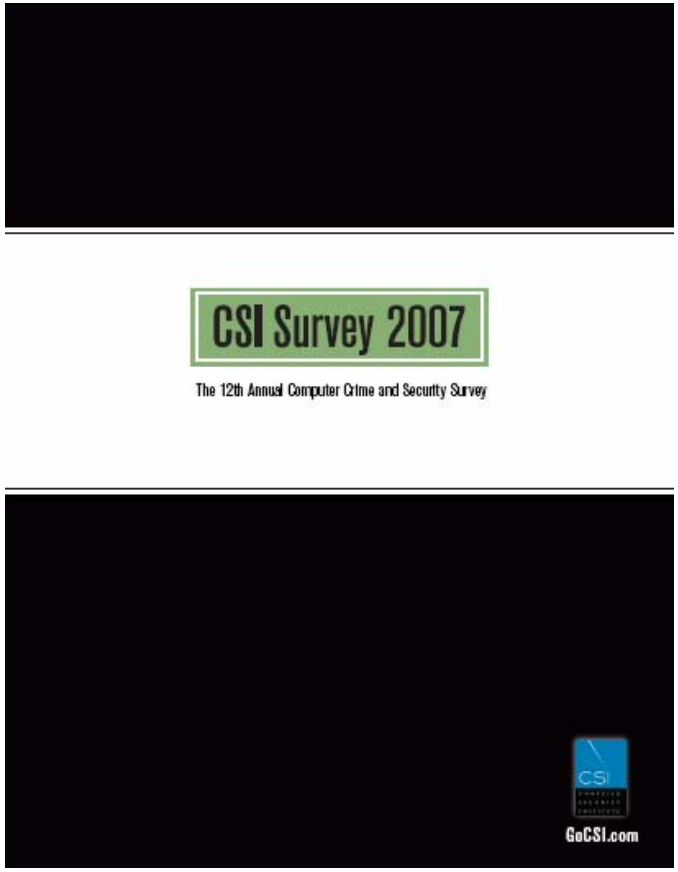
主要内容

- 信息安全基本概念
- 信息安全的现状
- 什么是信息安全工程

CSI/FBI 2007 计算机犯罪和安全调查



样本的行业分布

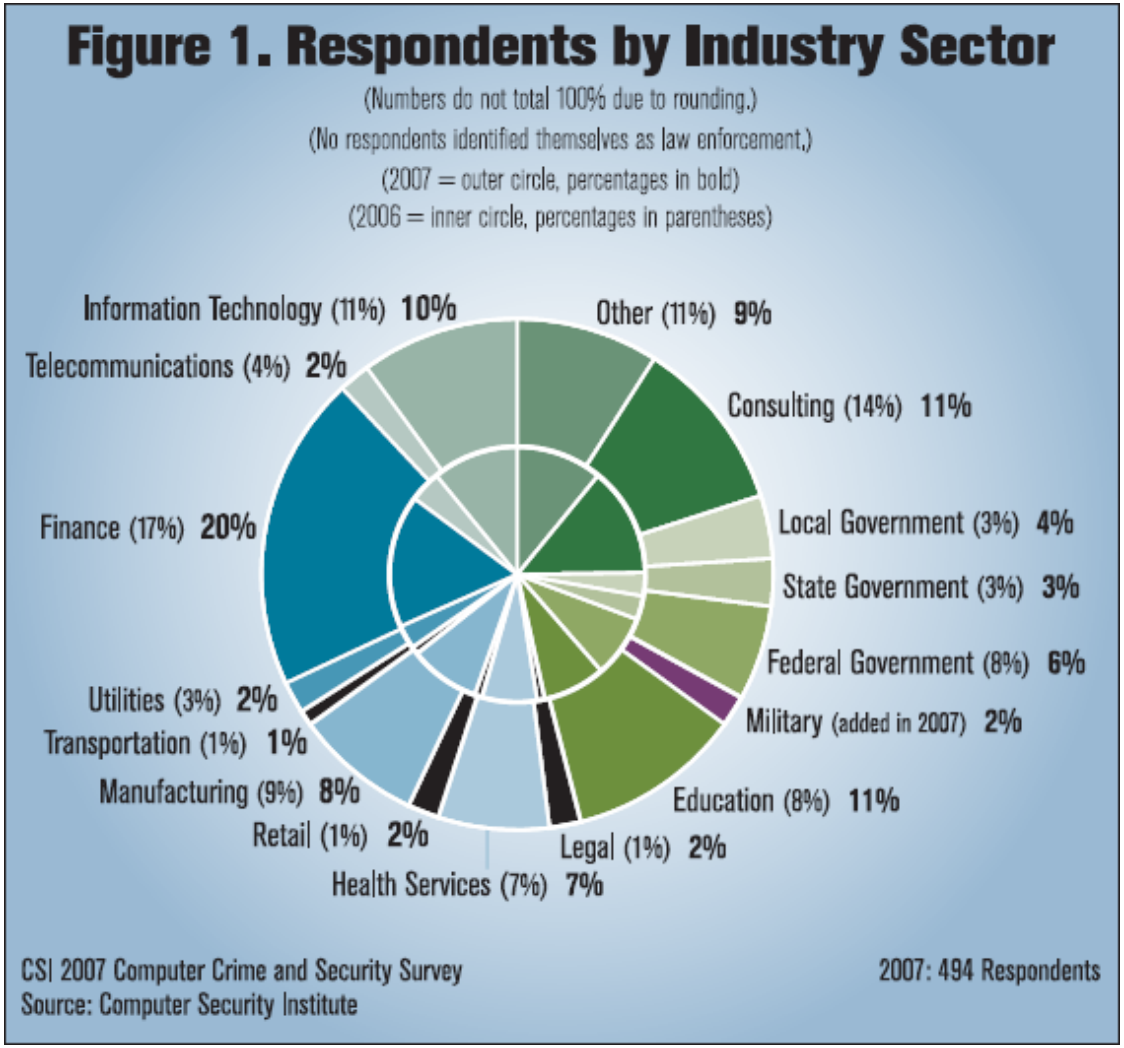


Figure 1. Respondents by Industry Sector
(Numbers do not total 100% due to rounding.)
(No respondents identified themselves as law enforcement.)
(2007 = outer circle, percentages in bold)
(2006 = inner circle, percentages in parentheses)
Information Technology (11%) 10%
Other (11%) 9%
Telecommunications (4%) 2%
Consulting (14%) 11%
Finance (17%) 20%
Local Government (3%) 4%
State Government (3%) 3%
Federal Government (8%) 6%
Utilities (3%) 2%
Military (added in 2007) 2%
Transportation (1%) 1%
Manufacturing (9%) 8%
Education (8%) 11%
Retail (1%) 2%
Legal (1%) 2%
Health Services (7%) 7%
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 494 Respondents

