Larry Clinton
President
Internet Security Alliance
lclinton@isalliance.org
703-907-7028
202-236-0001

Larry Clinton President ISA

- Former Academic came to DC in mid-80s
- Legislative Director for Chair Congressional Internet Committee
- 12 years w/USTA including rewrite of telecommunications law & WIPO
- Joined ISA in 2002 w/former Chair Congressional Intelligence Committee
- Written numerous articles on Info Security, edited Journals, testify before Congress, electronic and print media
- Boards: US Congressional I-net Caucus I-Net Education foundation, Cyber Security Partnership, DHS IT and Telecom Sector Coordinating Committee, CIPAC, CSCSWG

ISA Board of Directors

Ty Sagalow, Esq. Chair
President Innovation Division, Zurich
Tim McKnight Second V Chair,
CSO, Northrop Grumman

J. Michael Hickey, 1st Vice Chair
VP Government Affairs, Verizon
Marc-Anthony Signorino, Treas.
National Assoc. of Manufacturers

- **Ken Silva, Immediate Past Chair. CSO VeriSign**
- Gen. Charlie Croom (Ret.) VP Cyber Security, Lockheed Martin
- Jeff Brown, CISO/Director IT Infrastructure, Raytheon
- Eric Guerrino, SVP/CIO, bank of New York/Mellon Financial
- Lawrence Dobranski, Chief Strategic Security, Nortel
- Pradeep Khosla, Dean Carnegie Mellon School of Computer Sciences
- Joe Buonomo, President, DCR
- Bruno Mahlmann, VP Cyber Security, Perot Systems
- Linda Meeks, VP CISO Boeing corp.

INTERNET SECURITY ALLIANCE

Core Principles

1. **The Internet Changes Everything**
2. **Cyber Security is not an "IT" issue**
3. **Government and industry must rethink and evolve new roles, responsibilities and practices to create a sustainable system of cyber security**

ISAlliance Mission Statement

ISA seeks to integrate advancements in technology with pragmatic business needs and enlightened public policy to create a sustainable system of cyber security.

