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

INTERNET SECURITY ALLIANCE

- Who we are
- What we believe
- Why we must take action
- What should business should do?
- A coherent program of cyber security

The Internet Security Alliance

The **Internet Security Alliance** is a collaborative effort between Carnegie Mellon University's ***Software Engineering Institute (SEI)*** and its ***CERT Coordination Center (CERT/CC)*** and the ***Electronic Industries Alliance (EIA)***, a federation of trade associations with over 2,500 members.

INTERNET SECURITY ALLIANCE

Sponsors

INTERNET SECURITY ALLIANCE

What We Believe

INTERNET SECURITY ALLIANCE

What We Believe

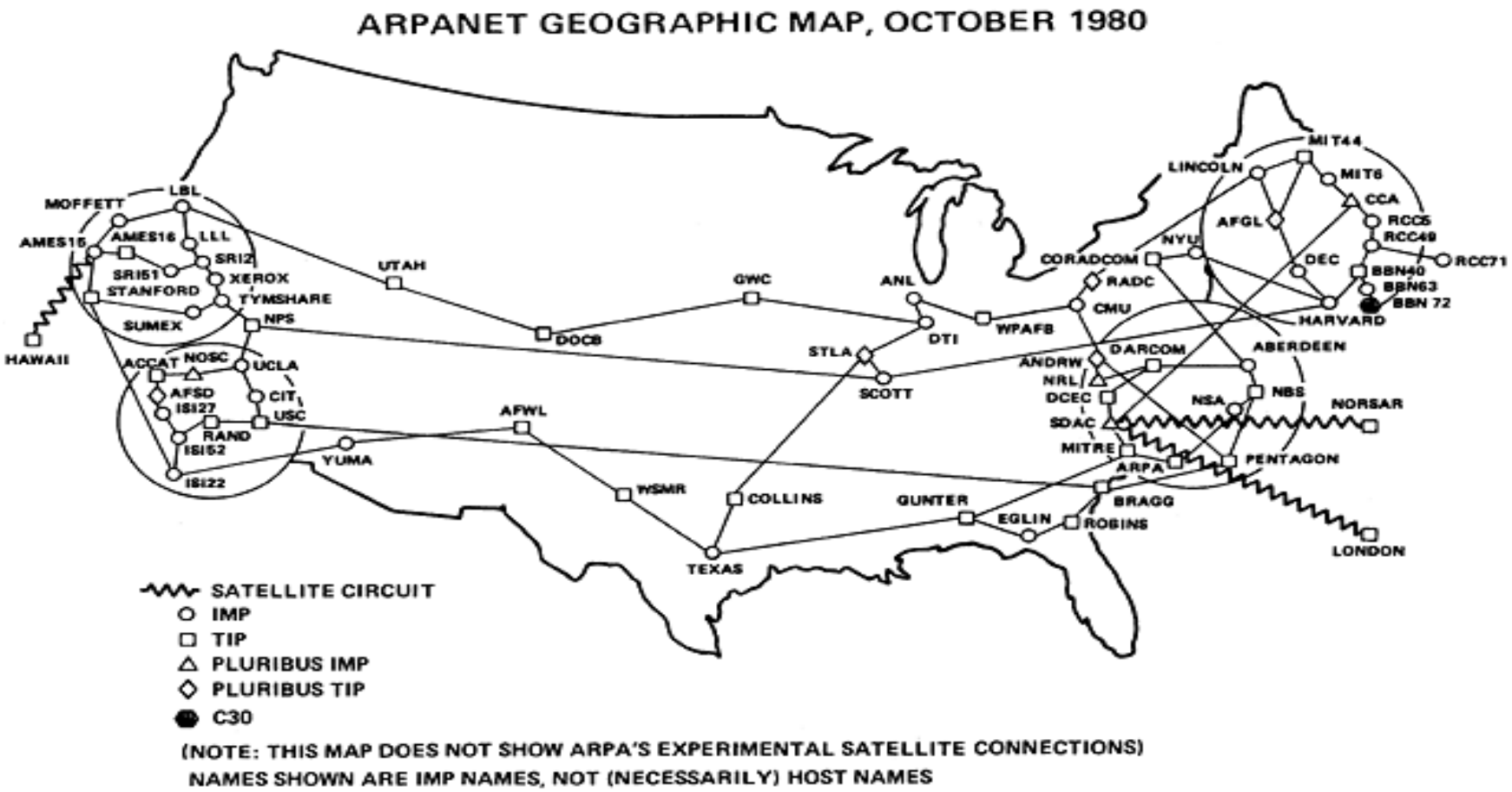
- Internet is privately owned and operated
- It's our responsibility to demonstrate leadership
- There will be national and international attempts to regulate
- Government mandates are doomed to fail
- Government mandates could be dangerous
- We must show real progress to forestall regulation

