



Network Security Considerations for 2010

Presented to ISACA Dallas

March 11, 2010





Brian Thomas, CISA, CISSP

- Brian is a partner in Weaver's Risk Advisory Services practice and is responsible for managing and developing the firm's IT Advisory services group. Brian has over 12 years experience providing management consulting and IT risk advisory services including IT audits (both internal and external), information security assessments and SAS 70s. Brian is based in Houston and has clients across the State of Texas, including the Dallas / Fort Worth Metroplex.

- Founded in 1950 in Fort Worth
- Approximately 400 people in 5 locations across the “Texaplex”
- Largest firm HQ’d in Texas, a Top 50 accounting firm nationally
- Risk Advisory Services consists of approximately 30 personnel spread across all locations



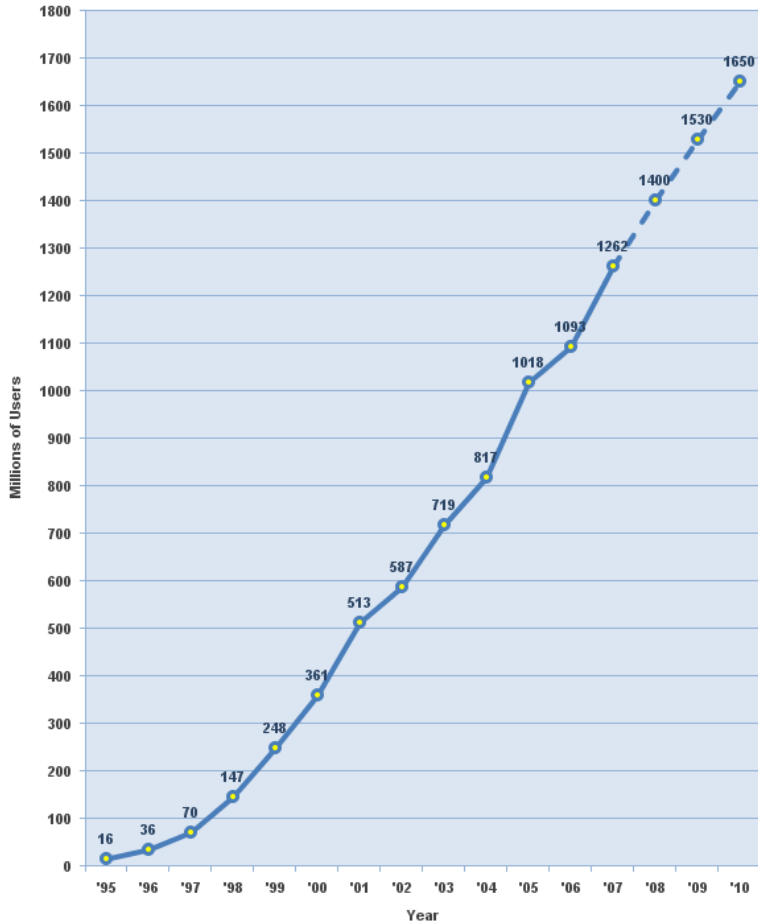
- Evolving Computer Use
- Evolving Threats
- Evolution of Network Security
- Notable Breaches
- Considerations for IT Auditors in 2010





Evolving Computer Use

Internet Users in the World
Growth 1995 - 2010



2010 and onward

- Dependence on the internet
- User based development
- Use of social media
- Online banking
- Unified communications
- Mobile users
- And on and on...



