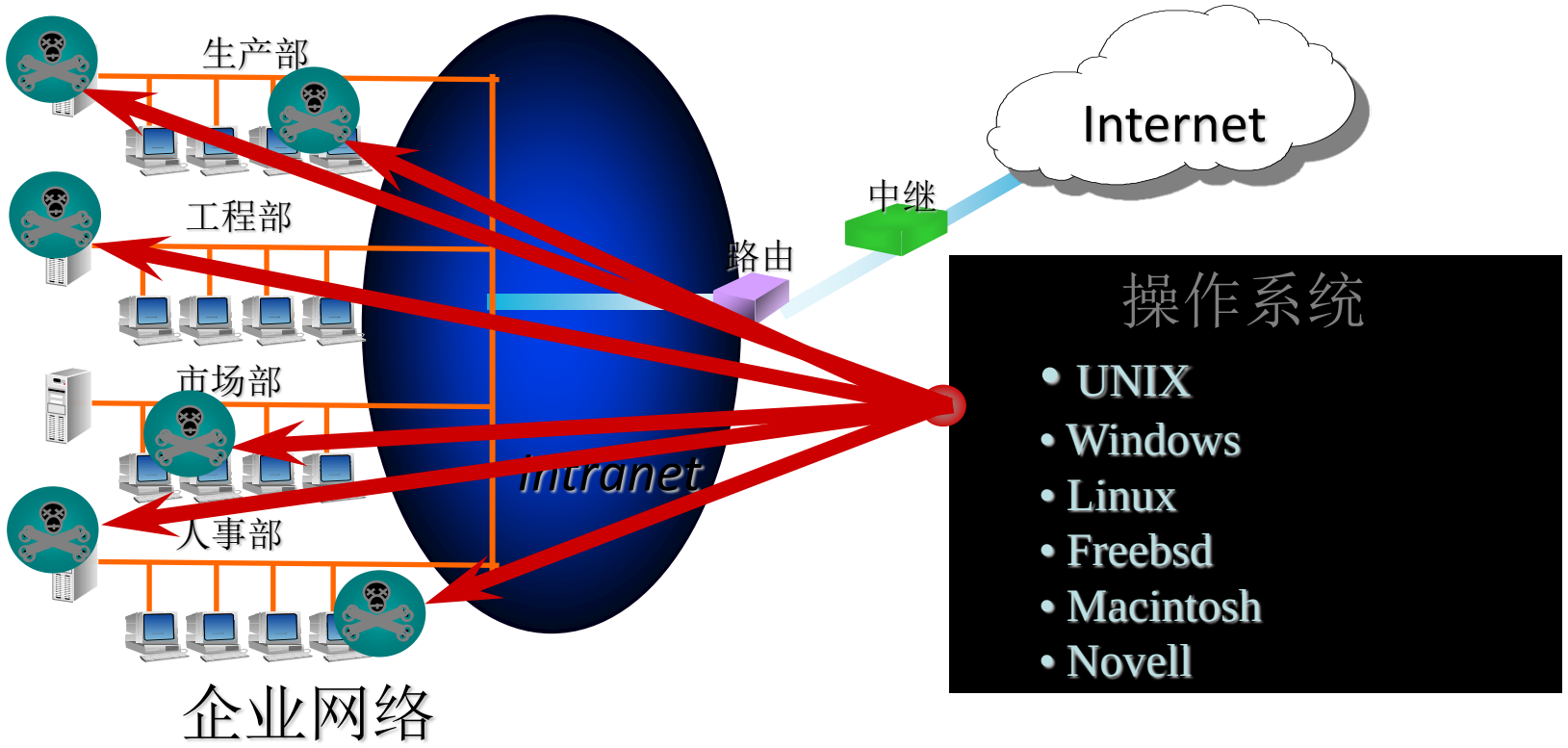
- 第一阶段：通信保密
  - 案例分析：微软「护照」问题
    - 资料來源：2001年11月4日台湾的联合报5版发表。
    - 1. 在西雅图网络安全研究员史蘭科发现一种欺骗微软公司保障网络购物的护照(Passport)主机，將他人的电子钱包资料传给他的方法并通知微软工程部之后，自2001年10月31日起，微软公司暫时关掉该项服务，以便進行网络修复与测试。
    - 2.「护照」是微软未來最重要的科技之一，至关闭时间为止，已有2,000,000人注册使用，而几乎所有XP的用户均无法使用到其服务。

1.1 信息与信息安全

- 信息安全发展历程
- 第二阶段：计算机安全(CompSEC)
  - 上世纪70—80年代（90年代中期）
    - 重点是确保计算机系统中硬件、软件及正在处理、存储、传输信息的机密性、完整性
    - 主要安全威胁扩展到非法访问、恶意代码、脆弱口令等
    - 主要保护措施是安全操作系统设计技术（TCB）
    - 主要标志
      - 1985年美国国防部公布的可信计算机系统评估准则（TCSEC）将操作系统的安全级别分为四类七个级别（D、C1、C2、B1、B2、B3、A1），后补充红皮书TNI（1987）和TDI（1991），构成彩虹（rainbow）系列。

1.1 信息与信息安全

- 第二阶段：计算机安全
  - 案例分析：操作系统安全



1.1 信息与信息安全

- 信息安全发展历程
- 第三阶段：IT安全(ITSEC)
  - 上世纪90年代（中期）以来
    - 重点需要保护信息，确保信息在存储、处理、传输过程中及信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击的措施。强调信息的保密性、完整性、可控性、可用性
    - 主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等
    - 主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN、安全管理等
    - 主要标志
      - 提出了新的安全评估准则CC（ISO 15408、GB/T 18336）