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®

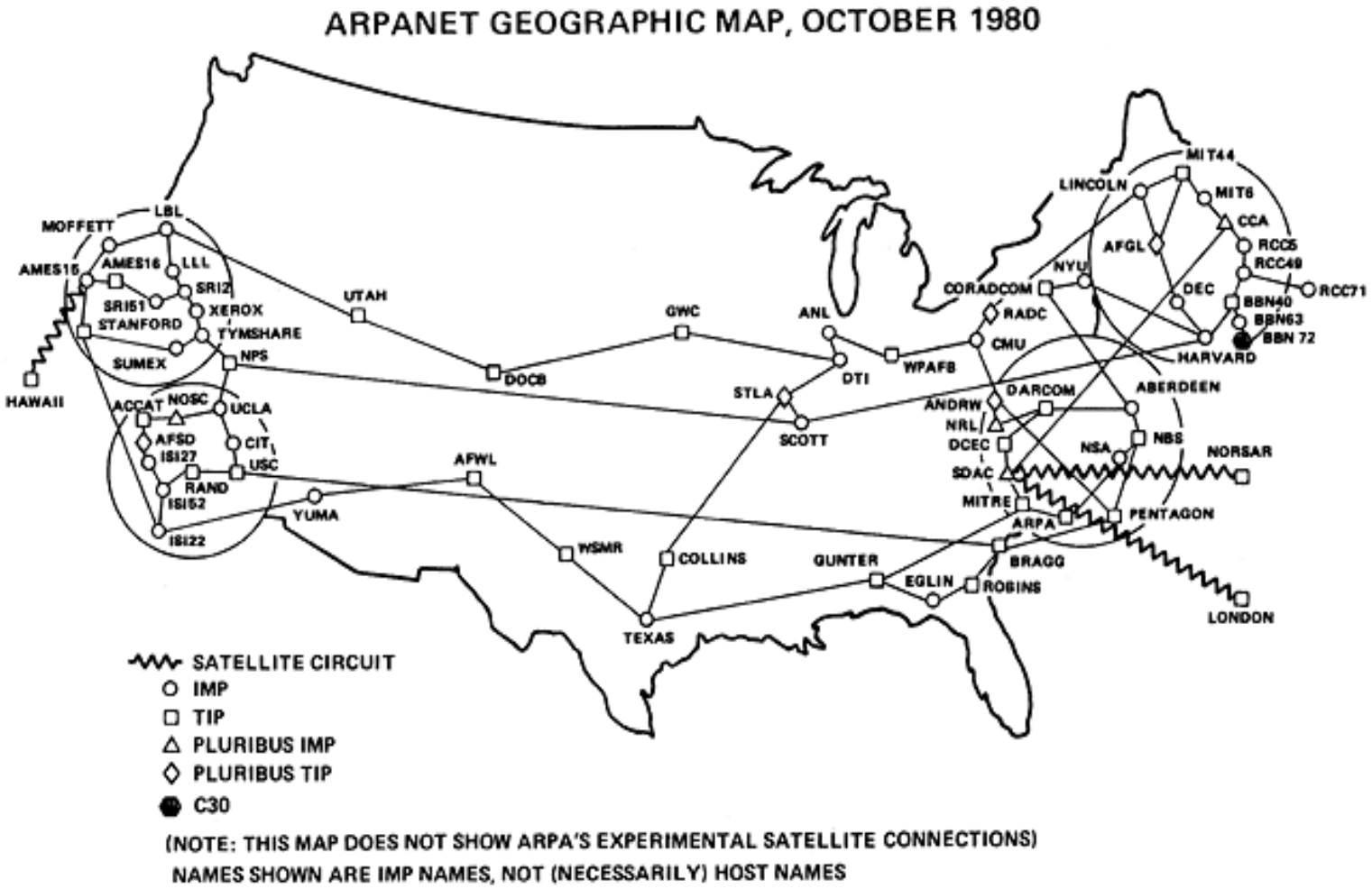
IT SCC
INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