INTERNET SECURITY ALLIANCE

Why We Must Act

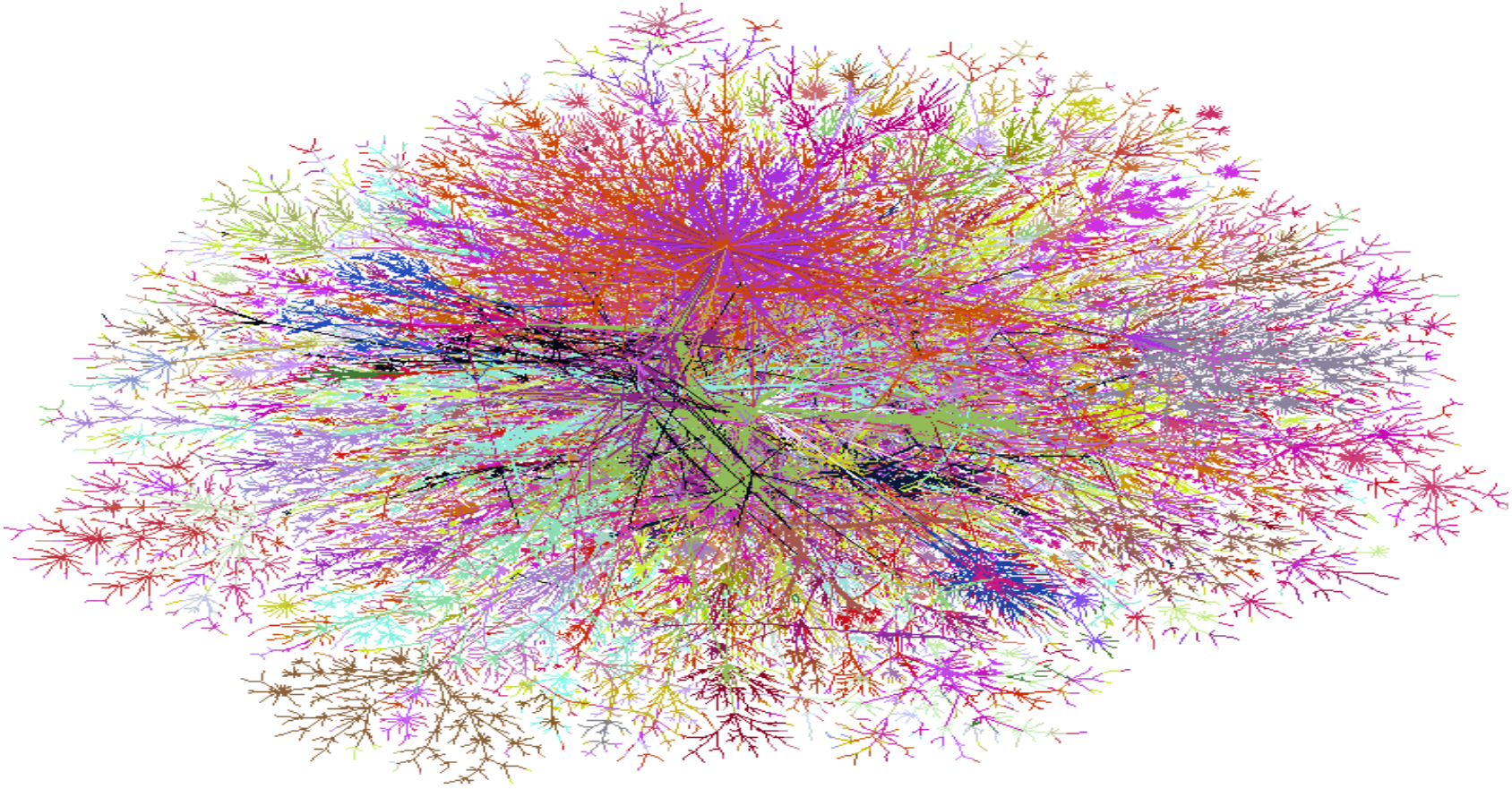
INTERNET SECURITY ALLIANCE

The Past



INTERNET SECURITY ALLIANCE

The Present