样本机构人数

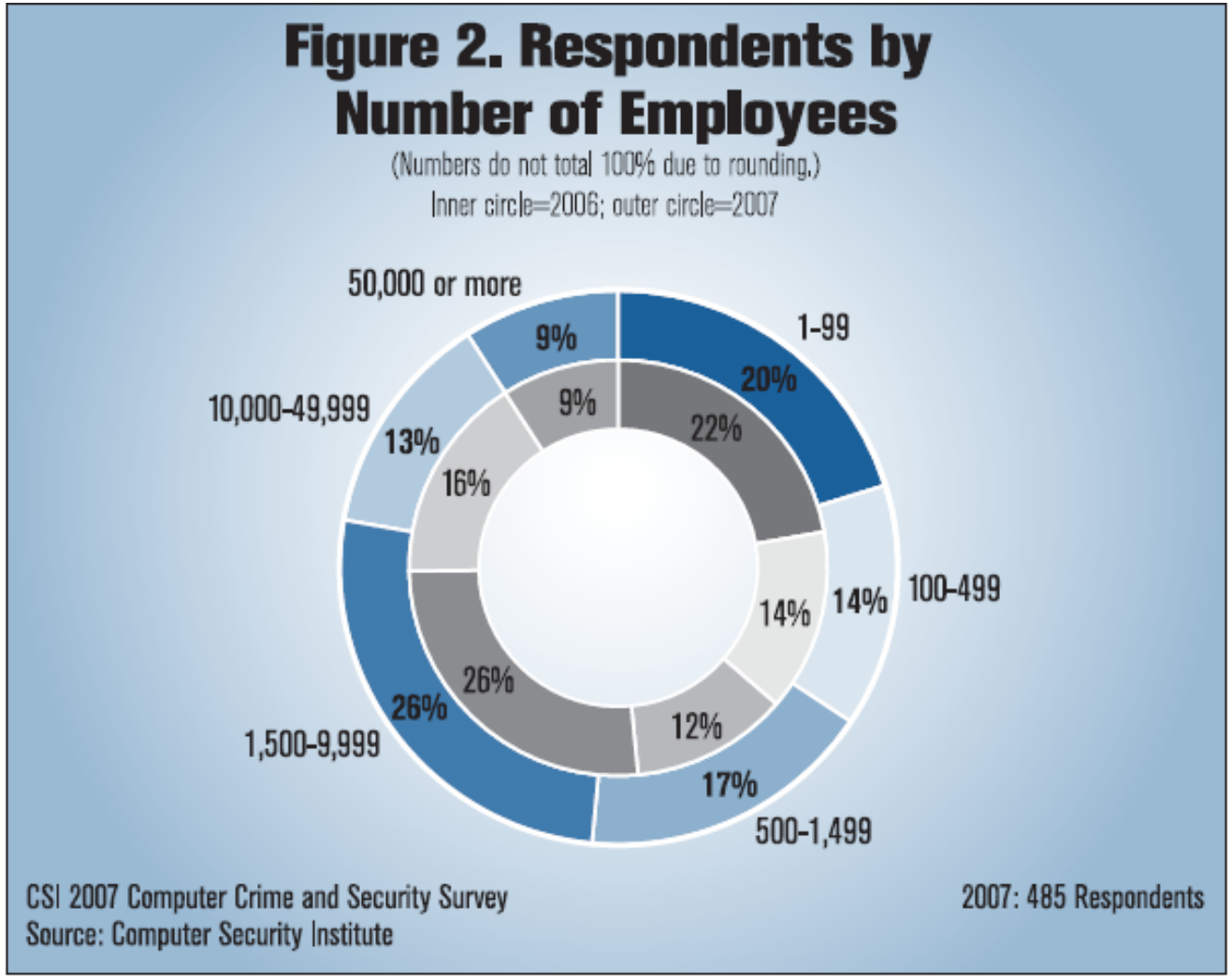
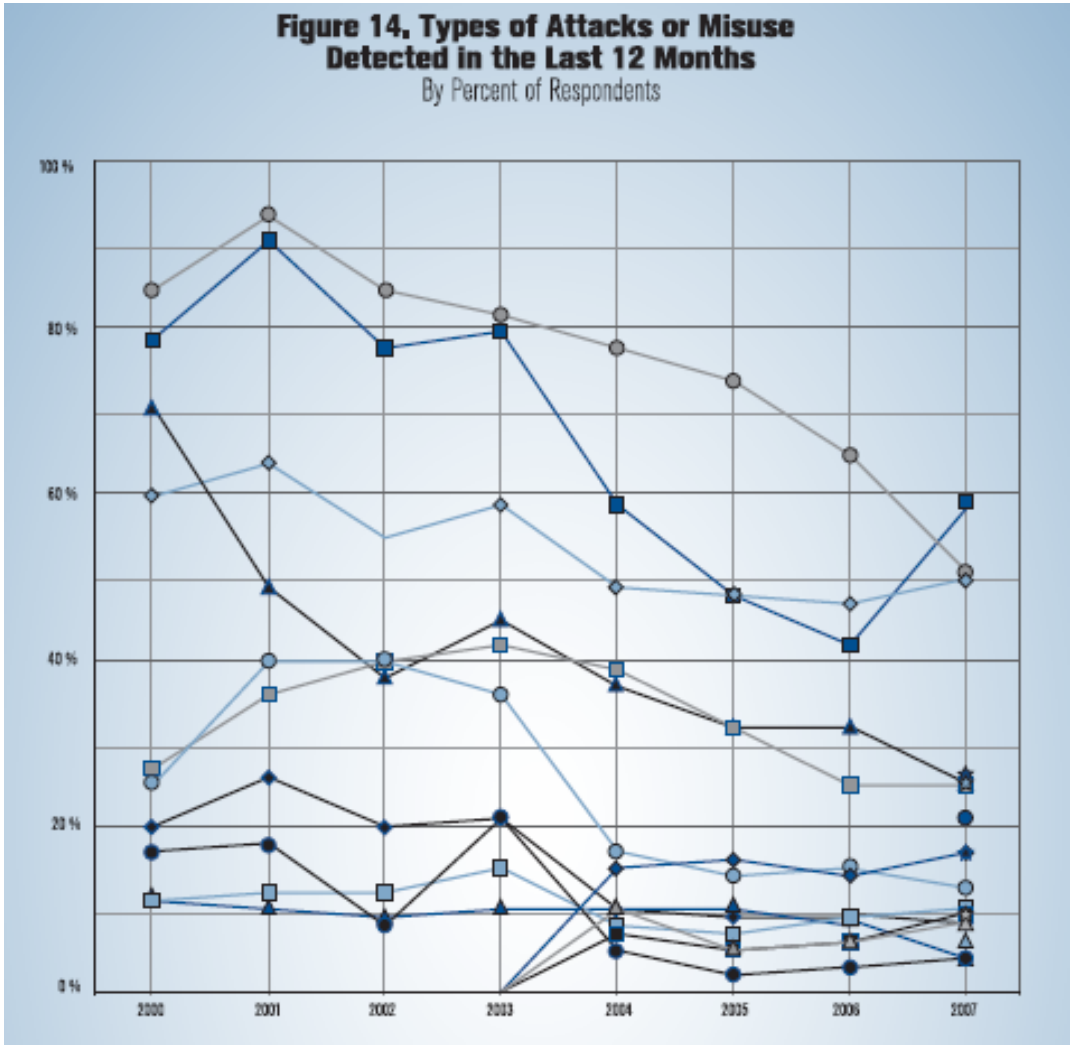


Figure 2. Respondents by Number of Employees
(Numbers do not total 100% due to rounding.)
Inner circle=2006; outer circle=2007
50,000 or more
9%
9%
1-99
20%
22%
10,000-49,999
13%
16%
100-499
14%
14%
1,500-9,999
26%
26%
500-1,499
12%
17%
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 485 Respondents

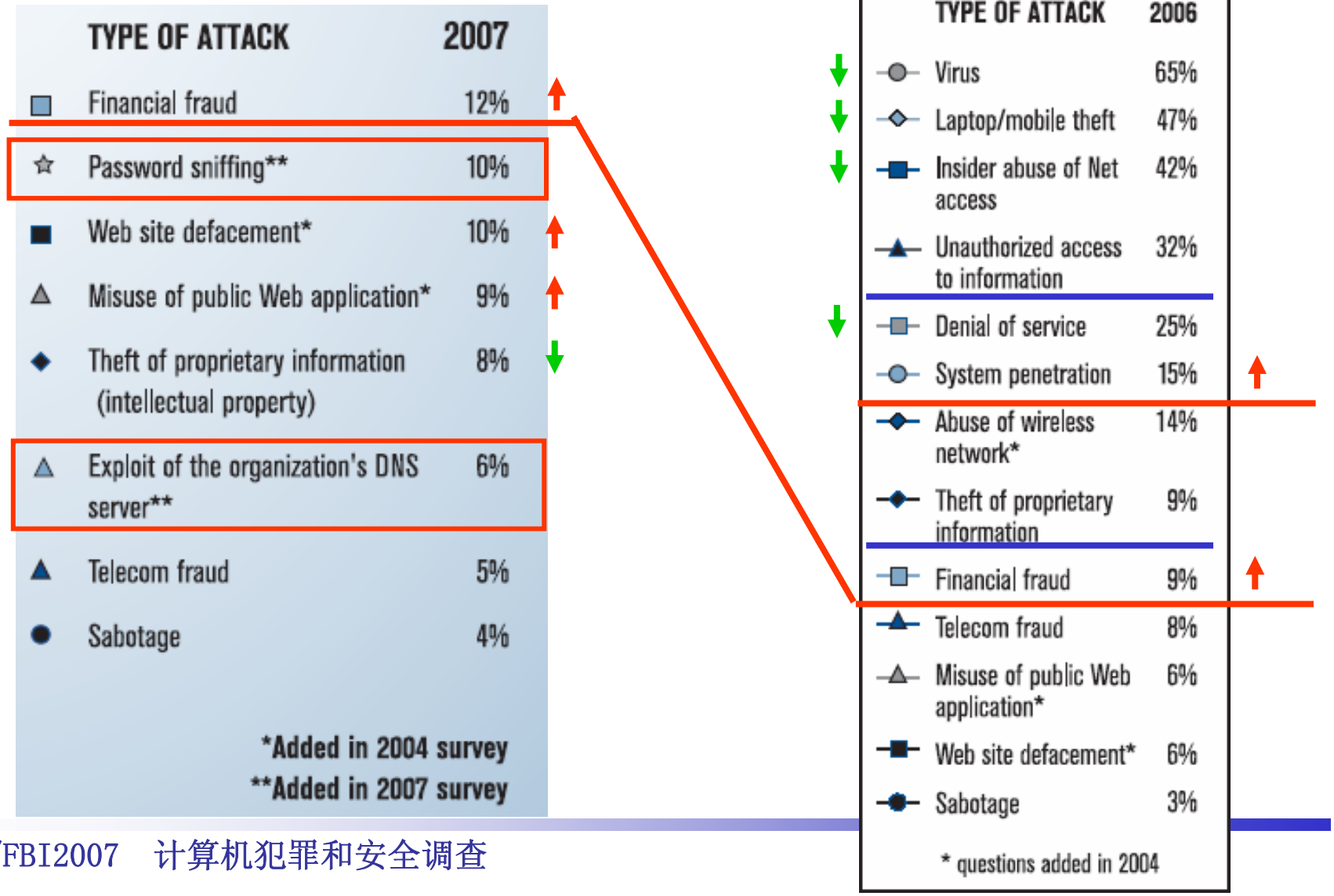
过去12个月检测到的攻击/误用类型



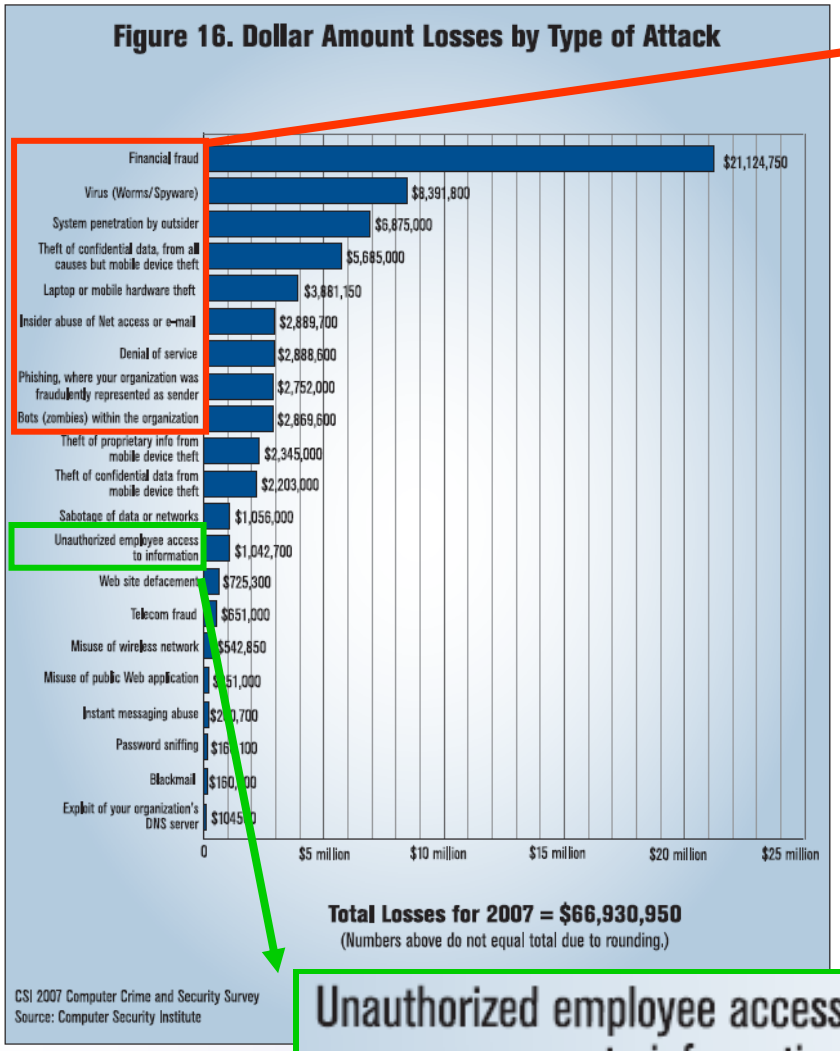
TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%
Abuse of wireless network*	17%
System penetration	13%

