



**INTERNET
SECURITY
ALLIANCE**

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

- 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.



Sponsors



What We Believe



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

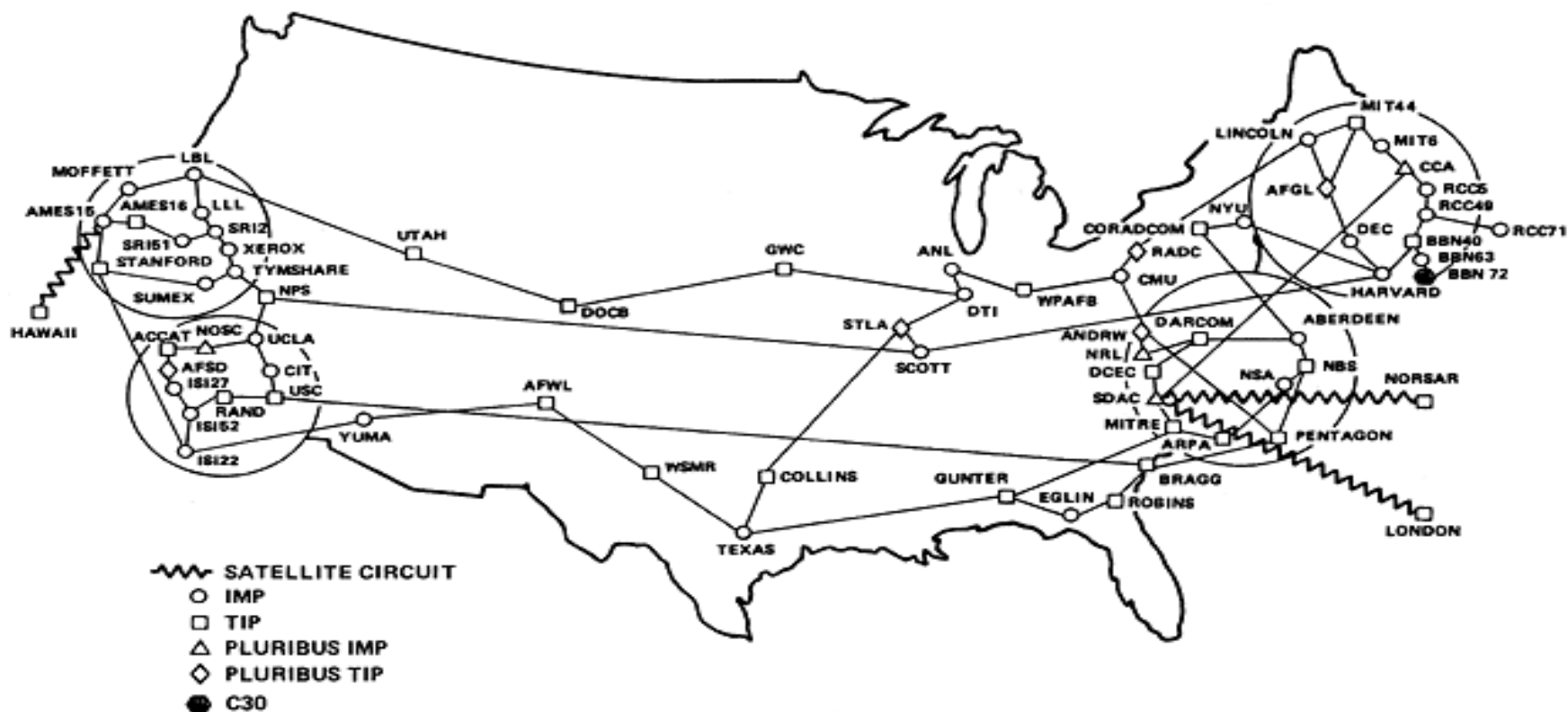
Why We Must Act



INTERNET
SECURITY
ALLIANCE

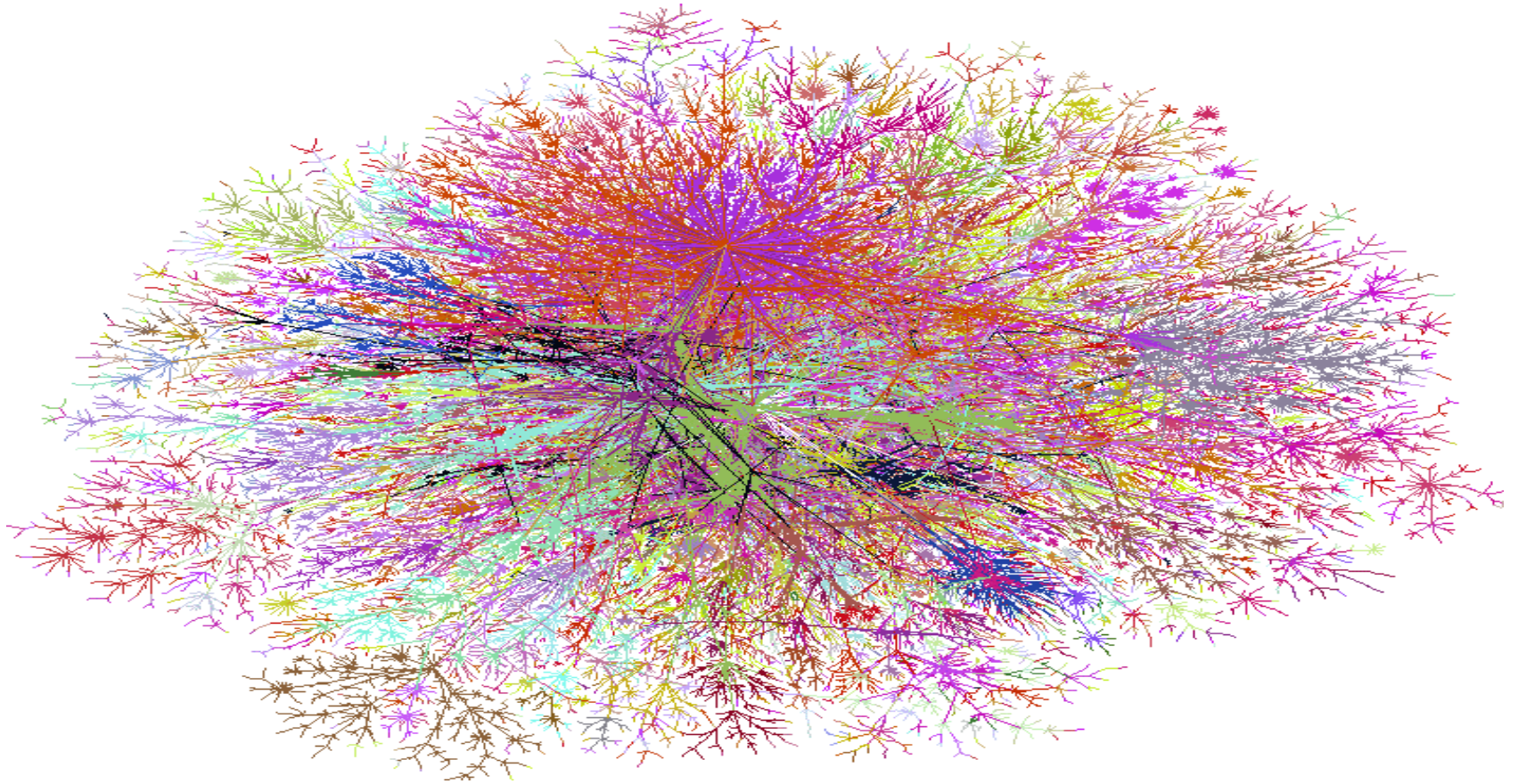
The Past

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>

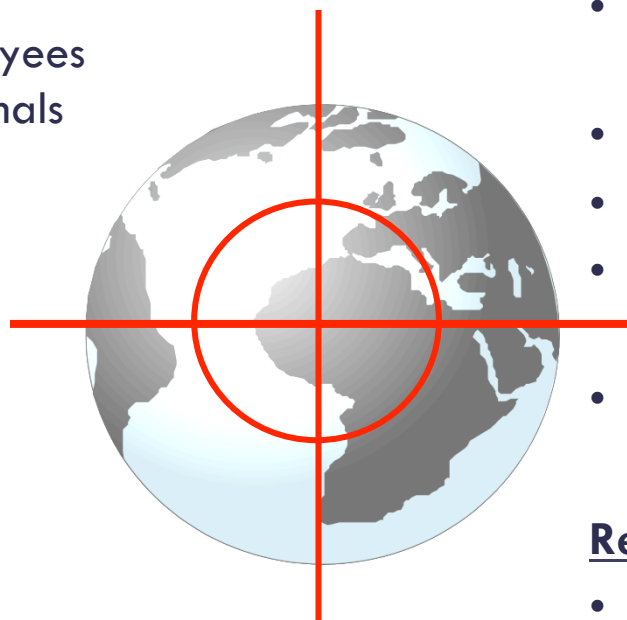
The Threats – The Risks

