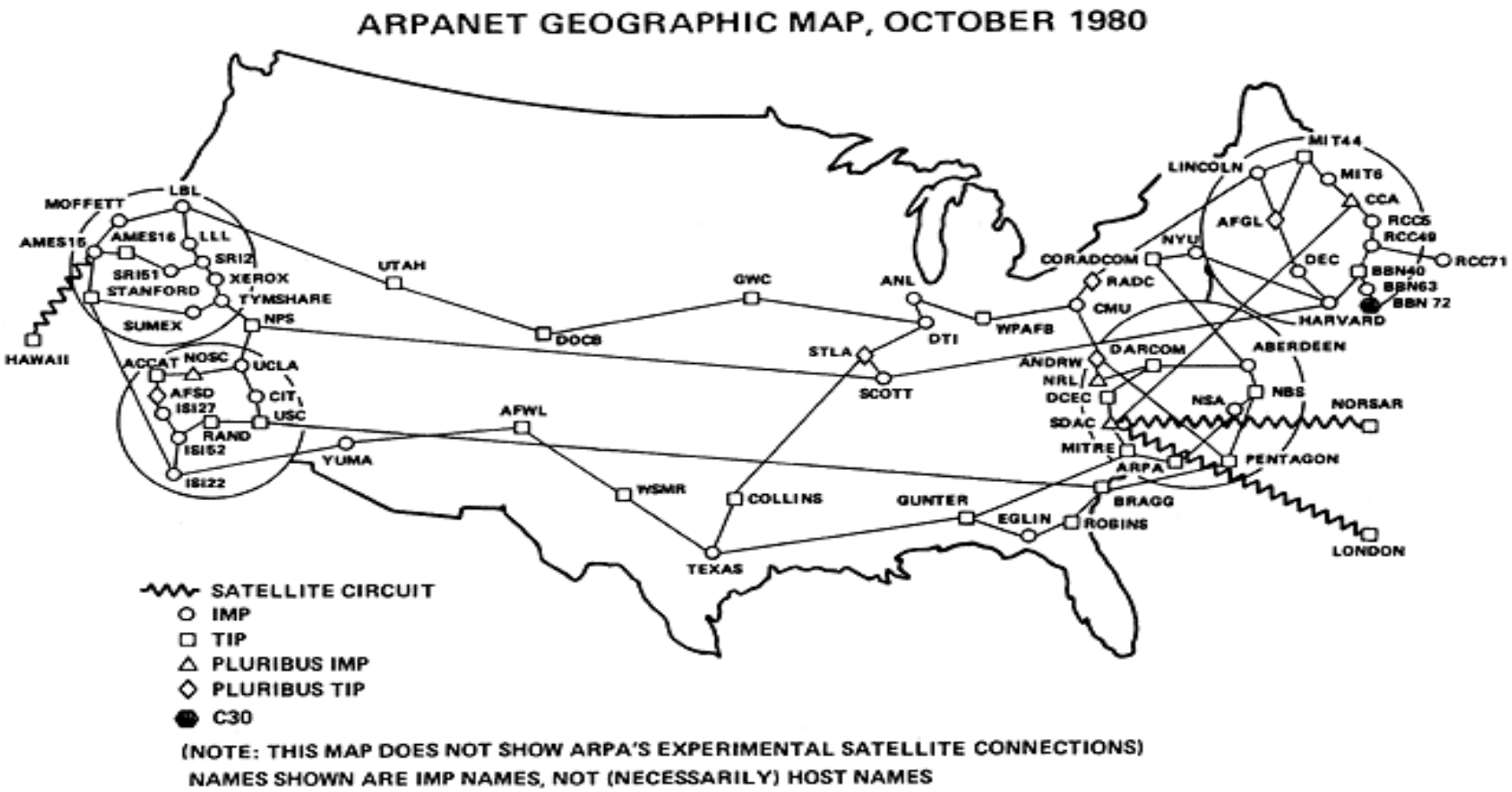
Larry Clinton
Operations Officer
Internet Security Alliance
lclinton@eia.org
703-907-7028
202-236-0001