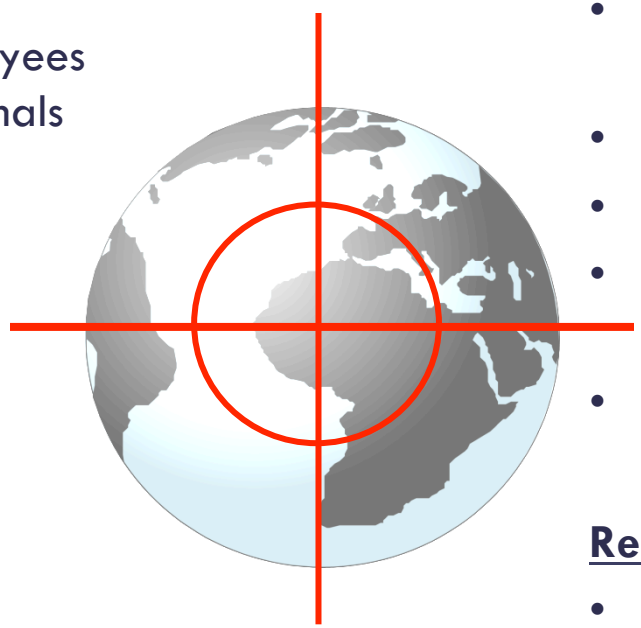


Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

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