Council on Competitiveness

AMERICAN BANKERS ASSOCIATION

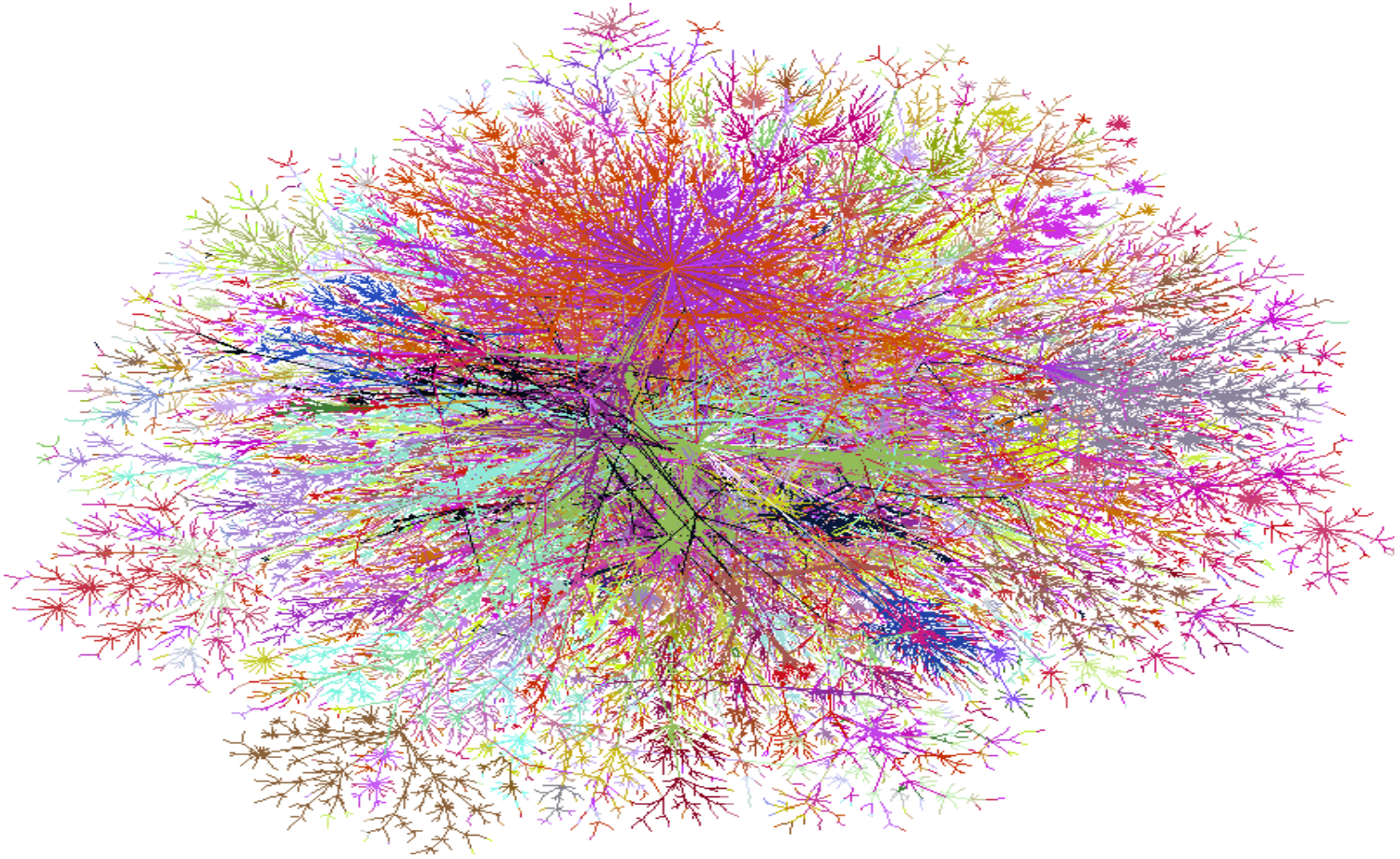
INTERNET SECURITY ALLIANCE

The Old Web



INTERNET SECURITY ALLIANCE

The Web Today



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

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

Post 9-11 Cyber Security Policy

- National Strategy to Secure Cyber Space
- DIB Effort
- Comprehensive National Cyber Initiative (CNCI)
- CSIS and ISA Proposals to Obama/ Congress
- 60-day review & Obama Speech (5/29/09)

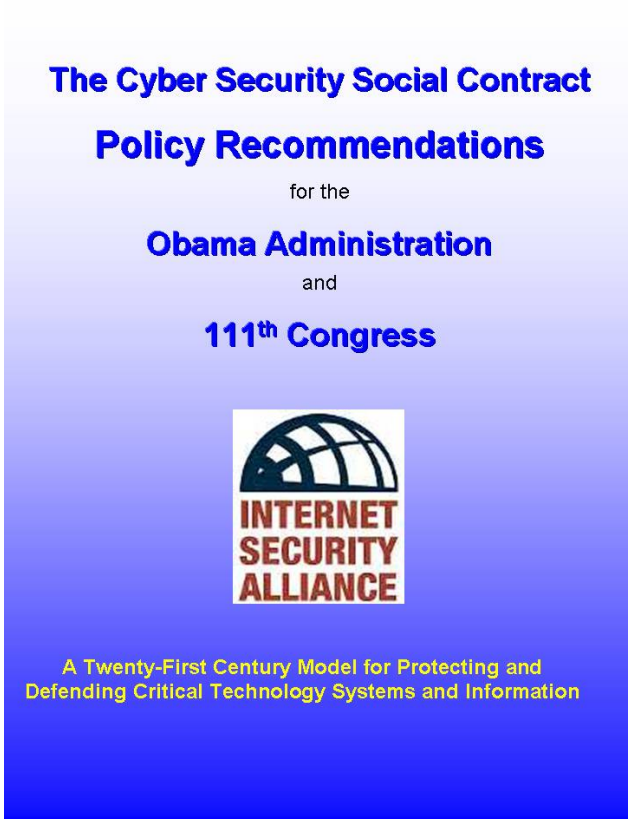
INTERNET SECURITY ALLIANCE

Releasing the Cyber Security Social Contract

November, 2008

ISA Cyber Social Contract

- Similar to the agreement that led to public utility infrastructure dissemination in 20th C
- Infrastructure develop -- market incentives
- Consumer protection through regulation
- Gov role is more creative—harder—motivate, not mandate, compliance
- Industry role is to develop practices and standards and implement them



