信息安全概念与安全风险

前言

- 在数据通信的过程中，由于各种不安全因素将会导致信息泄密、信息不完整不可用等问题，因此在通信过程中必须要保证信息安全。
- 本章节描述了信息安全的基本概念以及如何保障信息安全，列举了信息安全风险和如何评估规避这些风险。

目标

- 学完本课程后，您将能够：
  - 描述信息安全的定义和特点
  - 描述不同安全模型的特点和区别
  - 区分不同的安全风险

目录

信息

- 信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。

---《ISO/IEC IT安全管理指南（GMITS）》

什么是信息?

- 书本信件
- 国家机密
- 电子邮件
- 雷达信号
- 交易数据
- 考试题目

信息安全

- 信息安全是指通过采用计算机软硬件技术 、网络技术、密钥技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，信息的机密性、完整性和可用性不被破坏。
- 假如信息资产遭到损害，将会影响：

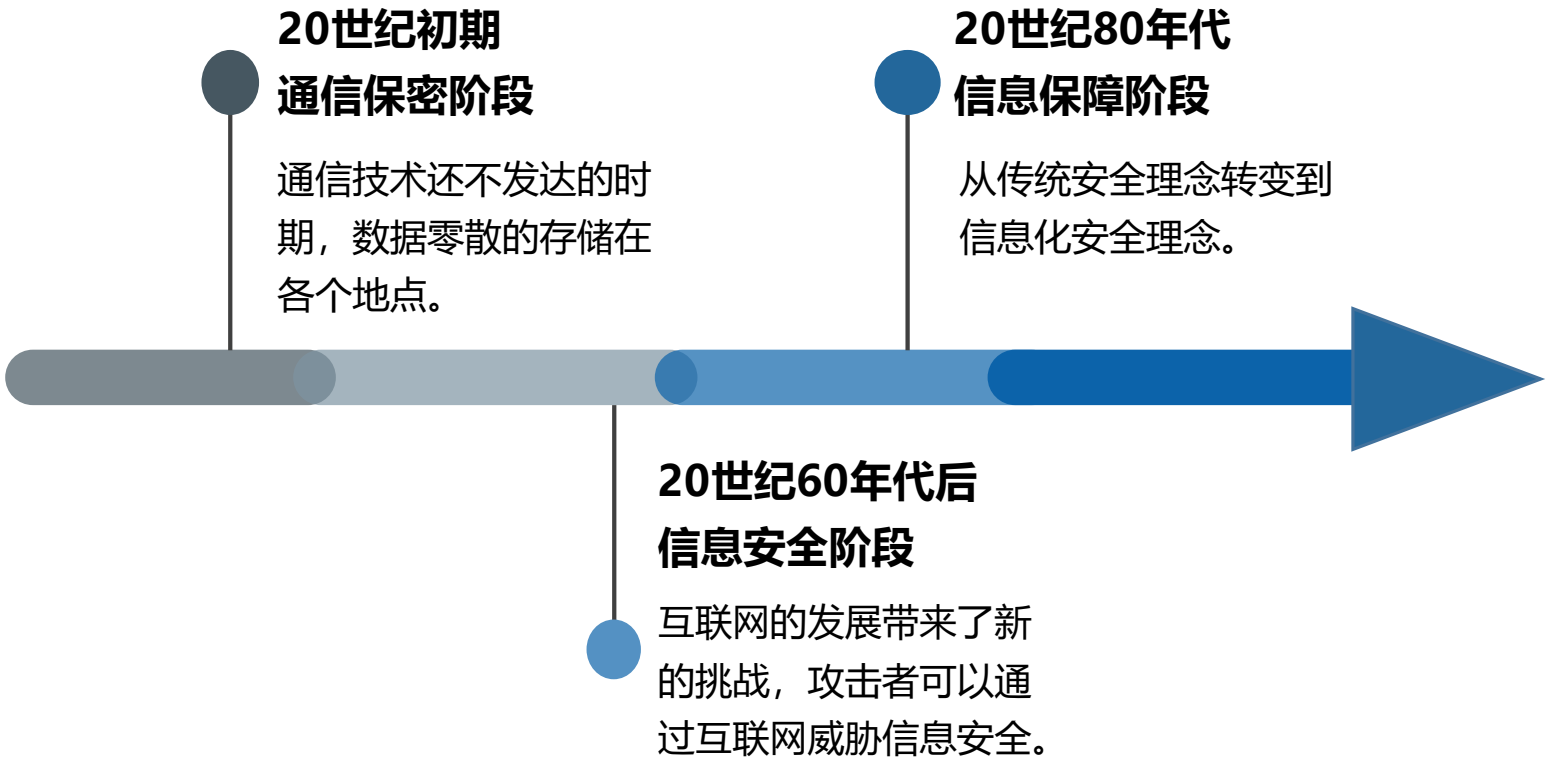
国家安全

组织系统正常运作和持续发展

个人隐私和财产

- 信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁。

信息安全发展历程



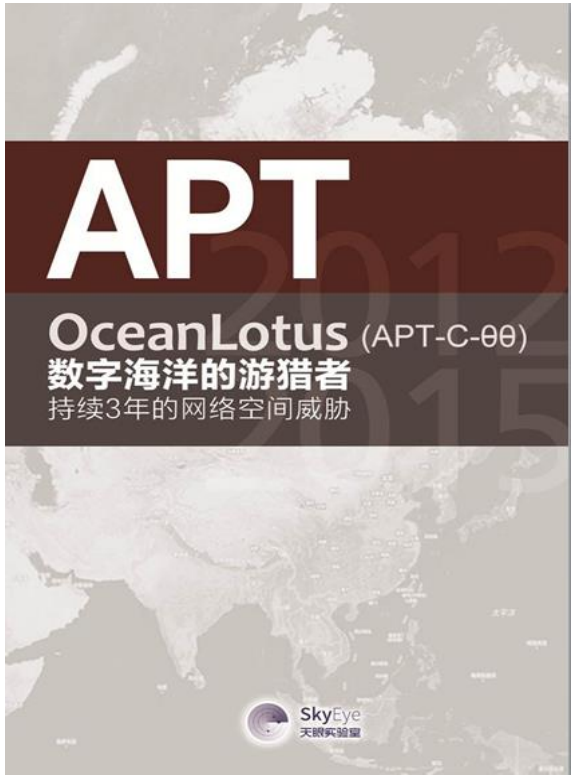
照片泄密案

- 中国最著名“照片泄密案”
  - 日本情报专家根据左图破解中国大庆油田的“秘密”，由照片上王进喜的衣着判断出油田位于北纬46度至48度的区域内；通过照片油田手柄的架式，推断出油井的直径；根据这些信息，迅速设计出适合大庆油田开采用的石油设备，在中国征求开采大庆油田的设备方案时，一举中标。

信息安全案例 - WannaCry

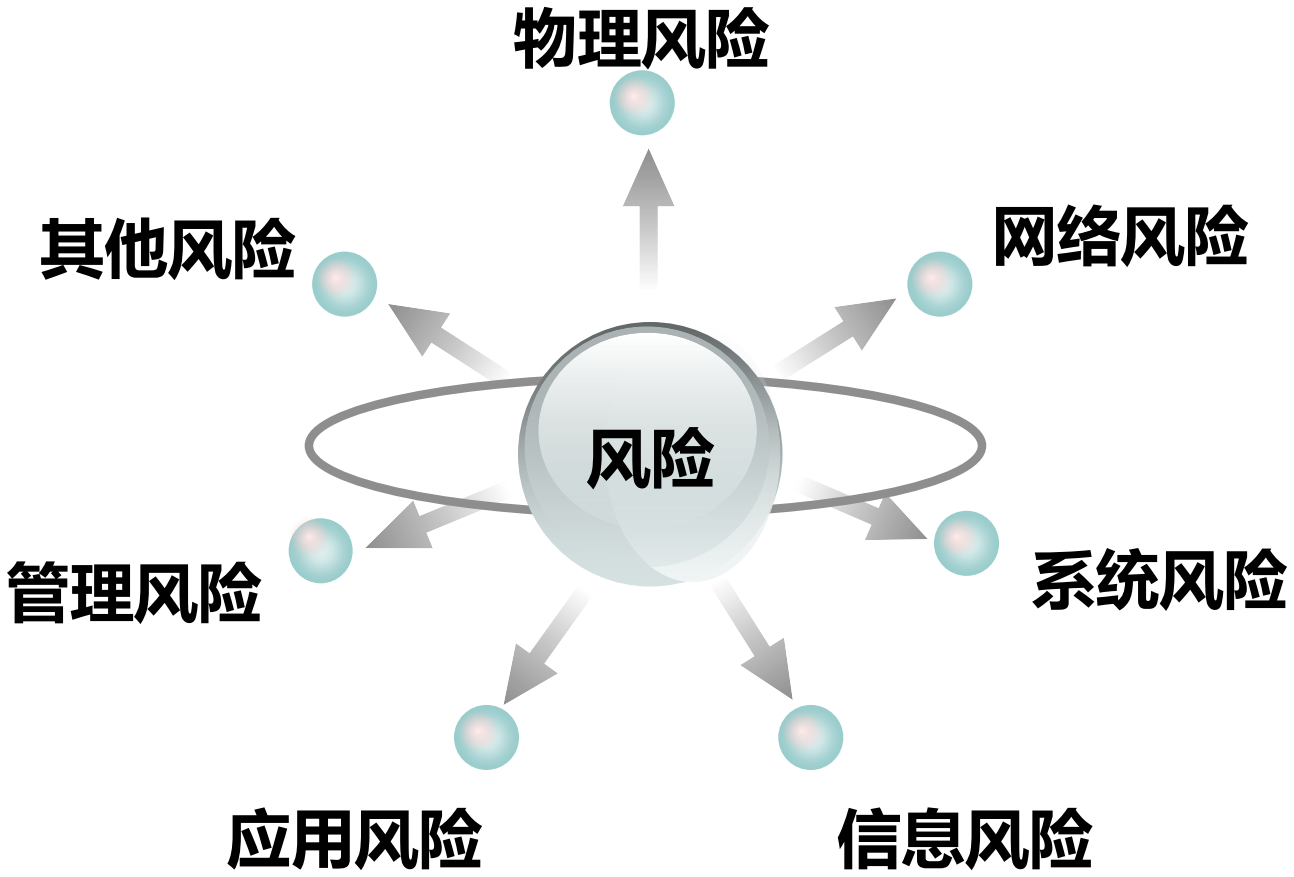
2017年不法分子利用的危险漏洞“EternalBlue”（永恒之蓝）开始传播一种勒索病毒软件**WannaCry**，超过**10万**台电脑遭到了勒索病毒攻击、感染，造成损失达**80亿**美元。