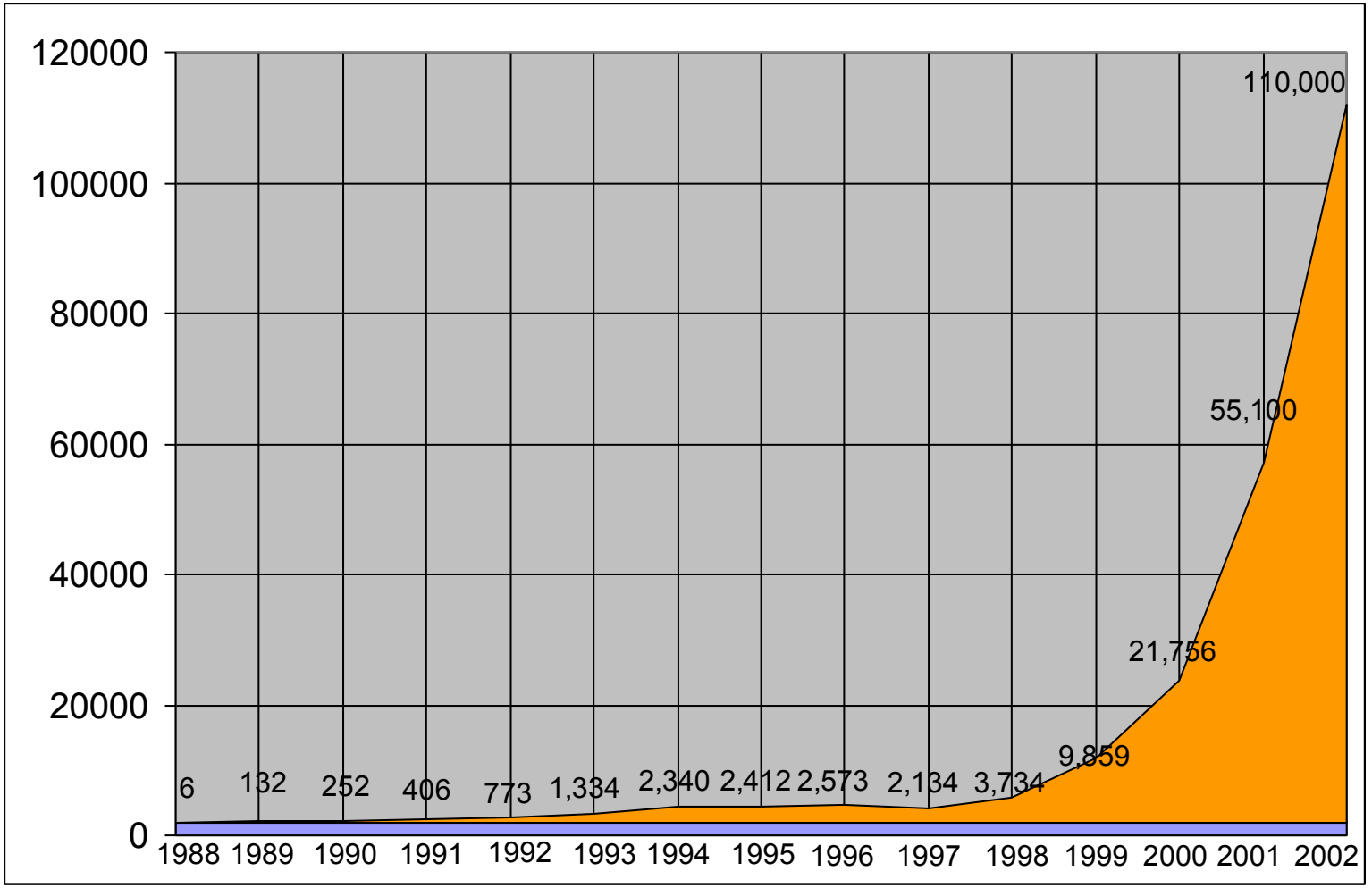
- Brute force
- Denial of Service
- Viruses & worms
- Back door taps & misappropriation,
- Information Warfare (IW) techniques

