



**INTERNET  
SECURITY  
ALLIANCE**

---

Larry Clinton  
Operations Officer  
Internet Security Alliance  
[lcClinton@eia.org](mailto:lcClinton@eia.org)  
703-907-7028  
202-236-0001



# *Presentation Outline*

---

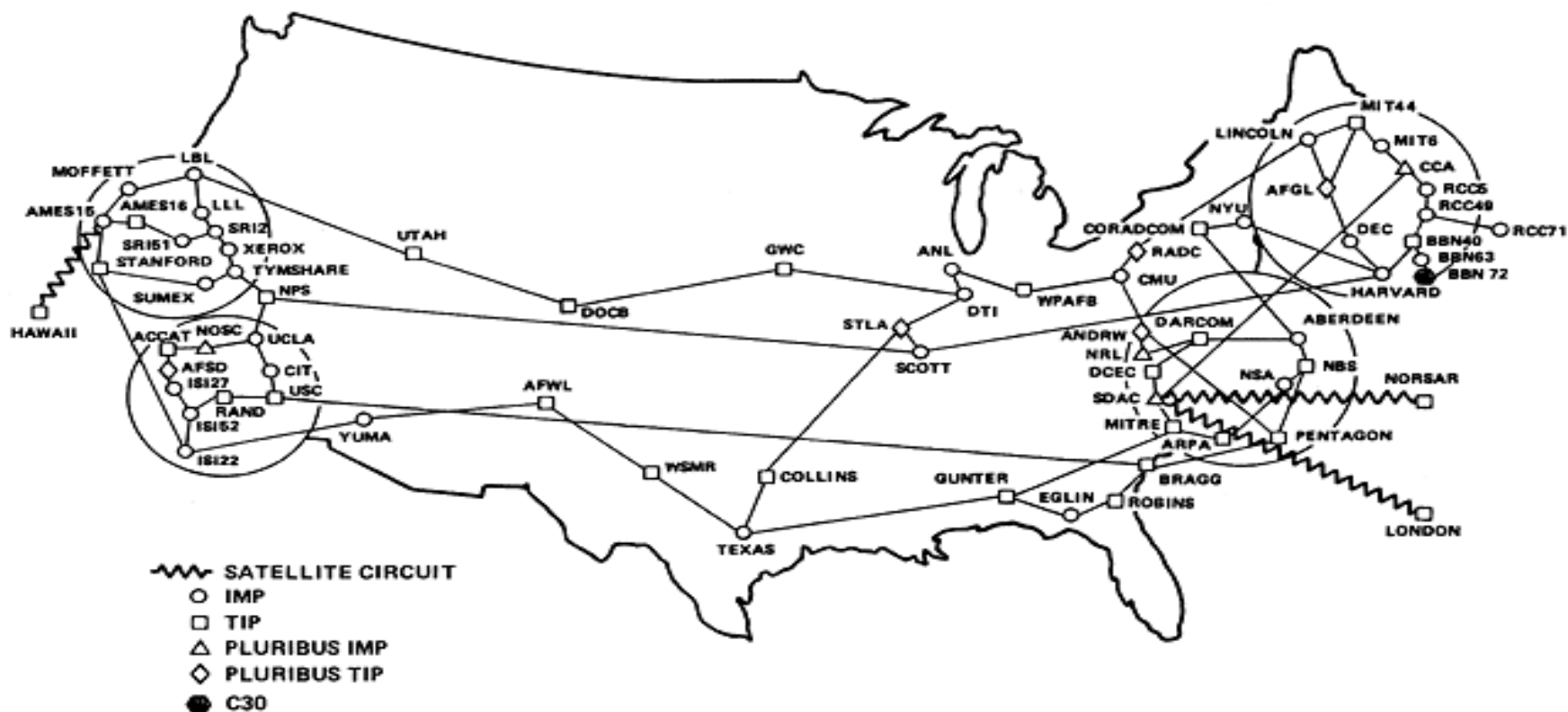
- The Growing Problem of Cyber Security
- Traditional Solutions and Why They Won't Work
- A New Paradigm (tools and incentives)
- Bringing it all Together