信息安全案例 - 海莲花组织



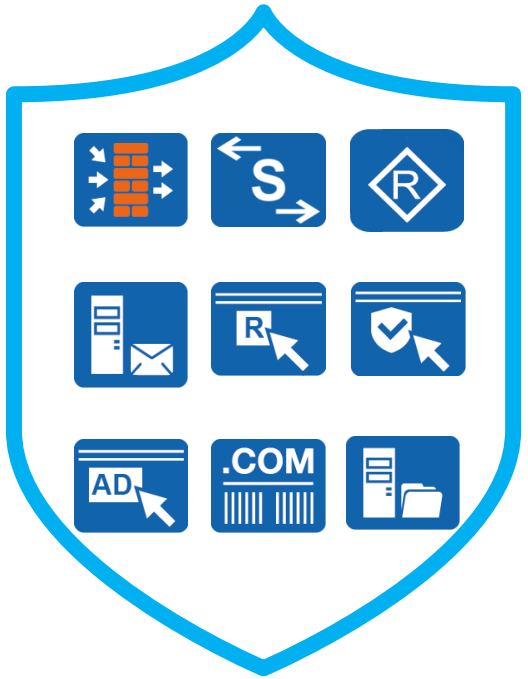
- 2012年4月起，某境外组织对政府、科研院所、海事机构、海运建设、航运企业等相关重要领域展开了有计划、有针对性的长期渗透和攻击，代号为OceanLotus(海莲花)。意图获取机密资料，截获受害电脑与外界传递的情报，甚至操纵终端自动发送相关情报。

