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

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, Treasure
National Association 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 Corporation

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

INTERNET SECURITY ALLIANCE

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

Implementing Obama's Cyber Policy via a Social Contract Model

- Developing a market for standards, practices through market incentives
- Corporate Cyber Financial Risk Management
- Digital-legal realignment
- Securing the Global IT Supply chain
- Creating an Actionable model for information sharing

INTERNET SECURITY ALLIANCE

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

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

INTERNET SECURITY ALLIANCE

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

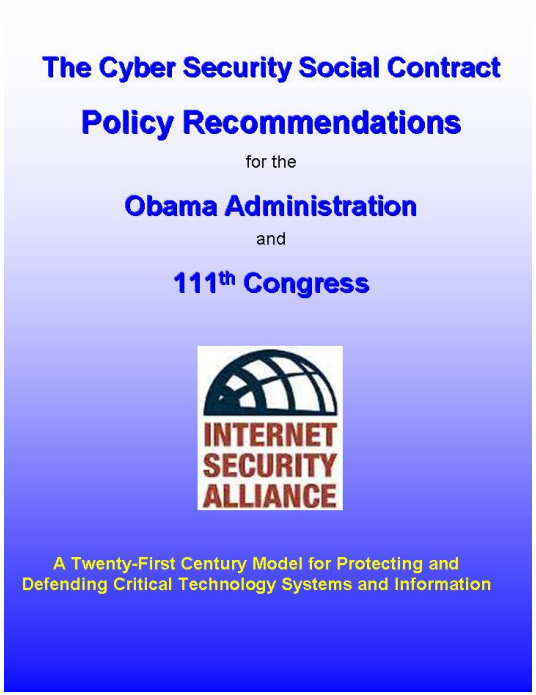
INTERNET SECURITY ALLIANCE

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



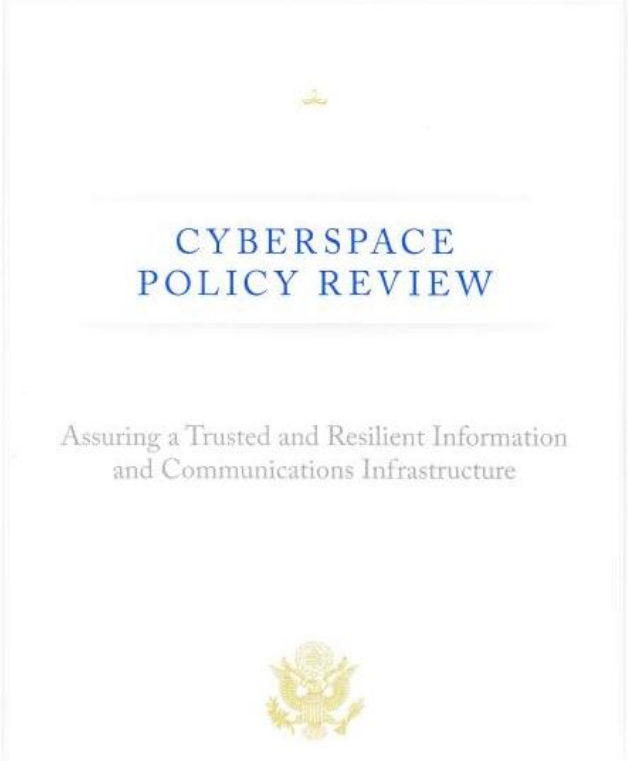
INTERNET SECURITY ALLIANCE

ISA Proposed Incentives

(Testimony E & C May 1, 2009)

1. R & D Grants
2. Tax incentives
3. Procurement Reform
4. Streamlined Regulations
5. Liability Protection
6. Public Education
7. Insurance
8. SBA loans
9. Awards programs
10. Cyber SAFETY Act

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, May 30, 2009 page iii

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

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

INTERNET SECURITY ALLIANCE

Obama Near Term Action Plan

1. **Appoint a Cyber Security policy coordinator directly responsible to the President and "dual-hatted' to both the NSC and the NEC.**

2. **Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.**

3. **Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.**

President's Cyber Space Policy Review, May 30, 2009 page vi

INTERNET SECURITY ALLIANCE

Congressional Testimony

October, 2007

ISA Model: Create a Market for Best Practices and Standards

- Studies show nearly 90% of breaches could be prevented by following known best practices and standards
- Priv Sector should continue to develop standards, practices & technologies
- Govt. test them for effectiveness
- Govt. should motivate adoption via sliding scale of market incentives

INTERNET SECURITY ALLIANCE

Financial Impact of Cyber Risk

October, 2008

Senior Exec do ARE NOT analyzing Cyber Risk adequately

There is still a gap between IT and enterprise risk management. Survey results confirm the belief among IT security professionals that Boards and senior executives are not adequately involved in key areas related to the governance of enterprise security.

