INTERNET SECURITY ALLIANCE

The Evolving Cyber Threat

and what businesses can do about it

Larry Clinton, President

Direct 703/907-7028 lclinton@isalliance.org

INTERNET SECURITY ALLIANCE

Founders

INTERNET SECURITY ALLIANCE

Our Partners

STAYSAFEONLINE.org
National Cyber Security Alliance

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

UNITED STATES DEPARTMENT OF THE TREASURY

FCC Federal Communications Commission

BSI

ANSI
American National Standards Institute

ISSA
Information Systems Security Association
The Global Voice of Information Security

NFIB
The Voice of Small Business®

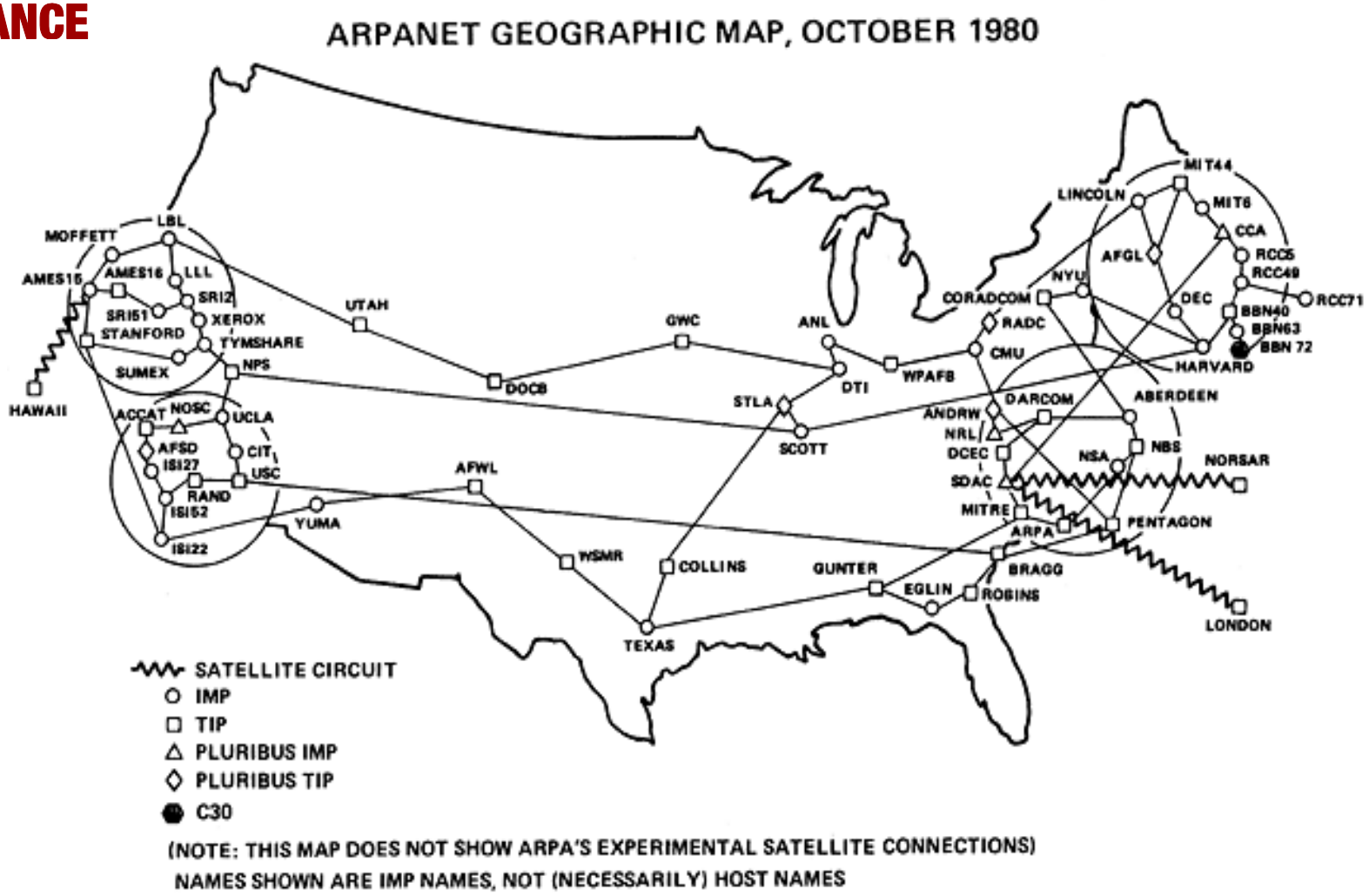
IT SCC
INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