信息安全涉及的风险



物理风险

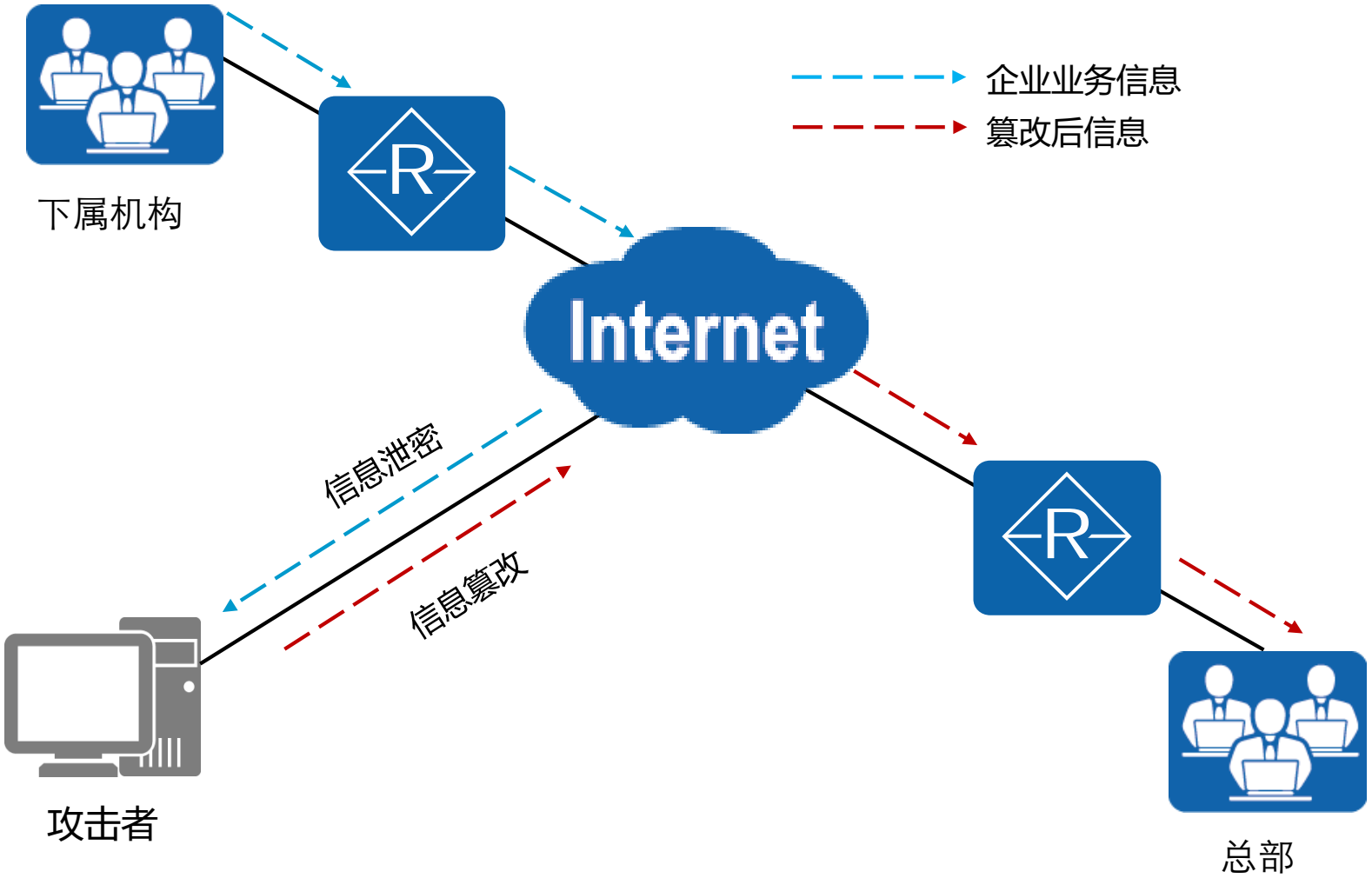
- 设备防盗，防毁
- 链路老化，人为破坏，被动物咬断等
- 网络设备自身故障
- 停电导致网络设备无法工作
- 机房电磁辐射