Representative Incidents

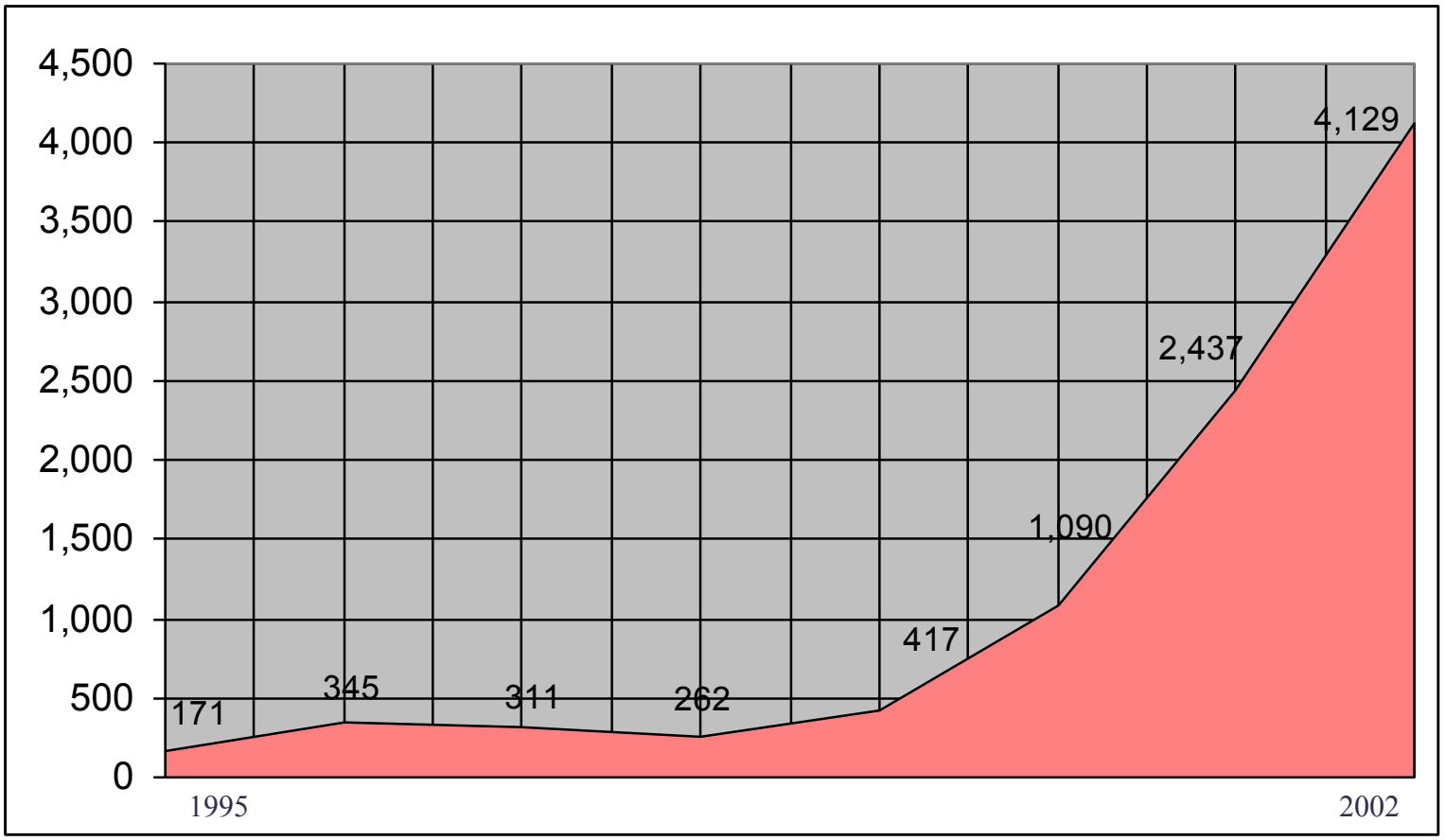
- Code Red, Nimda, Sircam
- CD Universe extortion, e-Toys "Hactivist" campaign,
- Love Bug, Melissa Viruses