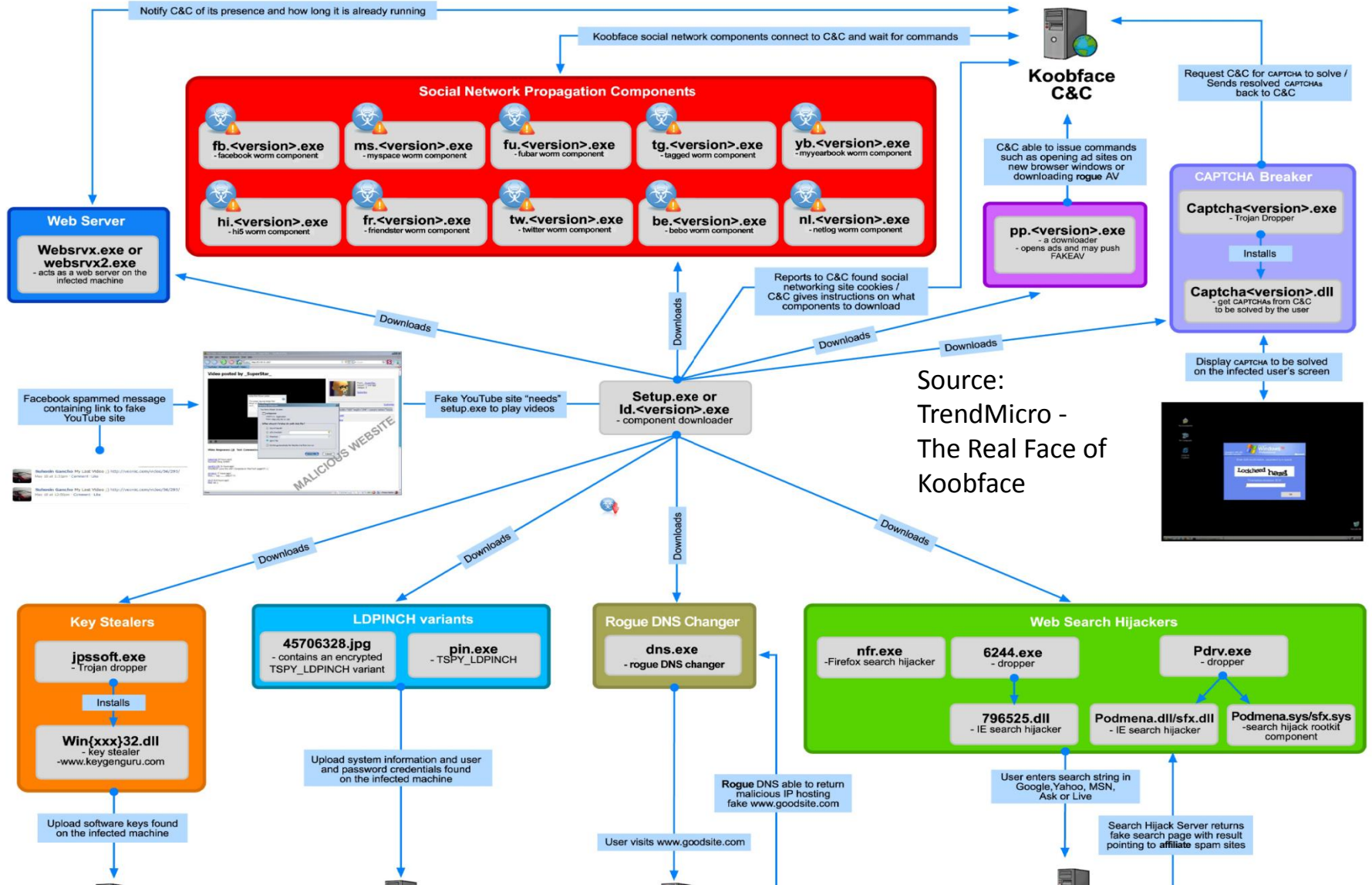


Source: Danny Allan, Web 2.0 How Secure are Your Apps?

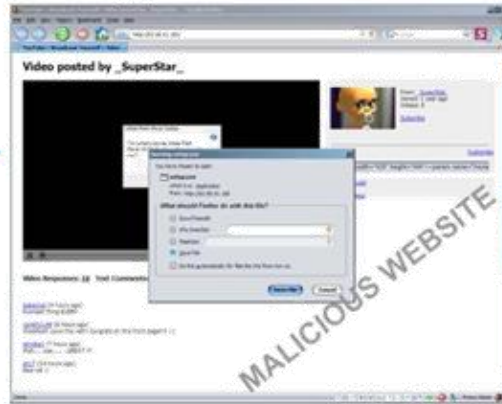
Evolving Threats

2000	2010
<ul style="list-style-type: none"> • First Distributed Denial of Service (DDoS) attack • Worms and Trojans • Microsoft Windows & IIS • Web Site Defacement • Going after the weak systems • Fairly static websites • Disgruntled souls • Bragging rights 	<ul style="list-style-type: none"> • Massive BotNets • Cross Site Scripting (XSS) • Adobe Acrobat Reader & Flash • Abbreviated URL Services • Malware distributed via Hacked Websites • Going after the weak humans • Facebook and iPhone Apps; Koobface • Organized crime • Profit