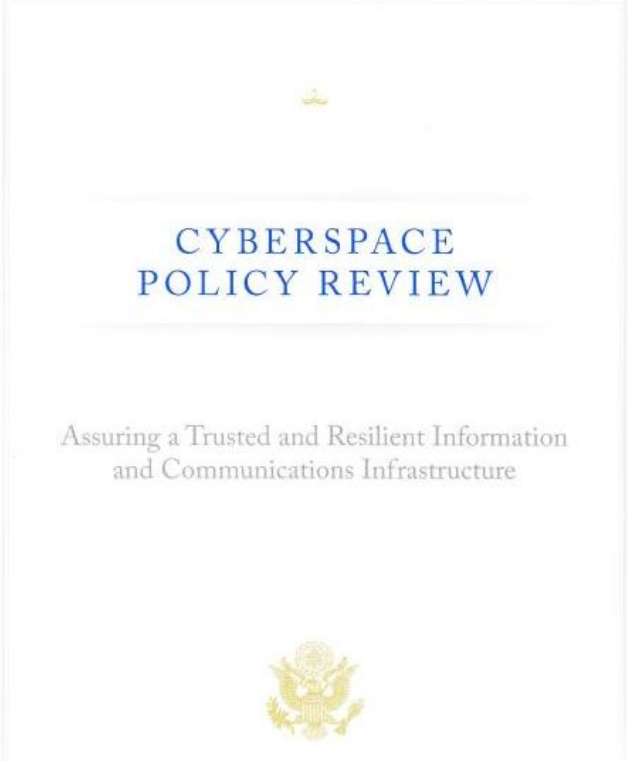
Obama speaks on cyber security

Presidential Priority

"My administration will pursue a new comprehensive approach to securing America's digital infrastructure. This new approach **starts at the top** with this **commitment from me**: From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a **national security priority**."

(President Obama, May 29, 2009)

President Obama's Report on Cyber Security (May 30 2009)



- The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights. (President's Cyber Space Policy Review page iii)

- Quoting from Internet Security Alliance Cyber Security Social Contract: Recommendations to the Obama Administration and the 111th Congress November 2008

The Economy is reliant on the Internet

- The state of Internet security is eroding quickly. Trust in online transactions is evaporating, and it will require strong security leadership for that trust to be restored. For the Internet to remain the juggernaut of commerce and productivity it has become will require more, not less, input from security. PWC Global Cyber Security Survey 2008

INTERNET SECURITY ALLIANCE

CURRENT ECONOMIC INCENTIVES FAVOR ATTACKERS

- Attacks are cheap and easy
- Vulnerabilities are almost infinite
- Profits from attacks are enormous ($ 1 TRILLION in 08)
- Defense is costly (Usually no ROI)
- Defense is often futile
- Costs of Attacks are distributed

INTERNET SECURITY ALLIANCE

The need to understand business economics to address cyber issues

» If the risks and consequences can be assigned monetary value, organizations will have greater ability and incentive to address cybersecurity. In particular, the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk. Government can assist by considering incentive-based legislative or regulatory tools to enhance the value proposition and fostering an environment that encourages partnership." --- President's Cyber Space Policy Review May 30, 2009 page 18

Regulation vs. Incentives

- ISA Social Contract argues vs. regulation which is slow/limited in effect/anti-US competitiveness/anti-security and won't work.
- Obama: "Let me be very clear, we are not going to regulate cyber security standards to the private sector." (May 29 2009)

President Obama's Report on Cyber Security (May 30, 2009)