CSI/FBI2007　计算机犯罪和安全调查

过去12个月检测到的攻击/误用类型



各种攻击类型造成的损失



Financial fraud ↑ 6--1

Virus (Worms/Spyware) ↓ 1--2

System penetration by outsider ↑ 10--3

Theft of confidential data, from all causes but mobile device theft

Laptop or mobile hardware theft ↓ 4--5

Insider abuse of Net access or e-mail ↑ 7--6

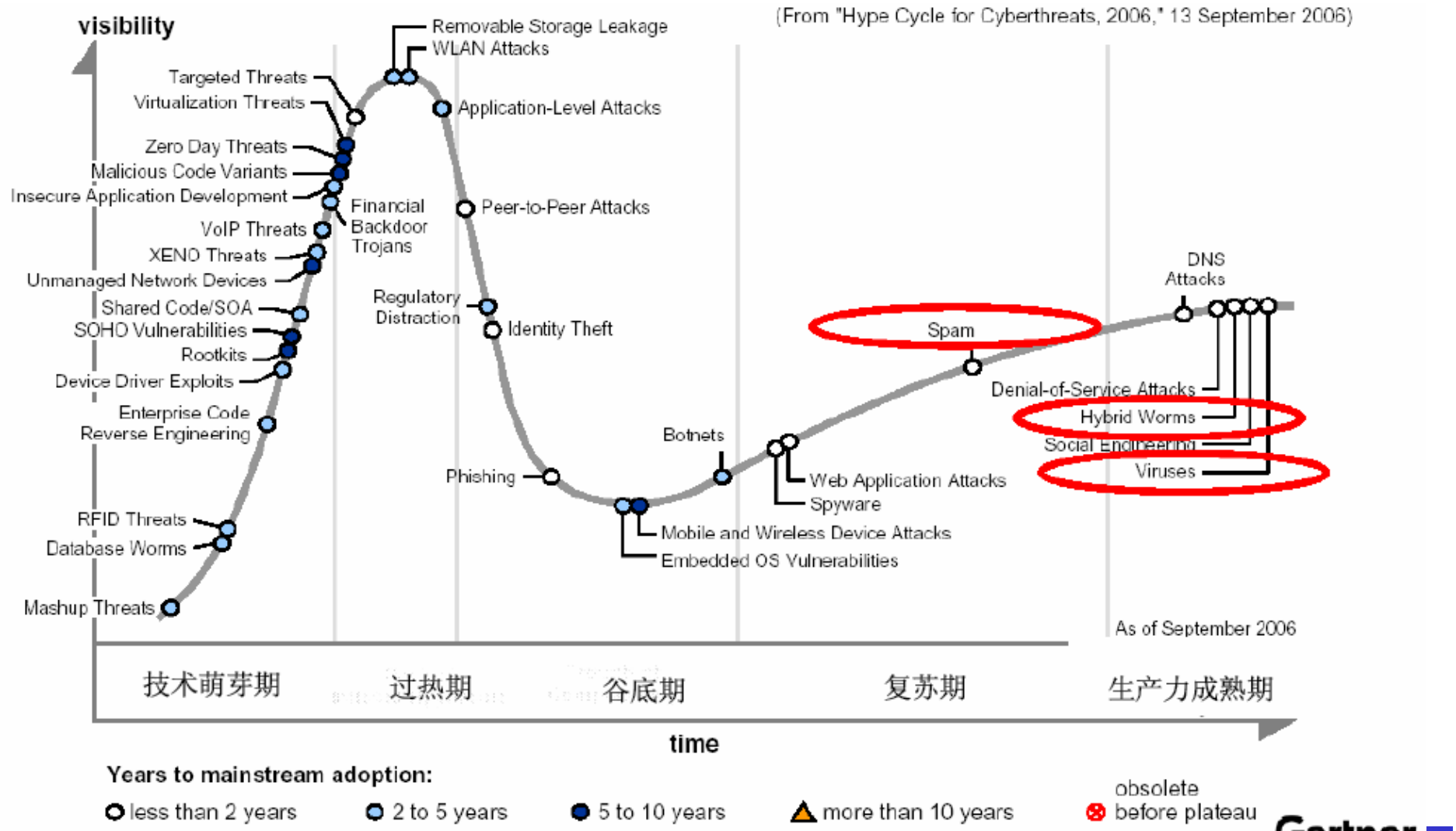
Denial of service ↓ 5--7

Phishing, where your organization was fraudulently represented as sender ↑ 11--8

Bots (zombies) within the organization

Unauthorized employee access to information ↓ 2--13

成熟的攻击技术带来巨大损失



Gartner's：网络空间安全威胁技术成熟度（2006年9月）

Gartner

平均损失

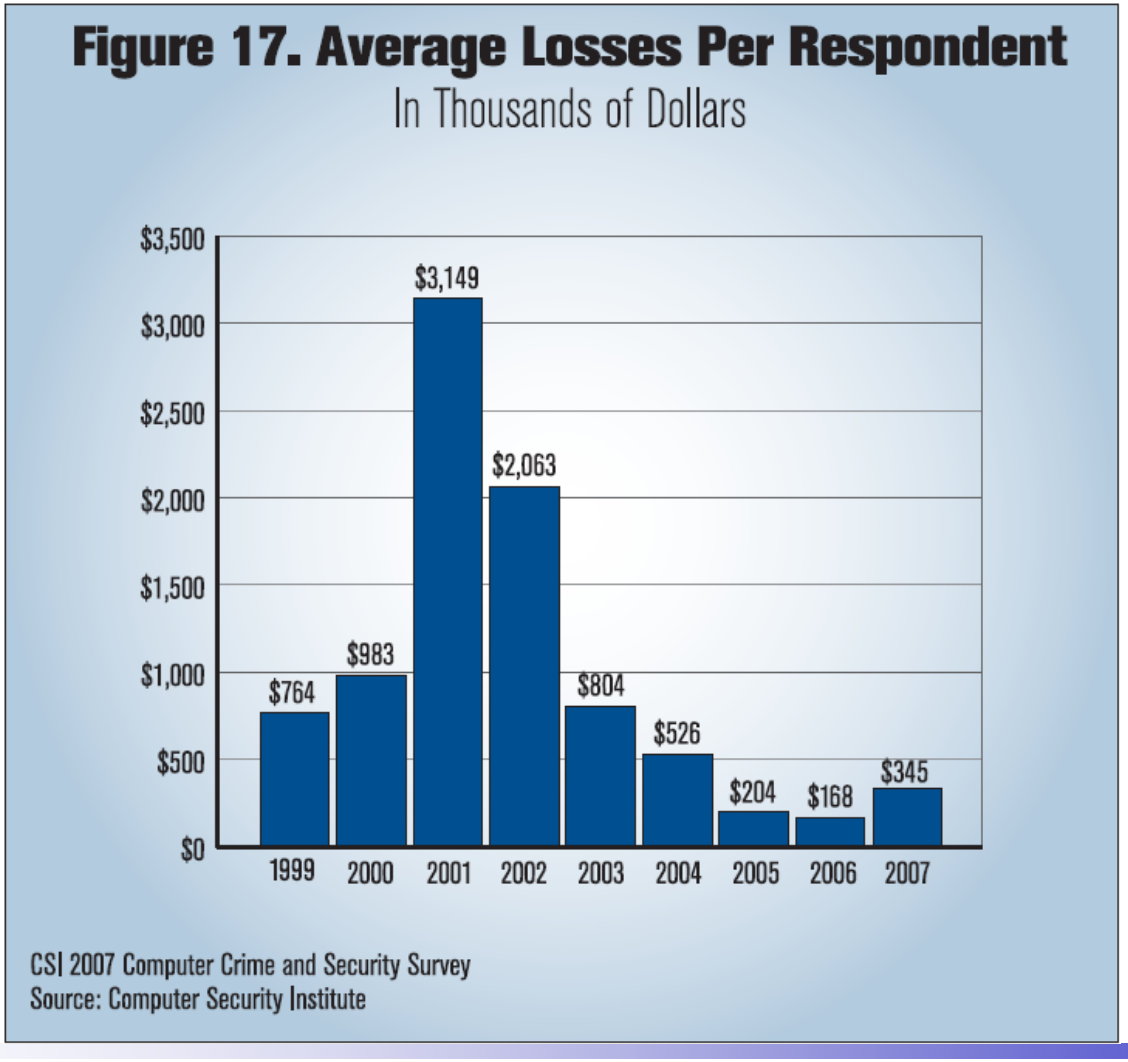
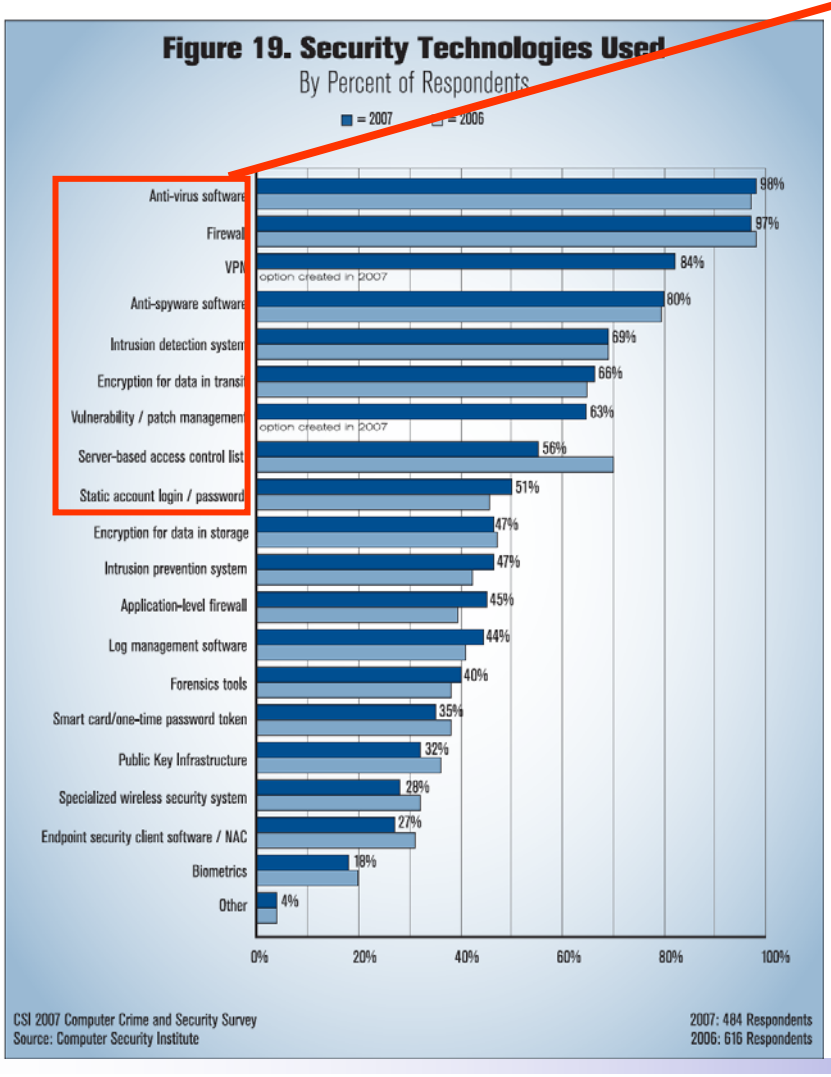