INTERNET  
SECURITY  
ALLIANCE

# The Past

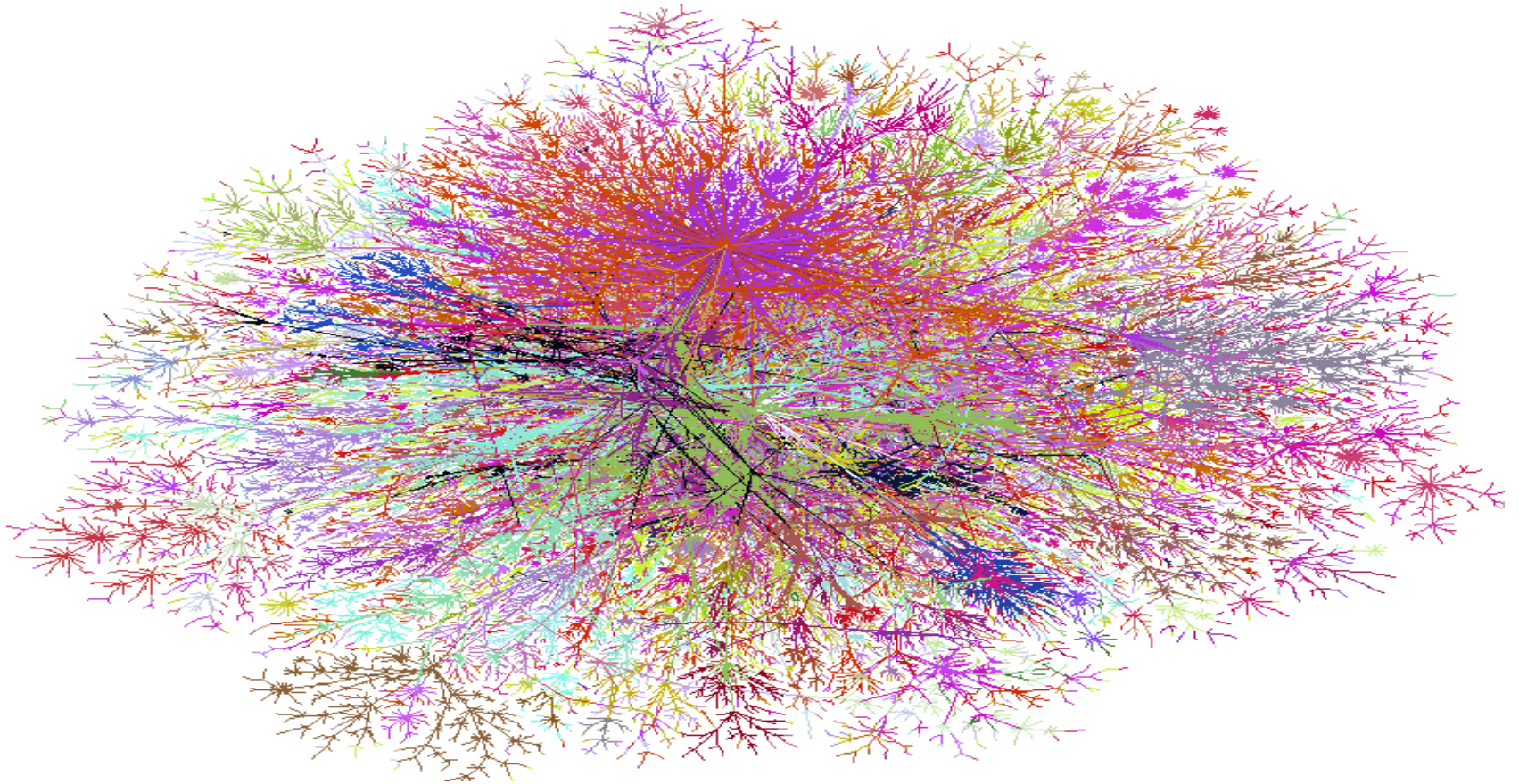
ARPANET GEOGRAPHIC MAP, OCTOBER 1980



(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)  
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

