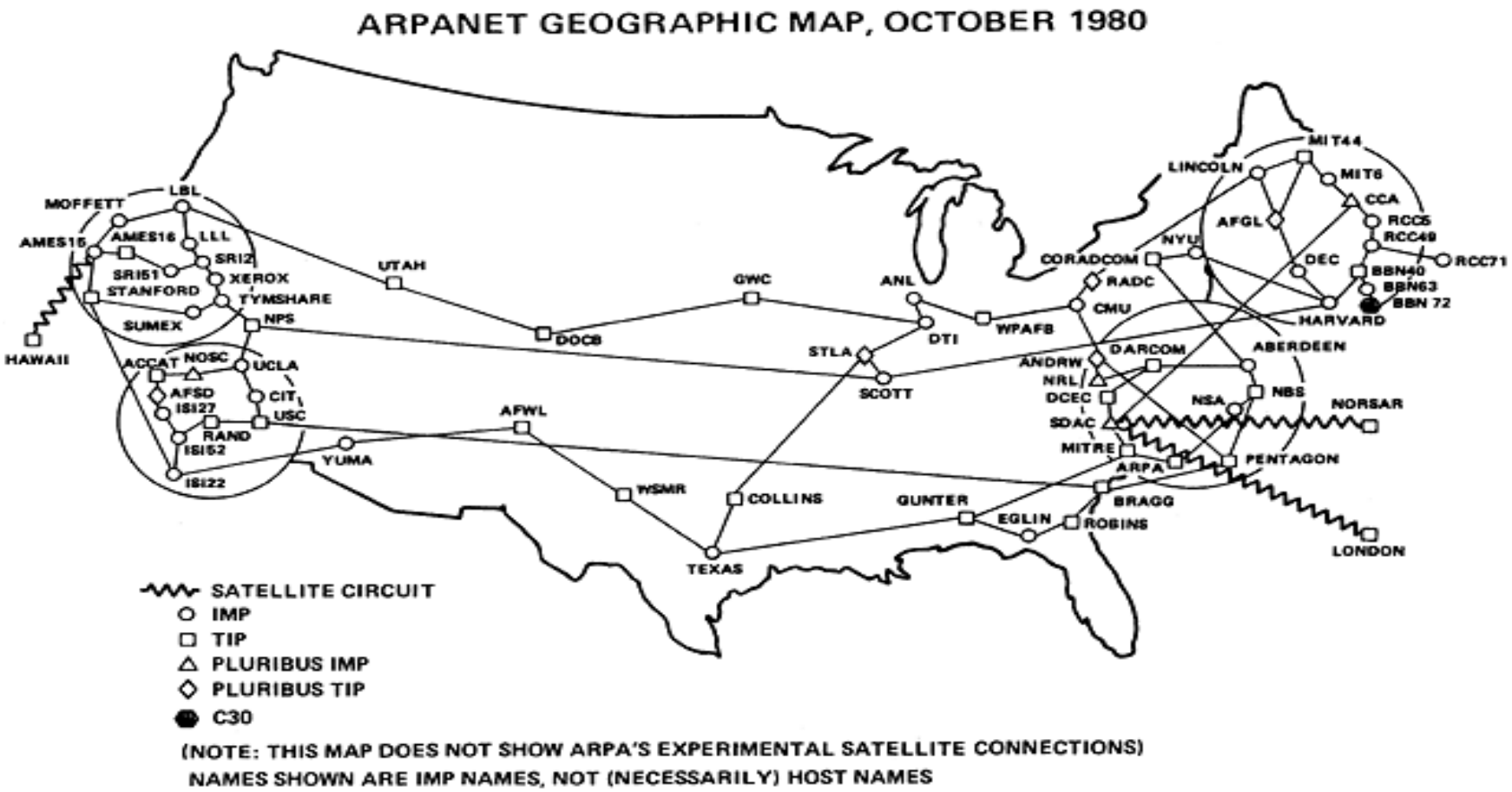
Larry Clinton
Operations Officer
Internet Security Alliance
lclinton@eia.org
703-907-7028
202-236-0001

Presentation Outline

- The Growing Problem of Cyber Security
- Traditional Solutions and Why They Won't Work
- A New Paradigm (tools and incentives)
- Bringing it all Together