INTERNET SECURITY ALLIANCE

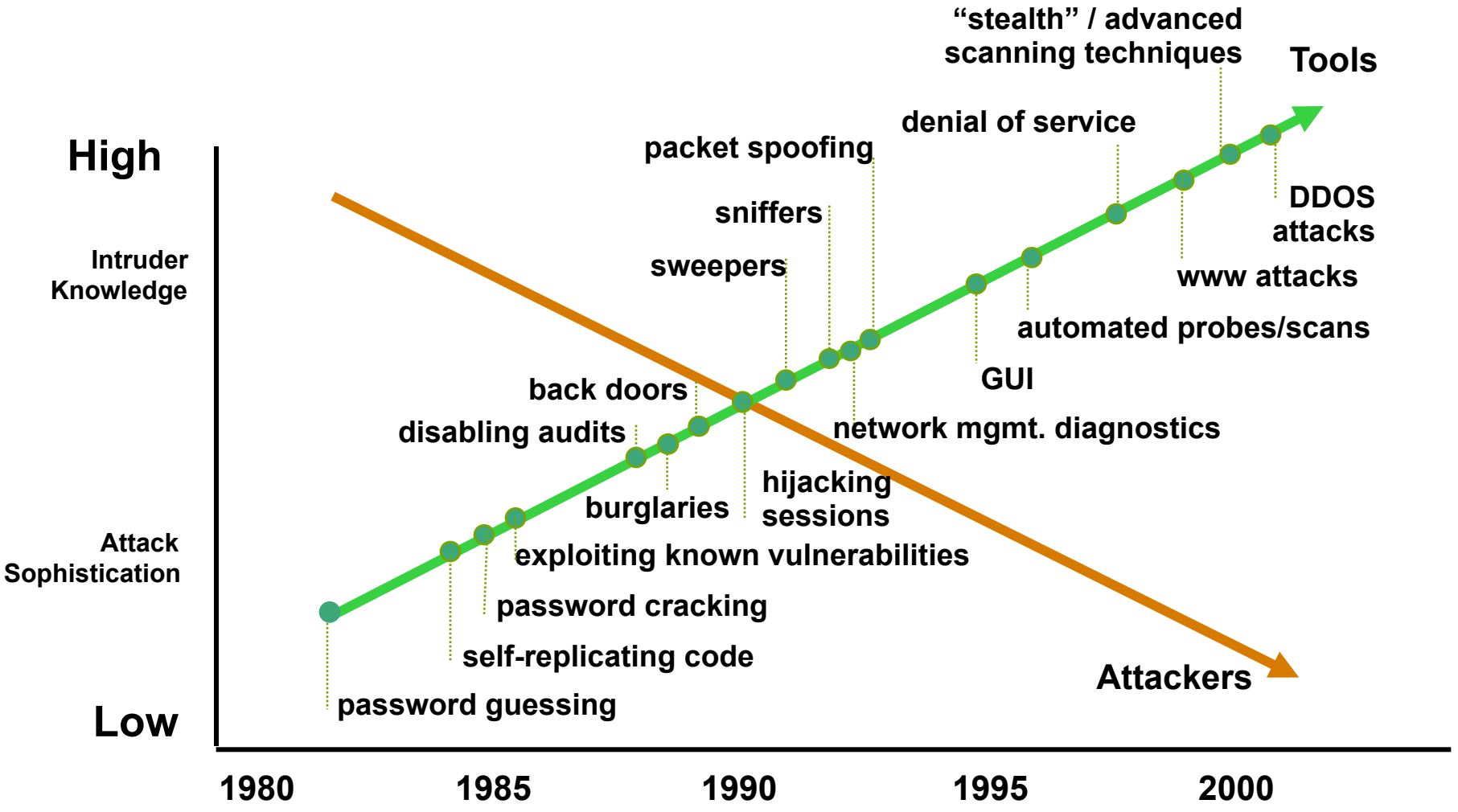
Growth in Incidents Reported to the CERT/CC