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

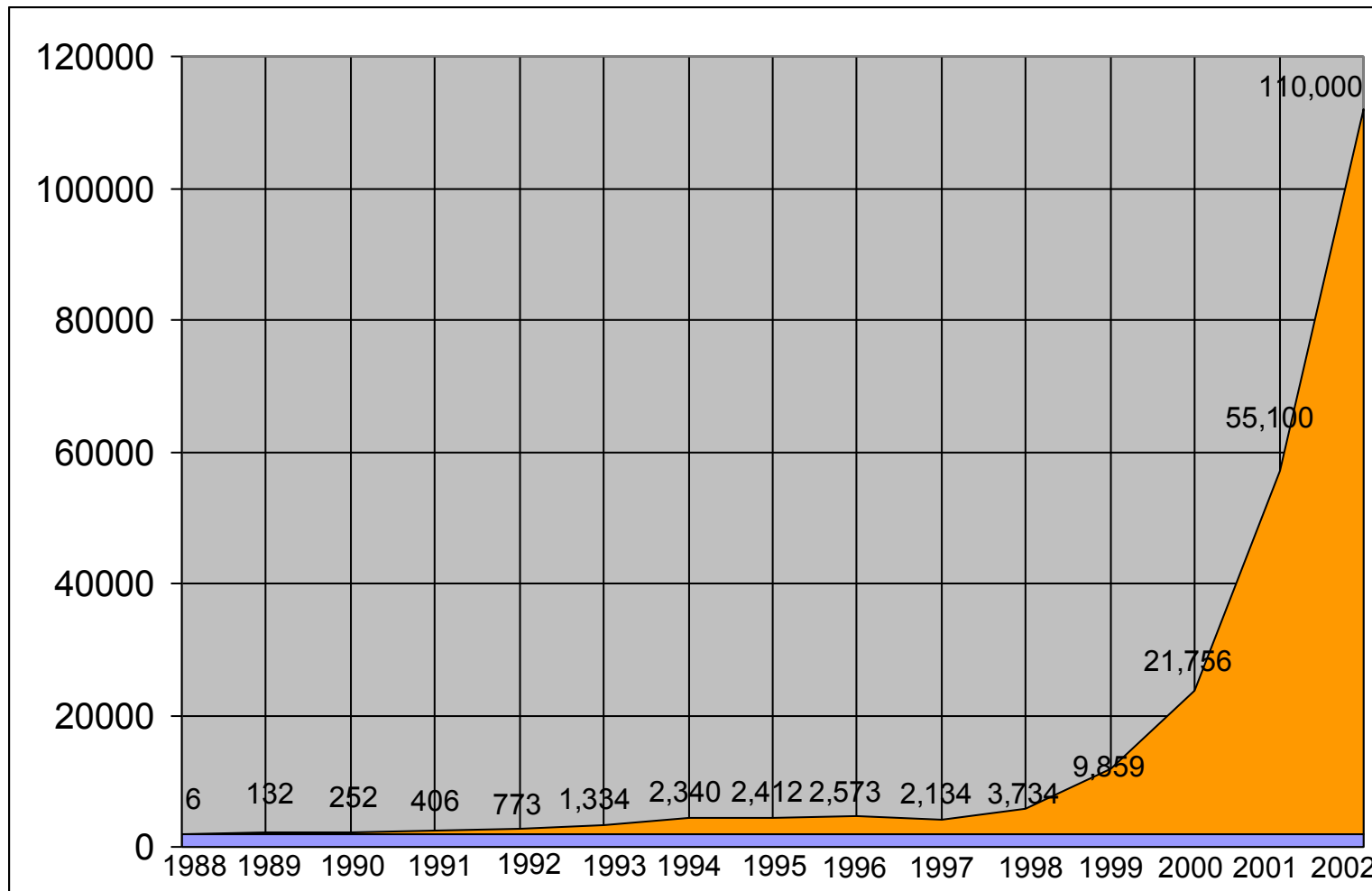
- Information theft, loss & corruption
- Monetary theft & embezzlement
- Critical infrastructure failure
- Hacker adventures, e-graffiti/defacement
- Business disruption