Figure 17. Average Losses Per Respondent
In Thousands of Dollars
$3,500
$3,000
$2,500
$2,000
$1,500
$1,000
$500
$0
$764
$983
$3,149
$2,063
$804
$526
$204
$168
$345
1999
2000
2001
2002
2003
2004
2005
2006
2007
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

使用的安全技术



Anti-virus software

Firewall

VPN

Anti-spyware software

Intrusion detection system

Encryption for data in transit

Vulnerability / patch management

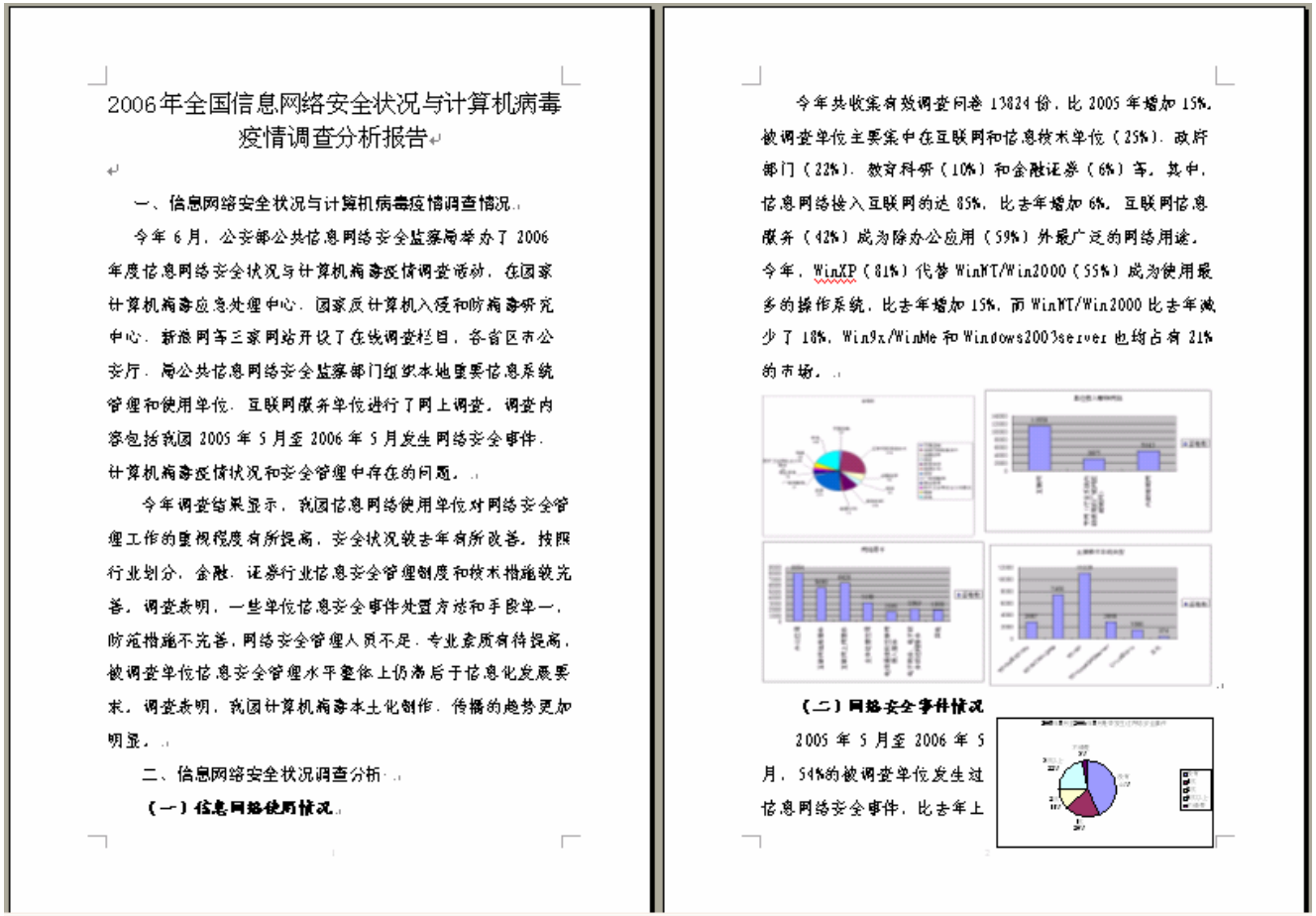
Server-based access control list

Static account login / password 51%

CSI/FBI2007 计算机犯罪和安全调查

2006/2007年全国网络安全状况调查

- 公安部公共信息网络安全监察局



2006年全国信息网络安全状况与计算机病毒疫情调查分析报告

一、信息网络安全状况与计算机病毒疫情调查情况

今年6月，公安部公共信息网络安全监察局举办了2006年度信息网络安全状况与计算机病毒疫情调查活动，在国家计算机病毒应急处理中心、国家反计算机入侵和防病毒研究中心、新浪网等三家网站开设了在线调查栏目，各省区市公安厅、局公共信息网络安全监察部门组织本地重要信息系统管理和使用单位、互联网服务单位进行了网上调查。调查内容包括我国2005年5月至2006年5月发生网络安全事件、计算机病毒疫情状况和安全管理中存在的问题。

今年调查结果显示，我国信息网络使用单位对网络安全管理工作的重视程度有所提高，安全状况较去年有所改善。按四行业划分，金融、证券行业信息安全管理制度和技术措施较完善。调查表明，一些单位信息安全事件处置方法和手段单一，防范措施不完善，网络安全管理人员不足、专业素质有待提高，被调查单位信息安全管理水平整体上仍滞后于信息化发展要求。调查表明，我国计算机病毒本土化制作、传播的趋势更加明显。

二、信息网络安全状况调查分析

（一）信息网络使用情况

今年共收集有效调查问卷13824份，比2005年增加15%。被调查单位主要集中在互联网和信息技术单位（25%）、政府部门（22%）、教育科研（10%）和金融证券（6%）等。其中，信息网络接入互联网的达85%，比去年增加6%。互联网信息服务（42%）成为除办公应用（59%）外最广泛的网络用途。今年，WinXP（81%）代替WinNT/Win2000（55%）成为使用最多的操作系统，比去年增加15%，而WinNT/Win2000比去年减少了18%，Win9x/WinMe和Windows2003server也均占有21%的市场。

（二）网络安全事件情况

2005年5月至2006年5月，54%的被调查单位发生过信息网络安全事件，比去年上

样本情况分析

- 2007共收集有效调查问卷14979份，比2006年增加10.4%。被调查单位中，互联网和信息技术单位（23%）、政府部门（24%）、教育科研（11%）和金融证券（8%）。信息网络接入互联网的占86.98%，比去年增加2%。

网络安全事件数量

2006年调查中，54%的被调查单位发生过信息网络安全事件，比2005年上升5%；其中发生过3次以上的占22%，比去年上升7%。

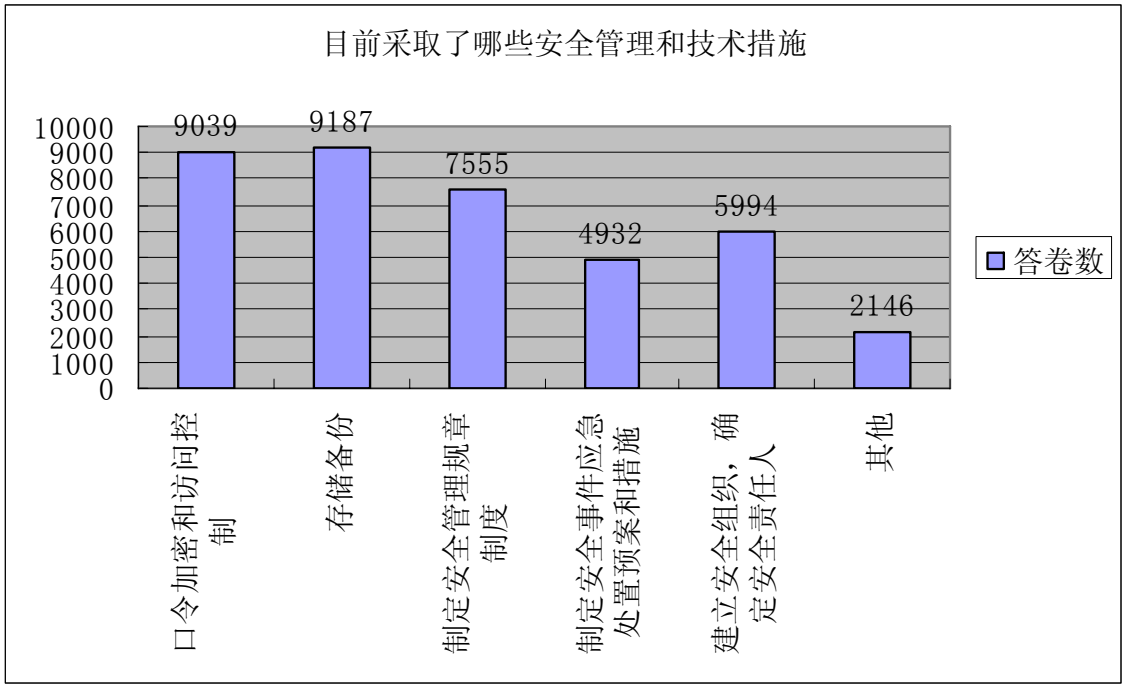
2007年调查中，65.7%的被调查单位发生过信息网络安全事件，比2006年上升12%；其中发生过3次以上的占33%，比2006年上升11%。信息网络安全事件的主要类型是：感染计算机病毒、蠕虫和木马程序（58%），垃圾电子邮件，遭到网络扫描（25%）、攻击和网页篡改，互联网和信息技术行业、政府部门和教育科研单位发生网络安全事件的比例较高。

