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

ISA Board of Directors

Ken Silva, Chairman
CSO Verisgn
Ty Sagalow, Esq. 1st Vice Chair
President Product Development, AIG

J. Michael Hickey, 2nd Vice Chair
VP Government Affairs, Verizon
Dr. M. Sagar Vidyasagar, Treasurer
Exec VP, Tata Consulting Services

- Angie Carfrae, VP Risk Management, Ceridian Corporation
- Tim McKnight, CSO, Northrop Grumman
- Jeff Brown, CISO/Director IT Infrastructure, Raytheon
- Paul Smocer, SVP/CIO, Mellon Financial
- Matt Broda, Chief Strategic Security, Nortel
- Marc-Anthony Signorino, Director Technology Policy, National Association of Manufacturers
- Pradeep Khosla, Dean Carnegie Mellon School of Computer Sciences
- Matt Flanagen, President, Electronic Industries Alliance

INTERNET SECURITY ALLIANCE

Our Partners

STAYSAFEONLINE.org
National Cyber Security Alliance

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

UNITED STATES DEPARTMENT OF THE TREASURY

FCC Federal Communications Commission

BSI

ANSI
American National Standards Institute

ISSA
Information Systems Security Association
The Global Voice of Information Security

NFIB
The Voice of Small Business®

IT SCC
INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

Council on Competitiveness

AMERICAN BANKERS ASSOCIATION

INTERNET SECURITY ALLIANCE

Industry Affairs/Government Relations






INTERNET SECURITY ALLIANCE

Business Services

- Integrating Information Security into the Business Plan (NASDAQ Conference)
- ISAlliance Integrated Security Services Program
  - E-Discovery
  - Outsourcing Risk Management
  - Security Breach Notification
  - Security Incident Handling
  - Auditing
- High Profile Speaking and Article Placements
- Preventing and Detecting Insider Threats
- Best Practices Development
  - Senior Managers Guide to Cyber Security
  - Small Businesses Guide to Cyber Security
  - Home Users & Mobile Executive Guide
- Cyber Insurance Discount Program for Best Practice Compliance (up to 15%)
- Exclusive Annual Privacy Policy Trends Report
- Contracting for Information Security, Model Commercial Agreements Guides
- IT Risk Management Quarterly Work Group