» The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public. Additional incentive mechanisms that the government should explore include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms. President's Cyber Space Policy Review May 30, 2009 page v

» Quoting Internet Security Alliance Cyber Security Social Contract: Recommendations to the Obama Administration and 111th Congress

Proposed Incentives: Liability

» The Federal government should consider options for incentivizing collective action and enhance competition in the development of cybersecurity solutions. For example, the legal concepts for “standard of care” to date do not exist for cyberspace. Possible incentives include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms. --- Obama Administration’s Report on Cyber Security May 2009 page 28)

Obama Action Plan: International

- Near Term Action Plan Item 7

"Develop US Government positions for an international cyber security policy framework and strengthen our international partnerships to create incentives that address the full range of activities, policies, and opportunities associated with cyber security" (Obama Cyber Space Policy Review P. 37)

Securing the IT Supply Chain

» The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover. Foreign manufacturing does present easier opportunities for nation-state adversaries to subvert products; however, the same goals could be achieved through the recruitment of key insiders or other espionage activities. ---- President's Cyber Space Policy Review May 30, 2009 page 34

INTERNET SECURITY ALLIANCE

The Danger

- Electronic Components (e.g. chips) could be infiltrated by hostile agents in the supply chain
- Alter the circuitry or substitute counterfeit circuitry
- Malicious firmware functions like malicious software giving attacker control of the information system
- EG a logic bomb could be triggered by certain activity
- Shut down the system or turn it against the owner
- Impossible to detect

INTERNET SECURITY ALLIANCE

Possible Solutions

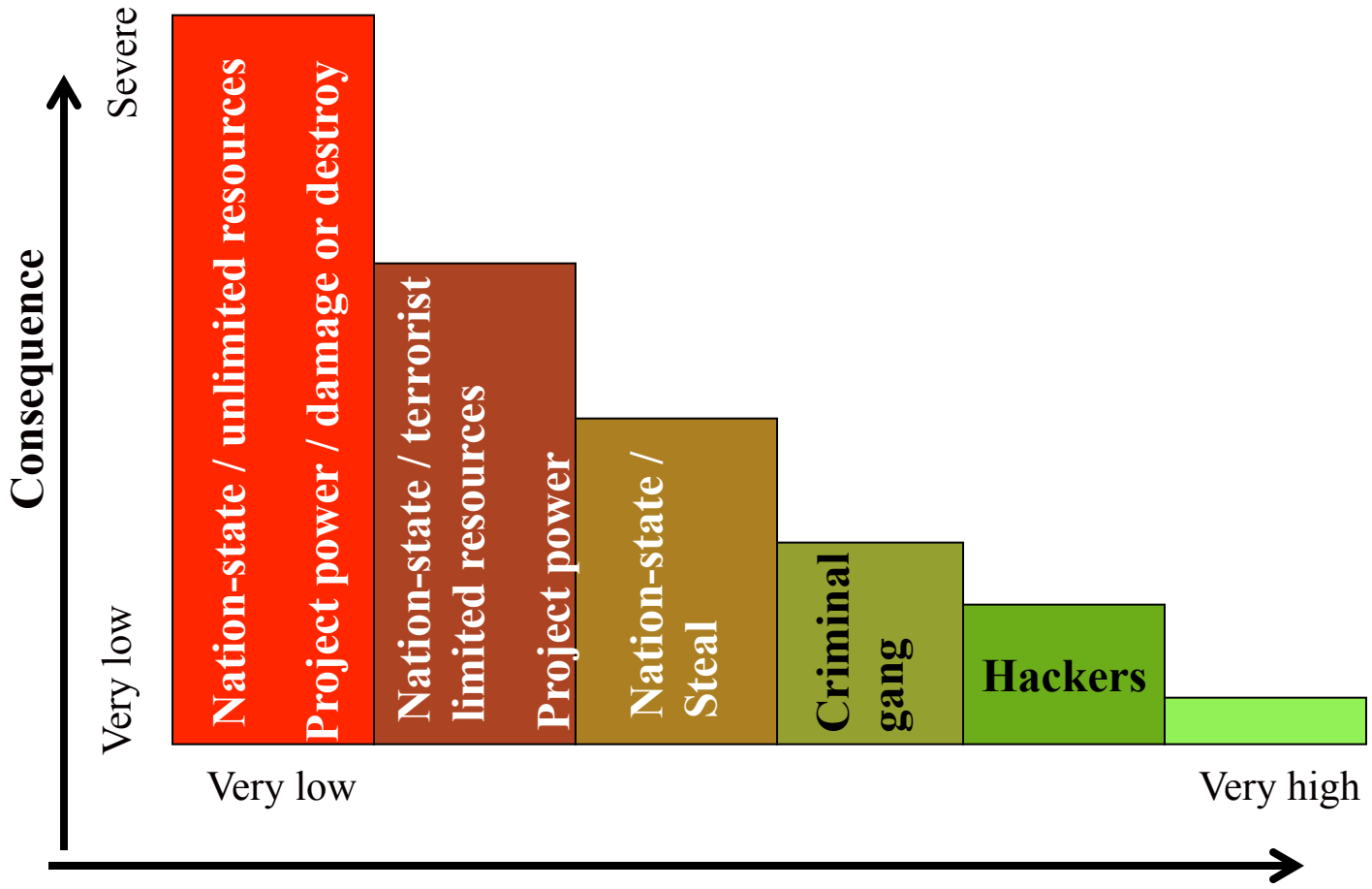
- Domestic only production?
- Inconsistent with Obama approach to Cyber Security
- Cost more than govt. willing to pay
- Crash critical portions of the industry
- Harm the US both from a security perspective and economic perspective