2008 Carnegie Mellon University CyLab Governance of enterprise Security Survey

Communication Across Corp. Structures is Inadequate

- Intra company communication on privacy and security risks was lacking. Only 17% of respondents indicated they had a cross organizational privacy/security team.
- Less than half had a formal enterprise risk management plan. (47%)
- 1/3 of those with a plan did not include IT-related risks in the plan.

2008 Carnegie Mellon University CyLab Governance of enterprise Security Survey

Cyber RISK is not being Appreciated

- 75% of US corporations do NOT have a Chief Risk Officer
- 5% of US corporations report to the CFO on security risks
- 65% of US corporations either do not have a documented process to assess cyber risk, or do not have a person in charge of the process --- meaning they have no process

Deloitte "Enterprise Risk," 2007

Financial Management of Cyber Risk

It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.

President's Cyber Space Policy Review May 30, 2009 page 15

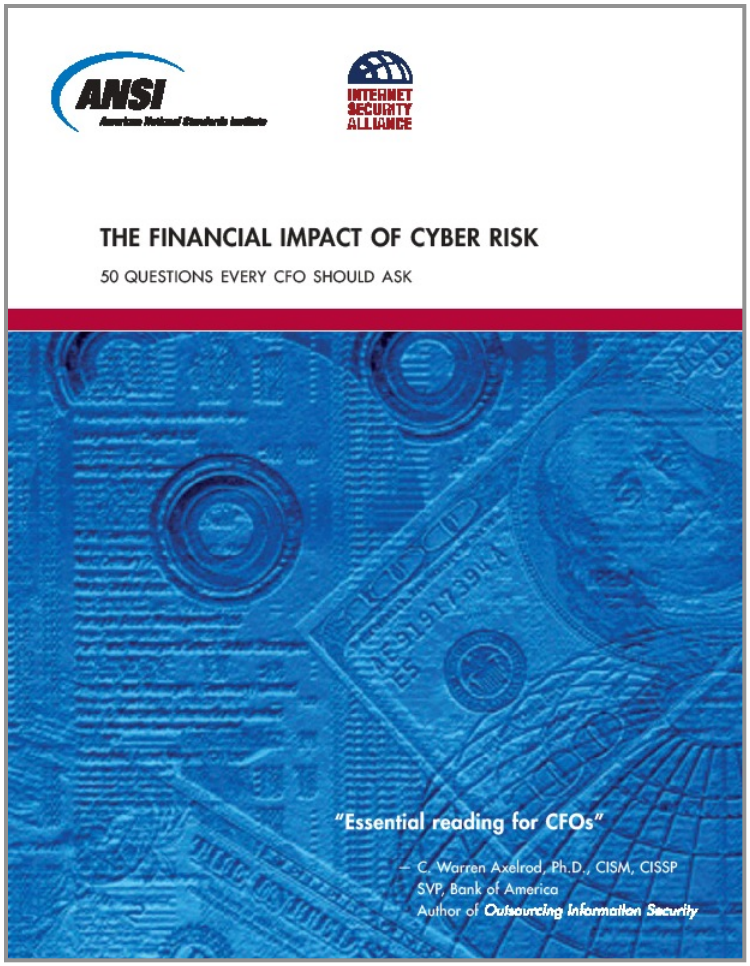
The need to understand business economics to address cyber issues

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

The Economic Assessment of Cyber Security: 50 ?s for CFOs

- Business Operations
- General Counsel
- Compliance Officer
- Media (Investors and PR)
- Human Resources
- Rick Manager/ Insurance



INTERNET SECURITY ALLIANCE

Calculate Net Financial Risk

- Threat (frequency of risk event/probably number of events per year) X
- Consequence (Severity of risk event/ possible loss form event) X
- Vulnerability (likelihood or % of damages/ given mitigation actions) MINUS
- Risk Transferred (e.g. insurance) =
- NET FINANCIAL RISK