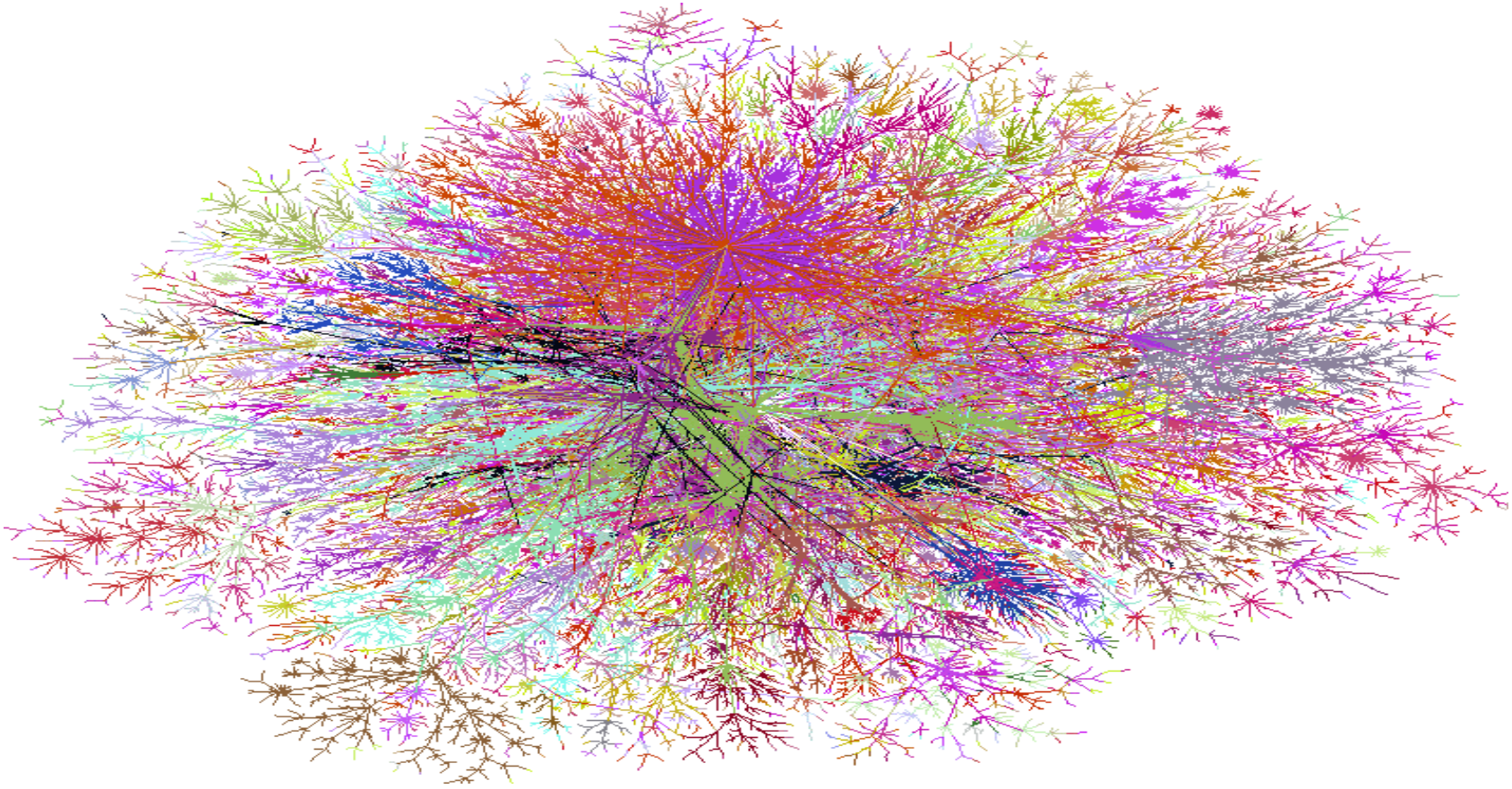
INTERNET SECURITY ALLIANCE

The Past



INTERNET SECURITY ALLIANCE

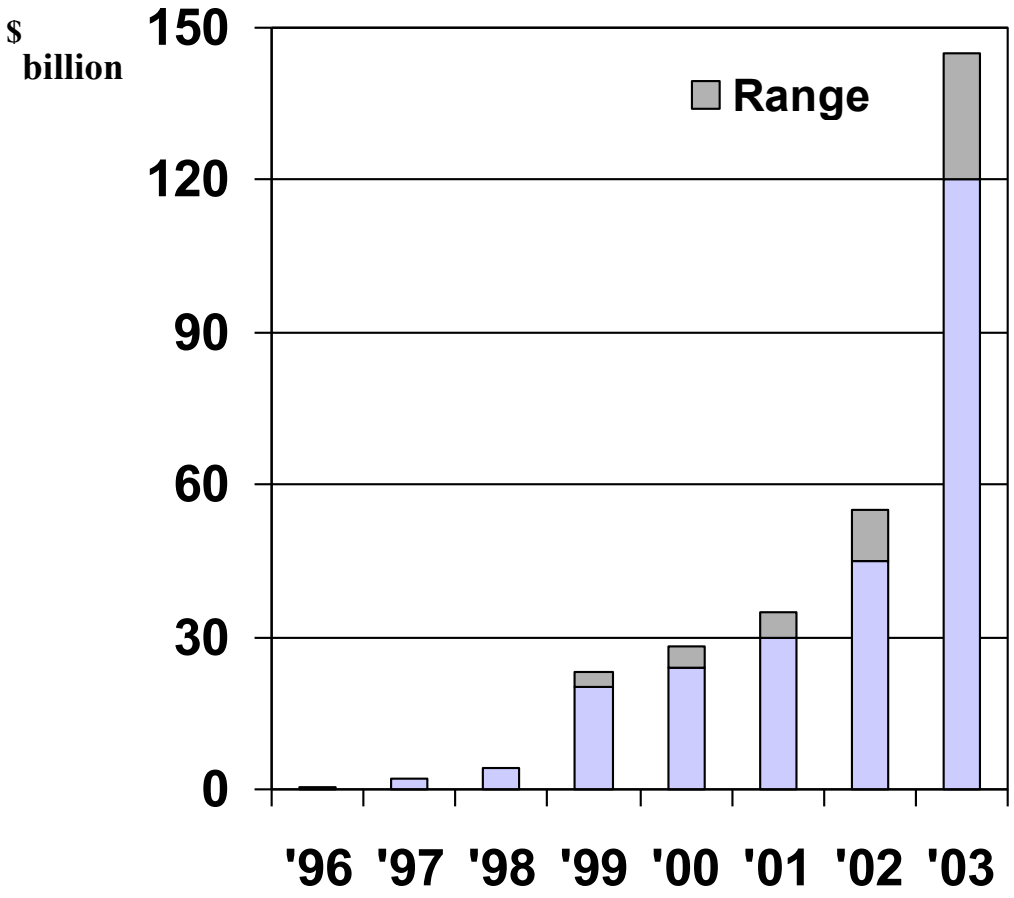
The Present



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

INTERNET SECURITY ALLIANCE

Computer Virus Costs (in billions)



(Through Oct 7)

III Model Adopted by ISA Fall 2003

1. Tie best practice adoption to reduced costs

2. Tie use of best practice as a prerequisite for access to markets

3. Private/Government use of market to prime the pump

4. Establish climate for market incentives

ISAlliance Incentive Model

Model Programs for market Incentives

---AIG

---Visa

----Nortel

----Verizon

SemaTech Program

Tax Incentives

Liability Carrots

Procurement Model

Research and Development

CISWG Incentive Principles 3/3/04

1. Positive incentives are more likely to generate long term and effective results in cyber security than government mandates. This will ultimately increase consumer and business confidence in the use of technology, promote homeland security and result in economic, cultural and national benefits for all.

CISWG PRINCIPLES

2. Market incentives are likely to be effective:

a) leverage industry's ability to innovate & maintain tools needed for cyber security

b) multi-national industry can work globally

c) industry can respond to technological change

d) ROI approach will attract Sr. Ex commitment

e) market programs can work cross industry

f) can compliment current sector initiatives

CISWG PRINCIPLES

3. Duplicative and conflicting international, national, state and local requirements create disincentives to effective cyber security

CISWG PRINCIPLES

4. Traditional Regulatory Structures can be ineffective and potentially counterproductive

a) International nature of the problem

b) Rapid tech change demands flexibility

c) Public notice and comment is inconsistent w/ security needs

d) Political process encourages compromise

e) Gov regulation may blunt innovation

CISWG Recommendation 1.Measurement/Seal of Approval/Certification

1. Continue to base measurement tools on widely accepted best practices

2. Private sector should develop programs of qualification/compliance/certification

3. Private Sector should create designations or award programs (e.g. Baldrige type programs)

