



**NSFocus Information Technology Co. Ltd.**

**CIO如何构建企业信息安全防护体系?**

---

厦门企业信息化和CIO实战研讨会

绿盟科技 何钦淋

2007年5月



# 企业信息安全风险现状

---

谁是我们的威胁者

# 失落的安全



- 没有专门的安全建设标准和规范
- 公司老总只关注信息化应用
- 缺乏足够的人员和技术
- 。 。 。



# 不可忽视的网络安全损失



## 业务系统安全的挑战

接受调查的美国企业在2004年因为网络犯罪而导致的成本:

**2.01亿美元**

因为专利信息失窃而导致的成本:

**7000万美元**

因为网络中断而导致的成本和因为病毒而遭受的损失:

**2700万美元**

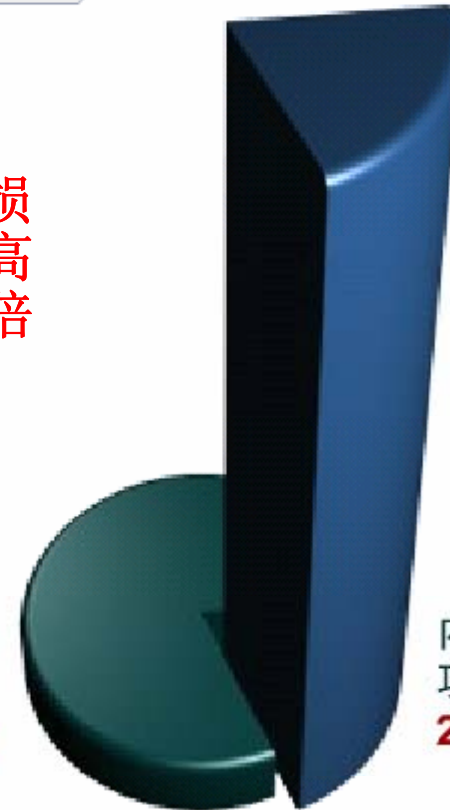
报告曾发生内部员工滥用网络行为的企业比例:

**80%**

每次损失却高达10倍

外部攻击  
78%

内部攻击  
22%



美国的安全攻击

# 任何组织都可能受到遭受攻击

网易 > 新闻中心 > 社会新闻 > 深圳“黑客”偷了北京移动370万

## 深圳“黑客”偷了北京移动370万

2006-02-24 00:36:43 来源: 南方报业网(广州) 收藏此页 网友评论

自称为了挑战中国移动价值1.2亿元的安全系统

COMPUTER

Home News Services Subscribe Events in Depth  
Management Careers Security Hardware Software Data Mgmt Networking Government Mobile

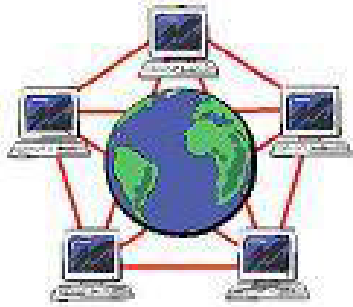
Home > Browse Topics > Security > Cybercrime

### FBI investigating Cisco source code leak

Two sample source code files were posted on a Russian

News Story by Paul Roberts





是P2P软件泄漏了军事机密



某游戏公司的玩家数据失窃案



又是外来笔记本……

## 更多现实存在的问题……

- 蠕虫爆发导致ERP系统瘫痪
- 收到大量的垃圾与反动邮件
- 修改自己的IP或者MAC导致网络冲突
- 重要终端上被种植了木马
- 大量的P2P下载流量占用网络出口带宽
- 新型病毒破坏应用软件
- 升级杀毒软件或系统补丁导致系统崩溃
- 公司的硬件被恶意替换或者拆卸
- 违规使用U盘拷贝机密文件
- 拨号外联或者跨接内外网络
- 非法使用的AP
- ……