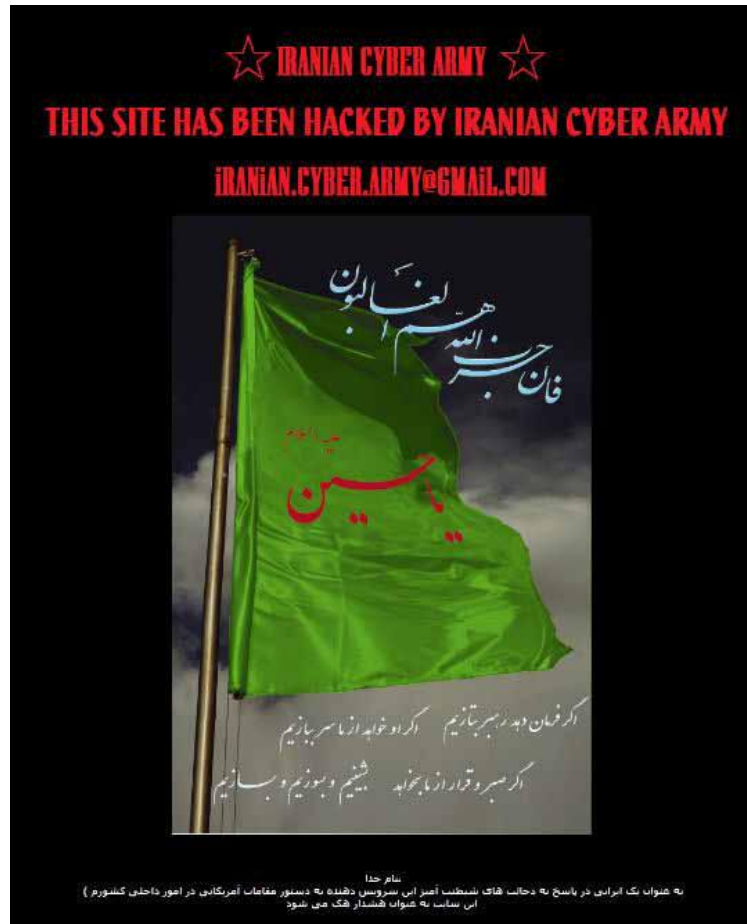


Facebook spammed message containing link to fake YouTube site



Fake YouTube site "needs" setup.exe to play videos

**Setup.exe or
Id.<version>.exe**
- component downloader



Twitter Hack

From McAfee's Q4 2009
Threat Report

Cyberwar declared as China hunts for the West's intelligence secrets - Times Online - Windows Internet Explorer

http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece

File Edit View Favorites Tools Help

cross site scripting example... Cyberwar declared as Chi... The security breach at TJX...

Style Event
Book your tickets now for exclusive Style events at Westfield London

TIMES ONLINE

“ Simply because the BBC does something well doesn't mean it should be doing it ” Rod Liddle


NEWS COMMENT BUSINESS MONEY SPORT LIFE & STYLE TRAVEL DRIVING ARTS & ENTS ARCHIVE OUR PAPERS SUBSCRIPTIONS

UK NEWS WORLD NEWS POLITICS SCIENCE ENVIRONMENT WEATHER TECH & WEB VIDEO PHOTO GALLERIES TOPICS MOBILE RSS

Where am I? Home News Tech & Web

From [The Times](#) March 8, 2010

Cyberwar declared as China hunts for the West's intelligence secrets



It is estimated that in the past year the number of attacks on US government agencies rose to 1.6 billion per month. Systems in the EU are even more vulnerable

Done Internet 100%



Evolving Security

2000

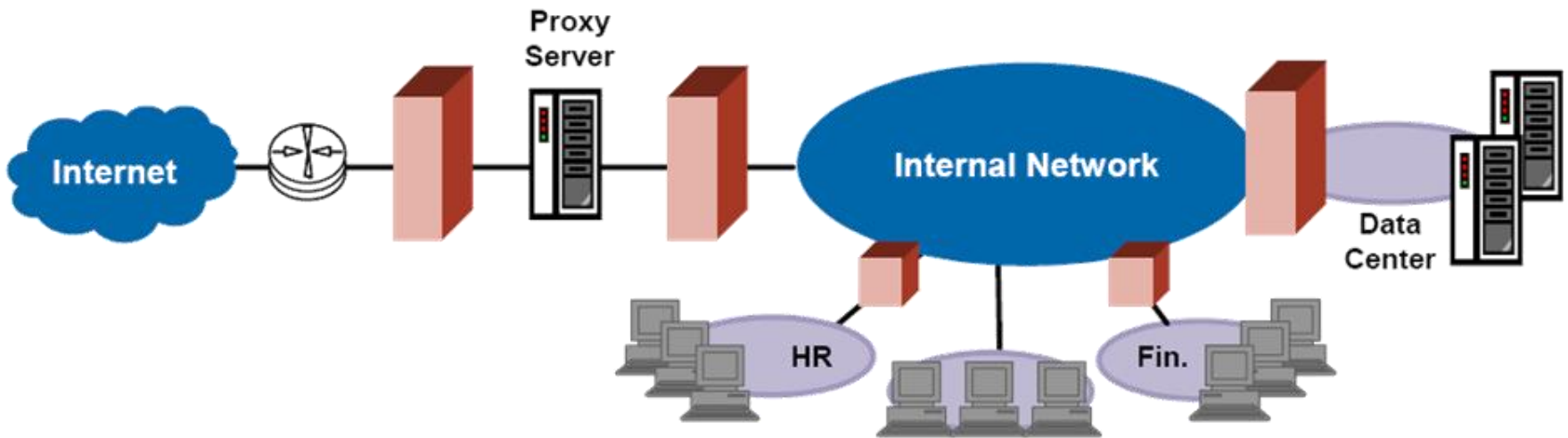
- Castle and Moat
- Trust within the walls
- Lock down O/S
- Eliminate Default Settings