1.1 信息与信息安全

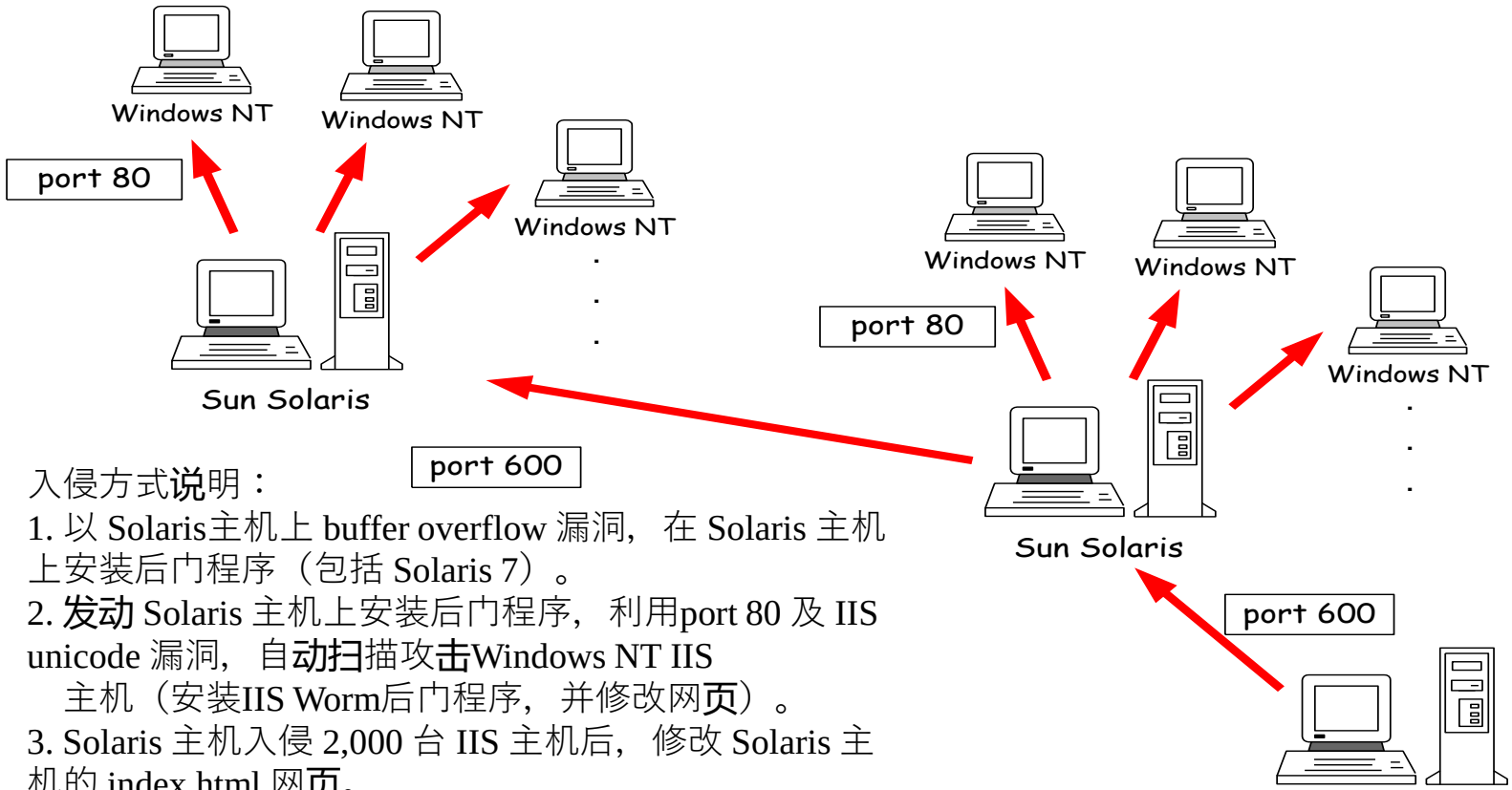
- 第三阶段：IT安全
  - 案例分析：入侵技术交流

1.1 信息与信息安全

- 第三阶段：IT安全
  - 案例分析：2001中美黑客大战
    - 1. 源起：2001年4月1日美国情报侦察机误闯中国领空与其所导致的歼八撞机失事、飞行员王伟先生失踪事件。
    - 2. 双方主力：
    - 中方：Lion联系了我国红客联盟（Honker Union of China，简称HUC）、第八军团、黑客联盟与鹰派黑客组织。
    - 美方：prOphet与poizonB0x黑客组织。
    - 3. 战争起迄时间：2001年4月30日晚上20时~2001年5月8日。
    - 4. 双方战果：
    - 美方被攻破网站：约1,600个。 （另一说法：5月2日92个）
    - 中方被攻破网站：约1,100个。 （另一说法：5月2日600多个）
    - 案例分析：2008年4月奥运保卫黑客大战
    - 目标：家乐福、CNN、www.frmtv.fr
    - 人数：据不完全统计3000多人，动用“肉鸡”15000多台。
    - 结果：家乐福被迫关闭，CNN亚洲频道受到干扰，frmtv在攻击期间短时瘫痪
    - 损失：三分之一的 “肉鸡”在攻击中被消耗。

1.1 信息与信息安全

- 第三阶段：IT安全
  - 案例分析： 5 2 0 前网站入侵描述图



入侵方式说明：

1. 以 Solaris主机上 buffer overflow 漏洞，在 Solaris 主机上安装后门程序（包括 Solaris 7）。
2. 发动 Solaris 主机上安装后门程序，利用port 80 及 IIS unicode 漏洞，自动扫描攻击Windows NT IIS 主机（安装IIS Worm后门程序，并修改网页）。
3. Solaris 主机入侵 2,000 台 IIS 主机后，修改 Solaris 主机的 index.html 网页。

1.1 信息与信息安全

- 第三阶段：IT安全
  - 案例分析： ５ ２ ０前网站入侵方法

– **1. Solaris 主机：**
– 检查是否存在以下目录：
– **/dev/cub - 包含受感染计算机的日志**
– **/dev/cuc - 包含蠕虫用来操作和传播的工具**
– 检查是否有下列后门程序在运行：
– **/bin/sh /dev/cuc/sadmin.sh**
  - **/dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111**
  - **/dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80**
  - **/bin/sh /dev/cuc/uniattack.sh**
  - **/bin/sh /dev/cuc/time.sh**
  - **/usr/sbin/inetd -s /tmp/.f**
  - **/bin/sleep 300**

2. NT IIS 主机：
n IIS 服务器日志文件（Winnt/System32/日志文件）：
2001-05-06 12：20：19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../ winnt/system32/cmd.exe /c+dir 200 –
2001-05-06 12：20：19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../ winnt/system32/cmd.exe /c+dir+..\ 200 –
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
获取 /脚本/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2 2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
获取 /scripts/root.exe /c+echo+<HTML 代码插入此处>../../索引.asp 502 -
3 3. 被入侵的网页文字如下：

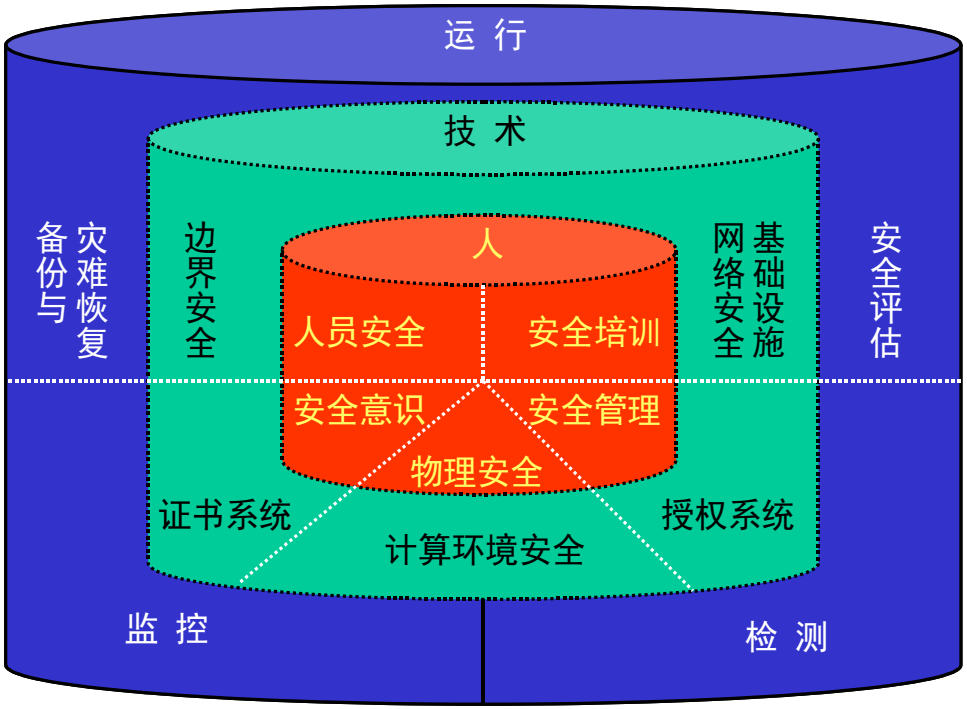
fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

1.1 信息与信息安全

- 信息安全发展历程
- 第四阶段：信息安全保障（IA）



1.1 信息与信息安全

- 第四阶段：信息安全保障
  - 信息保障(IA)定义
    - “确保信息和信息系统的可用性、完整性、可 认证性、保密性和不可否认性的保护和防范活动。 它包括了以综合保护、检测、反应能力来提供信息 系统的恢复。”
      - -----美国国防部（ DoD）国防部令S-3600.1
  - 信息保障包括什么
    - 一个宗旨:保障信息化带来的利益最大化(应用服务安全)
    - 两个对象
      - ★ 信息
      - ★信息系统