Representative Incidents

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

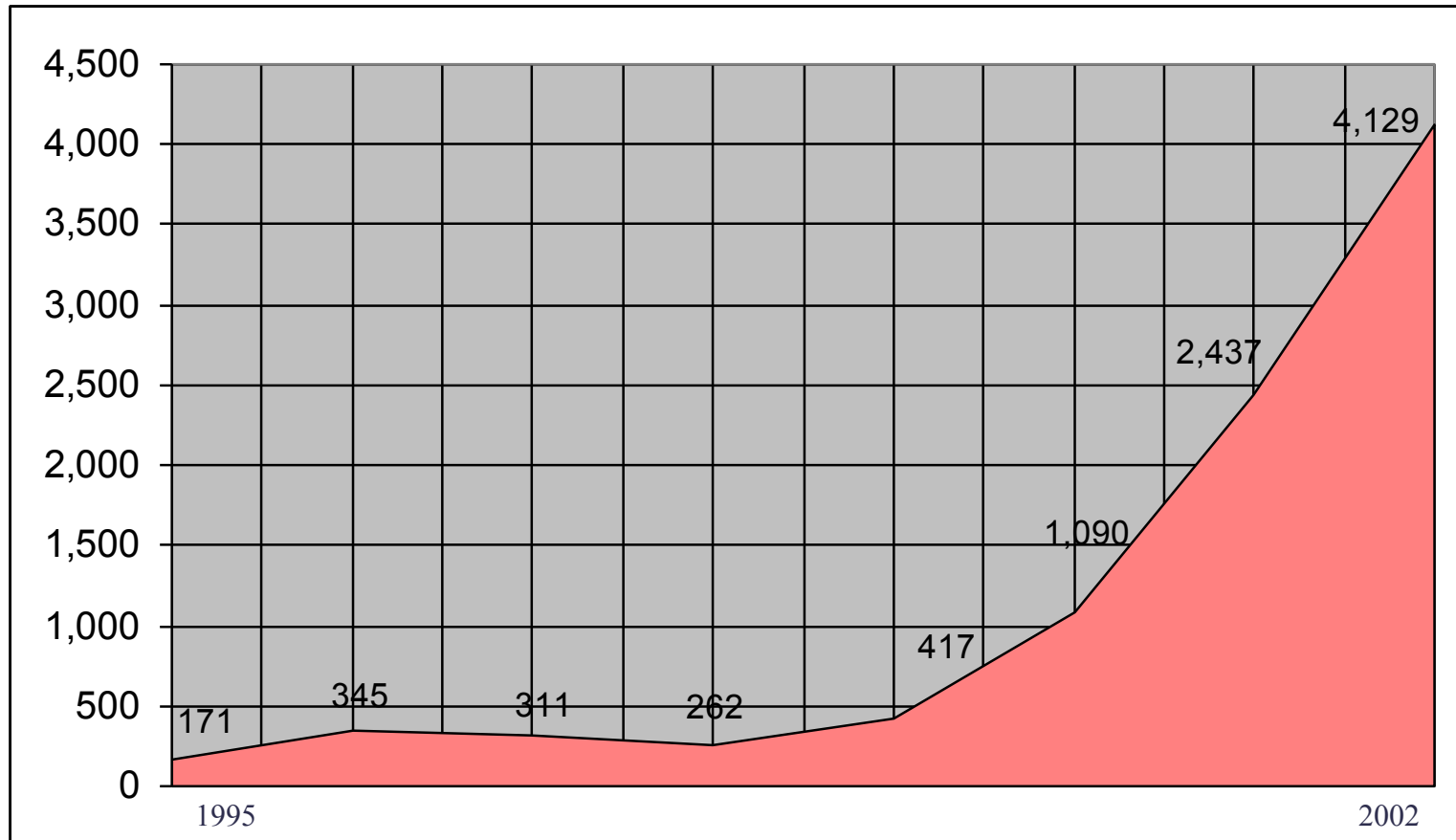


Growth in Incidents Reported to the CERT/CC



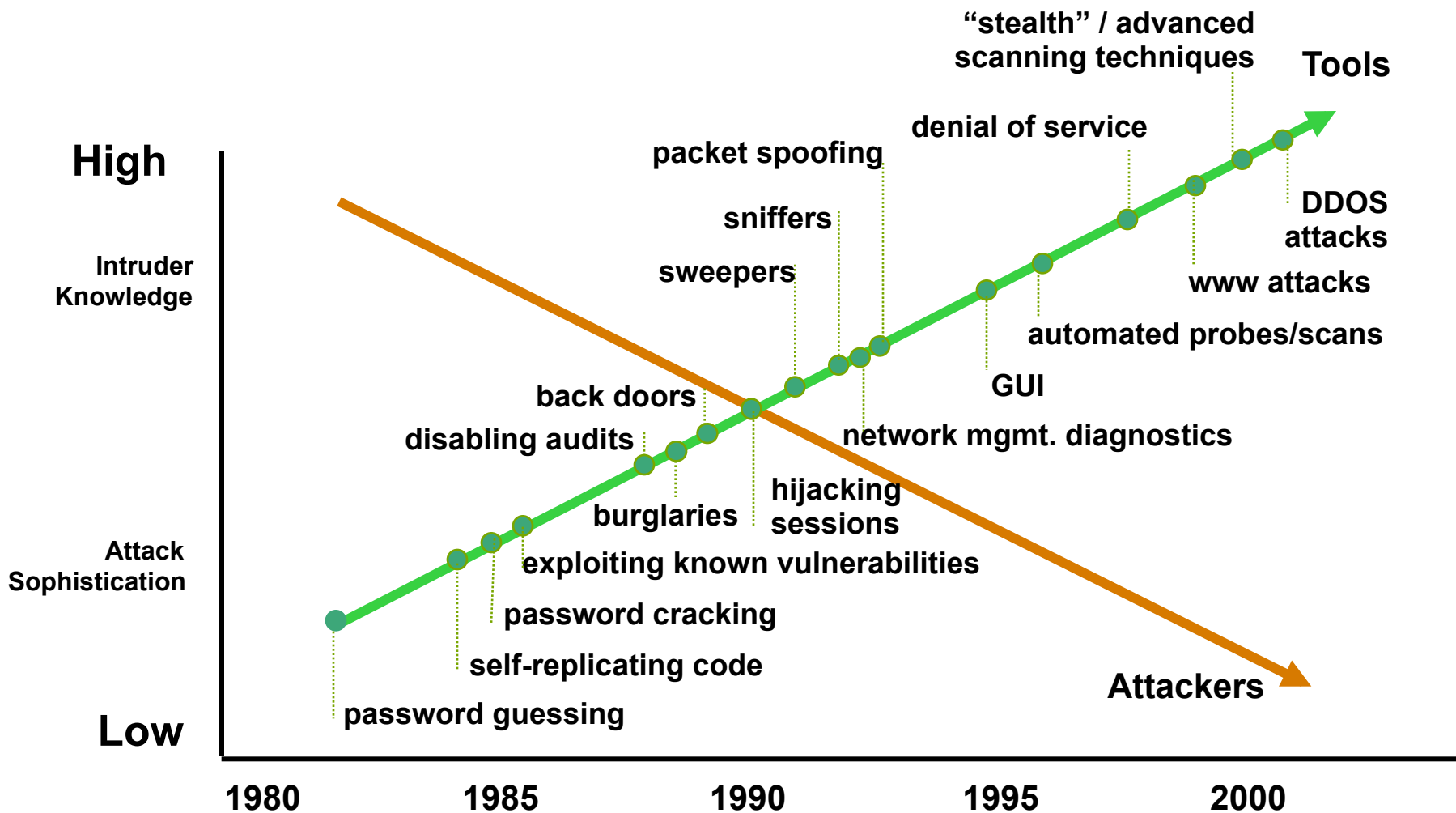