2010

- Where is the perimeter?
- Everything (should be) assumed compromised
- More secure O/S
- Browsers are vulnerable

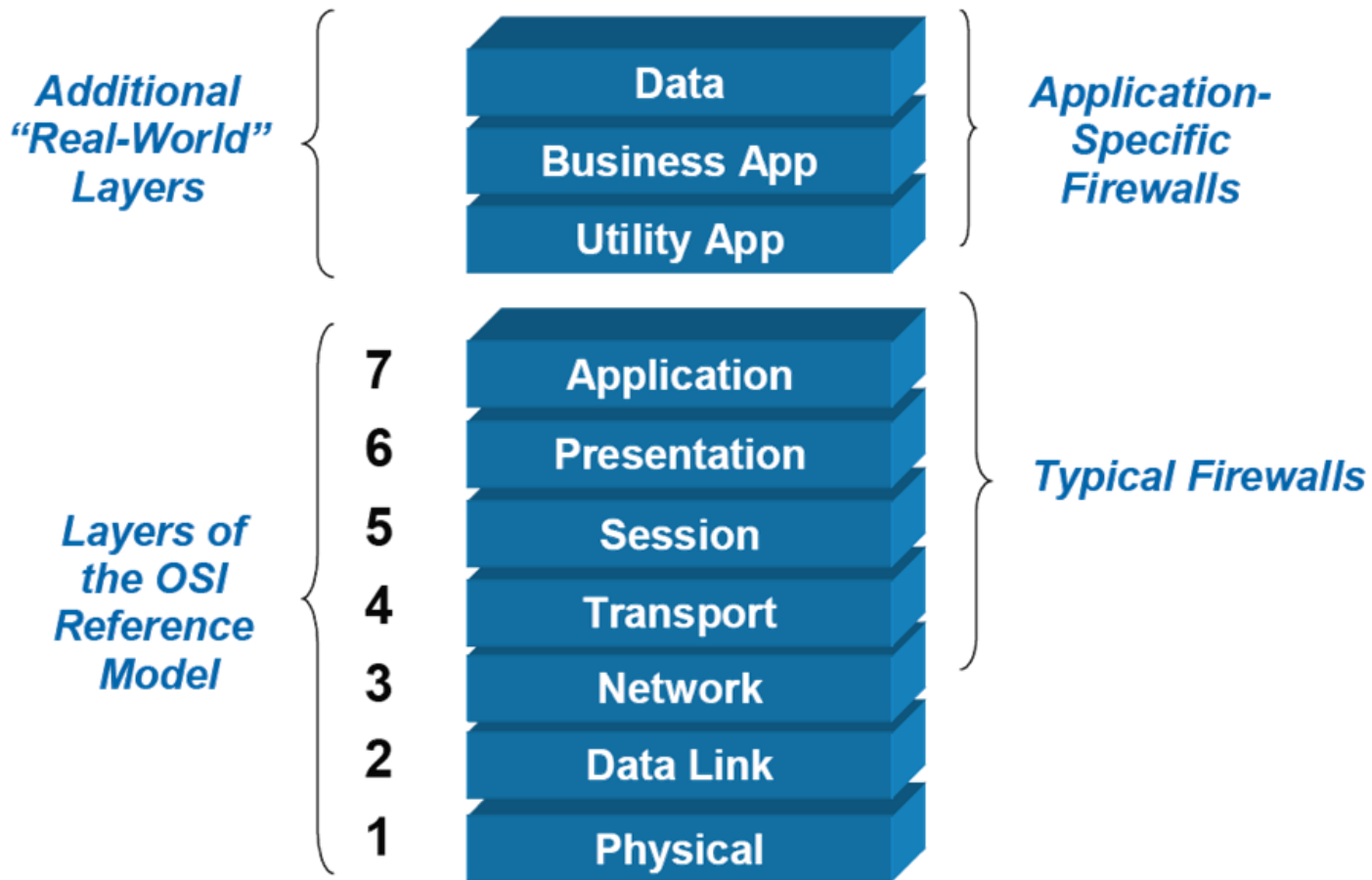




Source: META Group



Application Firewalls





- **Adobe** - Patches to mitigate issues that had been actively exploited for nearly three months. Malicious PDF files have been found hosted on websites that use obfuscation to thwart AV detection.



- **Cisco** - Cisco PIX and ASA vulnerabilities allow unauthorized access.



- **Clam AV** - A Buffer Overflow, which potentially facilitates remote code execution, can be executed with a specially formed URL in an email scanned by Clam AV. A malformed file analyzed by Clam AV can crash the application.



- **Java** - Multiple updates for 7 bugs. Users reporting that after installing the updates, older versions remained on PCs.



- **Mozilla Firefox** - Critical patch to mitigate a vulnerability with exploit code that could use a malicious XML file to install unauthorized code.



- **Nortel** - Vulnerabilities in the Nortel Communication Server 1000 platform could allow sensitive data disclosure and remote access.



- **Oracle** - 43 security fixes across hundreds of products from Oracle.



- **VMware** - Serious vulnerability that affects VMware Workstation, Player, ACE, Server, Fusion, ESXi, and ESX. A local user on the guest OS can obtain privileges on the target host system.



- **Wireshark** - Vulnerabilities in versions of Wireshark prior to 1.0.7 could allow remote compromise.



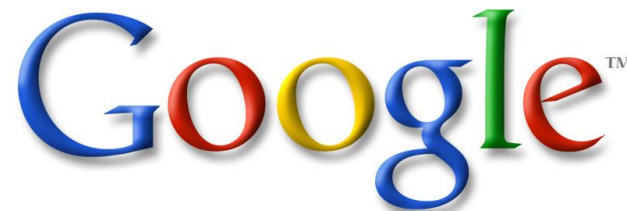
A Hacker Proof Computer



From Peter Wood's Presentation at the ISACA Security Conference in 2009

Breaches

- 2007 – TJX
- 2009 – Heartland Payment Systems
- 2009 / 2010 – Google
- 2010 – Mariposa



- 40 million credit cards stolen.
- Weak wireless encryption (WEP) lead to the attack.
- Breach was undetected for up to 2 years.
- Ukrainian sentenced to 30 years for attempting to sell hundreds of thousands of users' credit card details.



- Theft of 130 million credit and debit card numbers from Heartland Payment Systems discovered this year, affecting 7-Eleven Customers among others.