1.1 信息与信息安全

- 第四阶段：信息安全保障
  - 信息保障包括什么
    - 三个安全保障能力来源
      - ★技术
      - ★管理
      - ★人

■四个层面

★局域计算环境
★边界和外部连接
★基础设施
★信息内容

■五个信息状态

★产生
★存储
★处理
★传输
★消亡

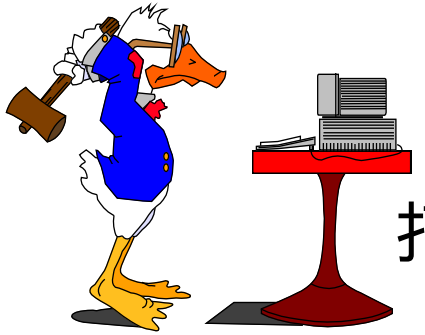
■六个信息保障的环节

★预警（W）
★保护（P）
★检测（D）
★响应（R）
★恢复（R）
★反击（C）

1.1 信息与信息安全

- 第四阶段：信息安全保障
  - 信息保障包括什么

■七个安全属性
★保密性
★完整性
★可用性
★可认证性
★不可否认性
★可控性
★可追究性

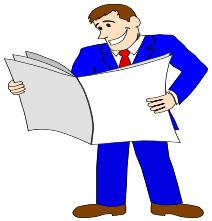


打不垮

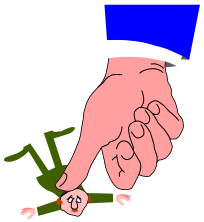
进不来

拿不走

改不了



看不懂

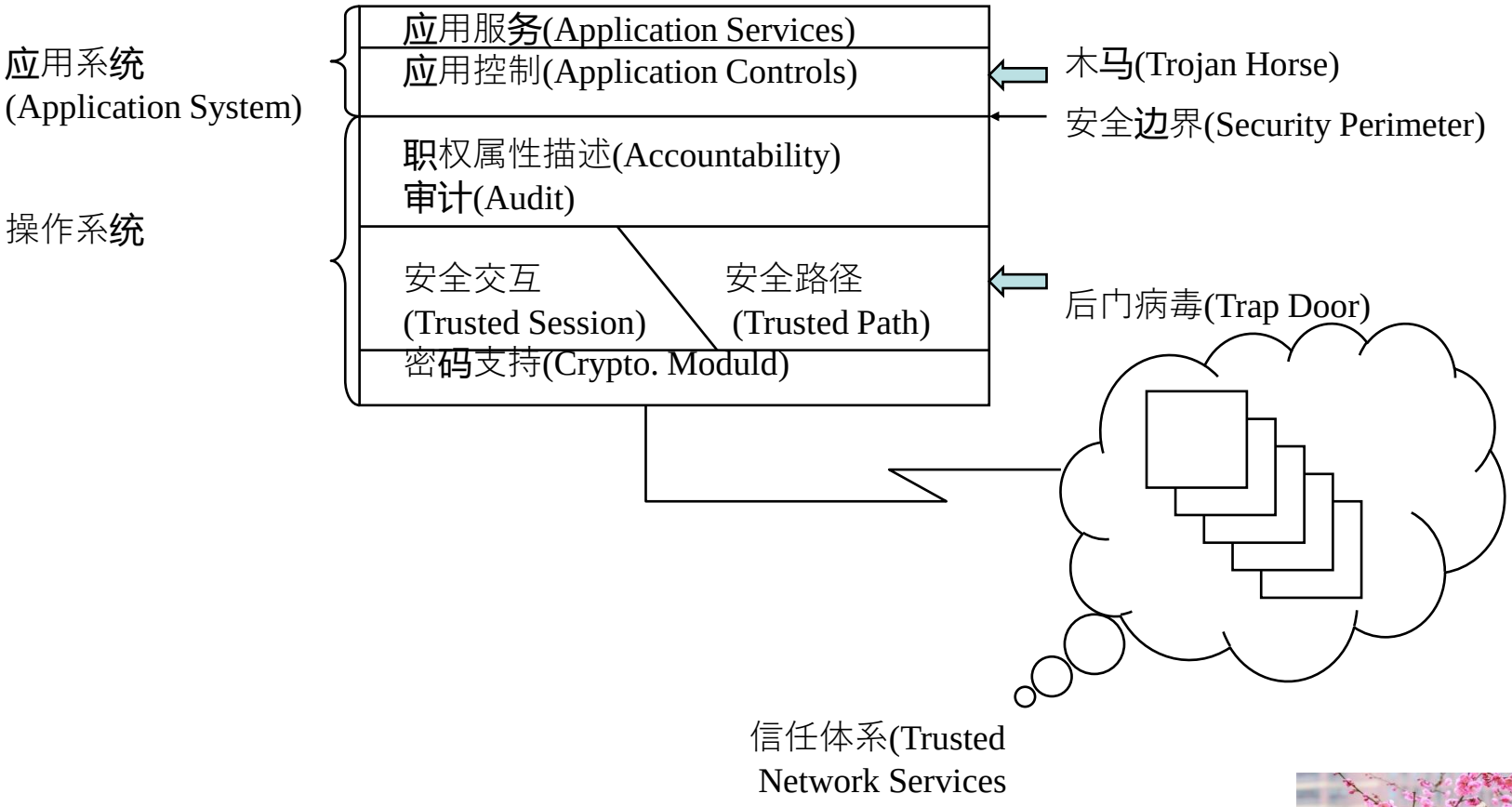


跑不了

可审查

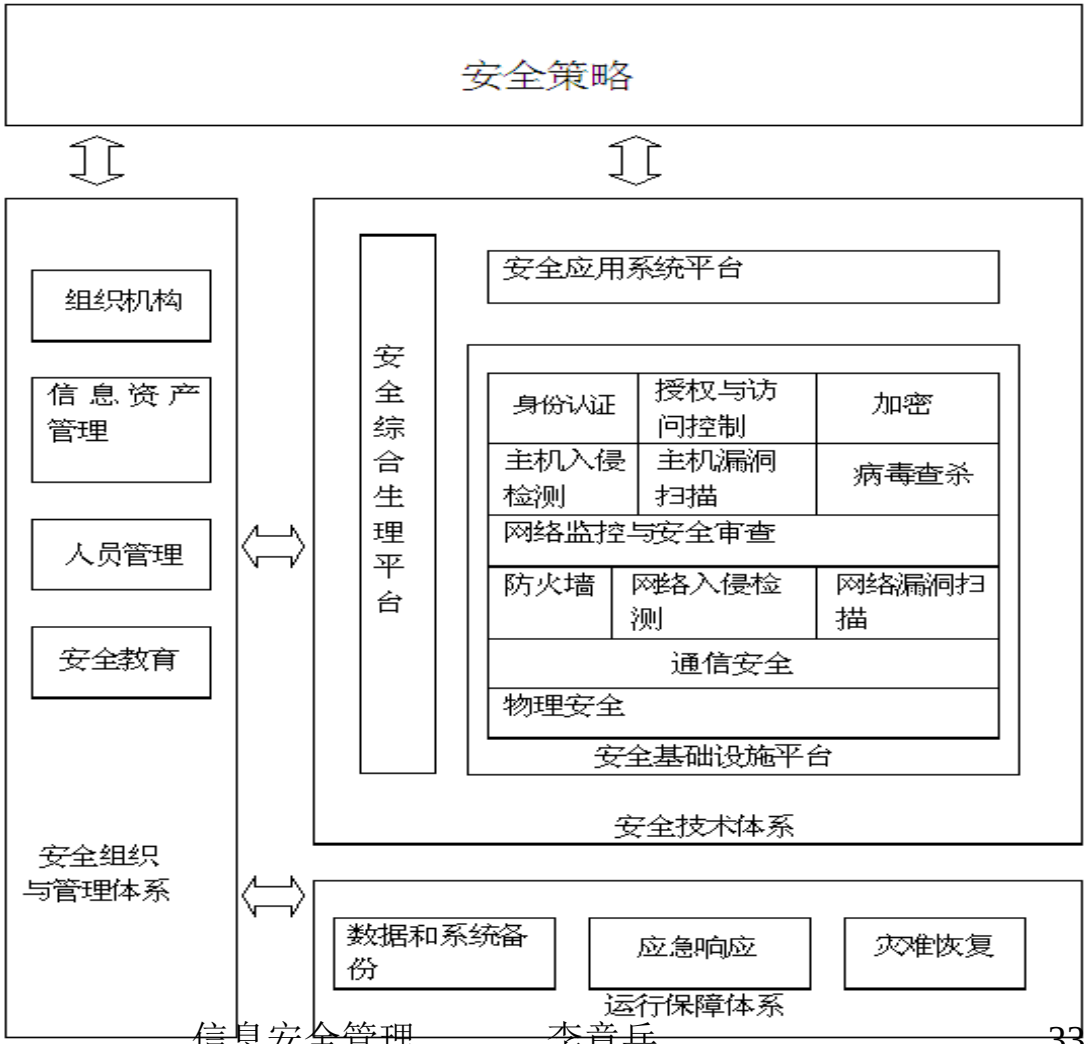
1.1 信息与信息安全

- 第四阶段：信息安全保障
  - 应用安全边界分析



1.1 信息与信息安全

- （五）信息安全保障体系



1.1 信息与信息安全

- 图表说明：
- 1.安全技术体系
  - 是整个安全体系的基础，包括3个平台
    - 安全基础设施平台
    - 安全应用系统平台
    - 安全综合管理平台
  - 安全基础设施平台
    - 从物理和通信安全防护、网络安全防护、主机系统安全防护、应用安全防护等多个层次出发，立足于现有的成熟的安全技术和安全机制，建立起防护体系。