Council on Competitiveness

AMERICAN BANKERS ASSOCIATION

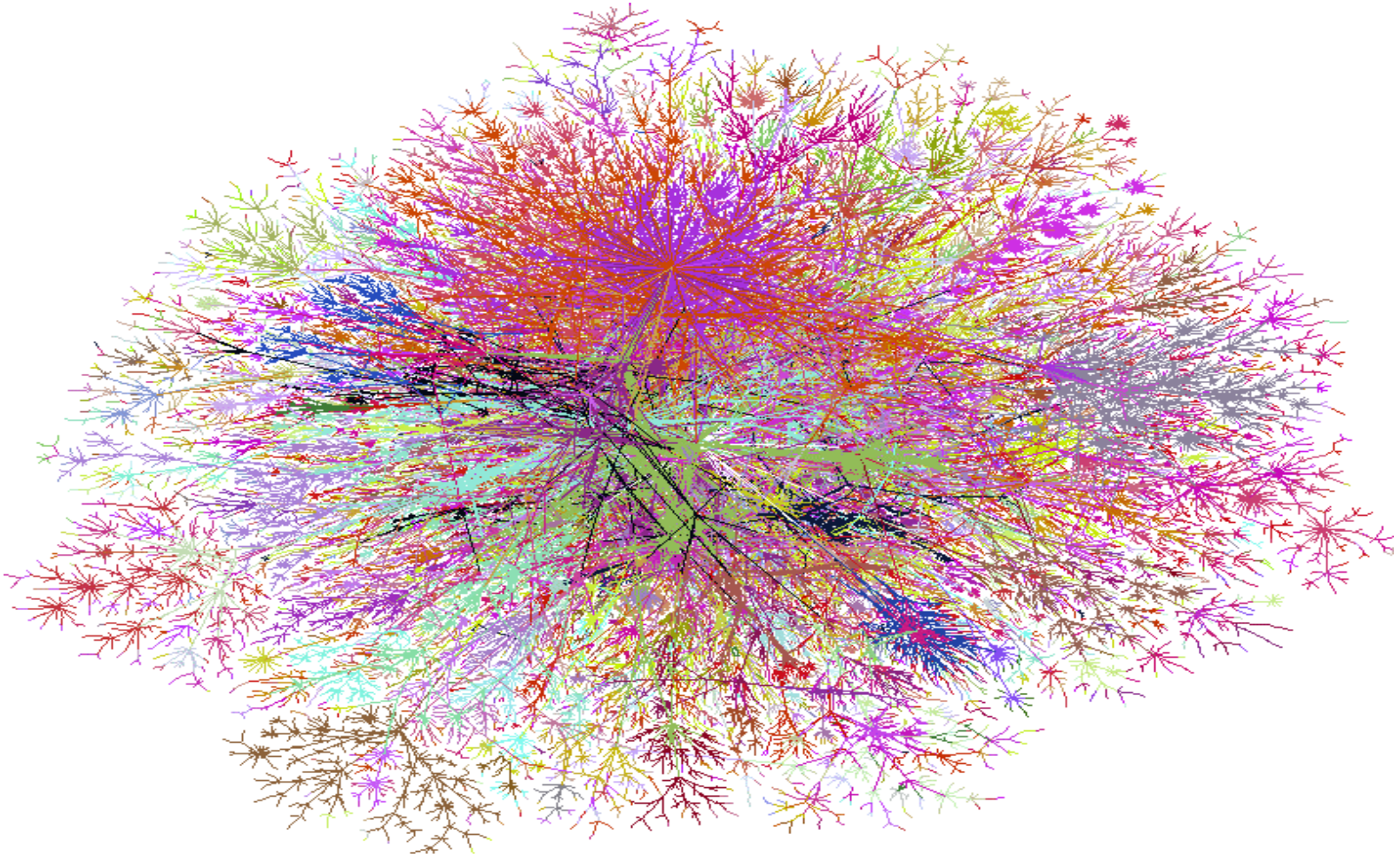
INTERNET SECURITY ALLIANCE

The Old Web



INTERNET SECURITY ALLIANCE