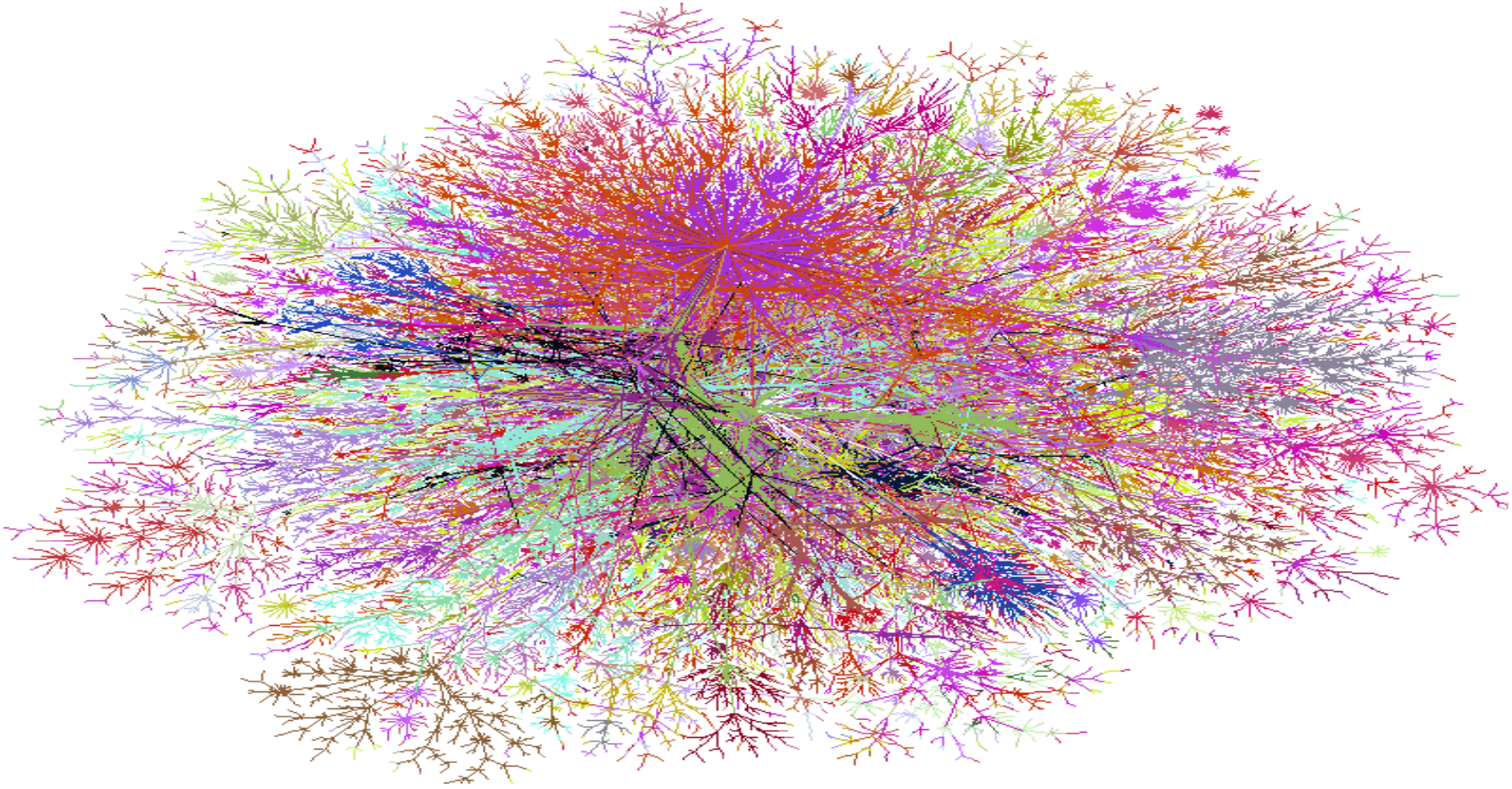
INTERNET SECURITY ALLIANCE

The Past



INTERNET SECURITY ALLIANCE

The Present

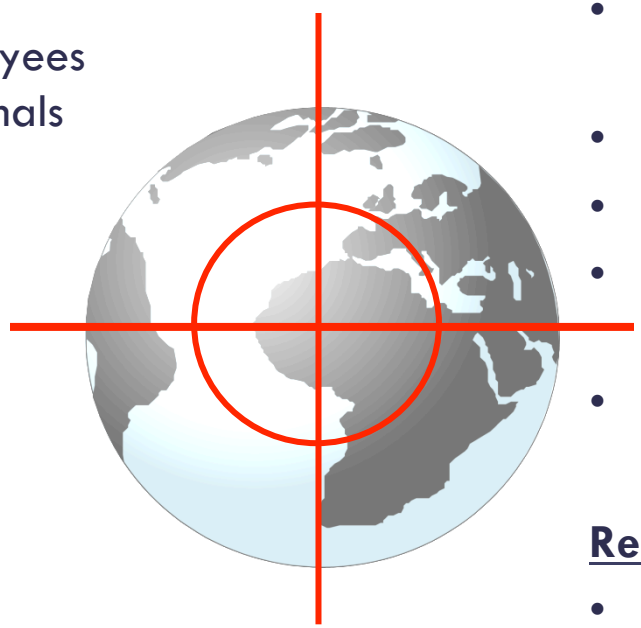


Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

The Threats – The Risks

Human Agents

- Hackers
- Disgruntled employees
- White collar criminals
- Organized crime
- Terrorists



Exposures

- Information theft, loss & corruption
- Monetary theft & embezzlement
- Critical infrastructure failure
- Hacker adventures, e-graffiti/ defacement
- Business disruption

Methods of Attack

- Brute force
- Denial of Service
- Viruses & worms
- Back door taps & misappropriation,
- Information Warfare (IW) techniques

Representative Incidents

- Code Red, Nimda, Sircam
- CD Universe extortion, e-Toys "Hactivist" campaign,
- Love Bug, Melissa Viruses

The Threats – The Risks

Terrorists may view cyber-attacks – standing alone or with a coordinated physical attack – as a way to cause economic harm.