The Dilemma: Growth in Number of Vulnerabilities Reported to CERT/CC

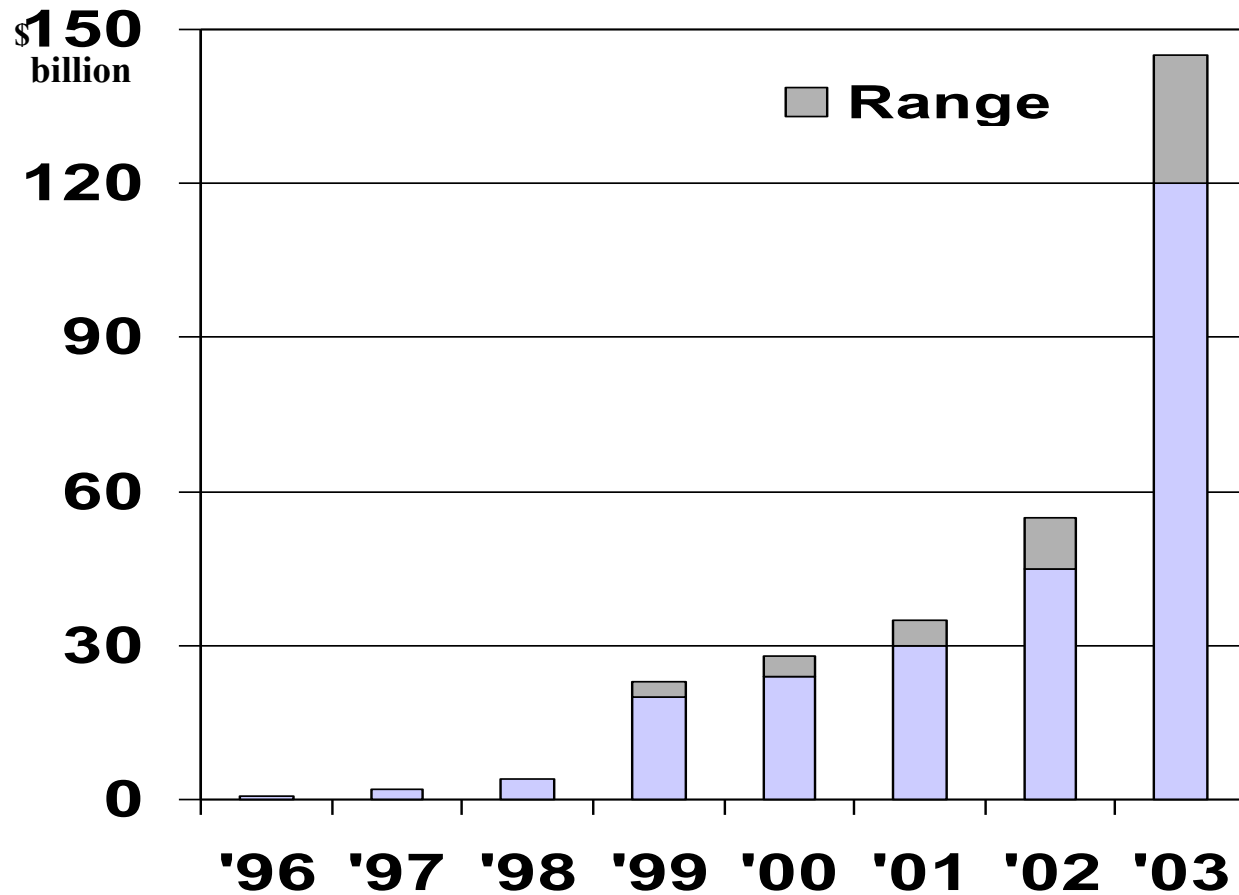




Attack Sophistication v. Intruder Technical Knowledge



Computer Virus Costs (in billions)



(Through Oct 7)



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*

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

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 Secretary 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