Technical Services

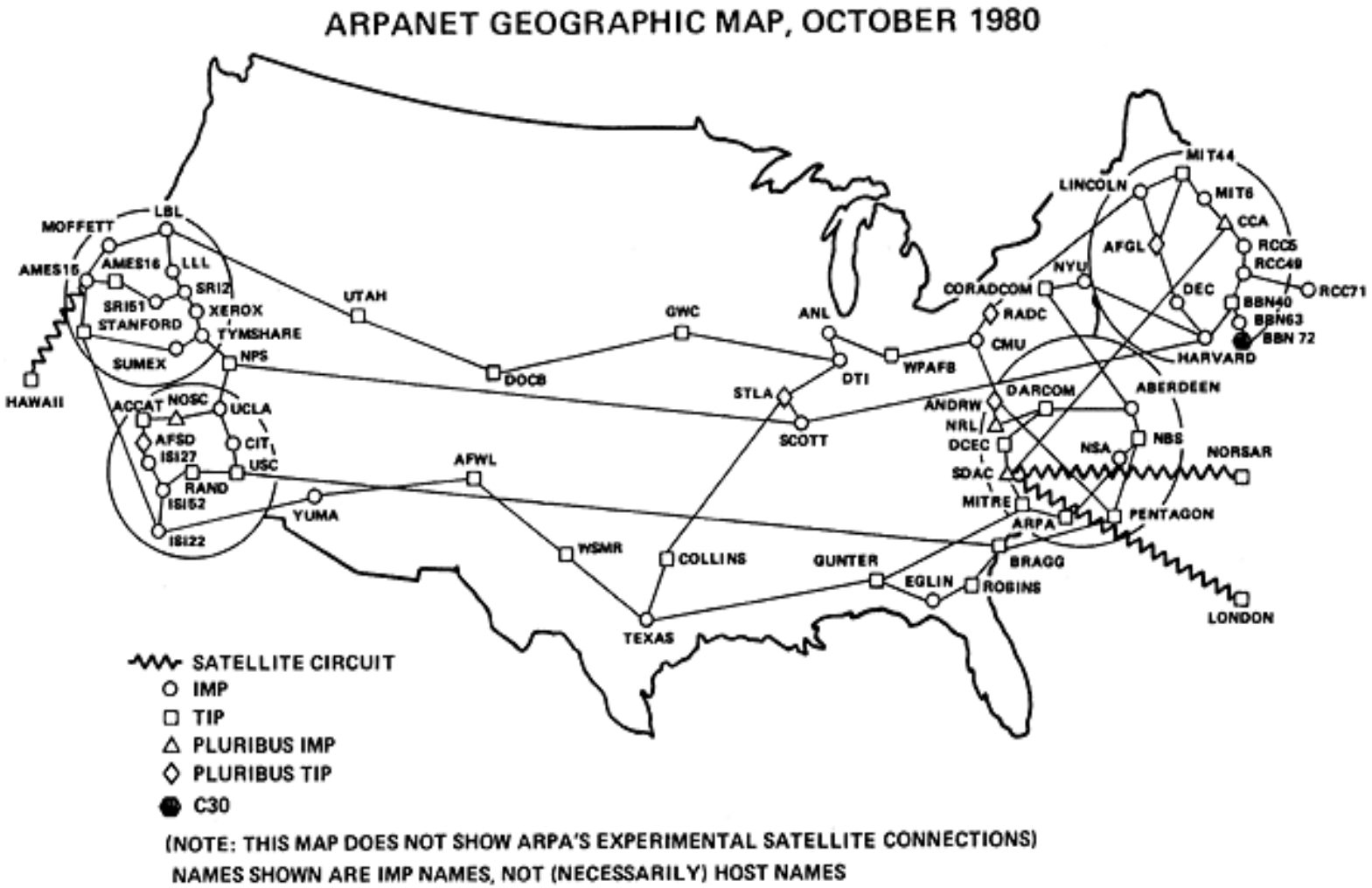
- Weekly Webinars from Carnegie Mellon University on Emerging Info Security issues
- Continuing Education Credit Program in Information Security
- ISAlliance/ANSI Model Terms for Certified ISMS featuring ISO/IEC 27001
- ISAlliance/ANSI Model Commercial Agreements featuring ISO/IEC 17799
- ISAlliance/ISSA Guide to Model Terms for Commercial Agreements
- SQUARE Methodology and Tool
- Online Assessment Tools and Insurance Discounts
- Exclusive Annual Software Assurance Report
- Participation in Critical Infrastructure Protection Planning with U.S. DHS
- Placement of Membership Articles in Professional Journals
  - Fixing Cyber Security Problems
- Daily Threat and Vulnerability Briefings from US-CERT

Legal & Policy Services

- Comprehensive Solutions for E-Discovery
- Interaction with Senior Policy Makers
  - Congress
  - Department of Homeland Security
  - US Department of Commerce Economic Security Working Group
- National Infrastructure Protection Plan
  - IT Sector Coordinating Council
- Member Speaking & Writing Opportunities
  - Cutter IT Journal
- Market Incentives for Cyber Security
  - Market Incentives White Paper
- Congressional Staff Briefings
  - Defense Issues
  - IT & Telecommunications Issues
  - Insider Threats
  - International Issues
- Exclusive Annual Privacy Policy Trends Report
- Privacy Quarterly Work Group