可能攻击来源（2007）

2006年攻击或传播源来自外部的占50%，比2005年下降7%
内外部均有的占34.5%，比2005年上升10.5%

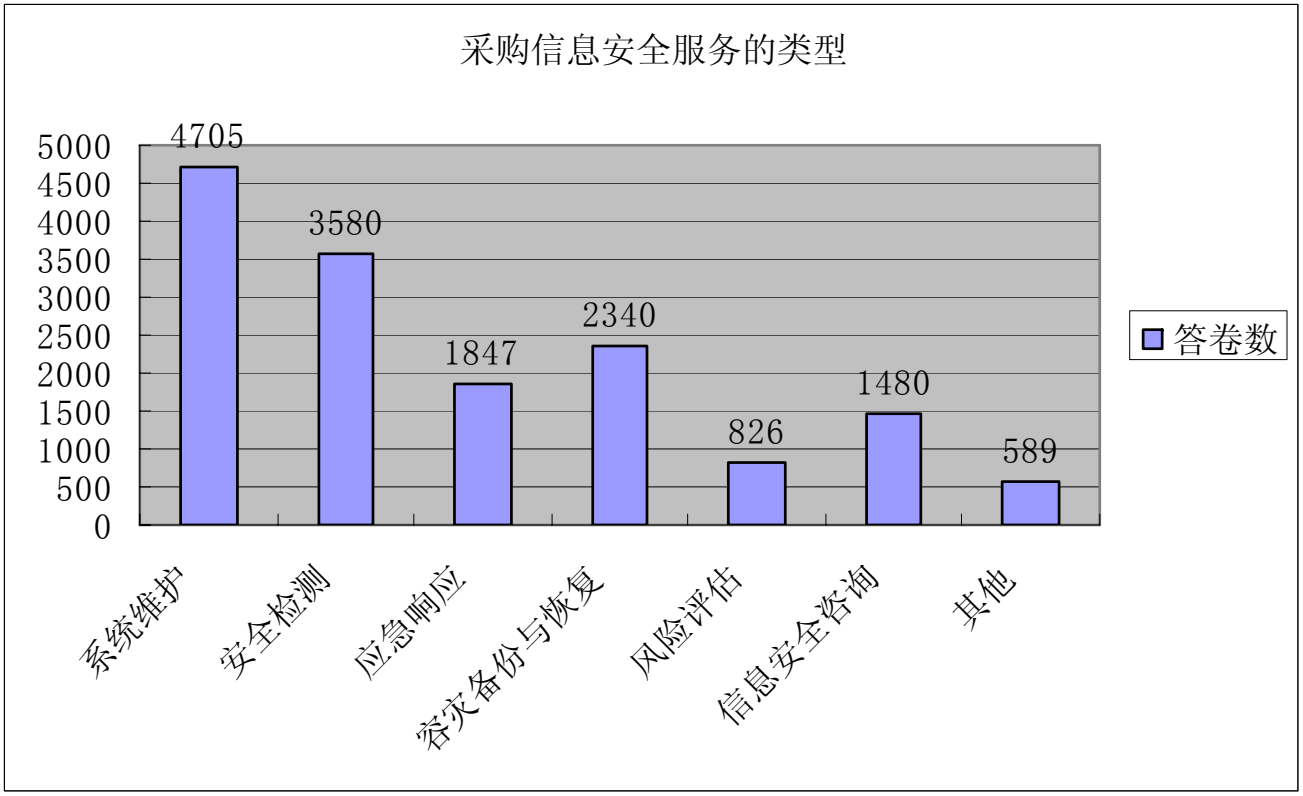
2007在发生的安全事件中，攻击或传播源来自外部的占52%。
发现途径，网络（系统）管理员通过技术监测发现占53.5%；通过安全产品报警发现占46.4%；事后分析发现的占35.4%。
未修补或防范软件漏洞仍然是导致安全事件发生的最主要原因（49.4%），但比去年下降15%，说明用户在这方面的防范意识有所提高。

采取的安全管理和技术措施



2007年调查显示：75%的被调查单位设立了专职或兼职安全管理人员，14%的单位建立了安全组织。在采取安全管理和技术措施方面，62%的单位进行存储备份，65%进行口令加密和访问控制，43%制定了安全管理规章制度。

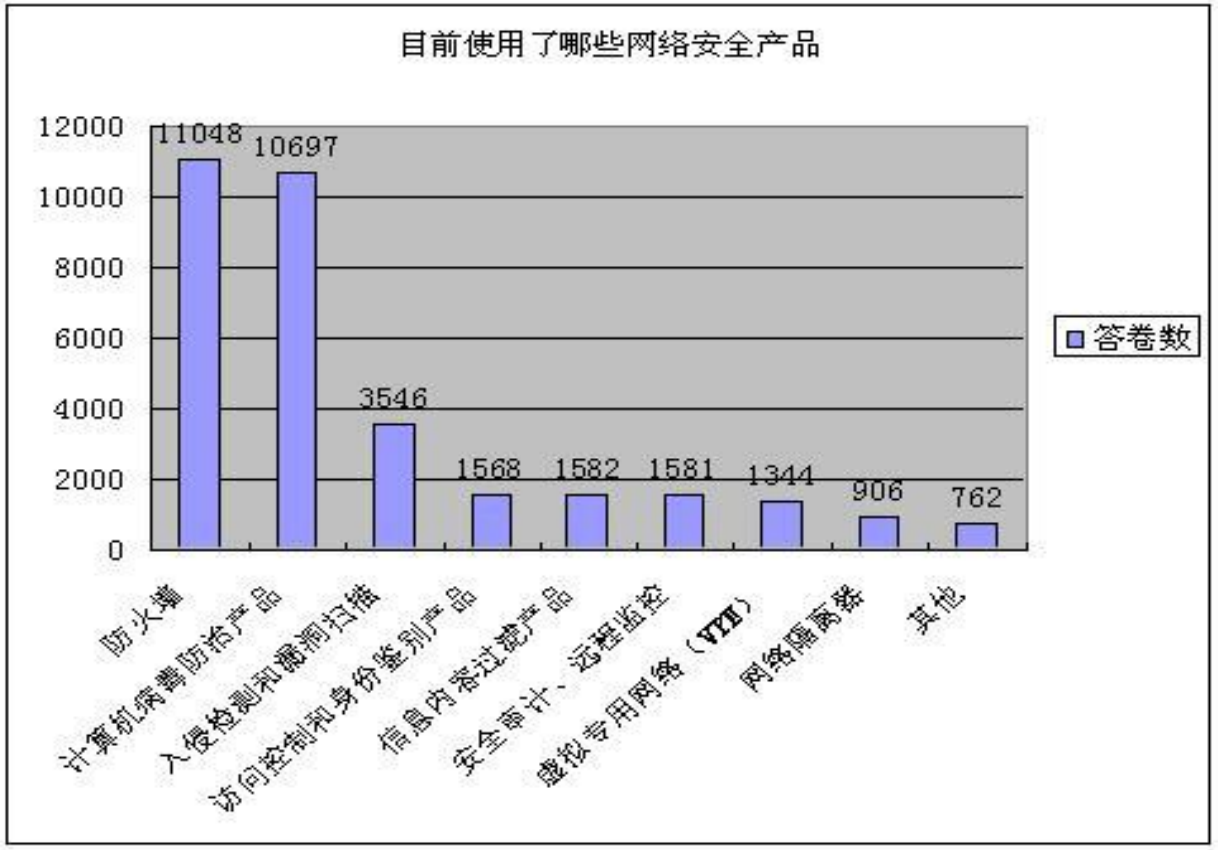
采购的信息安全服务类型



44%的被调查单位采购了信息安全服务，主要采购的服务有系统维护（67%）、安全检测（48%），其次是容灾备份与恢复（31%）、应急响应（19%）、信息安全咨询（25%）。