- Hackers installed malicious software that allowed backdoor access to the company's networks using SQL injection.



- The initial method used to draw a user to the infected website is unknown.
- Once the user visited the malicious site, their Internet Explorer browser was exploited to download an array of malware to their computer automatically and transparently. The programs unloaded seamlessly and silently onto the system, flowing one after the other.
- One of the malicious programs opened a remote backdoor to the computer, establishing an encrypted covert channel that masqueraded as an SSL connection to avoid detection. This allowed the attackers ongoing access to the computer and to use it as a “beachhead” into other parts of the network to search for login credentials, intellectual property, etc.
- Once the hackers were in systems, they siphoned off data to command-and-control servers in Illinois, Texas and Taiwan.
- The attacks appeared to have begun Dec. 15, but may have started earlier. They appear to have ceased on Jan. 4, when command-and-control servers that were being used to communicate with the malware and siphon data shut down.





- Infected 13 million machines in 190 countries
- Searched for credit card details on computer, recorded key strokes, communicated with centralized command
- Exploited a vulnerability found in IE, and spread through USB memory sticks as well
- Infected majority of Fortune 1000, 40 major banks
- Appear to have been caught when one inadvertently signed on to the botnet with his undisguised credentials
- “Hackers of less than average ability...”

IT Audit Considerations

Does management understand:

- The information security threats to the organization?
- The various ways data may be entering or leaving the organization?
- The level of security awareness within the organization?
- Where critical data is stored?
- Form over substance when it comes to security?





Meaningful Security?



- Internal threat assessment performed by your information security organization
- Procedures to monitor the data leaving the network
- Intrusion detection
- Incident response
- Application security
- Wire transfer systems



Q&A