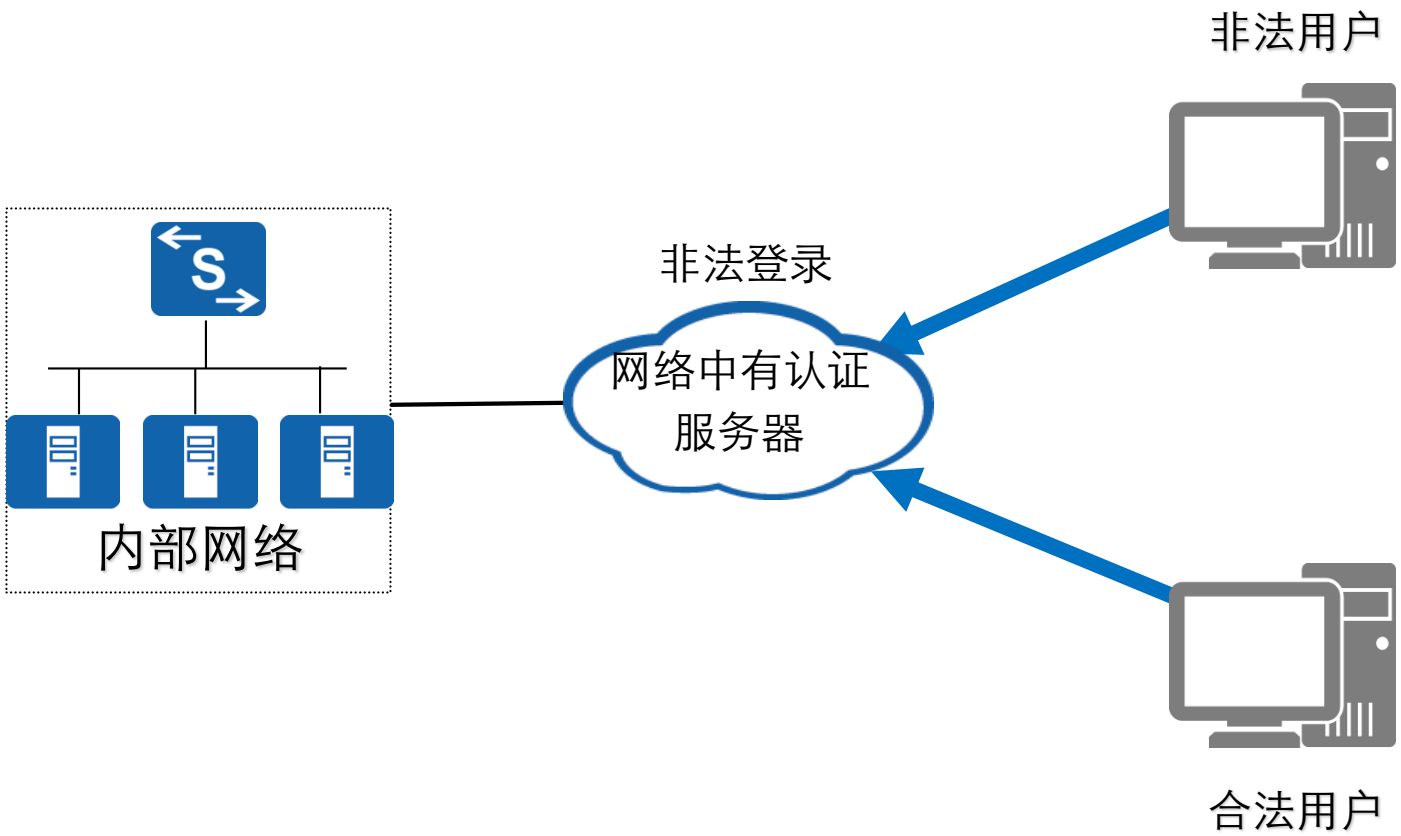
信息风险

- 信息存储安全
- 信息传输安全
- 信息访问安全

信息风险 - 信息传输安全



信息风险 - 信息访问安全



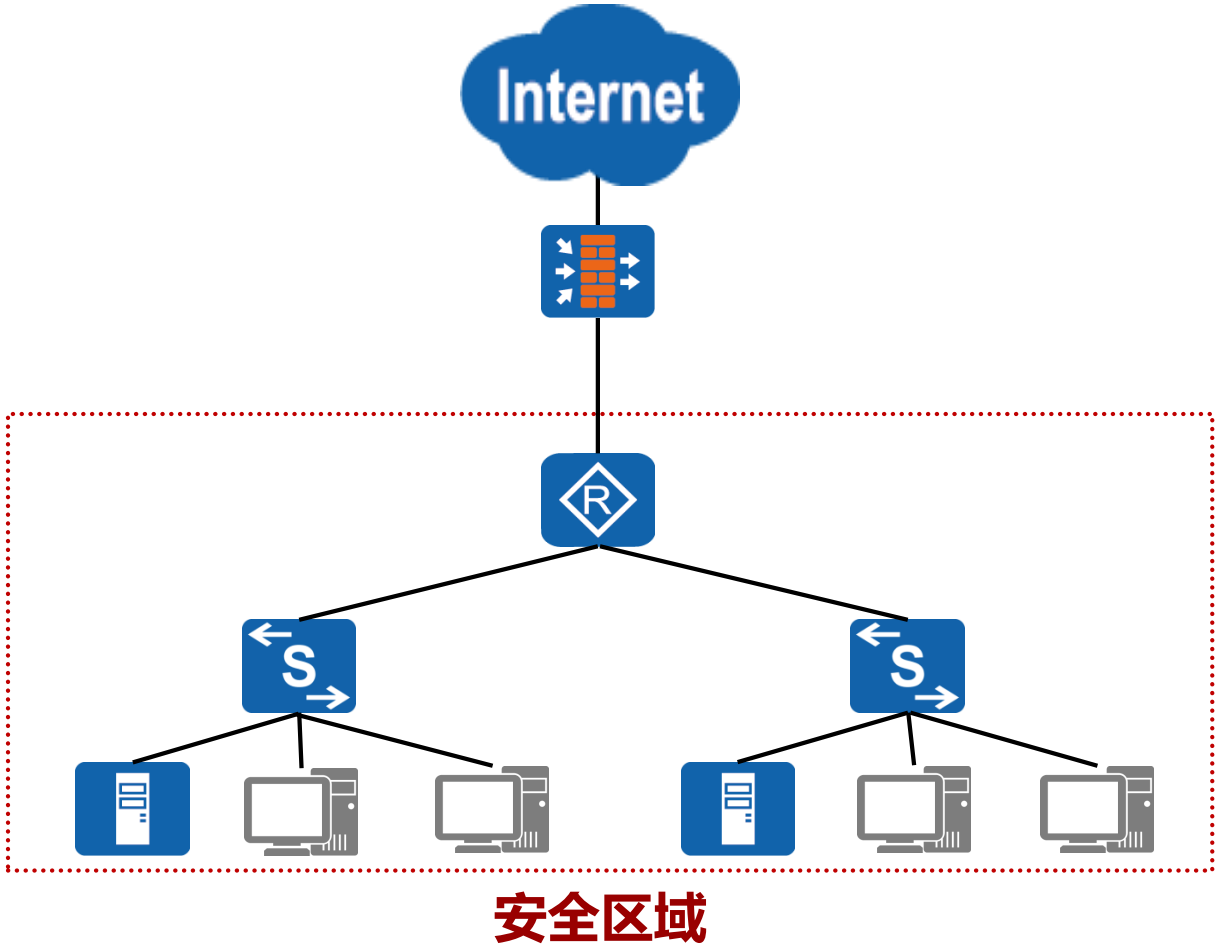
系统风险

- 数据库系统配置安全
- 安全数据库
- 系统中运行的服务安全

应用风险

- 网络病毒
- 操作系统安全
- 电子邮件应用安全
- WEB服务安全
- FTP服务安全
- DNS服务安全
- 业务应用软件安全

网络风险



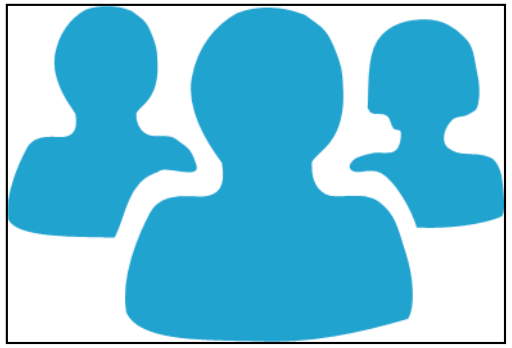
管理风险