Considering that critical infrastructures, upon which the American economy depend, are increasingly electronic and interconnected, attacks in or through cyberspace arguably support the terrorist *modus operandi*

Bin Laden: Goal is to bankrupt U.S.

Al-Jazeera releases full transcript of al Qaeda leader's tape

Monday, November 1, 2004 Posted: 8:07 PM EST (0107 GMT)

(CNN) -- The Arabic-language network Al-Jazeera released a full transcript Monday of the most recent videotape from Osama bin Laden in which the head of al Qaeda said his group's goal is to force America into bankruptcy.

Osama bin Laden delivers a videotaped message broadcast on Arabic-language network Al-Jazeera.

Al-Jazeera aired portions of the videotape Friday but released the full transcript of the entire tape on its Web site Monday.

"We are continuing this policy in bleeding America to the point of bankruptcy. Allah willing, and nothing is too great for Allah," bin Laden said in the transcript.

He said the mujahedeen fighters did the same thing to the Soviet Union in Afghanistan in the 1980s, "using guerrilla warfare and the war of attrition to fight tyrannical superpowers."

"We, alongside the mujahedeen, bled Russia for 10 years until it went bankrupt and was forced to withdraw in defeat," bin Laden said.

He also said al Qaeda has found it "easy for us to provoke and bait this administration."

"All that we have to do is to send two mujahedeen to the furthest point east to raise a piece of cloth on which is written al Qaeda, in order to make generals race there to cause America to suffer human, economic and political losses without their achieving anything of note other than some benefits for their private corporations," bin Laden said.

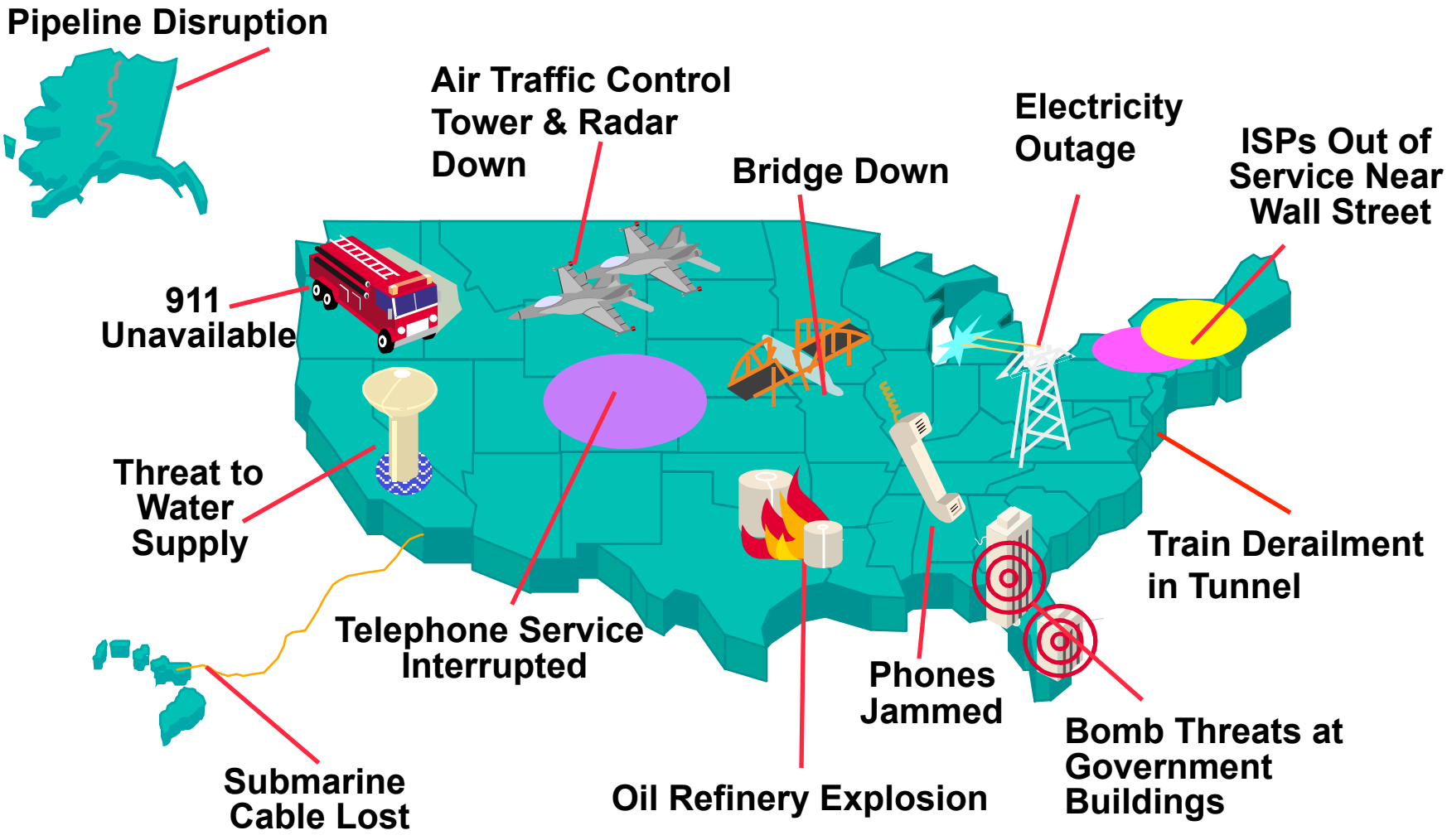
Al-Jazeera executives said they decided to post the entire speech because rumors were circulating that the network omitted parts that "had direct threats toward specific states, which was totally untrue."