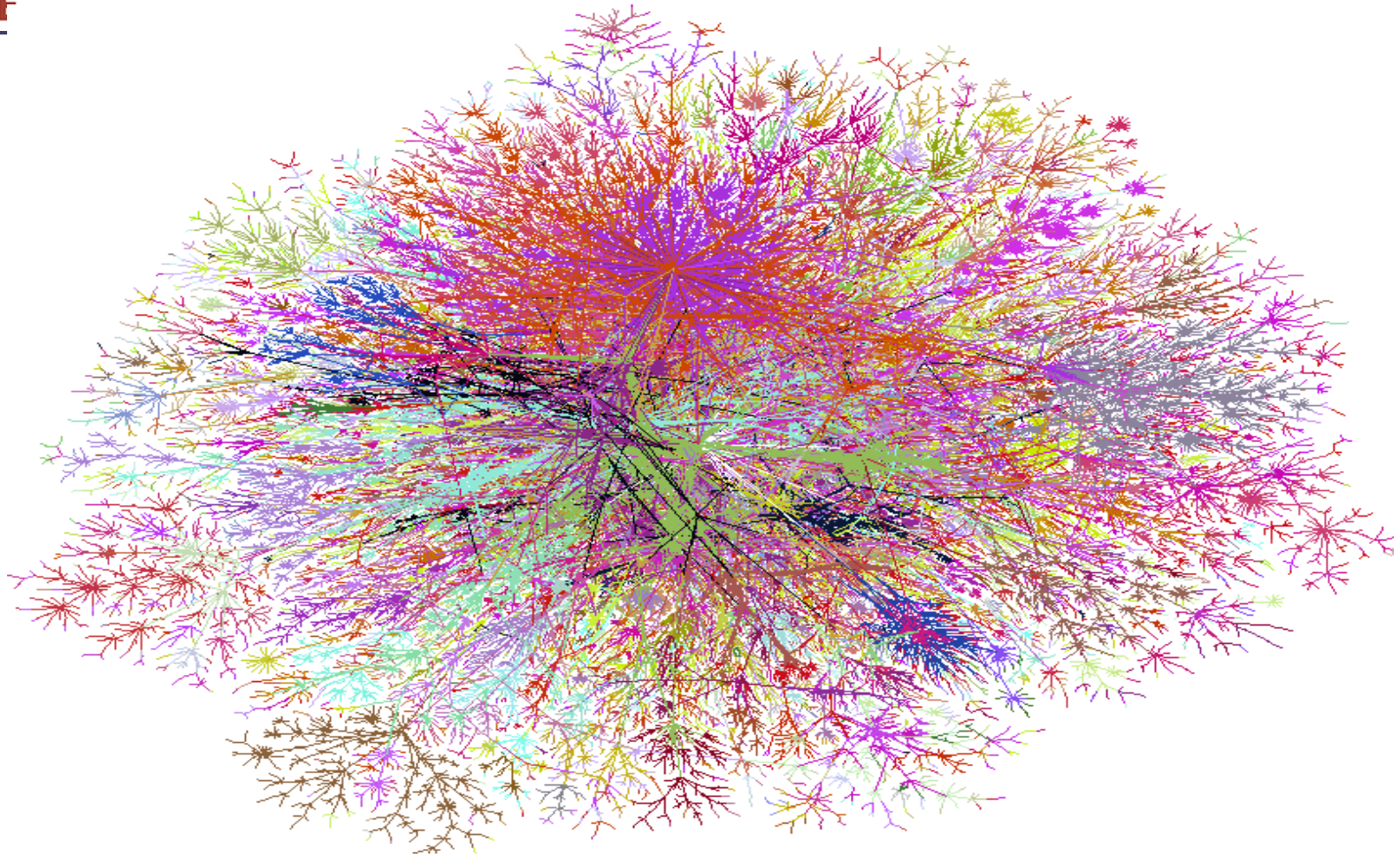
INTERNET SECURITY ALLIANCE

The Old Web



INTERNET SECURITY ALLIANCE

The Web Today



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

The Changing Threat

A fast-moving virus or worm pandemic is not the threat it was...

2002-2004 almost 100 medium-to-high risk attacks ("Slammer"; "SoBig").