# *The Present*

---



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

# ***The Threats – The Risks***

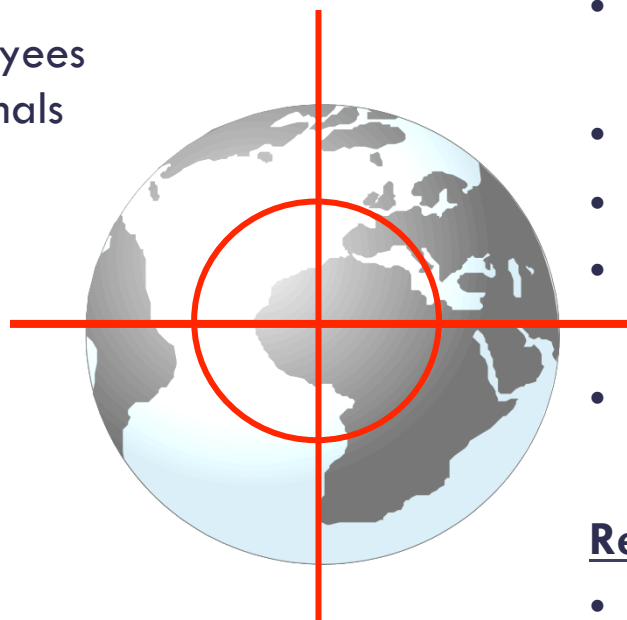
---

## **Human Agents**

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

## **Methods of Attack**

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



## **Exposures**

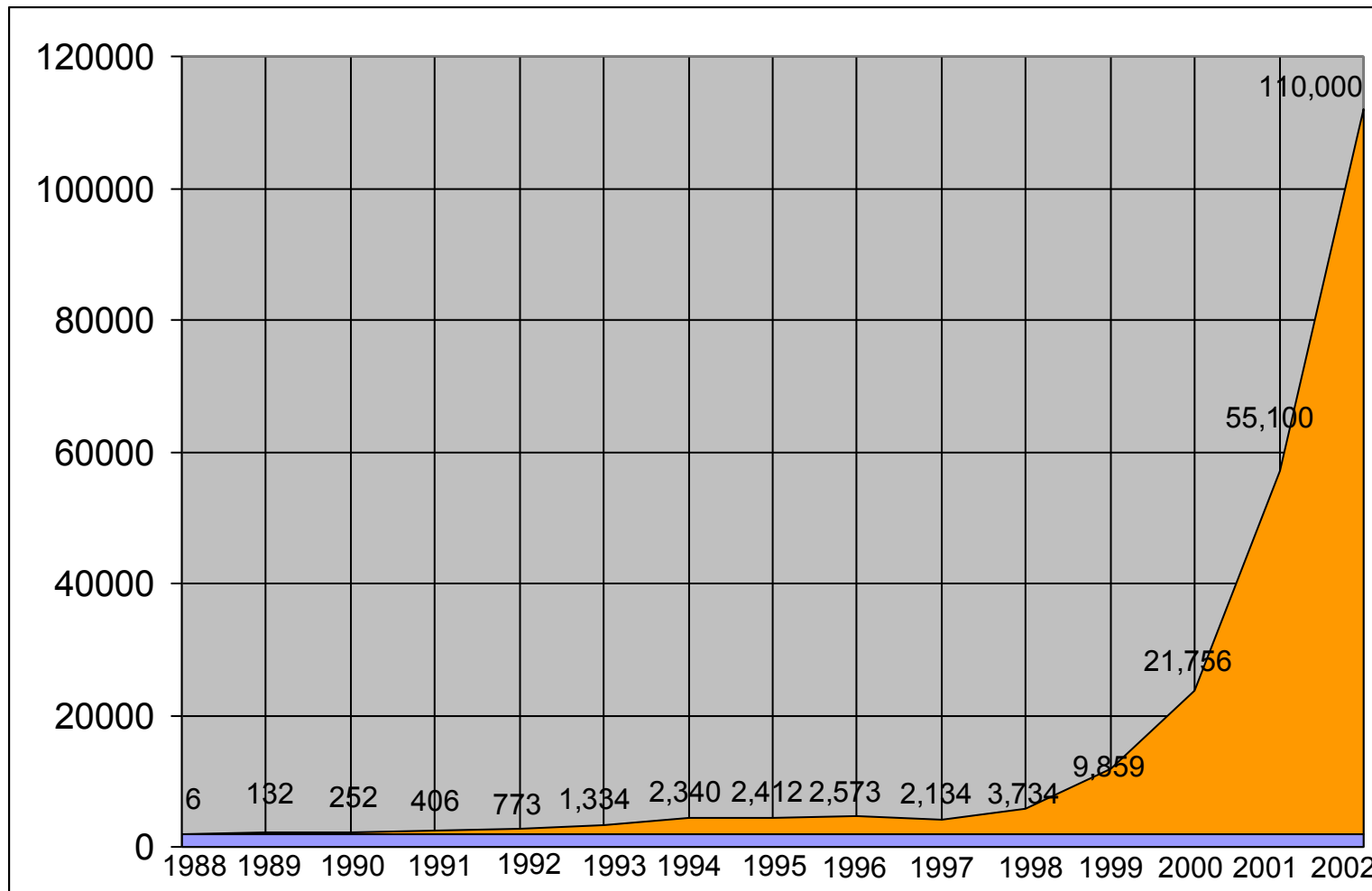
- Information theft, loss & corruption
- Monetary theft & embezzlement
- Critical infrastructure failure
- Hacker adventures, e-graffiti/defacement
- Business disruption