The Web Today

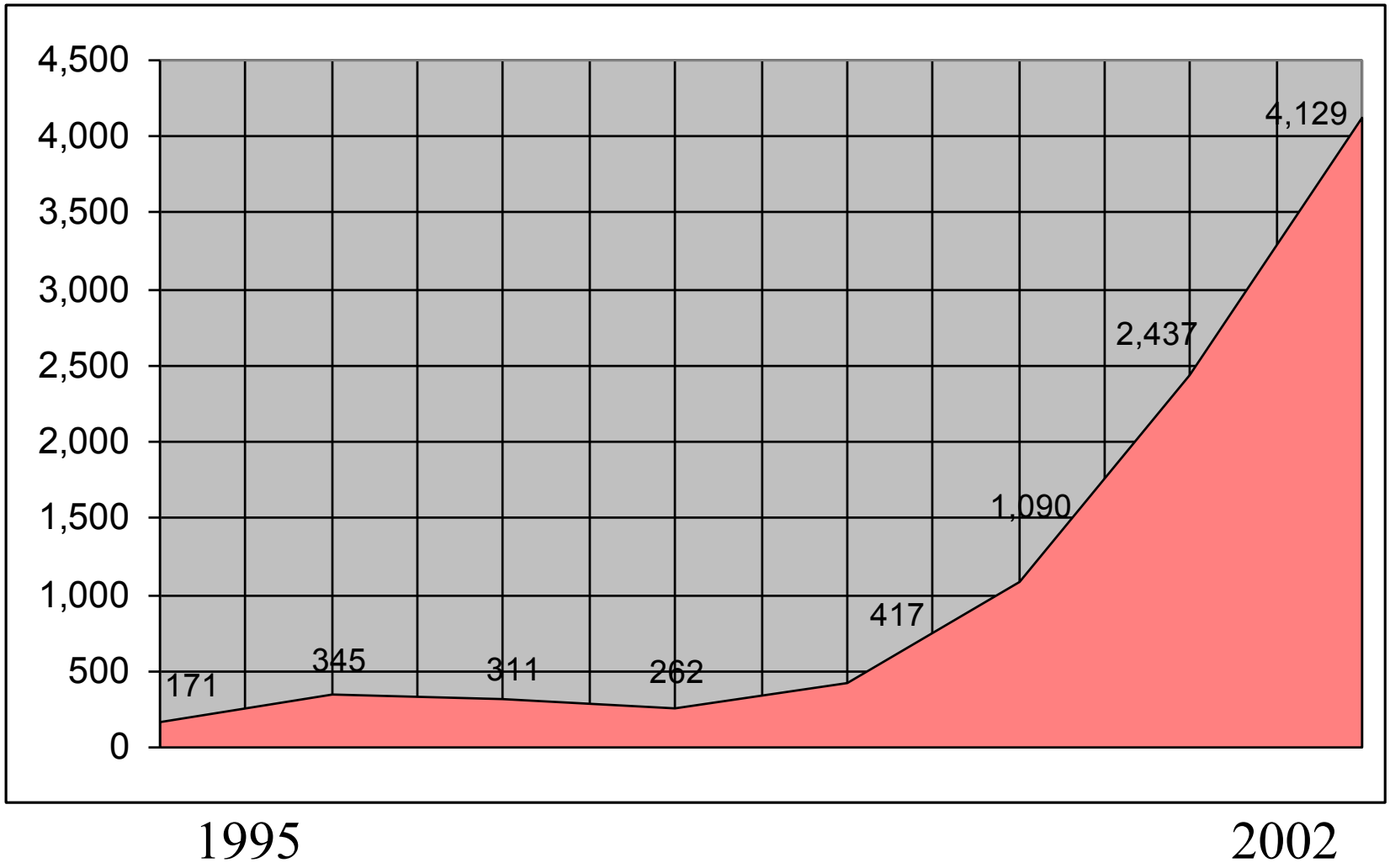


Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

INTERNET SECURITY ALLIANCE

The Earlier Threat:

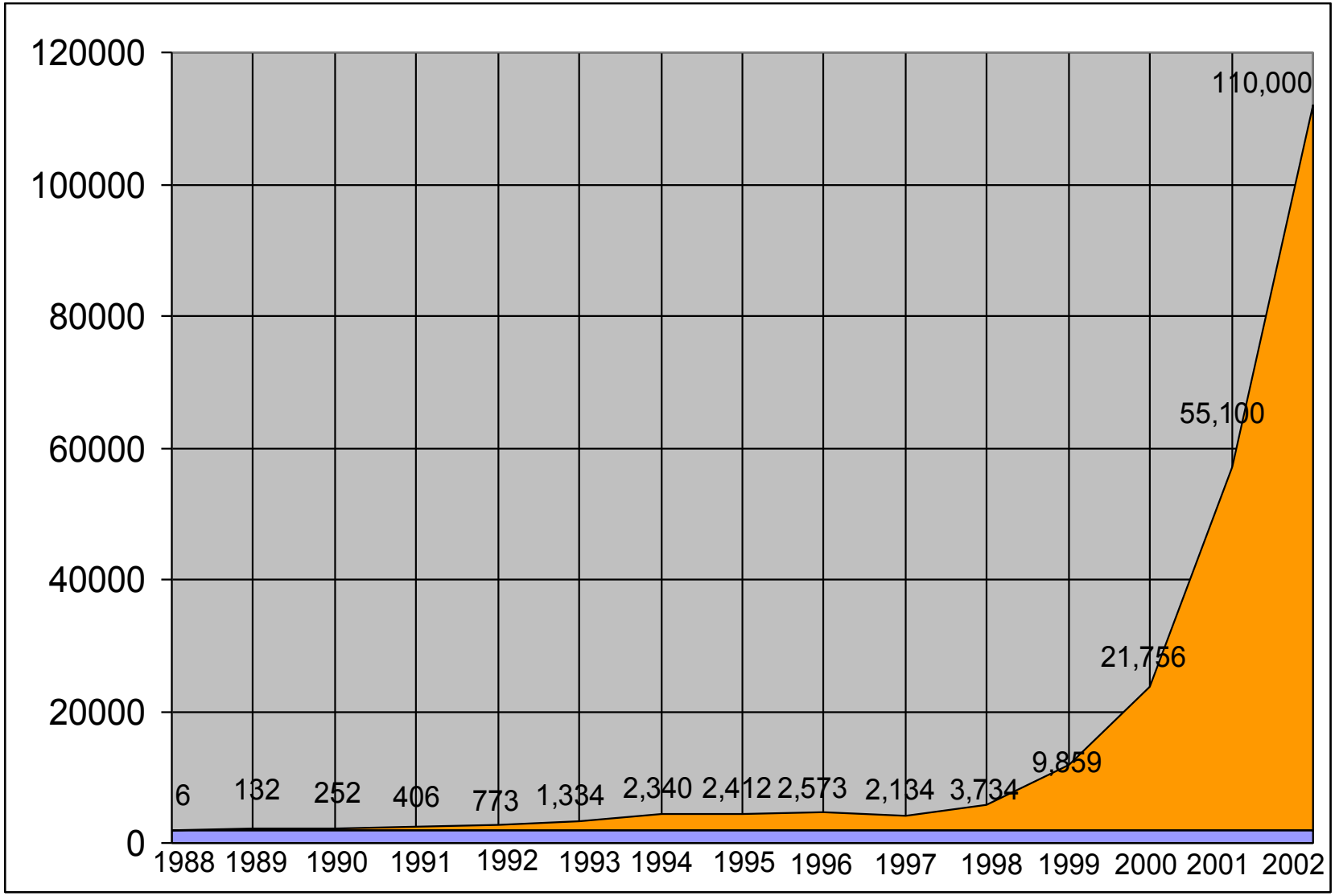
Growth in vulnerabilities (CERT/cc)