1.1 信息与信息安全

- 1.安全技术体系
  - 安全应用系统平台
    - 处理安全基础设施与应用信息系统之间的关联和集成问题。通过使用安全基础设施平台所提供的各类安全服务，提升自身的安全等级，以更加安全的方式，提供业务服务和信息管理服务。
  - 安全综合管理平台
    - 对安全机制和安全设备进行统一的管理和控制，负责维护和管理安全策略，配置管理相应的安全机制。促成各类安全手段能与现有的信息系统应用体系紧密地结合，是信息系统安全与信息系统应用一体化。

1.1 信息与信息安全

- **2.安全组织与管理体系**
  - 安全组织与管理体系
    - 设计立足于总体安全策略，并与安全技术体系相配合增强防卫效果，弥补安全缺陷。
  - 信息安全管理体系
    - 由若干信息安全管理类组成，每项信息安全管理类可分解为多个安全目标和安全控制。

1.1 信息与信息安全

- **3.运行保障体系**
  - 内容涵盖安全技术和安全管理紧密结合的部分，包括：
    - 系统可靠性设计
    - 系统数据的备份设计
    - 安全时间的应急响应计划
    - 安全审计
    - 灾难恢复计划等

1.1 信息与信息安全

- **4.信息安全保障策略**

使命和价值

人员和组织

数据和介质

应用和业务

主机和系统

网络与通信

物理和环境

1.2 信息安全管理的引入

管理学ABC

- 管理学的研究内容可以归为:
  - 管理内容、管理原理、管理方法等。
  - “管理是什么”是属于认识论的问题。
  - “如何进行管理”是属于的方法论的问题。
  - 认识论是基础，方法论是目的。

1.2 信息安全管理的引入

管理学ABC

- 管理的内容
  - 研究管理的概念、行为、职能、本质、性质和特征等，其中管理的各种行为和职能既体现管理的基本任务，又反映了管理的全过程。
- 管理原理、原则
  - 是一个具有层次结构的理论体系，是实施管理职能的理论依据，是人们进行管理活动的行动指南，是管理学研究的重要部分。

1.2 信息安全管理的引入

管理学ABC

- 管理方法
  - 宗旨在于运用有限的人力、物力和财力取得最佳经济效益和社会效益
    - 管理方法实现：管理功能的执行和完成；
    - 管理目标实现：正确运用各种有效的管理方法，充分发挥管理功能和顺利达到管理目标的。
    - 研究管理方法是现代管理学中最引人注目的领域。

1.2 信息安全管理的引入

管理学ABC

- 管理是一门科学。
  - 管理通常被解释为主持或负责某项工作。
    - “管理理论丛林”现象。
  - 管理追求效益效率
    - 孔茨：管理就是设计和保持一种良好环境，使人在群体里高效率地完成既定目标。
  - 管理强调结果
    - 彼得•F•德鲁克：归根到底，管理是一种实践，其本质不在于“知”而在于“行”，其验证不在于逻辑，而在于成果；其唯一权威就是成就。

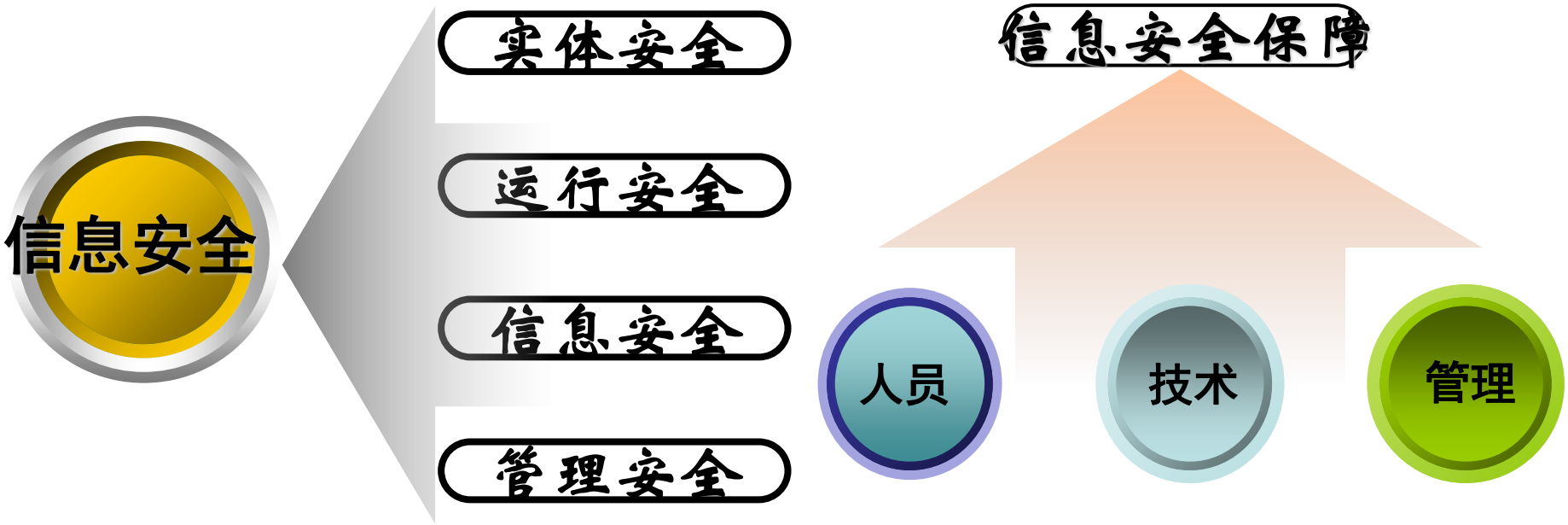
1.2 信息安全管理的引入

管理学ABC

- 管理是一个完整的过程
  - 过程由计划、组织、人事、领导和控制组成。
    - 法约尔：管理是所有的人类组织（不论是家庭、企业或政府）都有的一种活动，这种活动由五项要素组成：计划、组织、指挥、协调和控制。
    - 管理就是实行计划、组织、指挥、协调和控制。
- 管理活动的五个基本要素：
  - 谁来管：管理主体，回答由谁管的问题；
  - 管什么：管理客体，回答管什么的问题；
  - 怎么管：组织的目的要求，回答如何管的问题；
  - 靠什么管：组织环境或条件，回答在什么情况下管的问题。
  - 管得怎么样：管理能力和效果，回答管理成效问题。

1.2 信息安全管理的引入

- 信息安全管理的重要性



1.2 信息安全管理的引入

- 信息安全管理的重要性
  - 信息是资产，具有重要价值
  - 安全威胁
    - 信息的获取与发布；
    - 信息系统的外部、内部；
    - 个人、企业、国家。
  - 信息的安全需要管理
    - “三分技术，七分管理”
    - 信息系统的安全问题不能只局限于技术，更重要的还在于管理。

1.3 信息安全管理的内涵

- 信息安全管理定义
  - 是通过维护信息的机密性、完整性和可用性等，来管理和保护信息资产的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。
  - 信息安全管理是信息安全保障体系建设的重要组成部分 。

1.3 信息安全管理的内涵

- 信息安全管理的内容：
  - 安全方针和策略；
  - 组织安全；
  - 信息资产分类与价值评估；
  - 信息资产风险分析与测评；
  - 人员安全；
  - 物理与环境安全；
  - 通信、运行与操作安全；
  - 访问控制；
  - 系统获取、开发与维护；
  - 安全事故管理；
  - 业务持续性保障；
  - 符合性。