## **Representative Incidents**

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

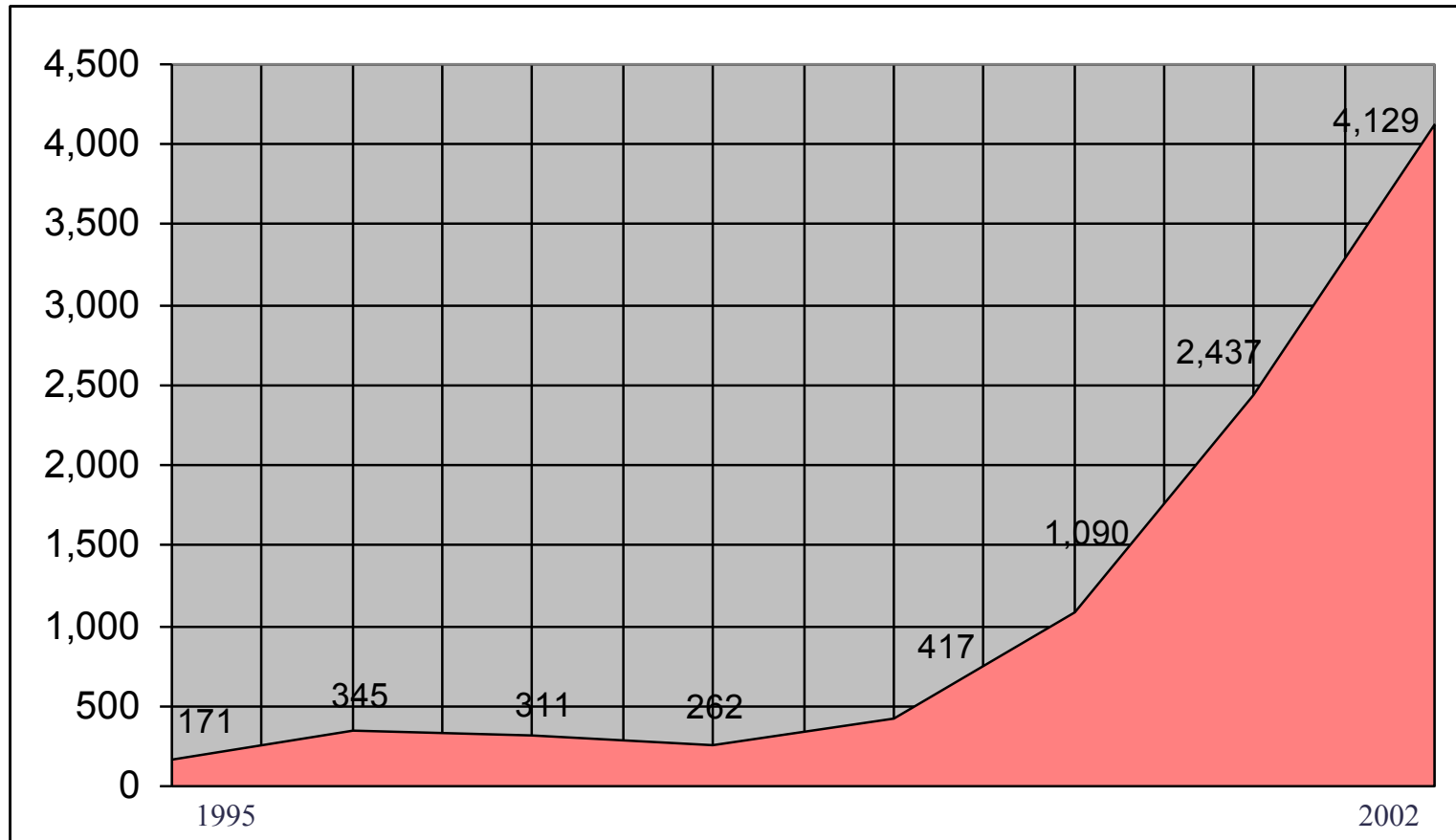


# ***Growth in Incidents Reported to the CERT/CC***



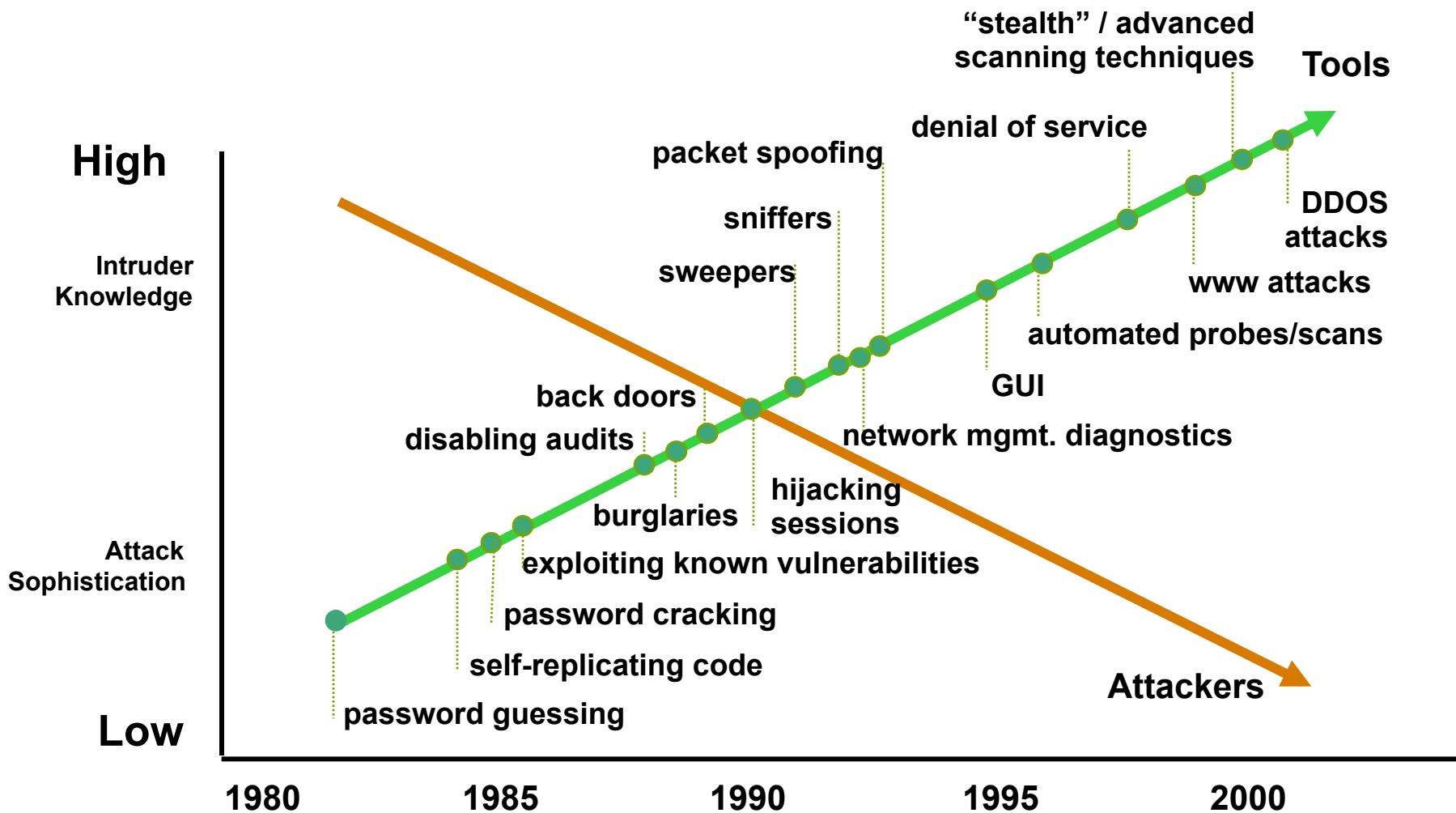


## ***The Dilemma: Growth in Number of Vulnerabilities Reported to CERT/CC***





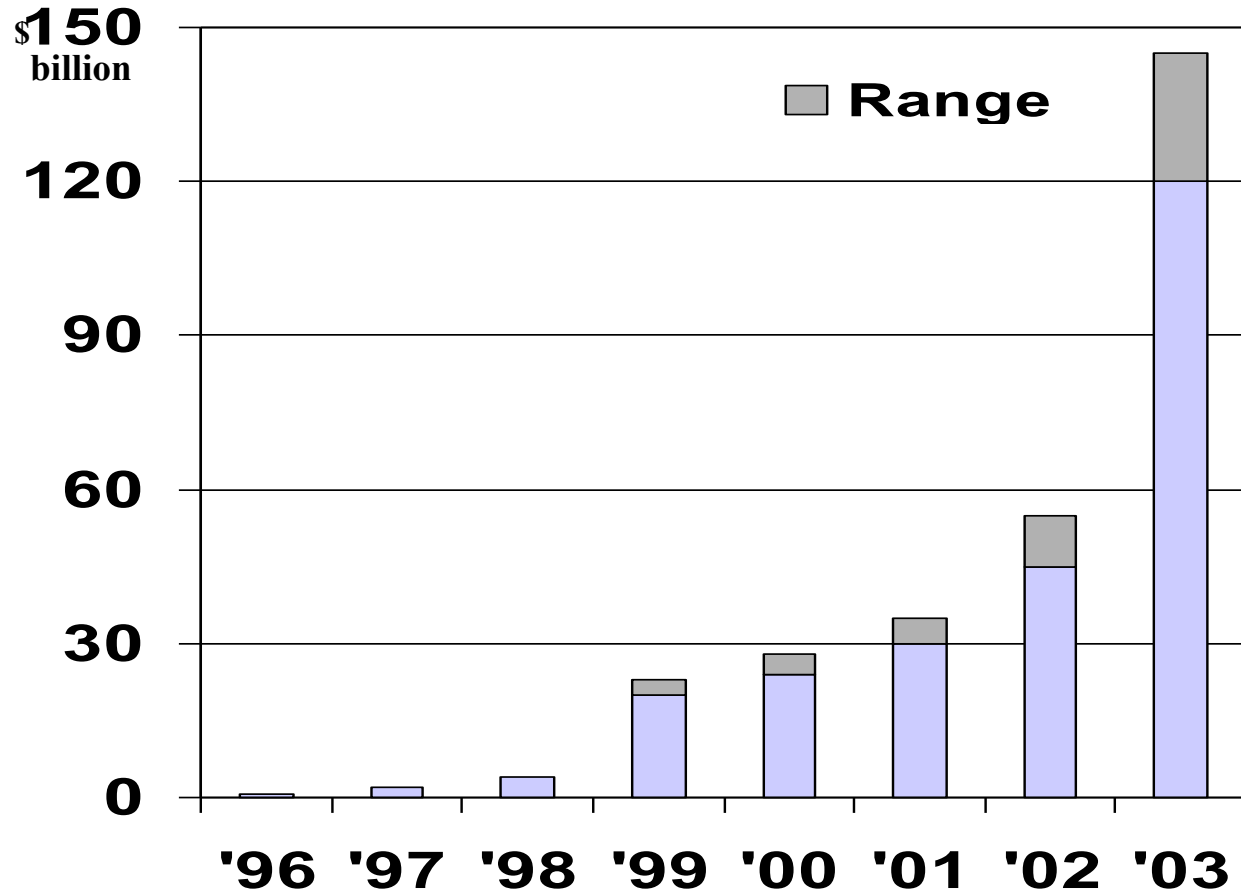
# Attack Sophistication v. Intruder Technical Knowledge







# 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 borders”)



# *Cyber Security is not an “IT” Problem*

---

- Y2K WAS:
- Simple
- 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 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 borders, 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 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*
- 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*





# *A New paradigm: Tolls and Incentives*

---

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



# ISAlliance/CERT Knowledgebase Examples

**CERT**  
Coordination  
Center

Figure 3: Special Communications index page

**Welcome to the CERT/CC Special Communications Database**

Welcome to the CERT/CC Special Communications database. Special Communications are information items written by technical staff for technical audiences of current interest or special concern. We use them as a forum to preview draft publications, distribute summary analyses, or share information privately that is not intended for public distribution.