- 据统计，企业信息收到损失的70%是由于内部员工的疏忽或有意泄密造成的。

- 安全技术知识信息安全控制的手段，要让安全技术发挥应有的作用，必然要有适当的管理程序的支持。

目录

讨论：造成此类攻击事件的原因是什么？

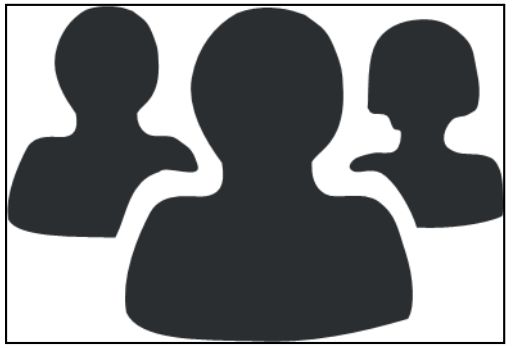


表面原因

- 病毒
- 漏洞
- 木马
- 后门程序
- DDOS攻击

…

VS



深层根源

- 信息系统复杂性
- 人为和环境

建设信息安全的意义

重要性

信息化越重要，信息安全越重要

- 信息网络成为经济繁荣、社会稳定和国家发展的基础。
- 信息化深刻影响着全球经济的整合国家战略的调整和安全观念的转变。
- 从单纯的技术性问题变成事关国家安全的全球性问题。