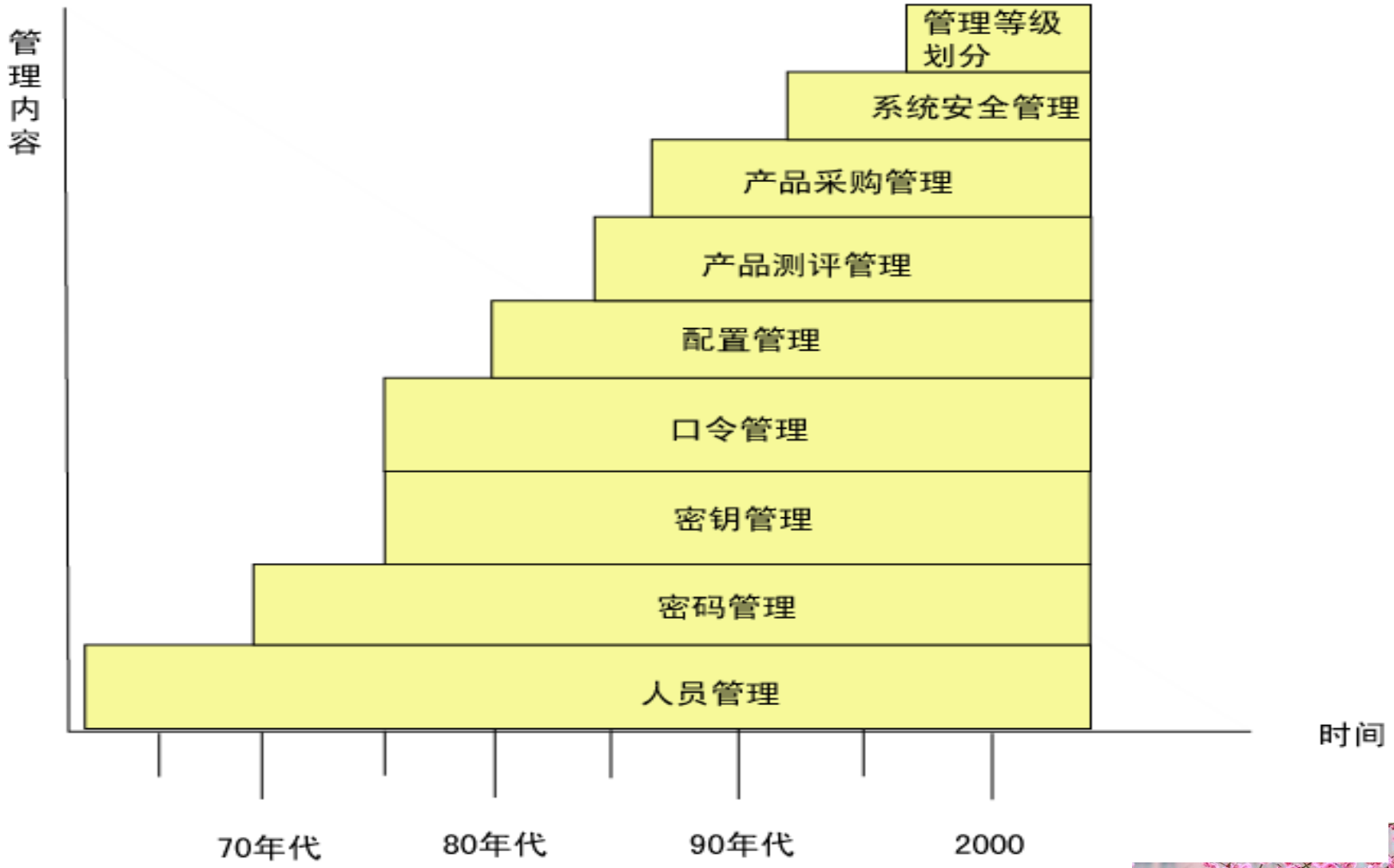
1.3 信息安全管理的内涵

做什么	如何做	做得怎样
• 明确目标和指导原则 • 多方面发掘需求 • 整体规划长远考虑 • 建立信息安全管理体系	• 建立并规范流程 • 提升人员意识和技能 • 实施技术解决方案 • 充分运用最佳实践	• 建立评价度量机制 • 内部和外部审计 • 反馈、纠正和预防 • 持续改进并提高

1.4 信息安全管理的国内外现状

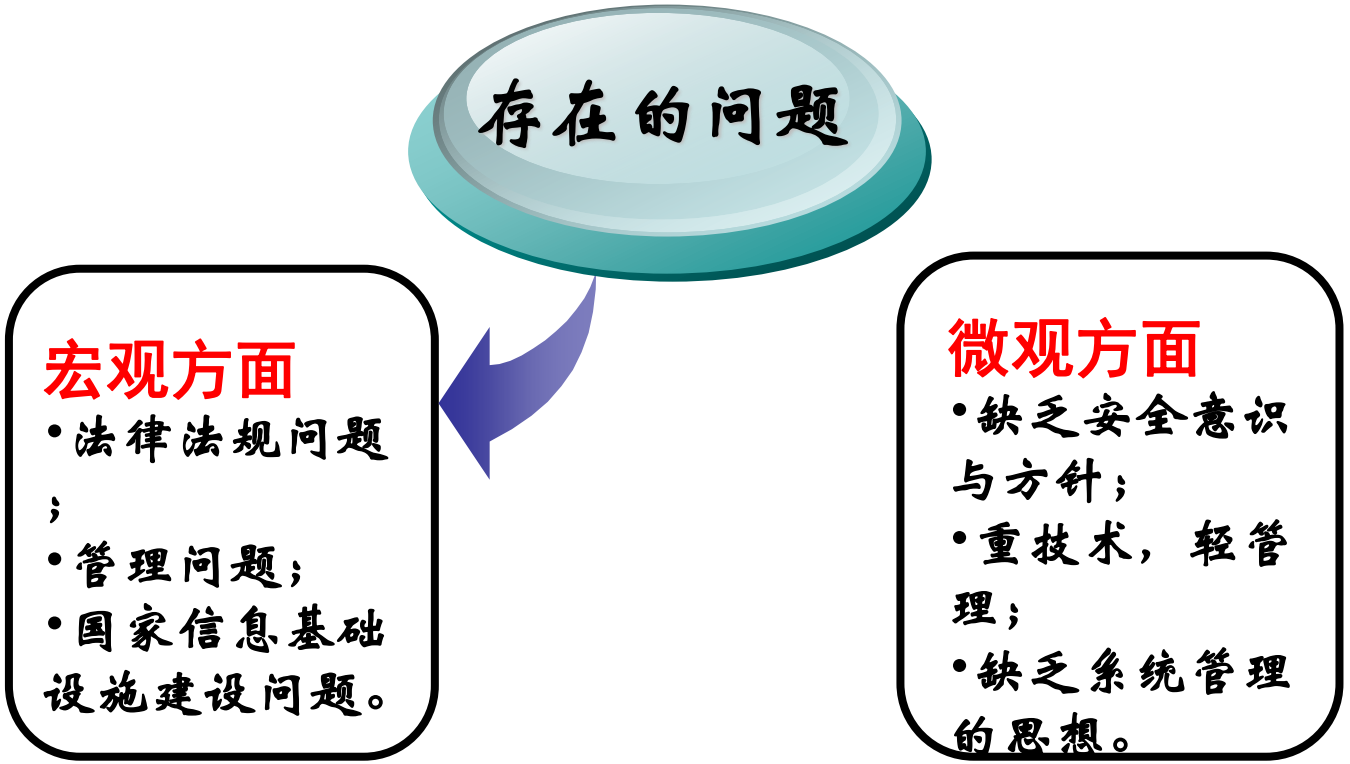
- 国际现状
  - 信息安全管理的大体发展阶段
    - “零星追加时期”(90年代中前期)
    - “标准化时期”(90年代中后期)
  - 制订信息安全发展战略和计划；
  - 加强信息安全立法，实现统一和规范管理；
  - 步入标准化与系统化管理时代。

1.4 信息安全管理的国内外现状



1.4 信息安全管理的国内外现状

- 国内现状



1.4 信息安全管理的国内外现状

- 存在的问题
  - 谁来管
    - 要求不明
      - 一把手工程 + IT 和应用服务两张皮
    - 多头参与，责任不清。
      - IT+人保+保密+内审稽核
  - 管什么
    - 传统明确的：保密
    - 上级抓得紧的：信息内容
    - 领导交办的：
    - 不得不办的：事件事故处理

1.4 信息安全管理的国内外现状

- 存在的问题
  - 怎么管
    - IT技术部门：
      - 上信息安全技术手段
    - 应用服务部门：
      - 上项目，快开通
    - 其它相关部门：
      - 无事不登三宝殿、有事登殿也无奈
    - 缺乏协调协同
  - 怎么才算管得好
    - 没凭据，无标准
      - 迫使标准出台