The first Special Communications was sent via e-mail in March of 1998, since that time we have produced over two hundred Special Communications. Our audience has grown and has the potential for a wider distribution of this information in a timely and secure manner. An SSL-secured web site will be the preferred distribution mechanism for Special Communications as well as an extension of our pre-work.

You can [search](#) or browse Special Communications by three key fields, including [name](#), [ID](#), and [date](#). You can also customize database queries to obtain specific information, such as the [ten most recently published Special Communications](#). [Detailed descriptions](#) of the ten Special Communications are available from our [help page](#). These are also available for customizing [search queries](#) and [reports](#).

This information is confidential and is available only to a limited audience. If you are not able to see this page, you've successfully been denied access to our web server and may view the archive.

If you have questions or comments about this database, please [let us know](#).

**Recent Special Communications**

ID Number	Title
SC-2002-040	Denial of Service Vulnerability in <a href="#">Cisco IOS</a>
SC-2002-039	Remotely exploitable buffer overflow in <a href="#">Microsoft Windows</a>
SC-2002-038	Multiple Vulnerabilities in <a href="#">Microsoft Windows</a>
SC-2002-037	Incident note about Exploitation of Vulnerabilities in <a href="#">Microsoft Windows</a>
SC-2002-036	<a href="#">Cisco Catalyst</a> fail to remove session table entries for traffic containing invalid Transport Layer checksums [VU#539363]
SC-2002-035	<a href="#">Cisco Catalyst</a> contains authentication enforcement-type vulnerability
SC-2002-034	Pre-release notification for CERT Advisory CA-2002-12
SC-2002-033	Buffer overflow in <a href="#">Microsoft Windows</a>



# ***Benefits of Information Sharing Organizations***

---

- May lessen 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



# *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)



Top Ten Recommended  
Information Security Practices  
1st Edition - July 2002



# *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
- American Security Consortium 3-Party Assessment program
- Bring cyber security to the C-level based on ISA Best Practices
- Risk Preparedness Index for assessment and certification
- Create a baseline of security even CEOs can understand
- 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

----Nortel

---Visa

----Verizon

SemaTech Program

Tax Incentives

Liability Carrots

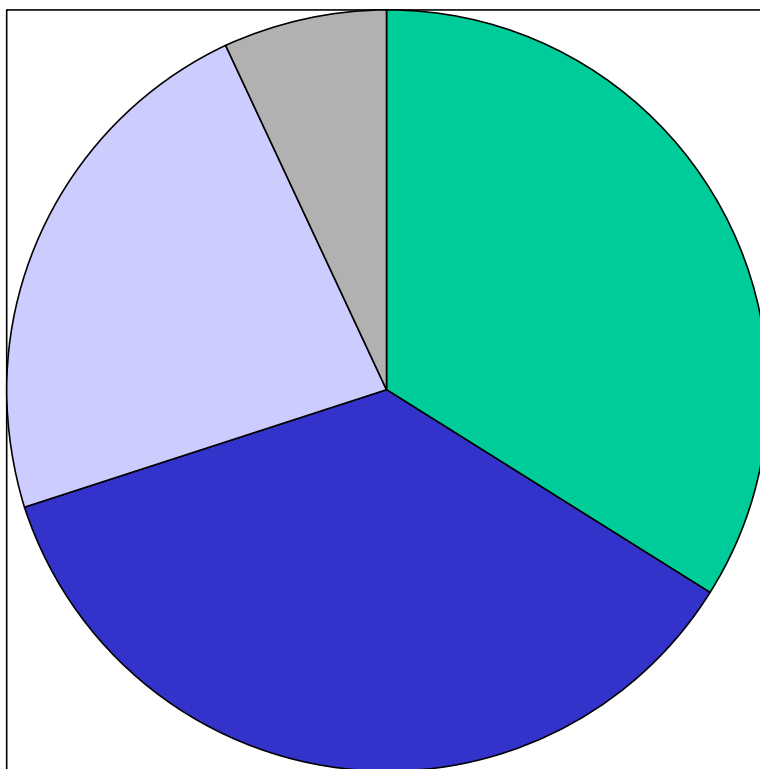
Procurement Model

Research and Development



## *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 borders



# *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



# *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.





# Sponsors





**INTERNET  
SECURITY  
ALLIANCE**

---

Larry Clinton  
Operations Officer  
Internet Security Alliance  
[lcClinton@eia.org](mailto:lcClinton@eia.org)  
703-907-7028  
202-236-0001