"We chose the most newsworthy parts of the address and aired them. The rest was used in lower thirds in graphics format," said one official.

U.S. intelligence officials Monday confirmed that the transcript made public Monday by Al-Jazeera was a complete one.

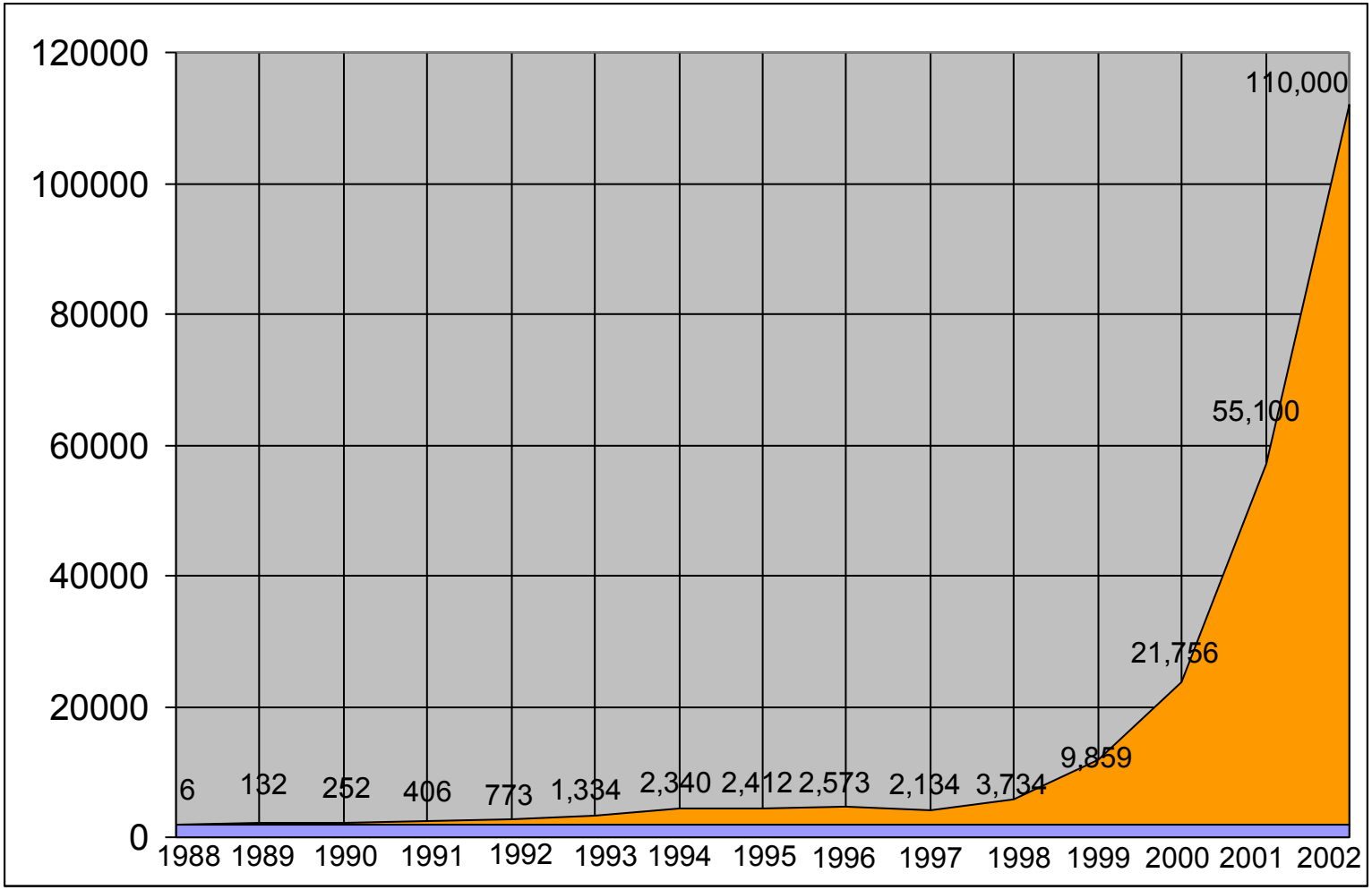
INTERNET SECURITY ALLIANCE

The Threats – The Risks