**机密资料外泄**  
**企业内部网络中断**  
**直接经济损失**  
**声誉受损**  
……

**CIO还是CSO?**

# 谁会威胁我们的企业网络安全?



- 爱炫耀的黑客
- 敌对破坏势力
- 竞争对手
- 恶意客户



- 缺乏安全意识的员工
- 违反内部规定的员工
- 误操作
- 不满的雇员



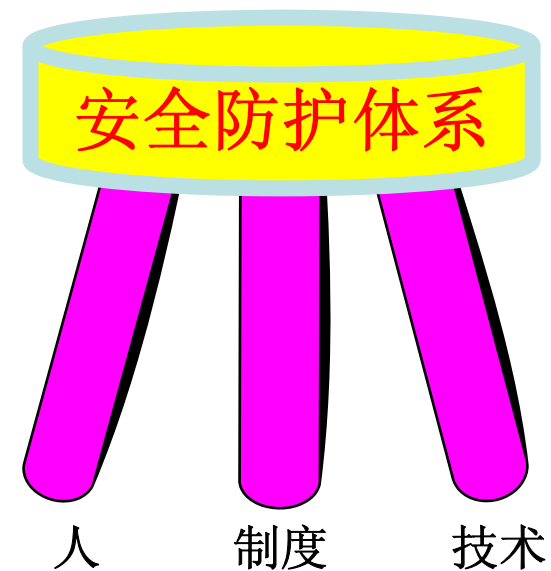


# 构建企业信息安全防护体系

---

## 安全防护体系的主要构成因素

- 人
- 制度
- 技术





## 人是安防体系中的最薄弱环节

- ❑ 对安全防护工作重视的领导是安防工作顺利推进的主要动力；
- ❑ 有强烈安全防护意识的员工是企业安防体系得以切实落实的基础；
- ❑ 杜绝内部员工攻击网络系统是加强安全防护的一项重要工作。

## 加强安全教育、提高网络安全意识

- 启蒙——为安全培训工作打基础，端正对单位的态度，让他们充分认识到安防工作的重要意义及在不重视安防工作的危险后果。
- 培训——传授安全技巧，使其更好的完成自己的工作。
- 教育——目标是培养IT安防专业人才，重点在于拓展应付处理复杂多变的攻击活动的能力和远见。



## 安防制度的定义和作用

安防制度是这样一份或一套文档，它从整体上规划出在单位内部实施的各项安防控制措施。

安防制度的作用主要有：

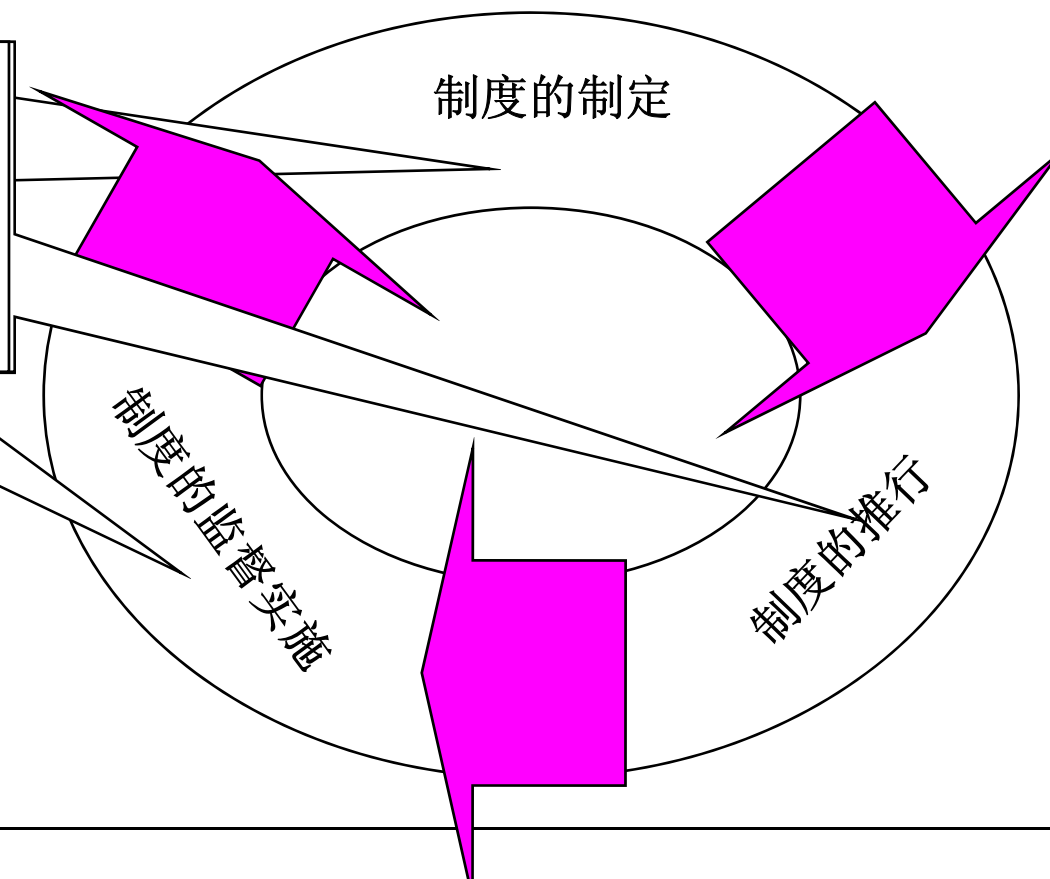
- ❑ 减轻或消除员工和第三方的法律责任
- ❑ 对保密信息和无形资产加以保护
- ❑ 防止浪费单位的计算机资源