2005, there were only 6

2006 and 2007…….. **Zero**

INTERNET SECURITY ALLIANCE

Faces of Attackers… Then

Joseph McElroy

Hacked US Dept of Energy

Jeffrey Lee Parson

Blaster-B Copycat

Chen-Ing Hau

CIH Virus

INTERNET SECURITY ALLIANCE

Faces of Attackers… Now

Jay Echouafni

Competitive DDoS

Jeremy Jaynes

$24M SPAM KING

Andrew Schwarmkoff

Russian Mob Phisher

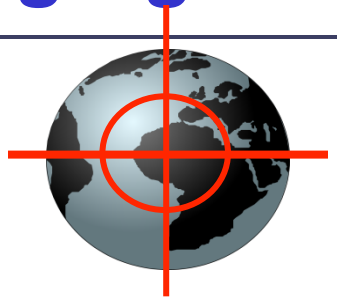
The Changing Threat

Today, attackers perpetrate *fraud*, gather *intelligence*, or conduct *blackmail*

Vulnerabilities are on client-side applications word, spreadsheets, printers, etc.

"The future threat landscape around the world will be dictated by the soon-to-be-released Apple iPhone, Internet telephony and Internet video-sharing, and other Web-based innovations" (McAfee 2007)

The Threat Landscape is Changing



Early Attacks

Who: Kids, researchers, hackers, isolated criminals

Why: Seeking fame & glory, use widespread attacks for maximum publicity

Risk Exposure: Downtime, business disruption, information loss, defacement

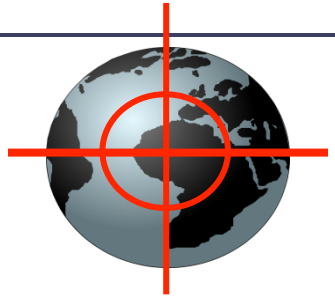
New Era Attacks

Organized criminals, corporate spies, disgruntled employees, terrorists

Seeking profits, revenge, use targeted stealth attacks to avoid detection

Direct financial loss via theft and/or embezzlement, breach disclosure, IP compromised, business disruption, infrastructure failure

The Threat Landscape is Changing



Early Attacks

Defense: Reactive AV signatures

Recovery: Scan & remove

Type: Virus, worm, spyware

New Era Attacks

Multilayer pre-emptive and behavioral systems

System wide, sometimes impossible without re-image of system

Targeted malware, root kits, spear phishing, ransomware, denial of service, back door taps, Trojans, IW

INTERNET SECURITY ALLIANCE

Characteristics of the New Attackers

Shift to profit motive

Zero day exploits

Increased investment and innovation in malcode

Increased use of stealth techniques

Digital Growth? Sure

"Companies have built into their business models the efficiencies of digital technologies such as real time tracking of supply lines, inventory management and on-line commerce. The continued expansion of the digital lifestyle is already built into almost every company's assumptions for growth."

---Stanford University Study, July 2006

Digital Defense? Maybe Not

29% of Senior Executives "acknowledged" that they did not know how many negative security events they had in the past year

50% of Senior Executives said they did not know how much money was lost due to attacks

Source: PricewaterhouseCoopers survey of 7,000 companies 9/06

INTERNET SECURITY ALLIANCE

Digital Defense

Not So Much

23% of CTOs did not know if cyber losses were covered by insurance.

34% of CTOs thought cyber losses would be covered by insurance----and were wrong.

"The biggest network vulnerability in American corporations are extra connections added for senior executives without proper security."

---Source: DHS Chief Economist Scott Borg

Problem Summary

Big, Growing, Scary (micro and macro economic impacts, real national security issues, physical danger)

Threats are constantly evolving (from love bug to designer malware, and worse)

Bad actors, and their motives are changing (not HS kids showing off it's Organized Crime, Nation states and terrorists seeking money & power)

There really is no coherent agreed upon program (current public-private partnership is good idea, but ill-defined, not properly balanced and not adequately supported)

INTERNET SECURITY ALLIANCE

What We need

Coherent sustainable system

Multi-faceted

Broad based

Capable of evolving quickly

Private Sector Schizophrenia

- The private sector has largely embraced the upsides of digitalization (inventory management/on line sales etc.)
- Much of the private sector has ignored the downsides of digitalization (e.g. sustained cyber security investment)
- The key to success is driving the private sector to WANT to provide internet security
- The core problem is that security is viewed as a cost center

Will the 20th Century (19th) Model of regulation work?