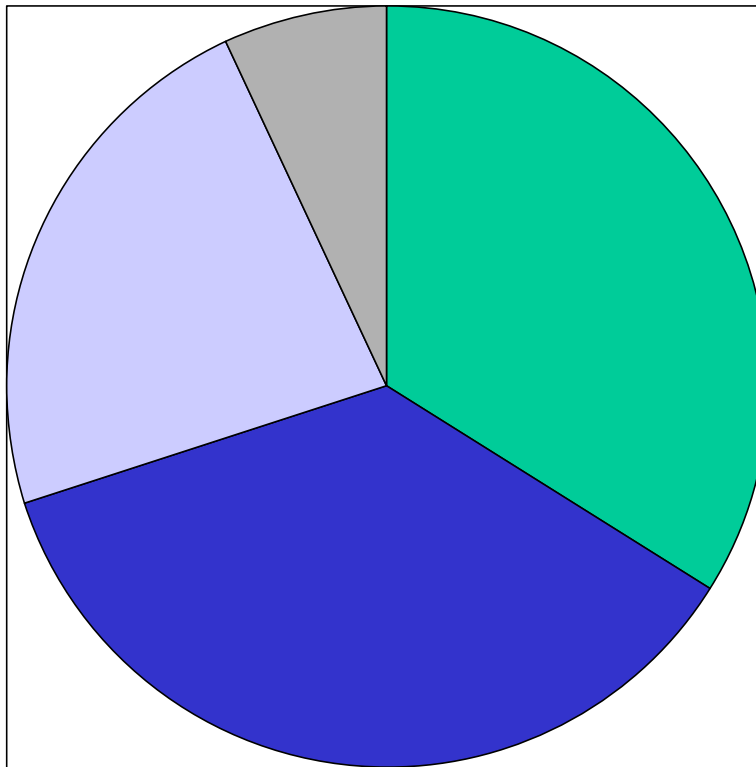
Step 3. Risk Mitigation/Cyber Insurance

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)



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



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



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



Macro Step 5

Join and participate in a cyber-security
information sharing organization



Benefits

- Share critical information across industries and across national borders
- 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



The screenshot shows the 'Special Communications Database' index page. The page has a red header with navigation links: Home, Site Index, Search, Contact, FAQ, Incidents, quick fixes & vulnerabilities, security practices & evaluations, survivability research & analysis, training & education. The main content area is titled 'Welcome to the CERT/CC Special Communications Database' and includes a search bar, a list of recent special communications, and a sidebar with links to 'View SCs By ID Number', 'Title', 'Date Published', 'Other CERT/CC Knowledgebase Vulnerability Notes', 'Vulnerability Categories', 'AIRCERT', 'Other Documents', 'Addresses', 'Incident Notes', 'Summaries', 'Current Activity', and 'Tech Tips'.

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 message 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 range of distributing this information in a timely and secure manner. An SSL-secured web site will be the preferred distribution method for Special Communications as well as an extension of our pre-existing work.

You can [search](#) or browse Special Communications by three key fields, including [name](#), [ID](#), and [date published](#). You can also customize database queries to obtain specific information, such as the [ten most recently published Special Communications](#). [Detailed descriptions](#) of the ten most recent 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're 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

- [SC-2002-040](#) Multiple vulnerabilities in [Microsoft Internet Explorer](#) products [VU#997403 VU#291555 VU#301059 VU#630091 VU#467555]
- [SC-2002-040](#) Denial of Service Vulnerability in [Microsoft Internet Explorer](#)
- [SC-2002-039](#) Remotely exploitable buffer overflow in [Microsoft Internet Explorer](#)
- [SC-2002-038](#) Multiple Vulnerabilities in [Microsoft Internet Explorer](#)
- [SC-2002-037](#) Incident note about Exploitation of Vulnerabilities in [Microsoft Internet Explorer](#)
- [SC-2002-036](#) [Microsoft Internet Explorer](#) fail to remove session table entries for traffic containing invalid Transport Layer checksums [VU#539363]
- [SC-2002-035](#) [Microsoft Internet Explorer](#) contains authentication enforcement-type vulnerability
- [SC-2002-034](#) Pre-release notification for CERT Advisory CA-2002-12
- [SC-2002-033](#) Buffer overflow in [Microsoft Internet Explorer](#)



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



Why ISA Info Sharing Works

- Carnegie 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 borders



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



**INTERNET
SECURITY
ALLIANCE**

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