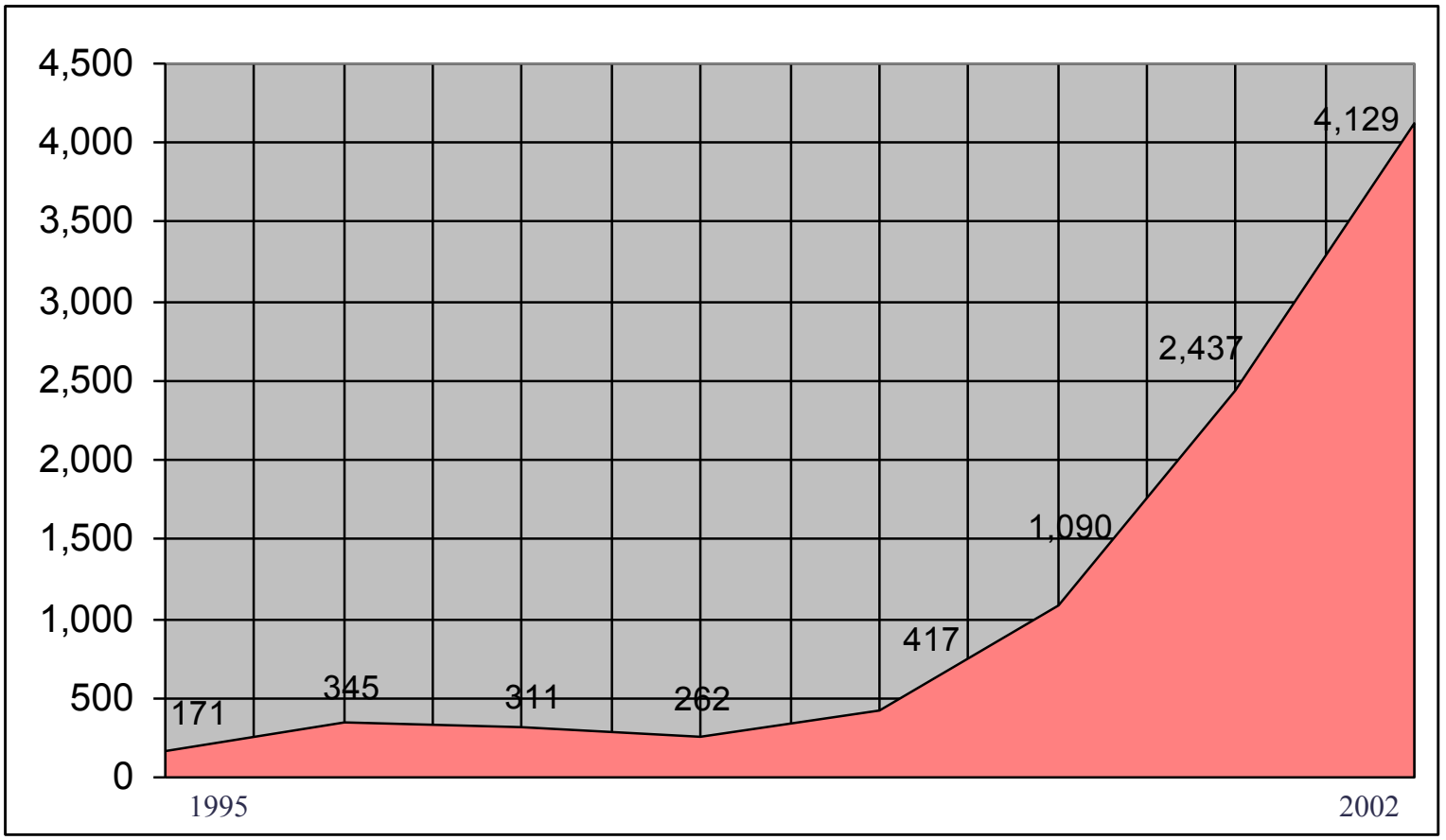


INTERNET SECURITY ALLIANCE

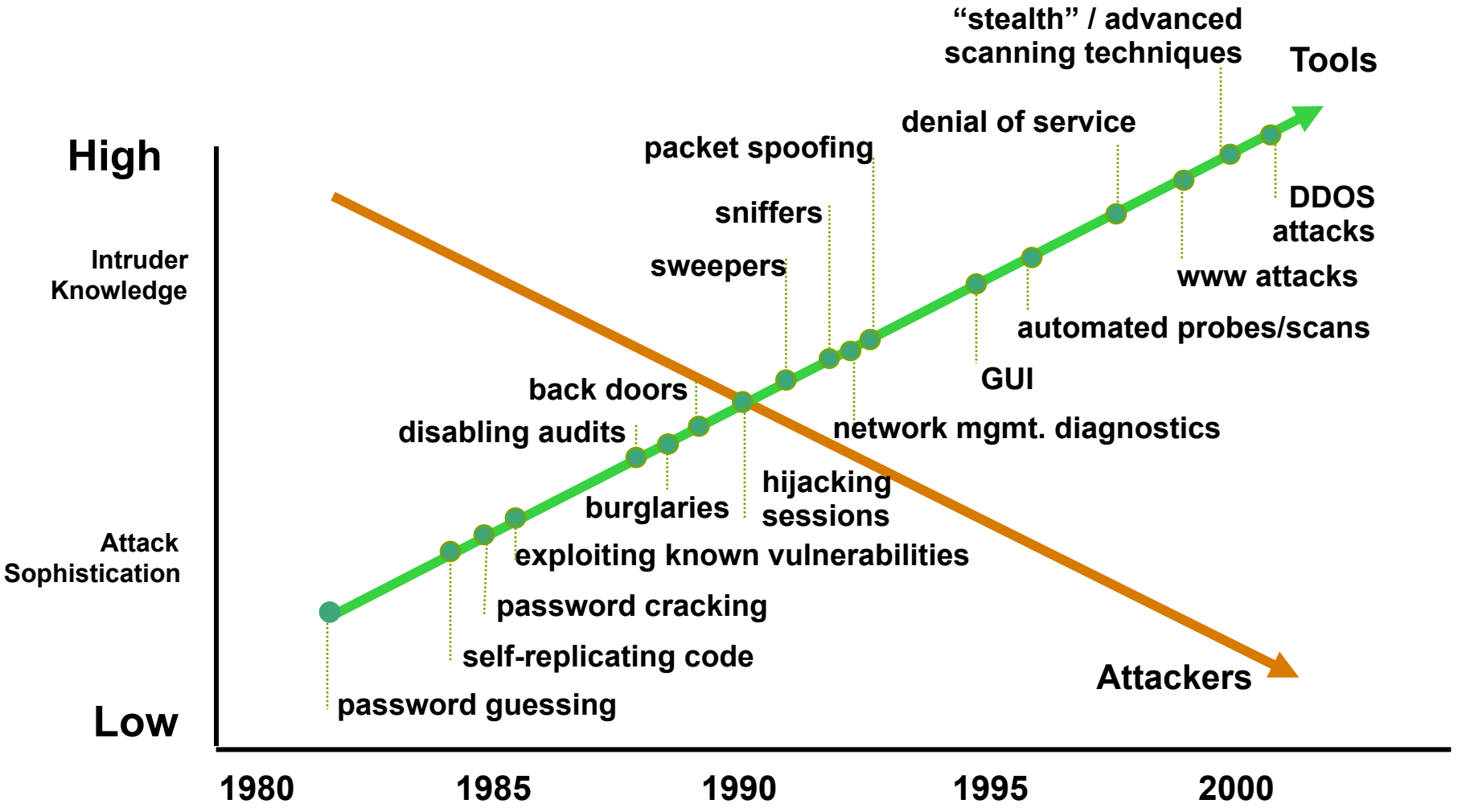
Growth in Incidents Reported to the CERT/CC