INTERNET SECURITY ALLIANCE

The Earlier Threat:

Cyber incidents



INTERNET SECURITY ALLIANCE

The Changing Threat

A fast-moving virus or worm pandemic is not the threat it was...

- 2002-2004 almost 100 medium-to-high risk attacks (“Slammer”; “SoBig”).
- 2005, there were only 6
- 2006 and 2007……. **Zero**

INTERNET SECURITY ALLIANCE

The Threat Landscape is Changing

Early Attacks

Who: Kids, researchers, hackers, isolated criminals

Why: Seeking fame & glory, use widespread attacks for maximum publicity

Risk Exposure: Downtime, business disruption, information loss, defacement

New Era Attacks

Organized criminals, corporate spies, disgruntled employees, terrorists

Seeking profits, revenge, use targeted stealth attacks to avoid detection

Direct financial loss via theft and/or embezzlement, breach disclosure, IP compromised, business disruption, infrastructure failure

INTERNET SECURITY ALLIANCE

The Threat Landscape is Changing

Early Attacks

Defense: Reactive AV signatures

Recovery: Scan & remove

Type: Virus, worm, spyware

New Era Attacks

Multilayer pre-emptive and behavioral systems

System wide, sometimes impossible without re-image of system

Targeted malware, root kits, spear phishing, ransomware, denial of service, back door taps, trojans, IW

INTERNET SECURITY ALLIANCE

Digital Defense? Maybe Not

- 29% of Senior Executives “acknowledged” that they did not know how many negative security events they had in the past year
- 50% of Senior Executives said they did not know how much money was lost due to attacks