INTERNET SECURITY ALLIANCE

Likelihood of Supply Chain Attacks

- Limited targets for supply chain attacks
- Expensive
- Time consuming
- Can only be deployed once
- Probably easier ways to do most attacks
- Nation states might not be deterred
- Sophisticated Criminal activity

National Risk Continuum



ISA Supply Chain Project

- 18 months long (start fall 07)
- Focus on firmware
- Carnegie Mellon University and Center for Cyber Consequences Unit
- 3 conferences
- 100 Gov., Industry and Academic participants
- Results are strategy and framework provided to USG for NSC 60-day review of cyber policy

ISA/CMU Study Results

1. Globalization of IT Supply Chain will increase
2. USG reliance on IT will also increase
3. Threat from IT supply chain significant for USG
4. “USG-only” solution impractical
5. Attackers will be fluid and creative so fixed policies will be ineffective long term
6. Need a flexible framework of solutions
7. Framework must account for both security and cost

The ISA Strategy/Framework

- Solve the supply chain problem in a way that ALSO produces other security benefits thus justifying the increased expenditure
- Businesses are not suffering greatly from supply chain attacks, but are suffering from other attacks
- Key is to make the entire supply chain secure, i.e. supply chain must be part of a comprehensive framework

Types of Attacks

- Interrupt the operation
- Corrupt the Operation
- Discredit the Operation
- Undermine the basis of the operation

Types of Supply Chain Attacks & Remedies

1. Interrupt Operation: Maintain alternative sources and continual sharing of production across chain

2. Corrupt Operation (e.g. insert malware): strict control of environment where key IP is being applied, logical and physical tamper proof seals/tracking containers

3. 3. Discredit the operation (undermine trust or brand value): logging operation and responsibility

4. 4. Loss of information: Versioning as a tool for protecting IP

Framework: Stages When Attacks May Occur

1. **Design Phase**
2. **Fabrication Phase**
3. **Assembly Phase**
4. **Distribution Phase**
5. **Maintenance Phase**

INTERNET SECURITY ALLIANCE

Framework: Legal Support Needed

1. Rigorous contracts delineating security measures
2. Locally responsible corporations w/long term interest in complying
3. Local ways of motivating workers and executives
4. Adequate provision for verifying implementation of security
5. Local law enforcement of agreements at all levels