适用性

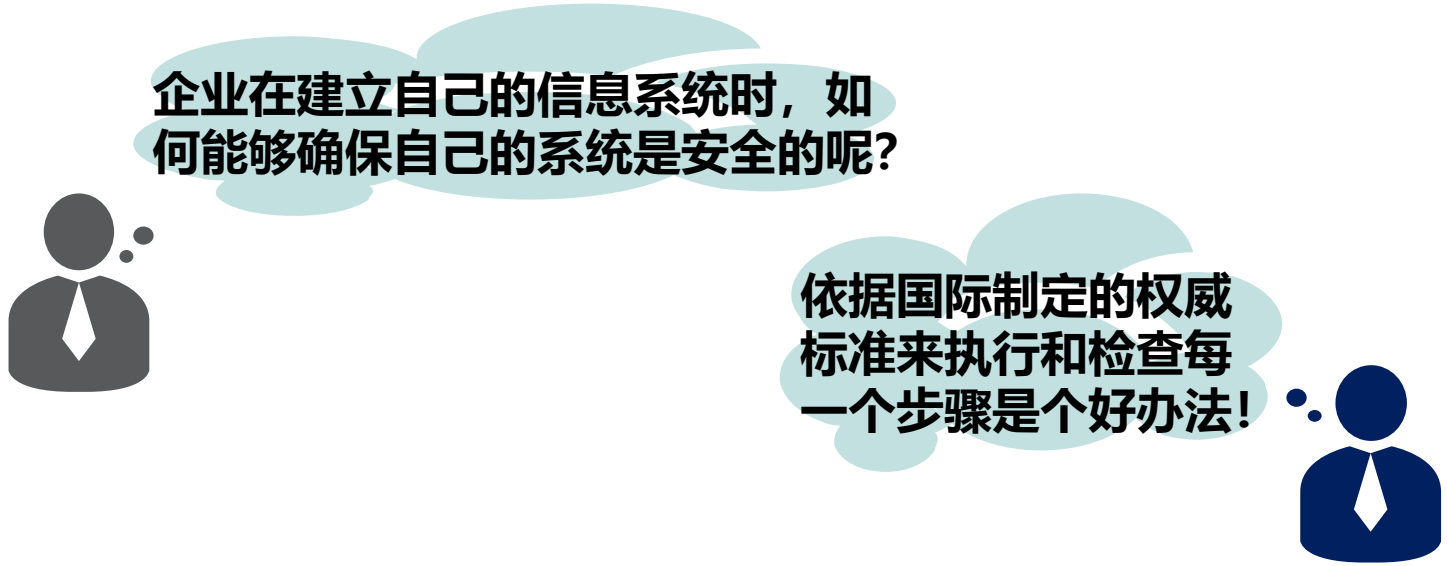
信息安全适用于众多技术领域

例如：

- 军事计算机通讯指挥控制和情报(C4I)系统；
- 电子商务系统；
- 生物医学系统；
- 智能运输系统(ITS)等。

信息安全标准的意义

- 标准是规范性文件之一。其定义是为了在一定的范围内获得最佳秩序，经协商一致制定并由公认机构批准，共同使用的和重复使用的一种规范性文件。



信息安全标准组织

- 在国际上，与信息安全标准化有关的组织主要有以下2个：
  - International Organization for Standardization (ISO) 国际标准化组织
  - International Electrotechnical Commission (IEC)国际电工委员会
- 国内的安全标准组织主要有：
  - 信息技术安全标准化技术委员会(CITS)
  - 中国通信标准化协会(CCSA)下辖的网络与信息安全技术工作委员会
- 其它一些制定标准的组织：
  - International Telecommunication Union (ITU)国际电信联盟
  - The Internet Engineering Task Force (IETF)Internet工程任务组

常见信息安全标准与规范

等级保护定义

信息安全等级保护:对信息和信息载体**按照重要性等级分级别进行保护**的一种工作。

是国家政策要求

中办发[2003]27号文:
加强信息安全保障工作的意见

主要内容:

- 实行信息安全等级保护政策
- 重视信息安全风险评估工作
- 建设和完善信息安全监控体系
- 保证信息安全资金
- 健全信息安全管理责任制

由公安监督检查

公通字[2004]66号:
关于印发《关于信息安全等级保护工作的实施意见》的通知

- 公安机关负责信息安全等级保护工作的监督、检查、指导
- 国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导
- 国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。

各机关和行业执行

（一）电信、广电行业的公用通信网、广播电视传输网等基础信息网络、经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统
（二）铁路、银行、海关、税务、银行、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源能源、交通、文化、教育、统计、工商行政管理、邮政行业部门的生产、调度、管理、办公等重要信息系统。