1.5 信息安全管理的相关标准

- 国际标准
  - 信息安全管理体系标准（BS7799）
  - IT基础设施库（ITIL）
  - 信息和相关技术控制目标（COBIT）
  - IT安全管理指南（ISO 13335）
  - 系统安全工程能力成熟度模型（SSE-CMM）

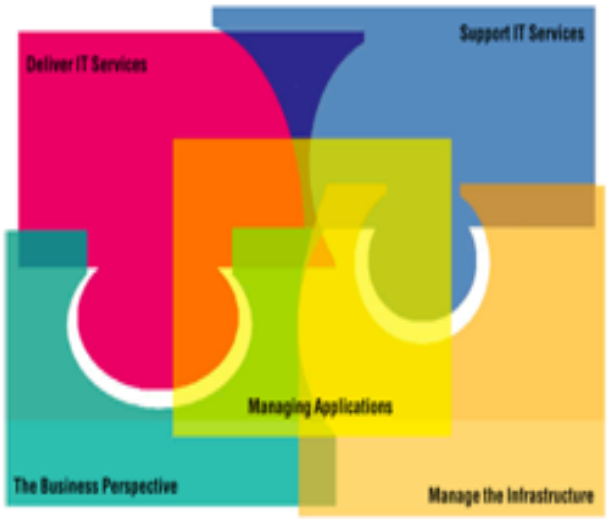
1.5 信息安全管理的相关标准

- 信息安全管理体系标准（BS7799）

最佳实践：控制目标及控制措施

1.5 信息安全管理的相关标准

- **IT基础设施库（ITIL）**



ITIL

Service Desk

Service Support

Service Delivery

最佳实践：
IT管理流程

1.5 信息安全管理的相关标准

- 信息和相关技术控制目标（COBIT）

C Control

ob objectives

i for information

T and related Technology

1.5 信息安全管理的相关标准

- 国内标准
  - GB17895-1999《计算机信息系统安全保护等级划分准则》；
  - 2001年制定了国家标准GB/T 18336《信息技术安全性评估准则》；
  - 2002年4月15日全国信息安全标准化技术委员会在北京正式成立；
  - 2002年7月公安部根据GB17895-1999制定了计算机信息系统安全等级保护技术要求系列标准。

1.5 信息安全管理的相关标准

- 国际执行监督机构：
  - 国际信息系统审计与控制协会 (ISACA)
    - COBIT-Control Objectives for Information and related Technology（直译为信息及相关技术的控制目标）
  - IT Governance Institute（1998）
  - 国际会计师联合会
  - 分布式管理任务组（DMTF ）
  - ……
- 国内执行监督机构：
  - 公安部
    - 1110工程
  - 金融标准化委员会
    - 银行和相关金融业信息安全管理规范
    - ……

1.5 信息安全管理的相关标准

- 关于管理标准的制定
  - 需要什么样的路线图
  - 什么样的结构更合理
  - 管理能力分级是否应该反映在标准之中
  - 对国际相应标准如何代表国家提出见解，表示态度
  - 管理标准中有那些代表国家利益的方面，对它们应该把握什么原则才能保护国家利益

1.5 信息安全管理的相关标准

- 关于管理标准的认证
  - BS 7799认证在国内已经有所开展
    - （截至到2004年2月24日，全球已经有563个组织获得了信息安全管理体系认证证书，其中包括我国的5家企业。）
    - 这些业务还都处在自发状态，我国还没有对应的制度对其进行有效的监督和规范。
  - 信息安全保障的管理认证依据BS7799是否足够？
    - 管理认证是否存在敏感性？
    - 我国应该如何开展信息安全管理认证，应该依据什么规范？
    - 如何避免认证工作的形式主义？
    - 如何避免发生过度的成本？

1.6 信息安全管理的趋势

- 着眼点越来越高
  - 国际
  - 国家
  - 企业
- 包括的范围越来越大
  - 时间：生命周期全过程
  - 空间：系统和网络
  - 手段：人和系统来执行行政和技术的安全策略
  - 目标：信息和内容安全
  - 目的：信息化应用服务的效率和效益

1.6 信息安全管理的趋势

- 管理思想越来越科学化
  - 没放弃追求最高境界：从保护提高到保障
  - 没要求绝对安全：风险分析，风险管理
  - 强调管理责任落实：角色和责任
  - 从IT管理发展到IT+应用服务管理：
  - 如 CoBIT和US Sarbanes-Oxley Act of 2002 的出现
  - 强调过程控制：落实到生命周期各个环节上

1.6 信息安全管理的趋势

- 定性定量结合：
  - “头脑风暴”
  - 信息收集
  - 信息分析
  - 科学决策
- 重视发展管理技术手段：
  - 信息获取工具
  - 信息交换手段
  - 信息分析工具
  - 测试评估工具
  - 实验演练平台

1.6 信息安全管理的趋势

- 人的因素第一
  - 重视队伍建设
  - 重视人员成长
    - 意识
    - 培训
    - 教育
  - 重视队伍的战斗力
- 向成熟度要管理能力：
  - 工程：**SSE-CMM**
  - 综合：**CMMI**
  - 评估：**INFOSEC-CMM**
  - 人员：**P-CMM**

1.6 信息安全管理的趋势

- 重视管理成本
  - 重视自评估：美国NIST SP 800-26
  - 重视先进经验的推广：Best Practice
  - 提出信息安全资金计划指南：NIST SP 800-65 《Integrating IT Security into the Capital Planning and Investment Control Process》（June 2004）
- 深化讨论在继续
  - P（计划），D（实施），C（检查），A（改进）（BS7799，ISO17799）
  - R（风险评估），P（规划），D（实施），C（检查），A（持续监控）（美国联邦IT系统认证认可指南）

1.7 信息安全政策

- 1.我国信息化发展战略与安全保障工作
- （1）信息化发展战略（P8）
  - 推进国民经济信息化
  - 推进电子政务
  - 建设先进网略文化
  - 推进社会信息化
  - 完善综合信息基础设施
  - 加强信息资源的开发利用
  - 提高信息产业竞争力
  - 建设国家信息安全保障体系
  - 提高国民信息技术应用能力，造就信息化人才队伍