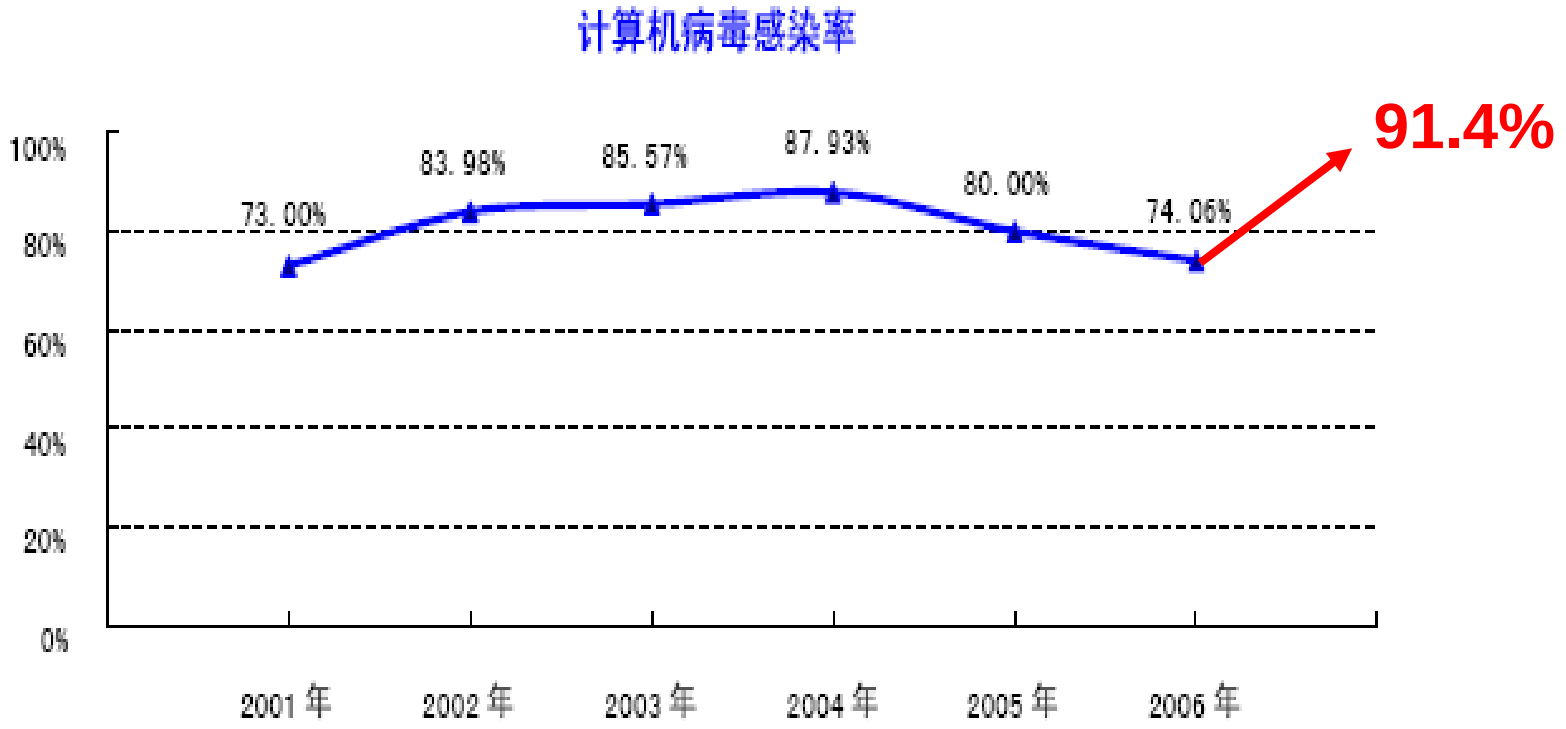
2007年全国网络安全状况调查（2006年5月至2007年5月）

网络安全产品的使用



近八成的被调查单位使用了防火墙和计算机病毒防治产品。

计算机病毒感染率

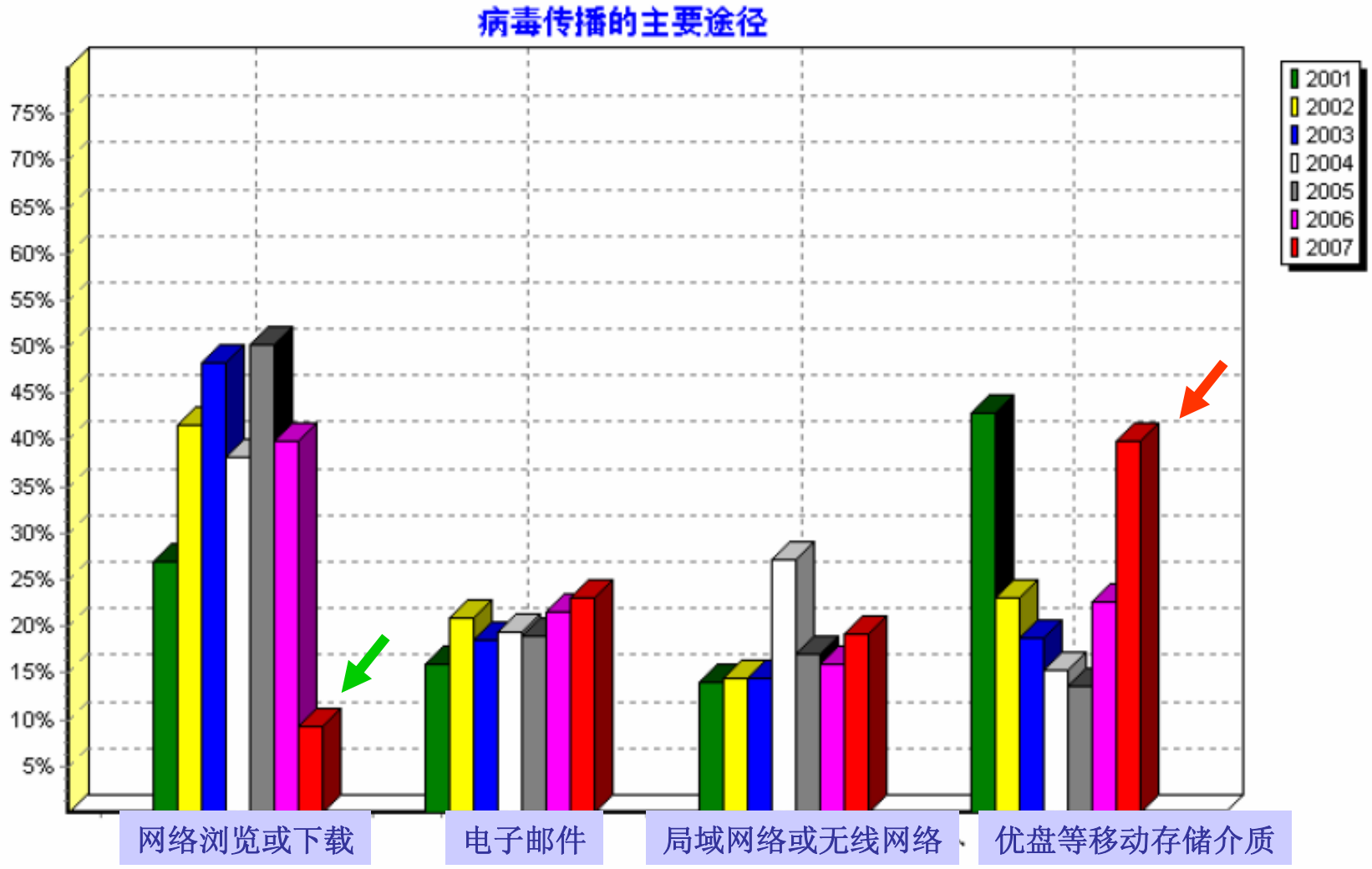


2007年计算机病毒感染率为91.4%，出现较大反弹，是历届调查中最高的。
多次感染计算机病毒的比率为53.64%，比2006年增加1.6%。

2007年感染率反弹的主要原因

- 计算机病毒通过优盘等移动存储介质传播的问题比较突出，从2006年的23%上升到2007年的40%；
- 互联网上以盗取用户帐号、密码为目的的“间谍软件”、木马病毒明显增多，“熊猫烧香”、“木马代理”、“网游大盗”和“传奇木马”等一批以侵财为目的的计算机病毒大量传播