The Multi-State Agency Problem

- US Federal Government Jurisdiction Diffuse
- Health Care=HIPPA
- Financial Services = GLB
- Chemical Facilities = DHS
- FTC ALSO covers all with “unfair or deceptive acts?
- 50 states have “mini-FTC” Acts

INTERNET SECURITY ALLIANCE

EU Has Right Solution

- Strictest laws and multi jurisdictions
- European Union Safe Harbor Framework
- US companies can comply by following 7 Principles (Notice/Op-Out choice/3-Party Transfer protections/Personal Access/ Data Integrity/Enforcement
- Consistent with Obama Policy

Outdated Laws in the Digital Age
Obama Report: Conclusion

- The history of electronic communications in the United States reflects steady, robust technological innovation punctuated by government efforts to regulate, manage, or otherwise respond to issues presented by these new media, including security concerns. The iterative nature of the statutory and policy developments over time has led to a mosaic of government laws and structures governing various parts of the landscape for information and communications security and resiliency. Effectively addressing the fragmentary and diverse nature of the technical, economic, legal, and policy challenges will require a leadership and coordination framework that can stitch this patchwork together into an integrated whole. President's Cyber Space Policy Review May 30, 2009 page C-12

INTERNET SECURITY ALLIANCE

Developing SCAP Automated Security & Assurance for VoIP & Converged Networks

September, 2008

ISA Unified Communications Legal Compliance Analysis (June 2009)

1. Descibes available Unified Communications (UC) Technologies
2. Describes Security Risks of Deployment
3. Inventory of Laws to be considered pre deployment
4. Analysis if ECPA creates a legal barrier to deployment
5 Toolkit for lawyers and clients to assist in avoiding exposure from deployment

INTERNET SECURITY ALLIANCE

Information Sharing

- Problem Clearly needs additional work
- DIB model results, good, but some problems and not scalable
- Trust is built on mutual exchange
- Alternatives:
- British Consultancy Model
- Roach Motel Model

Roach Motel: Bugs Get In Not Out

- No way to stop determined intruders
- Stop them from getting back out (w/data) by disrupting attackers command and control back out of our networks
- Identify web sites and IP addresses used to communicate w/malicious code
- Cut down on the “dwell time” in the network
- Don’t stop attacks—make them less useful

INTERNET SECURITY ALLIANCE

Old Model for Info Sharing

- Big Orgs may invest in Roach Motel (traffic & analytical methods) small orgs.never will
- Many entities already rept. C2 channels (AV vend/CERT/DIB/intelligence etc.)
- Perspectives narrow
- Most orgs don’t play in info sharing orgs
- Info often not actionable
- Lack of trust

INTERNET SECURITY ALLIANCE

New Model (based on AV model)

- Focus not on sharing attack info
- Focus IS ON disseminating info on attacker C2 URLs & IP add & automatically block OUTBOUND TRAFFIC to them
- Threat Reporters (rept malicious C2 channels)
- National Center (clearing house)
- Firewall Vendors (push info into field of devices like AV vendors do now)

INTERNET SECURITY ALLIANCE

Threat Reporters

- Govt/private/commecial orgs apply
- analytical capability to discover, C2 sites via malware reverse engineering
- Gov certified so there would be trust in their reports
- Only report malware C2 info (web site/Ip address) & type (e.g. botnet)
- Can use Certification for branding

National Clearinghouse

- Receive reports and rapidly redistribute to firewall device vendors
- Track validity of reports for re-certification
- Focus is rapid dissemination of automatically actionable info

INTERNET SECURITY ALLIANCE

Firewall Providers

- Producers of devices capable of blocking outbound web traffic
- Accept data from clearinghouse
- Reformat as needed
- Recalculate to customers as quickly as possible

INTERNET SECURITY ALLIANCE

Incentives

- Threat reporters: certification for branding
- Gov: secure industrial base low cost develop common operating picture
- Firewall device vendors: new market
- Medium & small companies; Security at low cost in both money and time
- Increase trust in internet

Larry Clinton
President
Internet Security Alliance
lclinton@isalliance.org
703-907-7028
202-236-0001