INTERNET SECURITY ALLIANCE

Securing The IT Supply Chain In The Age of Globalization

November, 2007

Carnegie Mellon CyLab

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

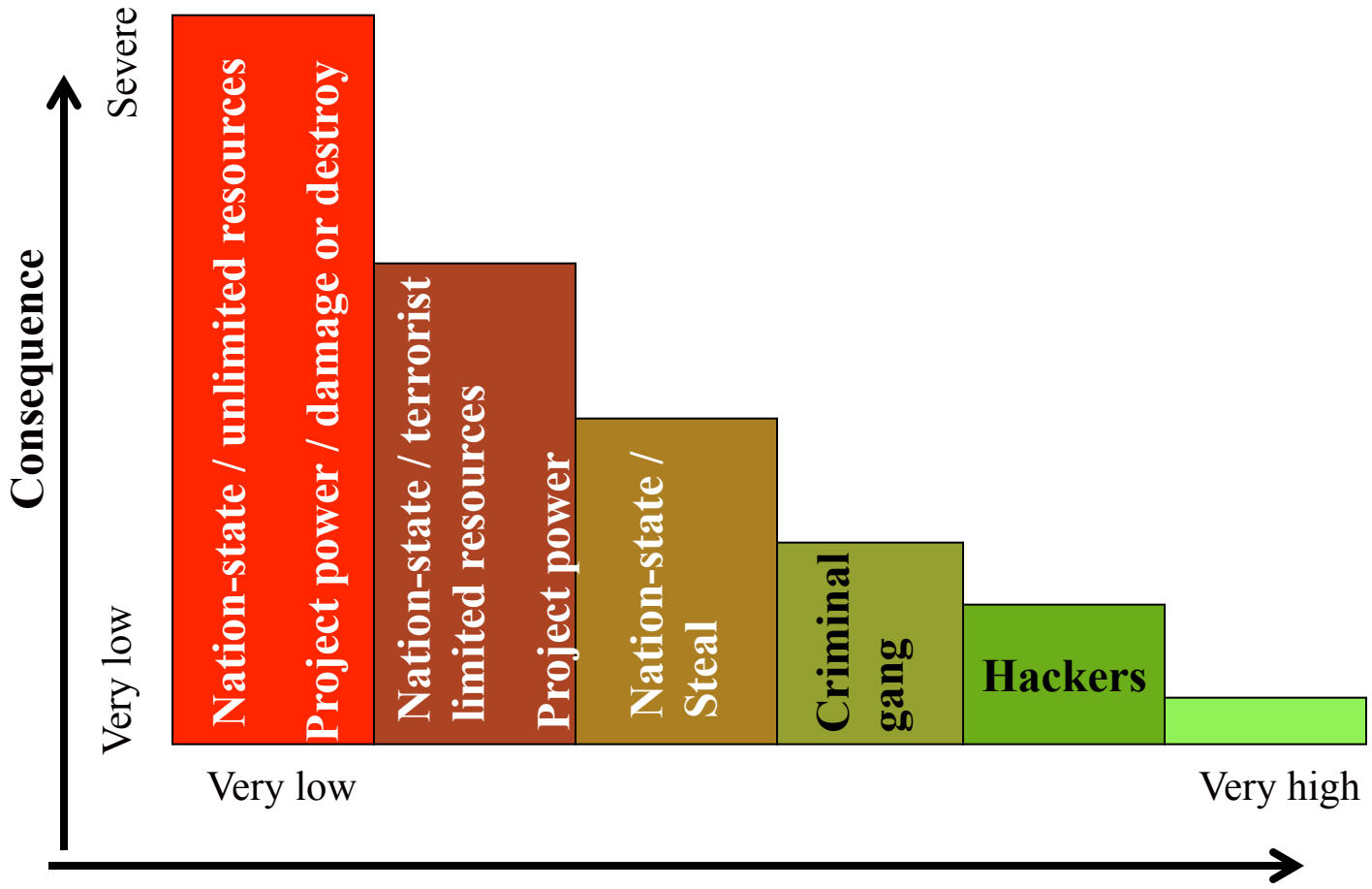
INTERNET SECURITY ALLIANCE

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

INTERNET SECURITY ALLIANCE

National Risk Continuum



INTERNET SECURITY ALLIANCE

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

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

INTERNET SECURITY ALLIANCE

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

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

INTERNET SECURITY ALLIANCE

Developing SCAP Automated Security & Assurance for VoIP & Converged Networks

September, 2008

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

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

INTERNET SECURITY ALLIANCE

Social Contract: Info Sharing

- We need to be sure information being shared can be put into action…We need to get the roadblocks out of the way
- Most companies w/limited budgets are locked into reactive defensive posture allowing for little more than signature based perimeter monitoring and if detected malware eradication.

INTERNET SECURITY ALLIANCE

Obama Cyber Review

Private sector engagement is required to help address limitations of law enforcement and national security. Industry leaders can help by engaging in information sharing…Information is the key to preventing & responding to cyber risk…A full and effective response may only be possible by brining information from all sources together to benefit all.

INTERNET SECURITY ALLIANCE

Obama Action Item #8

Develop mechanisms for cyber security related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial

INTERNET SECURITY ALLIANCE

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 address & 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

INTERNET SECURITY ALLIANCE

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