# 制度：安防体系的基础

## 安防制度的生命周期

安防制度的生命周期包括制度的制定、推行和监督实施。

第三阶段：规章制度的监督实施。制度的监督实施应常抓不懈、反复进行，保证制度能够跟上单位的发展和变化



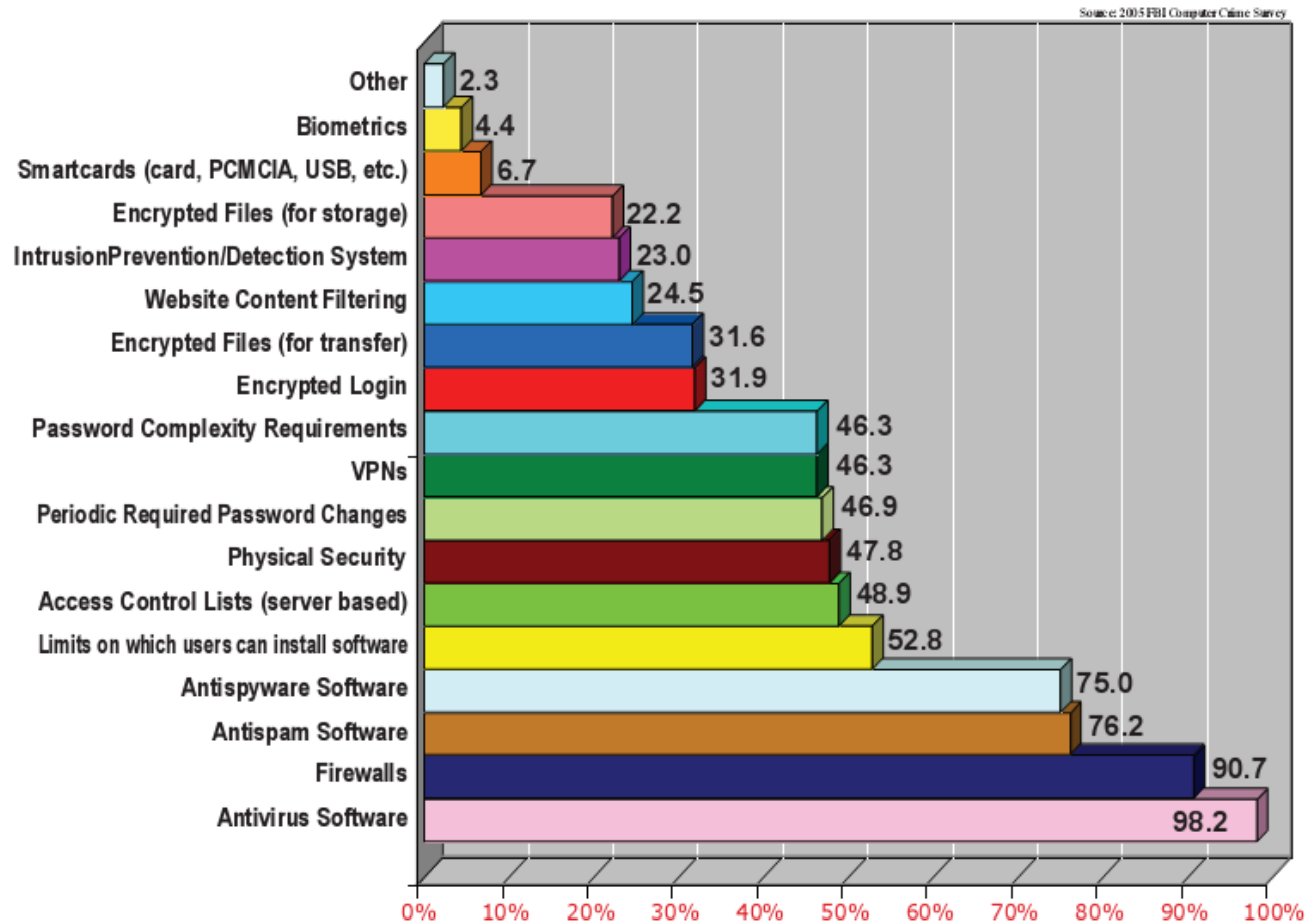
## 安防制度的主要组成部分

- ❑ 计算机上机管理制度
- ❑ 用户账户管理制度
- ❑ 远程访问管理制度
- ❑ 信息保护管理制度
- ❑ 防火墙管理制度
- ❑ 特殊访问权限管理制度
- ❑ 网络连接设备管理制度
- ❑ 商业伙伴接入管理制度

