



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





Bottom line: The unbalanced cyber economics equation

- Attacks are comparatively cheap and easy
- Profits from attacks are enormous
- Little risk of capture
- The perimeter to defend is endless
- We are inherently a generation behind the attacker
- Defense is hard and costly with little perceived ROI

ISA Cyber Social Contract

- Similar to the agreement that led to public utility infrastructure dissemination in 20th Century (RoR regulation)
- Infrastructure development -- market incentives.
- We know what to do technically & operationally, but the economics & strategy are not in place
- Partner at the business plan level and apply market Incentives from rest of the economy to cyber

The Cyber Security Social Contract

Policy Recommendations

for the

Obama Administration

and

111th Congress



**A Twenty-First Century Model for Protecting and
Defending Critical Technology Systems and Information**



Organizational Problems

- “The security discipline has so far been skewed to technology---firewalls, ID management, intrusion detection---instead of risk analysis and intel gathering. Security investment must shift from technology heavy tactical operation it has been to date to an intelligence centric, risk analysis and mitigation philosophy. We have to start addressing the human element of security not just the technical one only then will companies stop being punching bags.” PWC 2008 Info Survey



Organizational Problems

- “There is still a gap between IT and enterprise risk management. Survey results confirm the belief among IT security professionals that Boards & Sr. Execs are not adequately involved in key areas of enterprise risk security.” CMU Dec. 2008
- 17% have cross organizational security team
- Only 47% have formal risk management plan
- 1/3 of the 47% that had a plan did NOT include IT risks in the plan----CMU Dec. 2008



Organizational problems

- 75% of companies DO NOT have a Chief Risk Officer (Delloite 2009)
- 65% of US companies either don't have a documented process to assess cyber risk or do not have a person in charge of the process they do "have in place" (Delloite 2009)---which functionally translates into really not having a plan at all.



As a Result of the Organizational problems

- Nearly half (47%) of all the enterprises studied in the **2009** PricewaterhouseCoopers Information security survey reported they are **reducing or deferring the budgets for info security initiatives**
- Even though 42% acknowledged “threats to their information security have increased” and 52% acknowledged the cost reductions make adequate security more difficult to achieve---PWC 2009



President Obama's Report on Cyber Security

The image shows the front cover of the "CYBERSPACE POLICY REVIEW" report. At the top is a small gold seal. The title "CYBERSPACE POLICY REVIEW" is in blue. Below it is the subtitle "Assuring a Trusted and Resilient Information and Communications Infrastructure" in a smaller, grey font. At the bottom is a large gold seal of the United States.

CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information
and Communications Infrastructure

- 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

Social Contract II

Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model



Issues Covered in social Contract 2.0

- Economics of cyber security
- Information sharing
- Supply chain
- Financial Cyber Risk Management
- Analog laws governing digital technology
- Developing automated security standards for converged media (e.g. VOIP)



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