病毒传播的主要途径（2007）

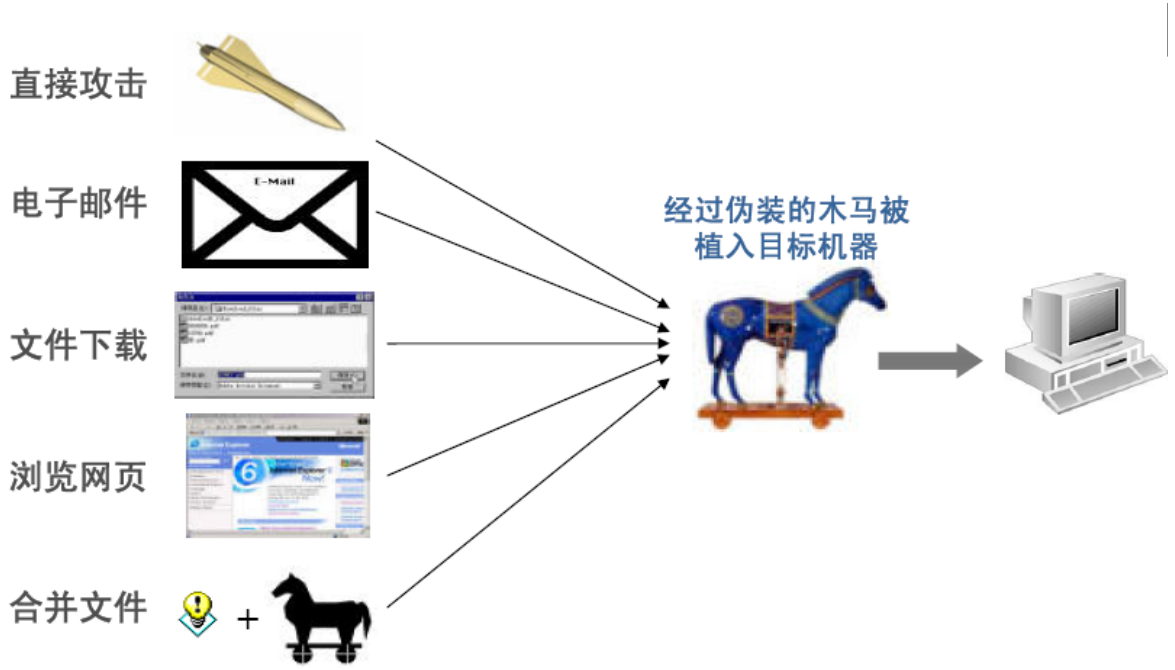


2007年中国计算机病毒疫情调查技术分析报告（2006年5月至2007年5月）

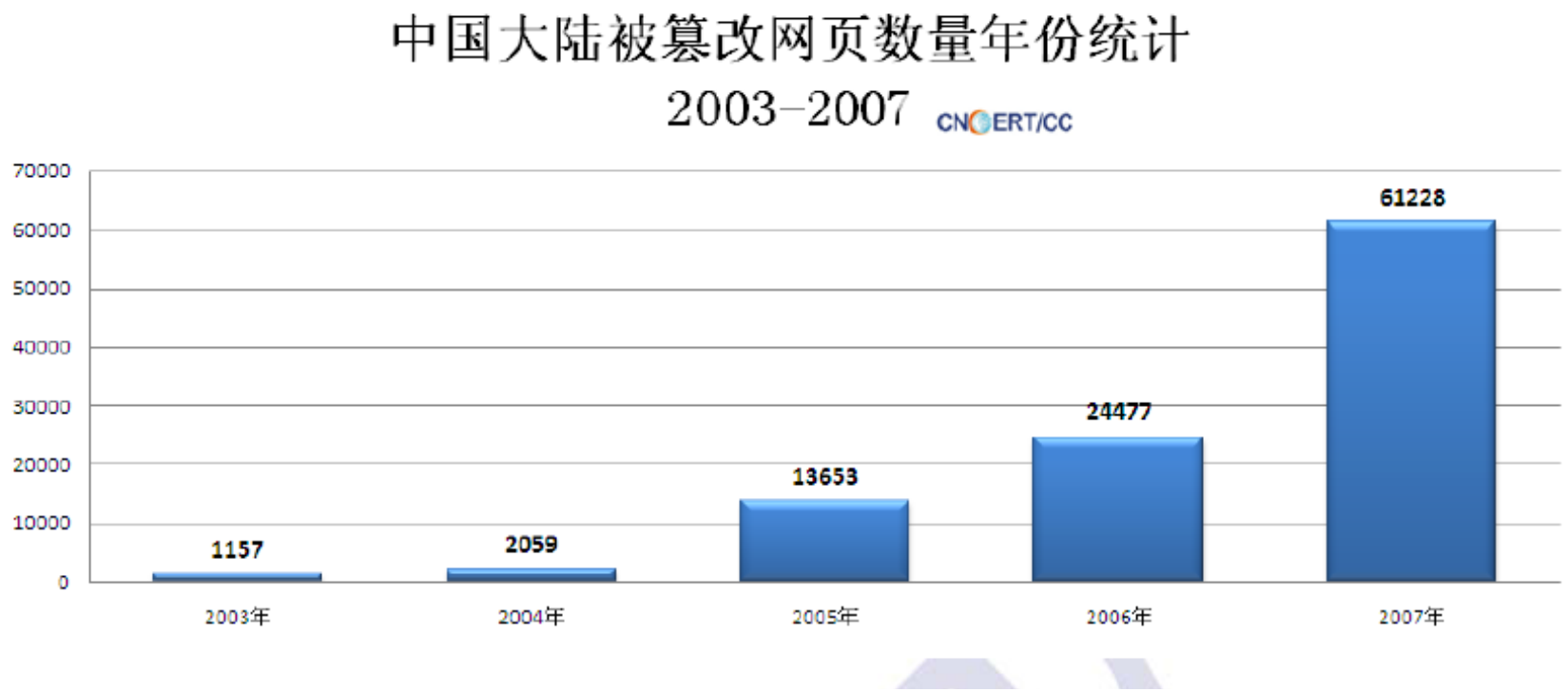
时间 / 排名	2001, 5	2002, 5	2003, 5	2004，5	2005，5	2006，6	2007，6
1	CIH	Exploit	Redlof	Netsky	Trojan.PSW.LMir	Trojan.DL.Agent（木马代理）	Trojan.DL.Agent（木马代理）
2	Funlove	Nimda	Spage	Redlof	Qqpass	Phel（下载助手）	Gamepass（网游大盗）
3	Binghe	Binghe	Nimda	Homepage	Netsky	Gpigeon（灰鸽子）	ANI/RIFF（艾妮）
4	W97M.marker	JS.Seeker	Trojan.QQKiller 6.8.ser	Unknown mail	Blaster exploit	Lmir/Lemir(传奇木马)	熊猫烧香
5	MTX	Happytime	Klez	Lovegate	Gaobot	QQHelper（QQ 助手）	Mnless（梅勒斯）
6	Troj.erase	Funlove	Funlove	Funlove	Mht exploit	Delf（德芙）	Delf（德芙）
7	BO	Klez	JS.AppletAcx	htadropper	Redlof	SDBot	Gpigeon（灰鸽子）
8	YAI	CIH	Mail.virus	Webimport	BackDoor.Rbot	StartPage	Small 及其变种
9	Wyx	Gop	Script.exploit.htm.page	activeXComponent	Beagle	Lovgate（爱之门）	Qqpass（QQ 木马）
10	Troj.gdoor	Troj.netthief	Hack.crack.foxmail	Wyx	Lovegate	Qqpass（QQ 木马）	Lmir/Lemir(传奇木马)

木马防不胜防

- 2007年我国大陆地区被植入木马的主机IP数量增长惊人，是去年的22倍，木马已成为互联网的最大危害。（CNCERT/CC）



国内恶意篡改数量高居不下



僵尸网络—攻击基本渠道

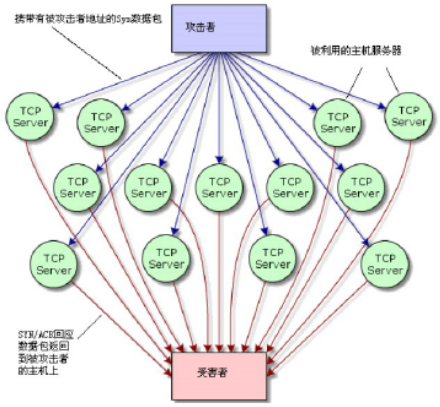
- 僵尸网络发展迅速，逐渐成为攻击行为的基本渠道，成为网络安全的最大隐患之一
- 2007年抽样监测发现我国大陆有3624665个IP地址的主机被植入僵尸程序。共发现各种僵尸网络被用来发动拒绝服务攻击10988次、发送垃圾邮件112次、实施信息窃取操作3949次。

应用软件安全日趋严重

- 层出不穷的应用软件安全漏洞的危害性已经与操作系统的安全漏洞平分秋色。我国普遍使用的微软操作系统的安全漏洞仍然是黑客攻击的首选目标，但近些年不断发展和广泛应用的各种应用程序（如IE浏览器、暴风影音多媒体播放器、VMware虚拟机和各种P2P下载软件）中存在的安全漏洞也被越来越多的披露出来，相关的漏洞机理、概念验证（POC）代码等可被利用来开发攻击程序的信息也很容易通过公开的搜索引擎收集，

黑色产业链--网络犯罪行为趋利性

- 木马、病毒等恶意程序的制作、传播、用户信息窃取、第三方平台销赃、洗钱等各环节的流水作业构成了完善的地下黑色产业链条，为各种网络犯罪行为带来了利益驱动，
- 拒绝服务攻击，窃取用户数据、帐号，篡改网页等
- 黑客往往利用仿冒网站、伪造邮件、盗号木马、后门病毒等，并结合社会工程学，实施黑客攻击。



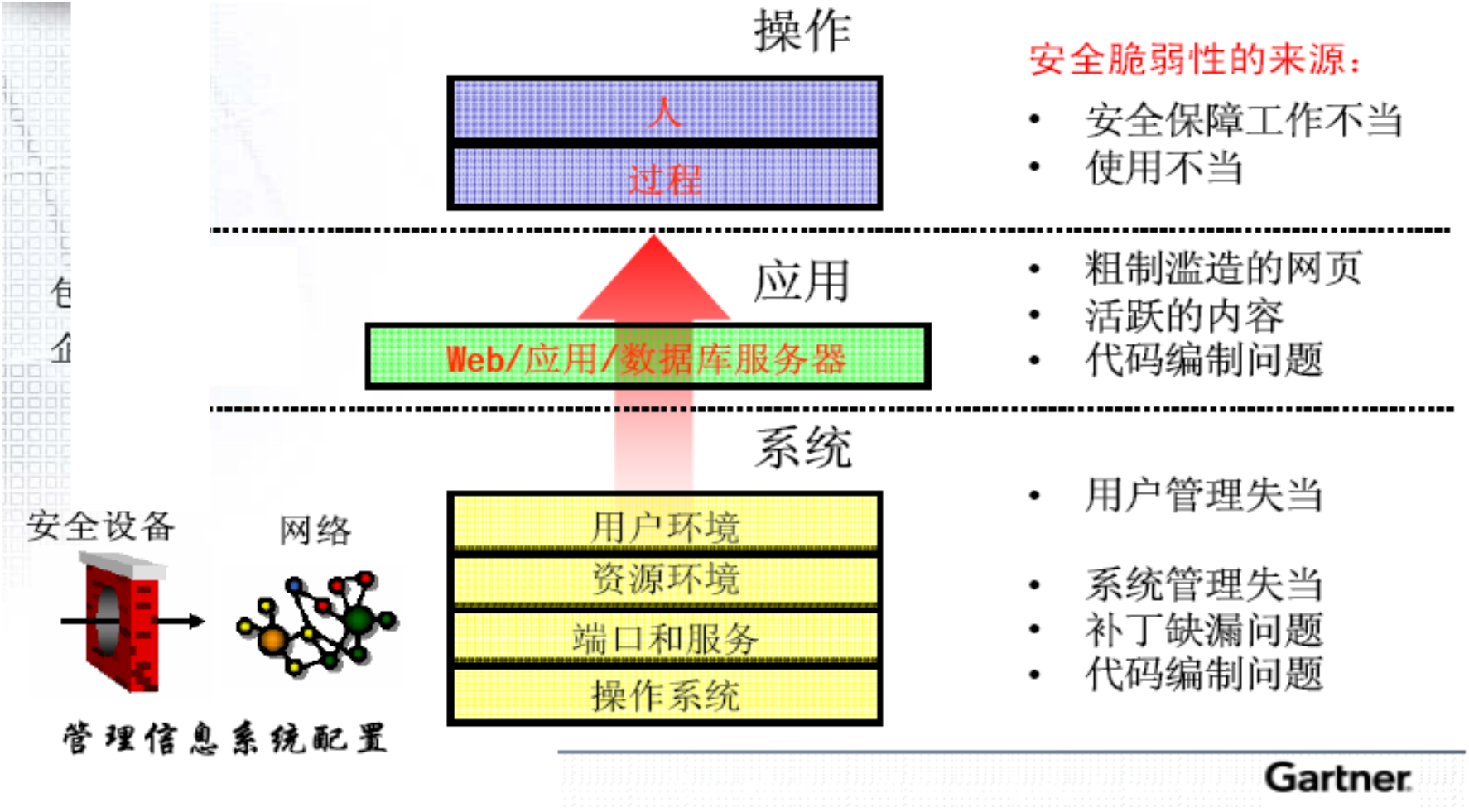
DNS和域名成为重要攻击对象

- 利用域名，攻击者可以灵活、隐蔽地实施大规模网页挂马、僵尸网络控制、网络仿冒等恶意活动。Fast-Flux等动态域名解析技术的出现，导致根据IP来对攻击行为的追查和阻断更加困难；

- 2007年还出现了利用域名解析服务程序存在的安全漏洞，对公共域名解析服务器进行域名劫持的安全事件，在大量用户毫不知情的情况下将其引诱到钓鱼网站或含有恶意代码的网站

- 安全公告：CN-VA08-05

漏洞在哪里 ？？？


操作
人
过程
安全脆弱性的来源：
• 安全保障工作不当
• 使用不当
应用
Web/应用/数据库服务器
• 粗制滥造的网页
• 活跃的内容
• 代码编制问题
系统
用户环境
资源环境
端口和服务
操作系统
• 用户管理失当
• 系统管理失当
• 补丁缺漏问题
• 代码编制问题
安全设备
网络
管理信息系统配置
Gartner

朔源一

75%的网络攻击和互联网安全侵害源于应用软件。

- Gartner

- **网页上的漏洞的根源还是来自程序开发者对网页程序编制和检测。未经过安全训练的程序员缺乏相关的网页安全知识；应用部门缺乏良好的编程规范和代码检测机制等等。解决此类问题必须在WEB应用软件开发程序上整治，仅仅靠打补丁和安装防火墙是远远不够的。**
  - PHP超文本预处理器一 PHP自身安全配置及PHP底层代码的缺陷，特别是程序编制时PHP脚本实现中普遍存在的脆弱性等。
  - SQL注入漏洞(injection) 一攻击者在普通用户输入中插入数据库查询指令。
  - 跨网页脚本攻击漏洞（XSS）一利用动态网页的特性、网页中的程序错误，以及利用开发者没有严格限制回传参数及过滤输入之特殊字符，将具攻击性的程序代码置入而所进行的攻击。
  - 其他，.....

