



---

Larry Clinton  
President  
Internet Security Alliance  
[lclinton@isalliance.org](mailto: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, 1<sup>st</sup> 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.



# ***ISAlliance Mission Statement***

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



# The Internet Changes Everything

- Concepts of Privacy
- Concepts of National Defense
- Concepts of Self
- Concepts of Economics
- We have been focused on the HOW cyber attacks we need to focus on the WHY (\$)
- Cyber security is an economic/strategic issue as much operational/technical one



# ***ISA Cyber Social Contract***

- Similar to the agreement that led to public utility infrastructure dissemination in 20<sup>th</sup> 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

## **The Cyber Security Social Contract**

### **Policy Recommendations**

for the

**Obama Administration**

and

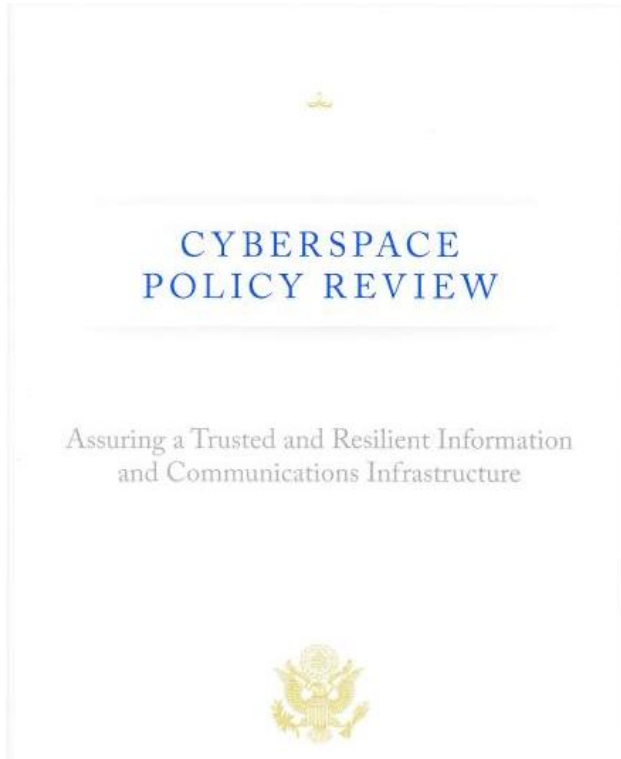
**111<sup>th</sup> Congress**



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



# ***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



# Roles and Responsibilities

- 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

# **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)



# 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



# ***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



# Administration Activities

- Cyber Command
- Expand NCSD at DHS
- Upgrade Law Enforcement
- FDIC initiative on financial system security
- Critical Infrastructure protection
- WH Initiatives---many on economics
- Department of Commerce Notice of Inquiry on Economics of Cyber Security

# 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



# Some Major Bills

- S 139 & HR 2221 Data Breach
- S 1438 & HR 4692 Internat Cyber Crime
- S 921 FISMA Reform
- HR 2071 Intel Reauthorization
- S 773 Comprehensive (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 and proactive 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***

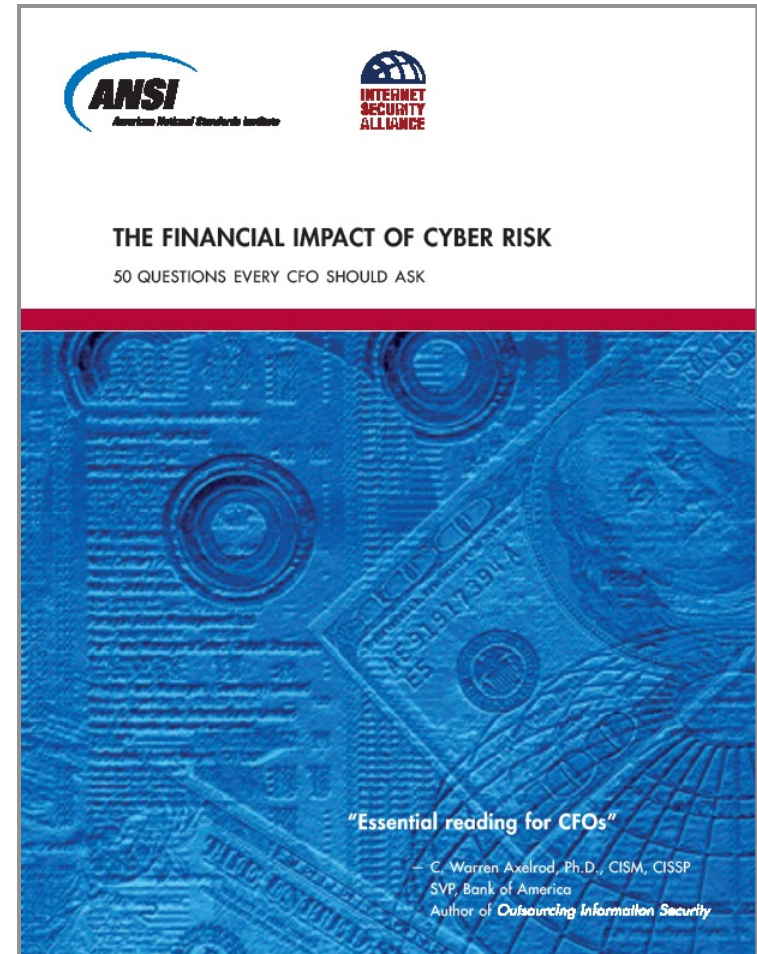
It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.

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



# ***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**



## **THE FINANCIAL MANAGEMENT OF CYBER RISK**

An Implementation Framework for CFOs

*"An excellent guide for organizations to manage the risk and exposure derived from digital dependence"*

– Melissa Hathaway  
President of Hathaway Global Strategies and  
former Acting Senior Director for Cyberspace  
for the National Security Council

*"An invaluable resource for  
every C-level executive"*

– David Thompson  
CIO and Group President  
Symantec Services Group





# 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



# Regulation is not the answer

- Compliance (not security) already eats up much of the “security” budget
- Specific Regs can’t keep up with attacks
- Vague regs show no effect
- Regs increase costs uniquely for American companies
- Regs can be counter productive ‘ceilings” (Campaign Finance)



# 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 111<sup>th</sup> Congress





---

Larry Clinton  
President  
Internet Security Alliance  
[lclinton@isalliance.org](mailto:lclinton@isalliance.org)  
703-907-7028  
202-236-0001