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

INTERNET SECURITY ALLIANCE

ISAlliance Mission Statement

ISA seeks to integrate advanced technology with business economics and effective public policy to create a sustainable system of cyber security.

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 Homeland Security, Verizon
Marc-Anthony Signorino, Treasure
National Association of Manufacturers

- Ken Silva, Immediate Past Chair, CSO VeriSign
- Lt. 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
- Pradeep Khosla, Dean Carnegie Mellon School of Computer Sciences
- Joe Buonomo, President, Direct Computer Resources
- Bruno Mahlmann, VP Cyber Security, Dell
- Linda Meeks, VP CISO Boeing Corporation
- Justin Somaini, CIO, Symantec
- Gary McAlum, Sr. VP & CSO, USAA
- Andy Purdy, Chief Cyber Security Strategist CSC Corp.

Roles and Responsibilites

- The private sector owns 95% of the cyber infrastructure
- Government must “provide for the common defense”
- The private sector must, by law, operate---not in the public interest---but to maximize shareholder value
- Economics must be at the core of the public private partnership

Cyber Security Economics are Skewed

- Responsibility, costs, harms and incentives are misaligned
- Individual and Corporate Financial loss
- National Defense
- Core investment is undermined by edge insecurity
- Enterprises are not structured to properly analyze cyber risk

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

Historic Role of Insurance in Cyber Security Policy

- 2002 The National Strategy to Secure Cyber Space---market approach but no need for incentives---policy makers think insurance not ready for prime time
- 2004 Congress Creates Corporate Information Security Working Group w/ Subgroup on incentives---cyber insurance is advocated

Cyber Insurance in National Policy

- 2006 ISA issues White Paper on the public policy benefits of cyber insurance—testifies before Commerce and HLS
- 2007 ISA to Department of Commerce Economic Security Working Group
- 2007 ANSI & ISA Publish “50 Questions CFOs Should Ask @ Cyber Security w/ Ch on insurance & financial risk mangement

Public Policy & Cyber Insurance History

- 2008 ISA Social Contract advocates use of cyber insurance
- 2009 President Obama's Cyber Space Policy Review advicates use of market incentives
- 2009 Dept. of Homeland Security Cross Sector Cyber Security Working Group (all critical sectors) advocates incentives including cyber insurance

History of Public Policy & Cyber Insurance

- 2010 White House holds spring conferece call w/industry academics and govt. on the use of cyber insurance
- FDIC holds conference on economics of cyber security
- Dept. of Commerce issues Notice of Inquiry on economics of cyber security including use of cyber insurace

INTERNET SECURITY ALLIANCE

Legislation

- Over 40 bills introduced covering
- Organizational Responsibilities
- Compliance and Accountability
- PII /data theft
- Cyber Security Education & R & D
- Critical Infrastructure/Vulnerability Analysis
- International Cooperation and Cyber crime
- Procurement Acquisition & Supply Chain

INTERNET SECURITY ALLIANCE

Some Major Bills

- S 139 & HR 2221 Data Breach
- S 1438 & HR 4692 Internat Cyber Crime
- S 921 FISMA Reform
- HR 2071 Intel Reauthoriztion
- S 773 Comprehenseive (Commerce Committee)
- S 3480 Comprehensive (Homeland Security Committee)
- HR 5026 Grid Reliability & Infrastructure

What (we think) is in the bill

- Establish Private Sector Responsibility for Critical Infrastructure Protection
- Govt. Role is oversight and assure compliance (not fund)
- Legislatively establish the “cyber czar”
- Create mandatory technical standards for “the most critical infrastructure”
- Require bi-annual cyber security audits w/ heavy civil fines for non-compliance

State of Play---Legislative

- Majority Leader Reid has asked for agreement on a cyber security package
- Combined Commerce/HLS bill circulating among other Senate Committies
- New “Draft’ expected shortly
- House has not weighed in
- White House has not weighed in
- Industry is fairly concerned

We need a total risk management approach

The security discipline has so far been skewed toward technology—firewalls, ID management, intrusion detection—instead of risk analysis andproactive intelligence gathering.

PWC Global Cyber Security Survey

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.

2010 Carnegie Mellon University CyLab Governance of Enterprise Security Survey

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

White House Meeting on Cyber Security July 14

- President Obama, Sec Locke, Sec. Napolitano, Howard Schmidt (others)
- Commerce speaks before DHS
- Schmidt: “need to up costs for attackers”
- Obama: “interconnected nature of the internet will make it difficult to regulate for security”
- Legislation moving in different direction

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 vs.

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

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