2. Insurance

1. Business should make use of risk management programs offered by insurance companies
2. Insurance industry should modify availability and cost of policies based on degree company complies with best practices
3. Government should encourage appropriate availability and use of cyber insurance

3. Market Entry

1. Companies should use market forces to encourage partner security (Visa/Nortel)

2. Industry leaders should identify and encourage such programs

3. Federal Gov. (Congress and DHS) should publicize good actors

What ISA is doing

1. ISAlliance Best Practices Endorsed by EIA, NAM, TechNet, ABA, CERT/cc, USIBC.
2. Work with Global Security Consortium on 3-party measurement based on best practices
3. Establish discount programs based on adoption of best practices.
4. Create "Champion of the Internet" Award for mutual security efforts
5. Expand ROI security programs for Members

Gov. Incentives Liability Protection, Tax, FEMA

Congress should consider lowering liability or providing safe harbors to companies who adopt and implement effective IT security controls

Congress should consider tax incentives for enhanced security

Congress should consider FEMA aid based on adherence to widely accepted best practices

CISWG PHASE II

- Liability seems to be growing (e.g. FTC)
- California has already established a reasonableness standard
- We now need to focus on the next step, how to craft an incentive system

INTERNET SECURITY ALLIANCE

Tentative Conclusions

1. There are not, and may not be consensus metrics/ standards/practices applicable to all.
2. There are an array of measurements across types of organizations that can be used.
3. There are a range of protections to use.
4. There are a variety of organizational mechanisms to set guides.
5. Best approach may be take existing tools and create sliding scale of protections

A new war a new strategy

1. The Internet is a 21st century technology, it can't be managed with 19th century regulatory models

2. The job of securing the Internet with market incentives is much HARDER

3. Creative thinking and market incentives are the best way to win the war in cyber-space

INTERNET SECURITY ALLIANCE

Sponsors

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