Source: PricewaterhouseCoopers survey of 7,000 companies 9/06

INTERNET SECURITY ALLIANCE

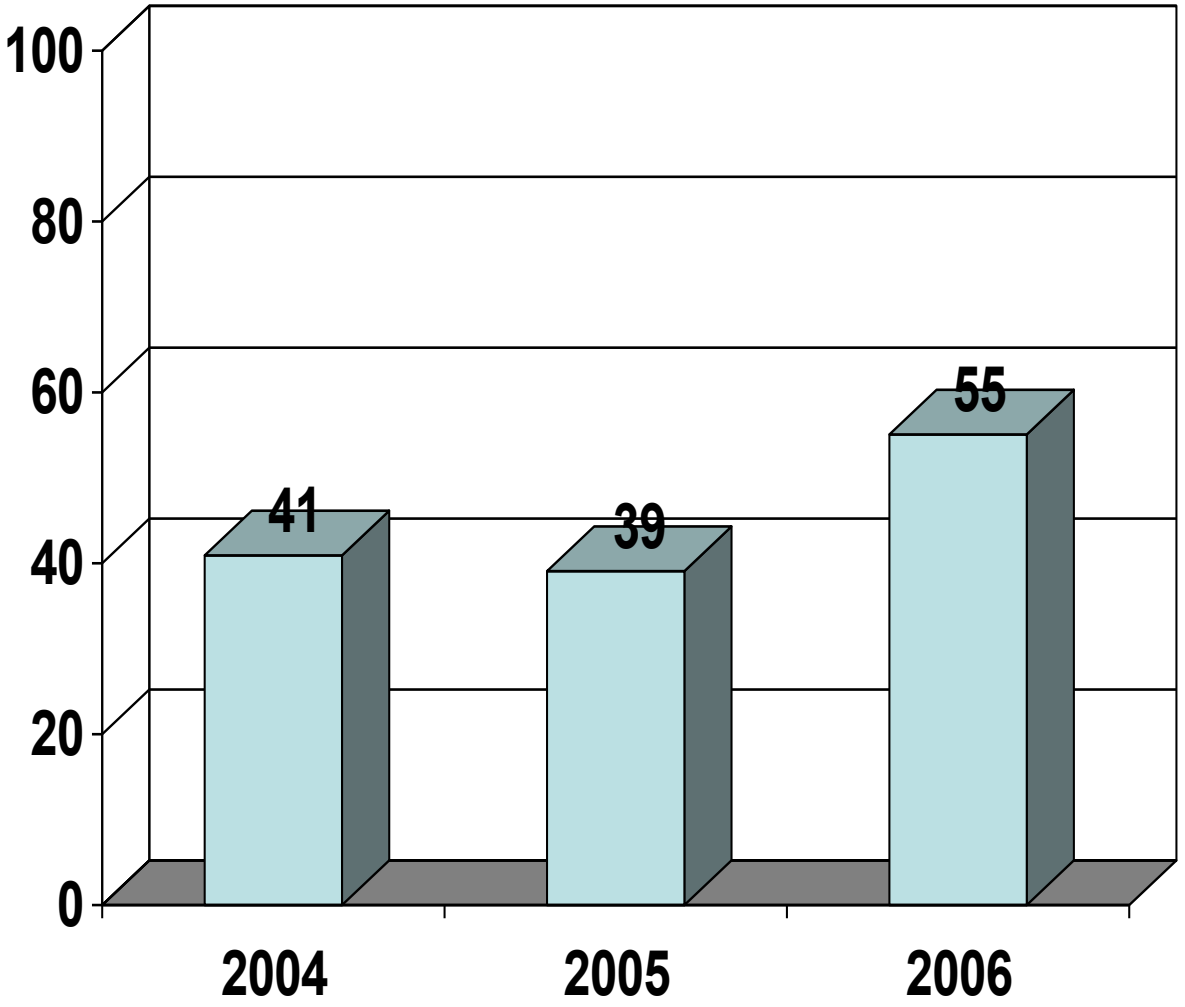
Digital Defense
Not So Much

- 23% of CTOs did not know if cyber losses were covered by insurance.
- 34% of CTOs thought cyber losses would be covered by insurance----and were wrong.
- “The biggest network vulnerability in American corporations are extra connections added for senior executives without proper security.”

---Source: DHS Chief Economist Scott Borg

INTERNET SECURITY ALLIANCE

Percentage of Participants Who Experienced an Insider Incident



INTERNET SECURITY ALLIANCE

Insider Incidents - 2006

	Total (%)	Insider (%)	Outsider (%)
Theft of IP	**30**	**63**	**45**
Theft of Proprietary Info.	**36**	**56**	**49**
Sabotage	**33**	**49**	**41**

Most common insider incidents in 2006 survey:

- rogue wireless access points (72%),
- theft of IP (64%),
- exposure of sensitive or confidential information (56%)

In 2006 insiders committed more theft of IP & proprietary information and sabotage than outsiders!

INTERNET SECURITY ALLIANCE

Economic Effects of Attacks

- 25% of our wealth-**--$3 trillion-**--is transmitted over the Internet daily
- FBI: Cyber crime cost business

  $26 billion (probably LOW estimate)

- Financial Institutions are generally considered the safest---their losses were up **450%** in the last year
- There are more electronic financial transfers than paper checks now: Only **1%** of cyber crooks are caught.

INTERNET SECURITY ALLIANCE

Cyber Attacks Effect Stock Price

"Investigations into the stock price impact of cyber attacks show that identified target firms suffer losses of one to five percent in the days after an attack. For the average *NYSE* corporation, price drops of these magnitudes translate into shareholder losses between $50 and $200 million."

Source: US Congressional Research Service 2004

INTERNET SECURITY ALLIANCE

Indirect Economic Effects

"While the tangible effects of a security incident can be measured in terms of lost productivity and staff time to recover and restore systems, the intangible effects can be of an order of magnitude larger. Intangible effects include the impact on an organizations trust relationships, harm to its reputation, and loss of economical and society confidence"

Source Carnegie Mellon CyLab 2007