等级保护的意义

1、提高保障水平、优化资源分配

■提高整体保障水平：

能有效的提高信息安全保障工作的整体水平，有效解决信息系统面临的威胁和存在的主要问题

■优化安全资源分配：

将有限的财力、物力、人力投入到重点地方，发挥最大的安全经济效益

2、合法、合规

第三章 网络运行安全
第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月

（四）采取数据分类、重要数据备份和加密等措施

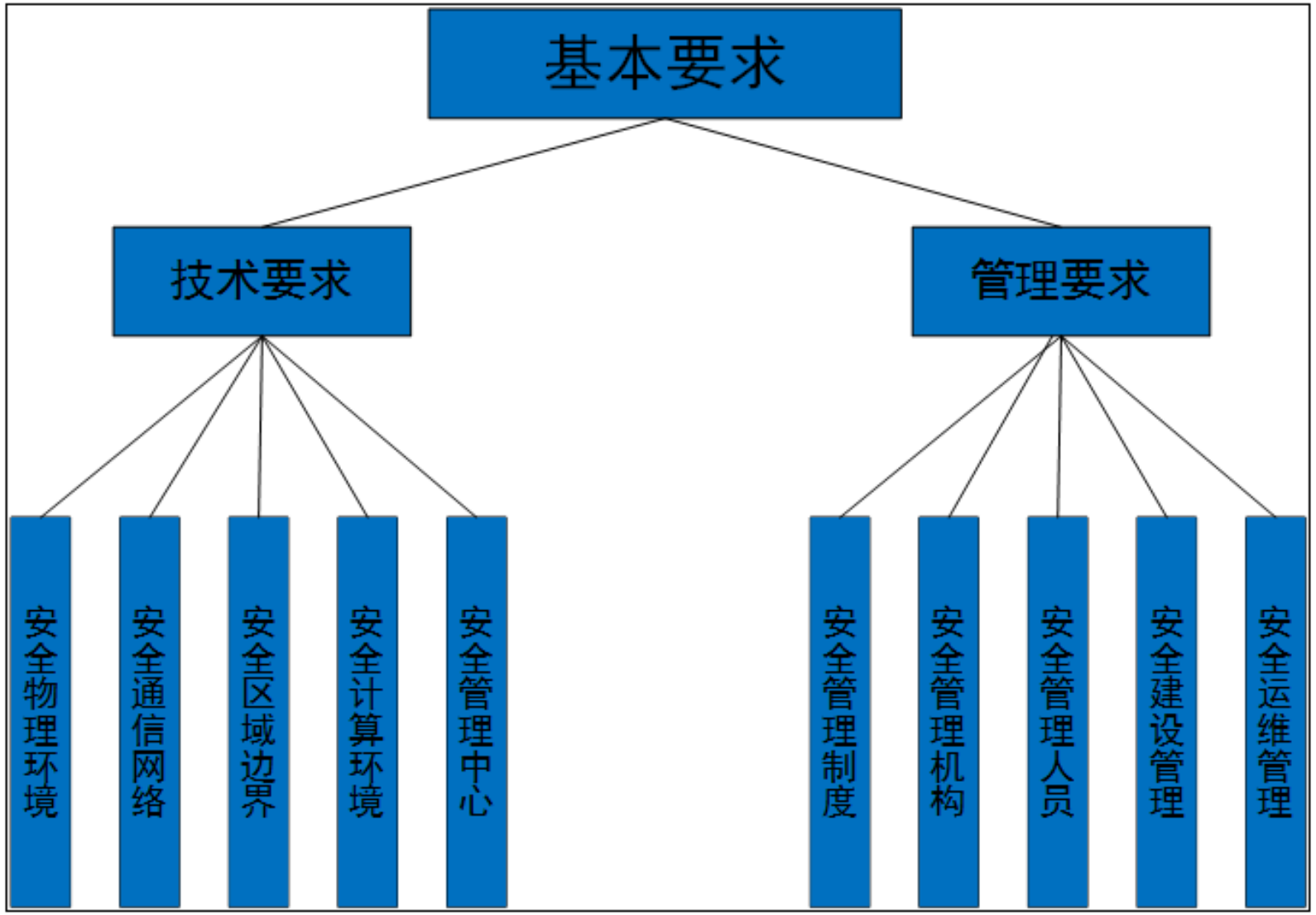
（五）法律、行政法规规定的其他义务

等级保护系统定级

- 主要依据：根据系统被破坏后，对公民、社会、国家造成的损害程度定级。

保护等级	公民、法人的合法权益	社会秩序和公共利益	国家安全
第一级	损害	否	否
第二级	严重损害	损害	否
第三级	/	严重损害	损害
第四级	/	严重损害	严重损害
第五级	/	/	严重损害

等级保护基本要求



等级保护流程

本章总结

- 描述信息安全的概念与安全风险
- 描述常见信息安全标准
- 描述信息安全标准的意义


谢 谢
www.huawei.com