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

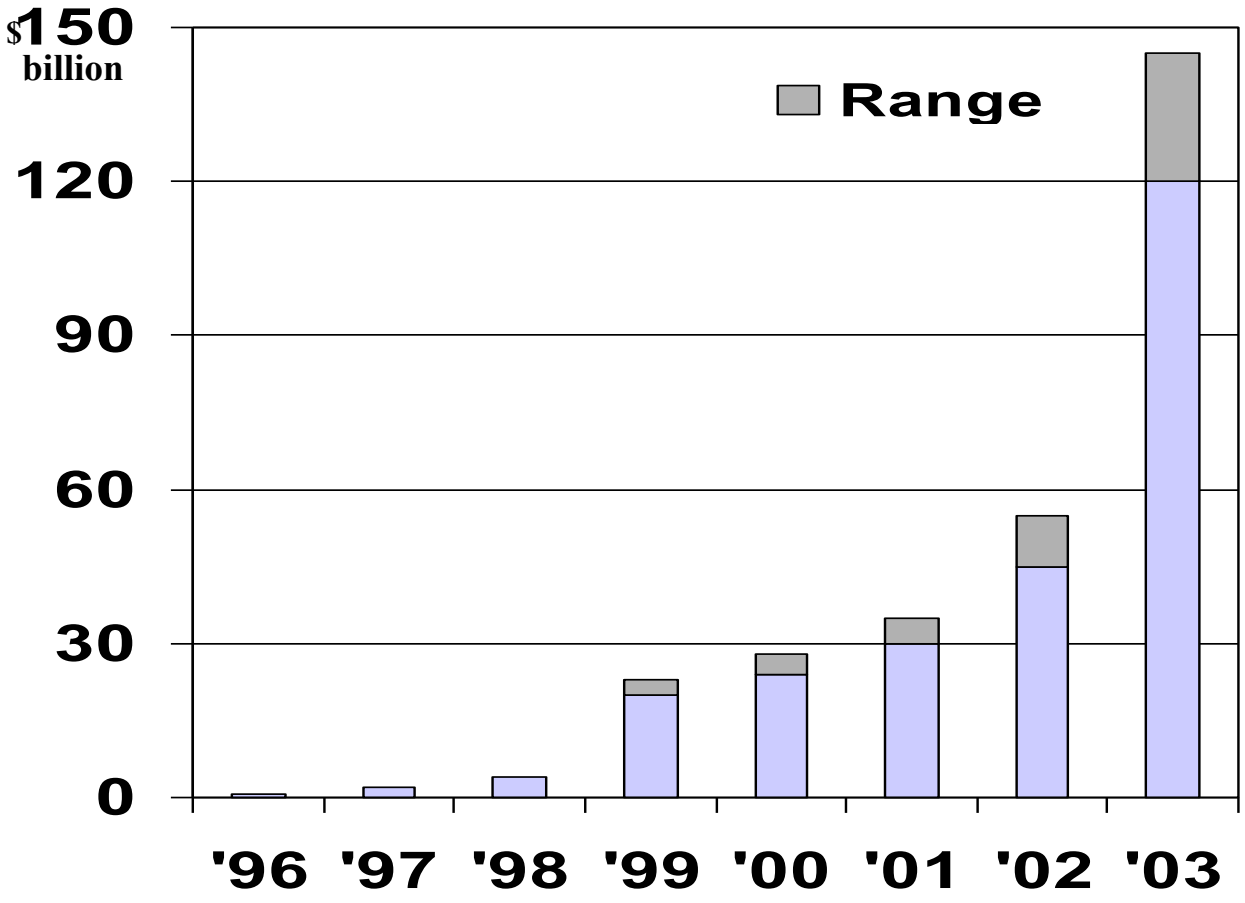


Attack Sophistication v. Intruder Technical Knowledge



INTERNET SECURITY ALLIANCE

Computer Virus Costs (in billions)



(Through Oct 7)

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*

- The significance of the NIMDA attack was not in the amount of damage it caused but it foreshadows what we could face in the future" – *CIPB*

- "Things are getting worse not better." – *NYT 1/30/03*

Won't Advanced Technology Protect Us?

"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*

INTERNET SECURITY ALLIANCE

What Should You Do?

The Private Sector and National CyberSecurity

- US government is holding companies responsible for their security
- Fiduciary and oversight responsibility is being enforced
- Corporate governance, vision and goals reside at the executive level

INTERNET SECURITY ALLIANCE

1. Invest in Cyber Security
2. Consider Risk Mitigation
3. Become Involved in the Policy Debate
4. Implement Best practices
5. Join with us in information sharing

Step 1 Invest in Cyber Security

- US Government increasing spending 64 % for cyber security.

*****

For Business there is a 21% ROI for early incorporation of security

- *CSO Magazine 12/02*

Step 2. Become Involved in Policy Debate

- Calls for security mandates are being heard federal, state and internationally
- The structures for dealing with these issues are being erected now
- If industry wants to maintain control over the Internet they must make it secure
- A coordinated message is needed

Putnam Legislation

- Risk Assessment
- Risk Mitigation
- Incident Response Program
- Tested Continuity plan
- Updated Patch management program

Ridge May Support Concept

"Companies that sell stock to the public may be required to disclose what they are doing to protect their computer systems," Homeland Security Secratery Tom Ridge said.