1.7 信息安全政策

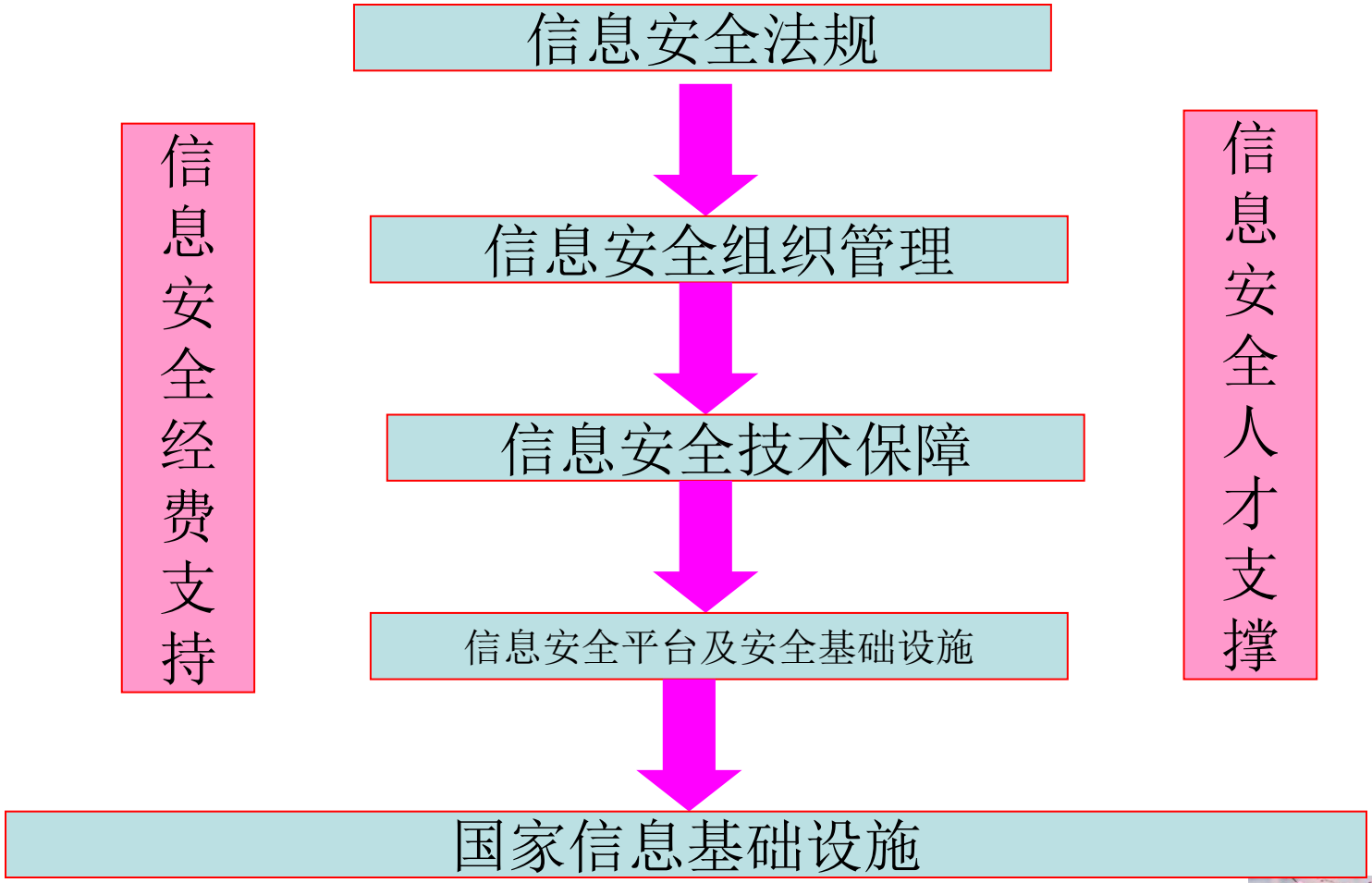
- （2）信息安全保障工作
  - 国务院《关于加强信息安全保障工作的意见》
    - 加强信息安全保障工作须遵循的原则：
    - 立足国情，以我为主，坚持管理和技术并重；
    - 正确处理安全与发展的关系，以安全保发展，从发展中求安全；
    - 统筹规划，突出重点，强化基础性工作；
    - 明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息安全保障体系。

1.7 信息安全政策

- 加强信息安全保障工作须遵循的原则：
  - 处理好发展与建设的关系
    - 正确处理发展与安全的关系
    - 坚持以改革开放求安全
    - 坚持管理与技术并重
    - 坚持统筹兼顾、重点突出

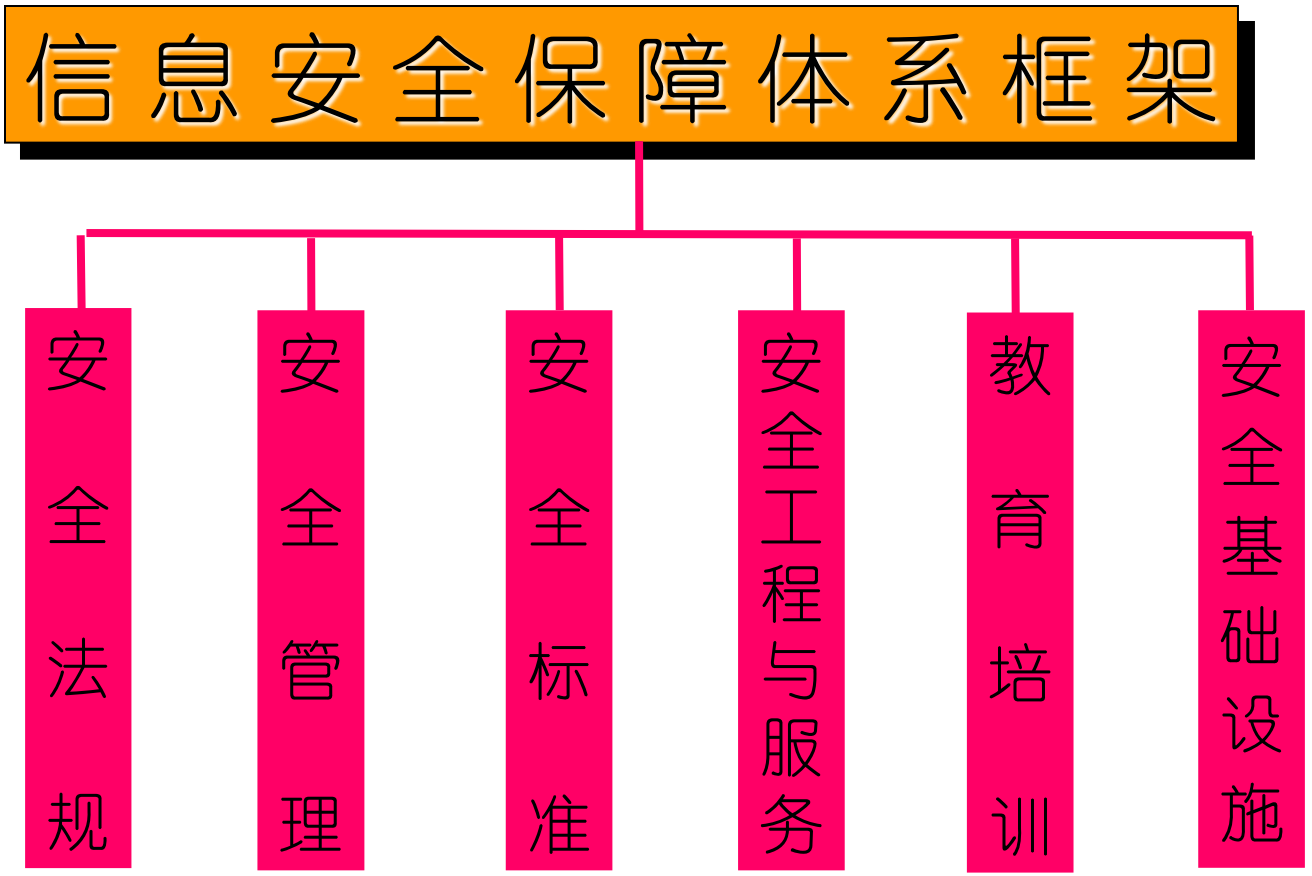
1.7 信息安全政策

- 国家信息安全体系框架



1.7 信息安全政策

- 国家信息安全保障体系框架



1.7 信息安全政策

- 2.美国信息安全国家战略简介：
  - 1998年5月美国政府颁发了《保护美国关键基础设施》总统令，围绕信息安全成立多个组织。
  - 1998年美国国家安全局制定了《信息保障技术框架》提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算机环境防御等深度防御在内的目标。
  - 2000年1月，发布了《保卫美国的计算机空间——保护信息系统的国家计划》，确定了计划的目标和范围。
  - 2003年2月公布《确保网络空间安全的国家战略》报告，强调发动社会力量参与保障网络安全，重视发挥高校和科研机构的力量。
  - 内容：三项总体战略目标和五项具体的优先目标。

1.7 信息安全政策

- 背景：
  - 美国是第一信息大国，对信息的依赖是其脆弱性的重要根源
    - 由大量信息系统组成的国家信息基础结构，已成为美国经济的命脉和国家的生命线，也成为容易受到攻击的高价值目标
  - 系统的安全漏洞、黑客的猖獗
    - 80年代以来，美国政府陆续发布若干制度，拥有最关键系统的政府部门被指定为第一批实施信息安全保护计划的要害部门，力图实现三个目标：准备和预防、侦查和反应、建立牢固的基础设施

1.7 信息安全政策

- 《确保网络空间安全的国家战略》作用与影响:
  - 1、确保网络安全已经被提升为美国国家安全战略的一个重要组成部分;
  - 2、是美国在9.11之后为确保网络安全而采取的一系列举措中的核心步骤;
  - 3、强调社会力量对网络安全进行全民防御，重视与企业和地方政府合作，重视发挥院校和科研机构力量，重视人才培养和公民安全意识教育。