# 技术：安防体系的基本保证



## 网络安防需要先进的信息安全技术



但并非都适合你现在的需求……

## 网络安全需要采用多层防护策略

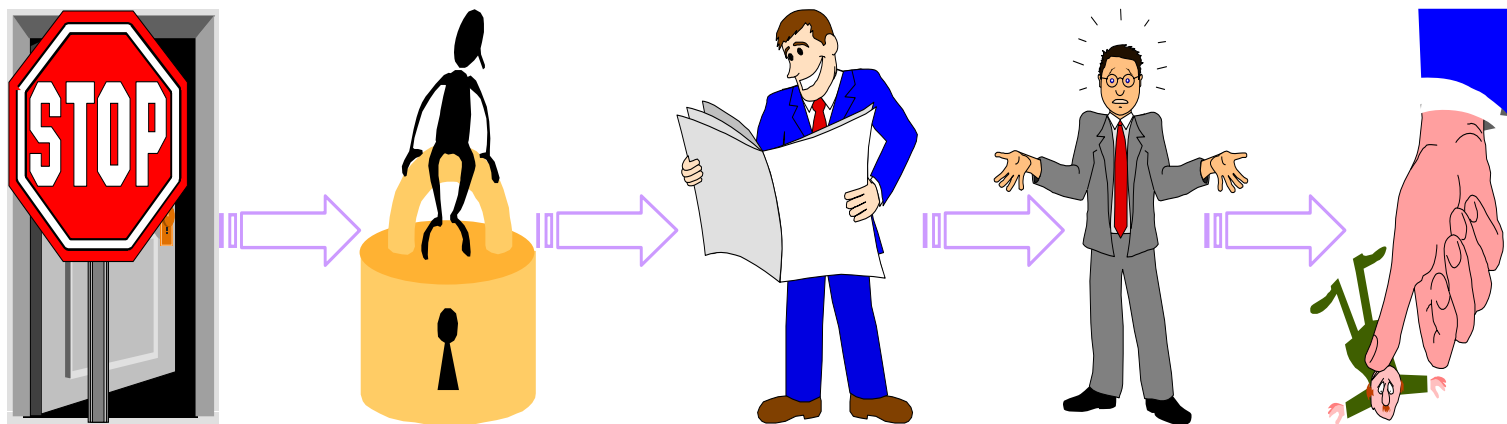
- ❑ 单一的安全保护往往效果不理想
- ❑ 目前的趋势——应用和实施一个基于多层次安全系统的全面信息安全策略
  - ✓ 在各个层次上部署相关的网络安全产品
  - ✓ 分层的安全防护成倍地增加了黑客攻击的成本和难度
  - ✓ 从而卓有成效地降低被攻击的危险，达到安全防护的目标。