Too narrow jurisdiction (must be world wide)

Regulation is good for minimum standards when we need increasingly higher standards

Too slow (not even counting court review)

Too inflexible (must keep pace with threats)

Subject to political dumbing down (e.g. campaign finance regulation)

Old Regulatory could be counter Productive

Could slow tech progress, the prime driver of US economy

Could drive business to “safe’ havens overseas creating not only monetary loss for US but less US tech control and thus less security

Could create false sense of security

We Need a New social Contract

E.g. 20th century social contract between telephone companies and government.

Phone companies agreed to provide universal service at regulated rates.

Government provided monopoly franchise and "guaranteed' rate of return on private investment

It worked well (if not perfectly) for nearly a century

Why Private Industry is better than Gov for this task

Industry owns, operates and creates most of the system

Industry can act much more quickly than government

Industry can upgrade security in information systems across nation state boarders.

Industry can enforce expanded security through contracts and other business practices

Industry is less prone to political pressures to water down standards

The key is return on investment

Gov. New Modern Role

A. Serve as a model---get their house in order

B. Regulation can provide incentive for regulated domestic industries

Develop market incentives to bring in non-regulated sectors and multi-national players (patriotism and education are not enough)

Coordinate and streamline among and between jurisdictions (eliminating unnecessary costs)

Address issues beyond the corporate reach (e.g. R&D on developing truly secure I-net protocols)

The "What" to be Encouraged

Good news: We actually know a good deal about providing cyber security

There are multiple agencies producing best practices, standards and technologies---often Gov and PS together

Research demonstrates that following these practices can be effective in managing risk and reducing harm

The Why/How: Market Incentives

Procurement---not just cost but security---really

Civil liability reform---a Cyber Safety Act

Tax breaks---- for small business only

Insurance

Stafford Act relief

Streamlined compliance relief

Anti-trust relief allowing partnerships like SemaTech

Awards program

Moving in the right Direction/ ISA Programs

- Apply the SAFETY Act to Cyber Security
- How to secure the Global IT supply chain
- How to secure the VOIP Platform
- Developing a Framework for Corporations to assess, manage and transfer cyber risks

Applying the SAFETY Act

- SAFETY Act Passed following 911 to encourage the development of anti-terrorism technologies
- Insurance benefits, liability protection, marketing benefits
- Initially difficult for Corporations to manage and focused on high value physical threats
- New focus on cyber including an expanded concept of threat and terrorism
- ISA providing aid to companies to get SAFETY

Securing the Global IT Supply Chain

- IT supply chain is inherently global
- This immutable reality brings new risks
- If not addressed Congress will do it for us, probably through protectionism
- Bad for everyone
- ISA/CMU/industry 3-phase program to analyze the situation and create a solution that takes into account market, business and policy reality

Securing the VOIP Platform

- VOIP is the paradigm case for corporate economics overcoming security concerns
- Platform itself not a profitable as products sold to use it
- ISA/NIST program to use SCAP (Security Content Automation Protocol) and National Vulnerability Database to create a free customizable framework -- better market security products.
- Better security and better markets

Develop a Framework for Corporate Cyber Risk

- Grows out of 911 legislation passed in 2007
- Bring cyber risk analysis to all relevant areas of corporate culture (not just IT)
- Develop a tool allowing for more standardized internal analysis and action
- Include legal/regulatory/ compliance/operations/ insurance/governance external communications

Summary

- Internet unlike anything before, must be managed in a new way
- Sustainable security is possible only if owners and operators want to make it happen
- New ways for industry and government to look at problems must be tried
- We actually can do a lot
- Cost must be an inherent consideration