小结

基础网络和重要信息系统面临着严峻的安全威胁

终端用户和互联网企业是主要的受害者

我们能做什么？

未来一年中，从战术层面上讲，你所在公司将采取下列哪些安全措施？

美国	中国	
16%	38%	安装应用软件防火墙
30%	33%	安装更好的访问控制软件
27%	31%	安装监控软件
12%	22%	部署身份管理软件
19%	21%	进行风险评估/安全测试
37%	21%	培养并提高用户的信息安全意识
27%	20%	确保远程接入安全
22%	18%	安装/监控入侵检测工具
16%	17%	整合安全系统
19%	14%	对业务部门进行信息安全培训

数据来源：《InformationWeek》和埃森哲咨询公司合作进行的2007年“全球信息安全调查”

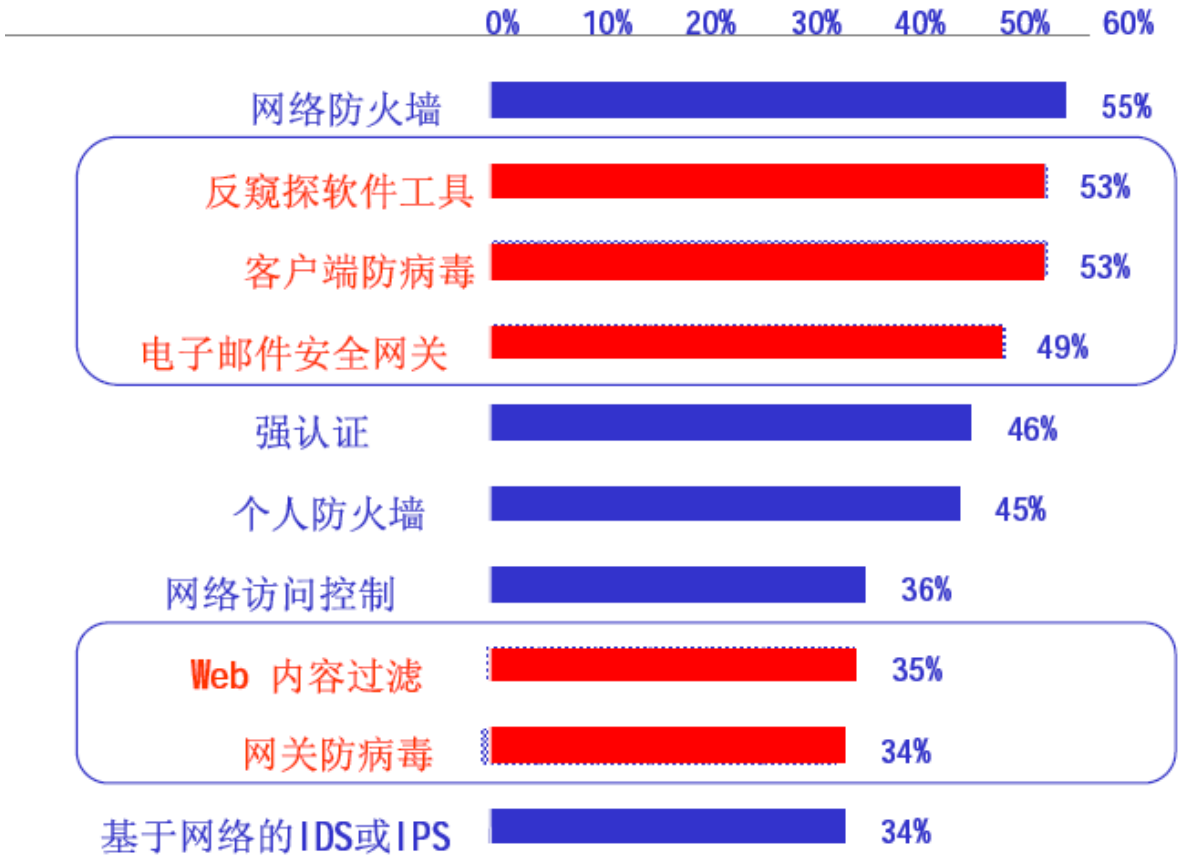
未来一年中，从战术层面上讲，你所在公司将采取下列哪些安全措施？

- 美国　中国

美国	中国	
37%	21%	培养并提高用户的信息安全意识
30%	33%	安装更好的访问控制软件
27%	31%	安装监控软件
27%	20%	确保远程接入安全
26%	6%	监控用户遵守安全策略的情况
23%	12%	进行安全审计
22%	18%	安装/监控入侵检测工具
19%	21%	进行风险评估/安全测试
19%	14%	对业务部门进行信息安全培训
18%	11%	建立无线网络安全

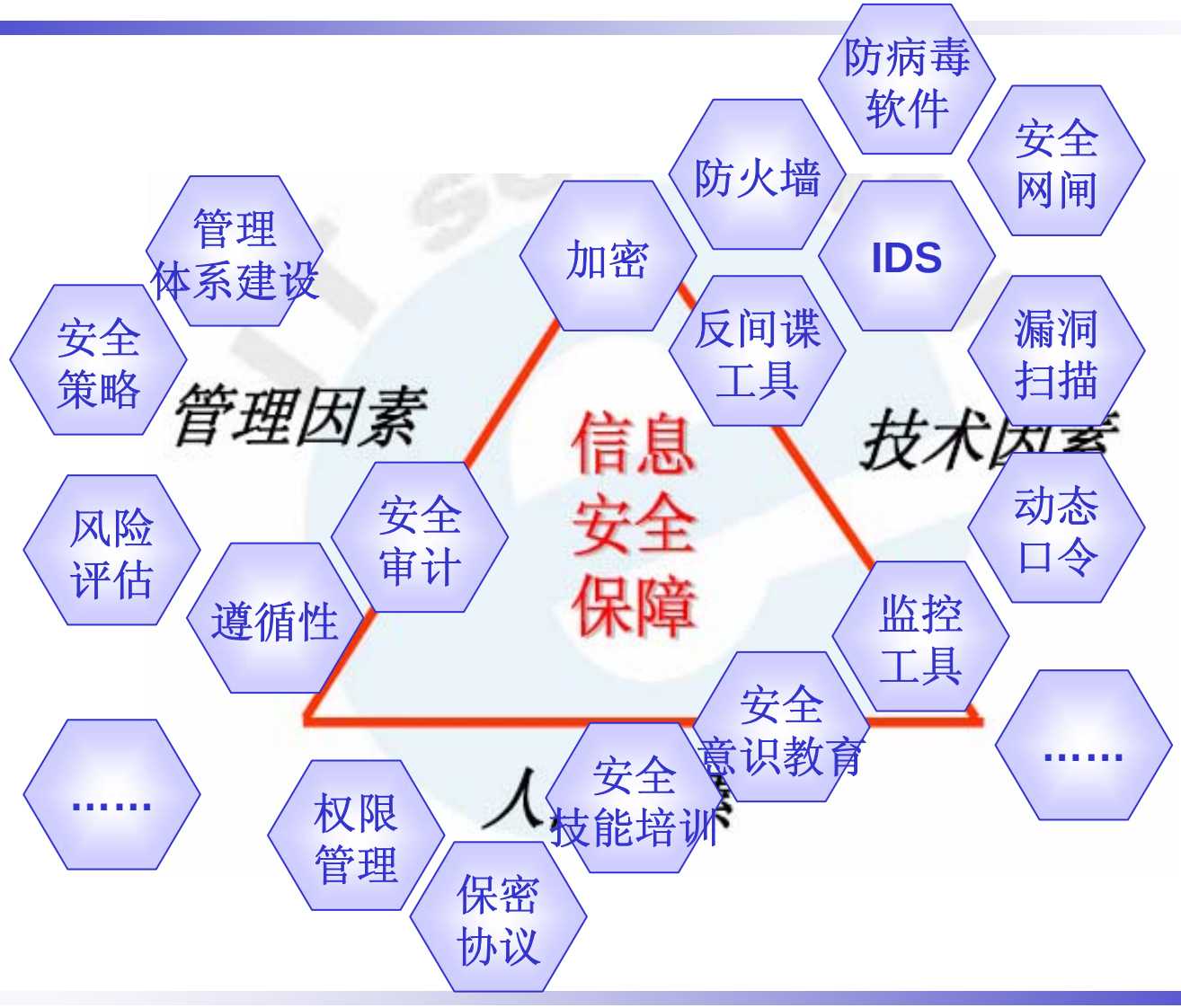
数据来源：《InformationWeek》和埃森哲咨询公司合作进行的2007年“全球信息安全调查”

2007年
企业最需要优先购置的10个重点安全项目



根据：149位技术决策者-北美中小型公司和企业
来源：福里斯特2006安全专门小组调查

三分技术，七分管理


防病毒软件
安全网闸
防火墙
IDS
加密
管理体系建设
安全策略
反间谍工具
漏洞扫描
管理因素
技术因素
信息安全保障
安全审计
动态口令
风险评估
遵循性
监控工具
安全意识教育
……
……
安全技能培训
人
权限管理
保密协议

信息安全发展的整体趋势

- 安全需求多样化
- 技术发展两极分化：专一和融合
- 安全管理体系化

我国信息安全保障现状

- 信息系统也逐步成为国家关键基础设施
- 安全问题不容乐观
  - 核心技术在他人之后
  - 信息安全政策、法规不完善
  - 信息安全管理机构混乱
  - 信息安全产业相对滞后
  - 信息安全保障战略规划不充分