The Dilemma: Growth in Number of Vulnerabilities Reported to CERT/CC

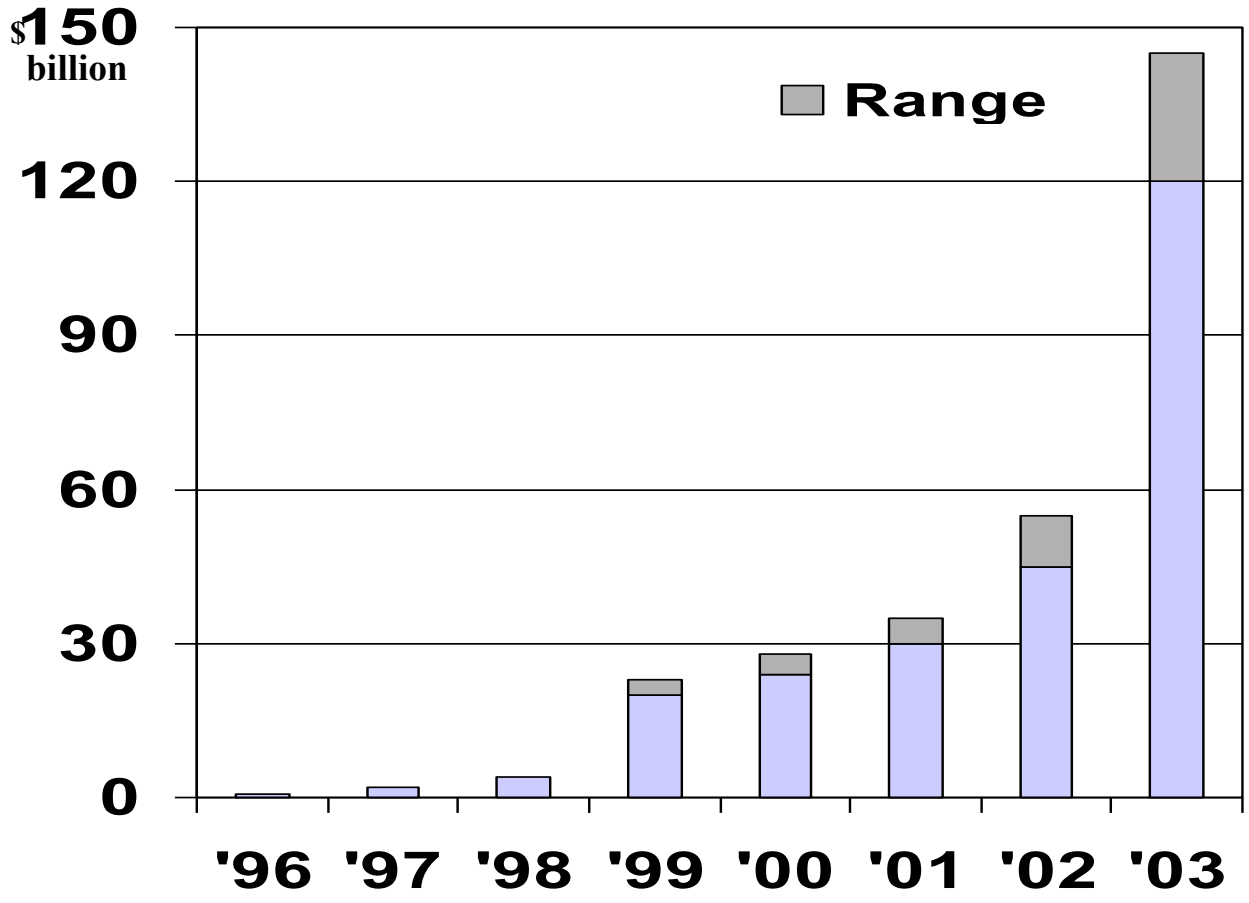


Attack Sophistication v. Intruder Technical Knowledge



INTERNET SECURITY ALLIANCE

Computer Virus Costs (in billions)



(Through Oct 7)

Traditional Solutions & Why They Won't Work

- Technology Solutions ("its like Y2K")
- Government Regulation ("just mandate security")
- Great Wall of China ("Secure our boarders")

Cyber Security is not an "IT" Problem

Y2K WAS:

- Finite
- Passive
- Not an attack

- Cyber Security requires people, processes, procedures and management of the risk.

A Risk Management Approach is Needed

"Installing a network security device is not a substitute for a constant focus and keeping our defenses up to date… There is no special technology that can make an enterprise completely secure."

– *National Plan to Secure Cyberspace, 2/14/03*

You Can't Mandate Cyber Security

- Policy must address the Internet as a new technology
- No one owns the Internet
- It is constantly evolving
- International operation makes regulation difficult
- Mandates will truncate innovation and the economy
- Beware the "Roadmap" for mischief

Putnam Legislation

- Risk Assessment
- Risk Mitigation
- Incident Response Program
- Tested Continuity plan
- Updated Patch management program
- Putnam has said it won't work.

Build a Great Wall around your Organization

- The Internet has no walls, no boarders -- No one actually owns it.

- You are only as secure as the organizations you interconnect with -- And that's pretty much everyone.

- The Internet is Interdependent, and Security, therefore, is Interdependent

Attacks are Inevitable

- "According to the US Intelligence community, American networks will be increasingly targeted by malicious actors both for the data and the power they possess."

- *National Strategy to Secure Cyberspace, 2/14/02*

A New paradigm:Tools and Incentives

TOOLS

INCENTIVES NOT MANDATES

- Information Sharing
- Best Practice Development
- Standards/Certification/Qualification
- Training
- Policy Development
- A Total Systems Approach

Benefits of Information Sharing Organizations

- May lesson the likelihood of attack

  "Organizations that share information about computer break ins are less attractive targets for malicious attackers." – NYT 2003

- Participants in information sharing have the ability to better prepare for attacks and respond to them.

Old and New Info Sharing

- 2002 ISAlliance informed its membership about SNMP event 6 months ahead of time---No ISAlliance members affected
- 2003 ISAlliance informed Membership about Slammer Vulnerability 9 months ahead of time---NO ISA members effected
- 2004---Events move too fast
- Now we focus on forecasting not analysis

Adopt and Implement Best Practices

- Cited in U.S. National Draft Strategy to Protect Cyber Space
- Endorsed by TechNet for CEO Security Initiative
- Small Bus. Best Pract.

Endorsed:DHS;ABA;

NAM;EIA; NCSA etc.