1.7 信息安全政策

- 3.俄罗斯信息安全学说
  - 2000年6月《国家信息安全学说》第一次明确指出了俄罗斯在信息领域的利益、威胁是什么，以及保卫措施。
  - （1）背景
    - 科索沃战争、爱虫病毒的爆发是催化剂
  - （2）内容
    - A.保证信息安全是国家利益的要求
    - B.保证信息安全的方法
    - C.国家在保证信息安全时应采取的基本原则
    - D.信息安全的组织基础
    - 此外，信息安全学说还对信息威胁做了评估，论证了信息斗争的打击目标和打击手段。

1.7 信息安全政策

- 3.俄罗斯信息安全学说
  - （3）措施
    - A.成立国家信息安全与对抗的领导机构
      - （国家信息政策委员会）
    - B.建立信息对抗教育防范体系
    - C.建立信息斗争特种部队
    - D.发展信息斗争的关键技术和手段
    - E.改组指挥控制系统，增强战场生存能力

1.8 信息安全法律体系

- 1.信息安全法律体系
- （1）体系结构
  - a.法律体系 部门法
  - b.政策体系（拘束力、责任）
  - c.强制性技术标准（强制力）

1.8 信息安全法律体系

- 1.信息安全法律体系
  - （2）信息系统安全保护法律规范的法律地位
    - a.信息系统安全立法的必要性和紧迫性
    - b.信息系统安全保护法律规范的作用
      - 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
      - 指引作用
      - 评价作用
      - 预测作用
      - 教育作用
      - 强制作用
      - （预防作用）

1.8 信息安全法律体系

- 2.法律法规介绍
  - （1）刑法：主要罪名 新增加的罪名及含义
  - （2）治安管理处罚法：相关条文及含义
  - （3）计算机信息系统安全保护条例（计算机信息系统能够发生的案件，应在24小时内向人民政府公安机关报告）
  - （4）关于维护互联网安全的决定
  - （5）计算机信息网络国际互联网安全保护管理办法
  - （6）互联网安全保护技术措施规定
  - （7）网络安全法、数据安全法、个人信息法

1.8 信息安全法律体系

- 网络安全法
  - 2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过，2017年6月1日起施行。立法本意是要在我国领域内推广“安全可控”的产品和服务。产品的安全可控、数据的自主可控、用户的选择可控。
  - 网络安全定义
    - 指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。（侧重运行）
  - 要点：
    - 网络空间主权原则制度。
    - 网络安全等级保护制度。（等保2.0）
    - 实名认证制度。
    - 关键信息基础设施运营者采购网络产品、服务的安全审查制度。
    - 安全认证检测制度。
    - 重要数据强制本地存储制度。
    - 境外数据传输审查评估制度。
    - 个人信息保护制度。
    - 个人信息流通制度。
    - 网络通信管制制度。

1.8 信息安全法律体系

- 数据安全法
  - 2021年6月10日，十三届全国人大常委会第二十九次会议通过，2021年9月1日起施行。
  - 数据合规立法：“利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务”。
- 数据安全涉及各行业各领域，涉及多个部门的职责
- 数据安全法确立了我国数据安全监管体制，加强了对数据安全工作的组织领导。
  - 建立数据分级分类管理制度。
  - 建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。
  - 建立数据安全应急处置机制。
  - 与相关法律相衔接，确立数据安全审查制度和出口管制制度。
  - 针对他的歧视性等不合理措施，根据实际情况对等采取措施。

1.8 信息安全法律体系

- 个人信息保护法(隐私保护)
  - 2021年8月20日，经第十三届全国人大常委会第三十次会议审议通过，2021年11月1日起施行。
  - 构建数字时代个人信息和隐私保护的民法基础
- 明确“个人信息”定义
  - 个人信息是以电子或其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
  - 个人信息的处理包括收集、存储、使用、加工、传输、提供、公开、删除等。
- 个人信息处理的核心原则：告知-同意
- 个人信息处理的“三最”边界：
  - 对个人权益影响最小；收集范围最小；保存期限最短
- 严格保护敏感个人信息、禁止“大数据杀熟”
- 规范处理活动、信息的个人权利、处理者的义务

1.8 信息安全法律体系

- 移动APP法规
  - 移动APP危害：恶意扣费、流量恶意消费、隐私窃取、恶意传播、诱骗欺诈和流氓行为、超范围采集用户信息。
  - 2022年8月1日国家网信办发布《APP新规》
  - 2020年9月15日,国家计算机病毒中心发布违规App和SDK（软件开发工具包）名单：
    - MOMO陌陌(版本8.18.7)、今日头条(版本7.2.7)、京东金融 (版本: 5.2.32)、云闪付(版本: 6.2.6) 。
    - 《正中靶心》(版本1.0)、《高效办公软件》(版本2.0.0)、《宝石大消除》(版本2.4.2)、《聚看影视》(版本18.11.11.123)、《青青草视频在线》(版本5.4.9)、《星星苹果消消乐》(版本5.12.20)、《互动第一课堂》(版本2.4.4)、《开火车》(版本1.4)、《地域边境》(版本6.3.24)、《开心消消乐2016》(版本V1.0)。

1.9 信息安全就业

- 1. 信息安全职业前景
  - 经济、军事、政治越来越依赖信息技术；
  - 信息安全成为国家安全的重要砝码；
  - 政策推进，行业成长再上新台阶；
  - 人才缺口千万级。
- 2. 信息安全就业领域
  - 信息安全专业学生毕业后可在政府机关、国家安全部门、银行、金融、证券、通信领域从事各类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作。

1.9 信息安全就业

- **3. 信息安全职业发展方向**
  - 渗透测试
    - 验证企业网络的安全性
    - 指导企业进行安全防御
  - 安全产品研发
    - 安全工具与硬件研发
    - 安全系统产品研发
      - 涉及脚本、网络、内核、驱动、具体业务
  - 系统安全维护
    - 安全网络设计
    - 防御产品的部署与配置使用
    - 系统运维与安全保障
    - 灾难备份与恢复

1.9 信息安全就业

- **2. 信息安全职业发展方向**
  - 企业系统安全评估与等保评级
    - 安全风险分析
    - 安全等级保障与评级
  - 安全事件服务
    - 攻击追踪与取证
    - 合法取得攻击证据，提交法庭
    - 分析并还原攻击过程
    - 追踪黑客

1.9 信息安全就业

- **2. 信息安全职业发展方向**
  - 职业黑客(个人或政府)
    - 漏洞挖掘（白帽黑客）
      - 涉及代码、脚本、系统架构
    - 情报战场
      - 信息情报获取与传递
      - 信息咨询
    - 攻击出租（黑客）
      - 攻击工具研发
      - 攻击武器投递
      - 攻击具体实施

1.9 信息安全就业

- 4. 十大信息安全岗位
  - 首席信息安全官（CISO）
    - 企业整体与日常安全，IT战略和安全体系
  - 安全架构师（SAO）
    - 安全规划、基础架构、风险评估、边界控制
  - 安全主管
    - 安全政策、人员教育培训、安全审查
  - 安全经理（SEO）
    - 安全措施实施、安全工具、预算和人员
  - 安全工程师（SEE）
    - 安全解决方案(协议、漏洞、渗透、虚拟化、加密)

1.9 信息安全就业

- 4. 十大信息安全岗位
  - 应急响应人员
    - 威胁响应、漏洞监控、逆向工程、电子鉴定
  - 安全顾问
    - 安全标准、安全策略、安全系统、协议验证
  - 计算机鉴定专家
    - 法律证据鉴定、电子鉴定工具
  - 恶意软件分析师
    - 软件指纹、动态跟踪与分析
  - 安全专家
    - 安全需求、安全解决方案、事件管理

第一章 小结

- 信息保障的三大要素（人员、技术、管理）中，管理要素的作用和地位越来越得到重视;
- 信息安全管理的内涵;
- 三分技术,七分管理;
- 信息安全管理现状;
- 信息安全管理标准日渐完善。
- 政策与法律

第一章 作业

- **1.1** 什么是信息安全？其发展经历哪几个阶段？各关注什么？标志是什么？
- **1.2** 什么是信息安全管理？为什么要引入信息安全管理？
- **1.3** 叙述信息安全管理的内容。
- **1.4** 什么是信息保障，技术体系包括什么？
- **1.5** 结合信息安全如何理解 “三分技术,七分管理 ”？
- **1.6** 个人信息处理的核心原则和三最边界是什么？