---Atlanta Journal Constitution October 10, 2003

Mandates or Incentives ?

- Government mandates standards ?
- SEC reporting ?
- California style reporting ?
- Tax Credits for security investment?
- Insurance Discounts?
- Model Private Sector Programs ?

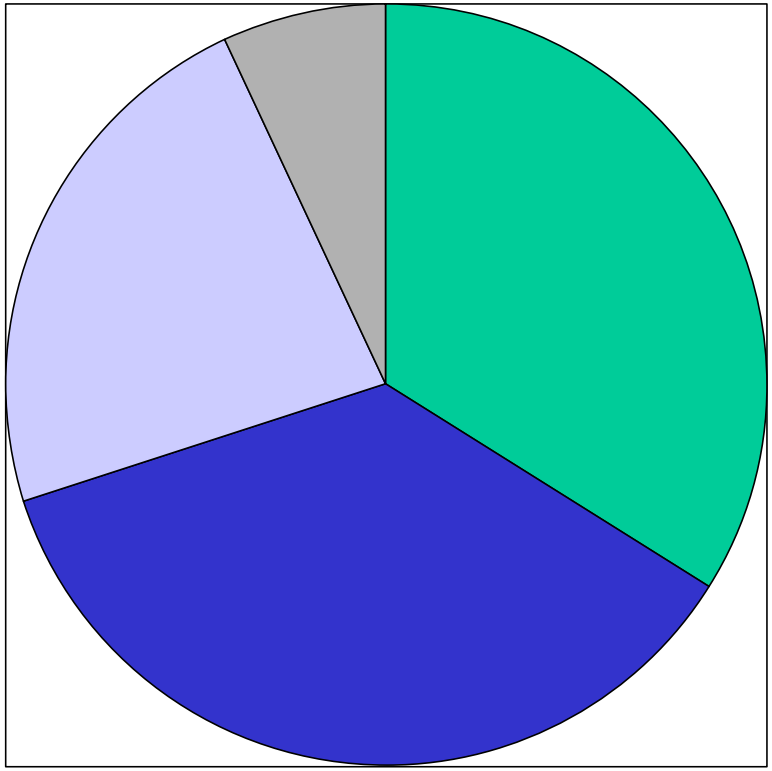
AIG	Visa
Nortel	Verizon

Step 3. Risk Mitigation/Cyber Insurance

Consider Cyber Insurance

- Are you covered?
- Should you be covered?

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)

Step 4. Adopt and Implement Best Practices

- Cited in US National Draft Strategy to Protect Cyber Space (September 2002)
- Endorsed by TechNet for CEO Security Initiative (April 2003)
- Endorsed US India Business Council (April 2003)

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 Prearadness Index for assessment and certification
- Develop quantitative independent ROI for cyber security

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

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

INTERNET SECURITY ALLIANCE

Macro Step 5

Join and participate in a cyber-security information sharing organization

Benefits

- Share critical information across industries and across national boarders
- Provide secure setting to work on common problems
- Provide economic incentive programs
- Develop model industry programs
- Give policy makers an alternative to regulatory models

CERT Knowledgebase Examples

CERT Coordination Center

Figure 3: Special Communications index page

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

Benefits of Information Sharing Organizations

- SNMP vulnerability
  - CERT notified Alliance members Oct. 2001
  - Publicly disclosed Feb. 2002
- Slammer worm
  - CERT notified Alliance members May 2002
  - Worm exploited Jan. 2003

Why ISA Info Sharing Works

- Carnigie Mellon/CERT leadership and credibility
- History, and regularity build up trust
- Enforce the rules builds trust
- Cross-sector/international model lessens competitive concerns
- Success breeds greater success

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 for consistent maintenance of cyber security
9. Integrate sound theory and practice into public policy
10. Constantly expand the perimeter of cyber security by adding new members

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