Common Sense Guide
Top Ten Practice Topics

- Practice #1: General Management
- Practice #2: Policy
- Practice #3: Risk Management
- Practice #4: Security Architecture & Design
- Practice #5: User Issues
- Practice #6: System & Network Management
- Practice #7: Authentication & Authorization
- Practice #8: Monitor & Audit
- Practice #9: Physical Security
- Practice #10: Continuity Planning & Disaster Recovery

Cooperative work on assessment/certification

- TechNet CEO Self-Assessment Program
- Bring cyber security to the C-level based on ISA Best Practices
- Create a baseline of security even CEOs can understand
- American Security Consortium 3-Party Assessment program
- Risk Preparedness Index for assessment and certification
- Develop quantitative independent ROI for cyber security

ISAlliance/CERT Training

- Concepts and Trends In Information Security
- Information Security for Technical Staff
- OCTAVE Method Training Workshop
- Overview of Managing Computer Security Incident Response Teams
- Fundamentals of Incident Handling
- Advanced Incident Handling for Technical Staff
- Information Survivability an Executive Perspective

ISAlliance Incentive Model

- Model Programs for market Incentives

---AIG

---Visa

SemaTech Program

Tax Incentives

Liability Carrots

Procurement Model

Research and Development

----Nortel

----Verizon

Congress Appoints CISWG

- INCENTIVES & LIABILITY GROUP FOUND INCENTIVES FOR PUB & PRIVATE SECTOR

--Insurance Incentives

--Liability Incentives

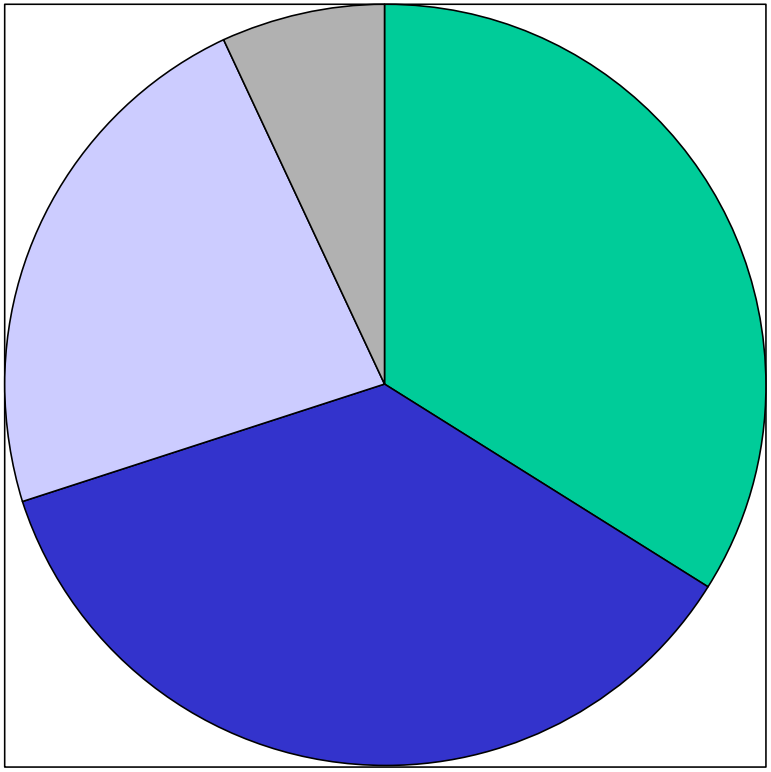
--Tax Incentives

--Expedited Permitting

--FEMA credits

--Awards Programs

Chief Technology Officers' Knowledge of their Cyber Insurance



- **34% Incorrectly thought they were covered**
- **36% Did not have Insurance**
- **23% Did not know if they had insurance**
- **7% Knew that they were insured by a specific policy**

ISAlliance Cyber-Insurance Program

- Coverage for members
- Free assessment through AIG
- Market incentive for increased security practices
- 10% discount off best prices from AIG
- Additional 5% discount for implementing ISAlliance Best Practices (July 2002)

ISAlliance Qualification Program

- No Standardized Certification Program exists or will exist soon
- ISAlliance, in cooperation with Big 4 and insurance industry, create quantitative measurement for "qualification" for ISA discounts as proxy for certification
- ISA works with CMU CyLab on Certification

A Coherent 10 step Program of Cyber Security

1. Members and CERT create best practices

2. Members and CERT share information

3. Cooperate with industry and government to develop new models and products consistent with best practices

A Coherent Program of Cyber Security

4. Provide Education and Training programs based on coherent theory and measured compliance

5. Coordinate across sectors

6. Coordinate across boarders

A coherent program

7. Develop the business case (ROI) for improved cyber security
8. Develop market incentives and tools for consistent maintenance of cyber security
9. Integrate sound theory and practice and evaluation into public policy
10. Constantly expand the perimeter of cyber security by adding new members

INTERNET SECURITY ALLIANCE

Sponsors

Larry Clinton
Operations Officer
Internet Security Alliance
lclinton@eia.org
703-907-7028
202-236-0001