# 网络安全工作的目的

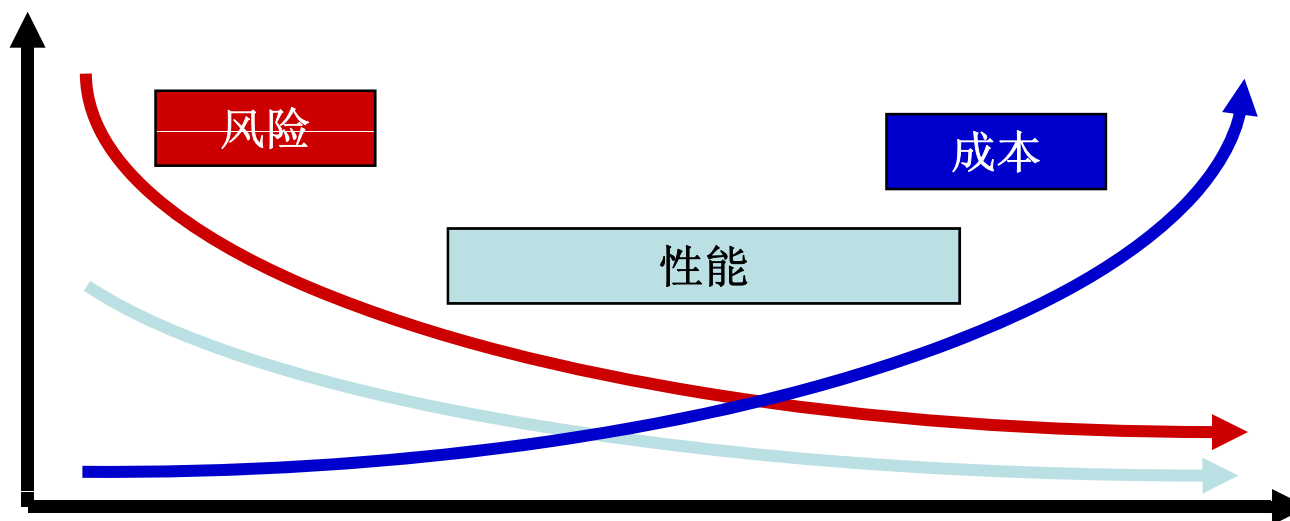


进不来      拿不走      看不懂      改不了      跑不了



## 没有100%安全的网络

- ❑ 安全建设是风险、性能和成本之间的折衷
- ❑ 安全建设的成本应该小于系统受损后可能造成的损失



## 没有一蹴而就的安全防护系统

- ❑ 安全建设必须统一规划，分步进行，不同时期侧重不同的安全内容，先解决燃眉之急。
- ❑ 安全产品只是安全体系的一个部分，完善的安防体系应是技术和管理的结合。安全管理需要常抓不懈。
- ❑ 对员工的安全教育必须持之以恒。

# 网络安全建设是一个过程

---

## 没有一成不变的安全防护系统

- ❑ 网络安全防护系统是个动态的系统，攻防技术都在不断发展。安防系统必须同时发展与更新。
- ❑ 定期的风险评估是保证系统安全的有效手段。
- ❑ 系统的安全防护人员必须密切追踪最新出现的不安全因素和最新的安防理念，以便对现有的安防系统及时提出改进意见。
- ❑ 网络安全建设是一个循序渐进不断完善的过程。

## 安防工作是一个周而复始、循环上升的过程

- ❑ 100%安全的网络是不存在的；
- ❑ 安防系统需要不断的变化和调整；
- ❑ 安防工作是循序渐进、不断完善的过程。





# 绿盟科技 - 巨人背后的专家

---

谢谢!