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 Homeland Security, Verizon
Marc-Anthony Signorino, Treasurer
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

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.

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

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

The Private Sector

- The private sector owns 95% of the cyber infrastructure
- The private sector must, by law, operate---not in the public interest---but to maximize shareholder value
- The private sector makes decisions based on economics
- The way to improve cybersecurity is to alter the economics of cybersecurity

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

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

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

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

Structural / economic misalignment

- Symantec: attacks up 500% between 6-07 & doubled again between 2009-10
- Cyber Space Policy Review: Cost to American business = $1 TRILLION
- PWC/CSIS/Forrester all report investment in information security is down in 50%-66% of American companies----and most of the security spending is for audit compliance not security

INTERNET SECURITY ALLIANCE

We are not cyber structured

- In 95% of companies the CFO is not directly involved in information security
- 2/3 of companies don't have a risk plan
- 83% of companies don't have a cross organizational privacy/security team
- Less than ½ have a formal risk management plan—1/3 of the ones who do don't consider cyber in the plan

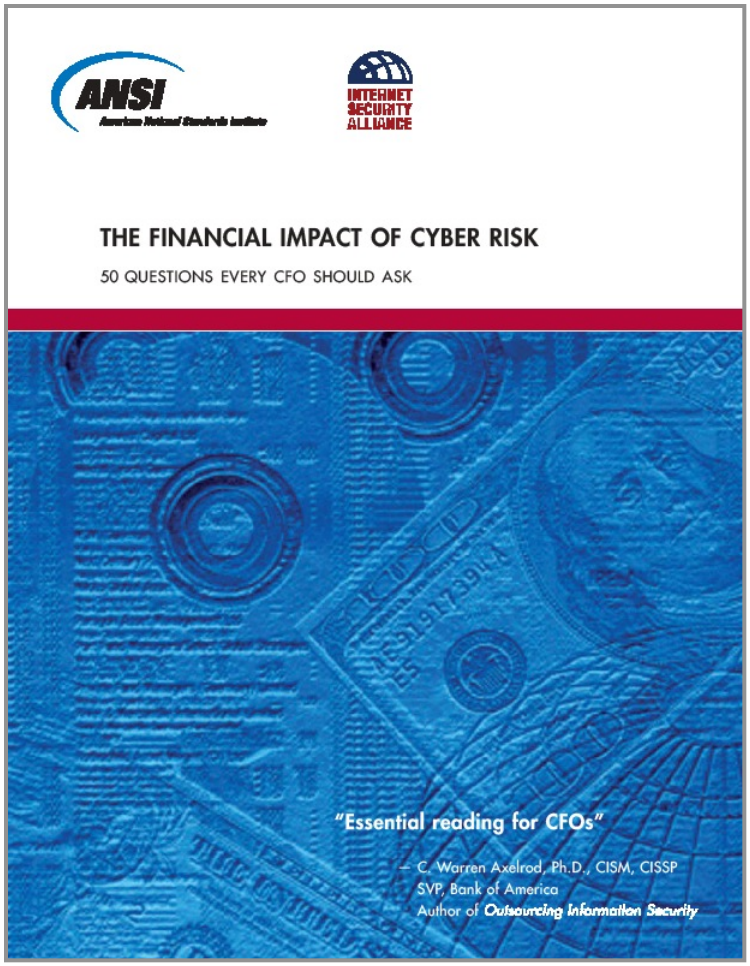
Financial Management of Cyber Risk

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.

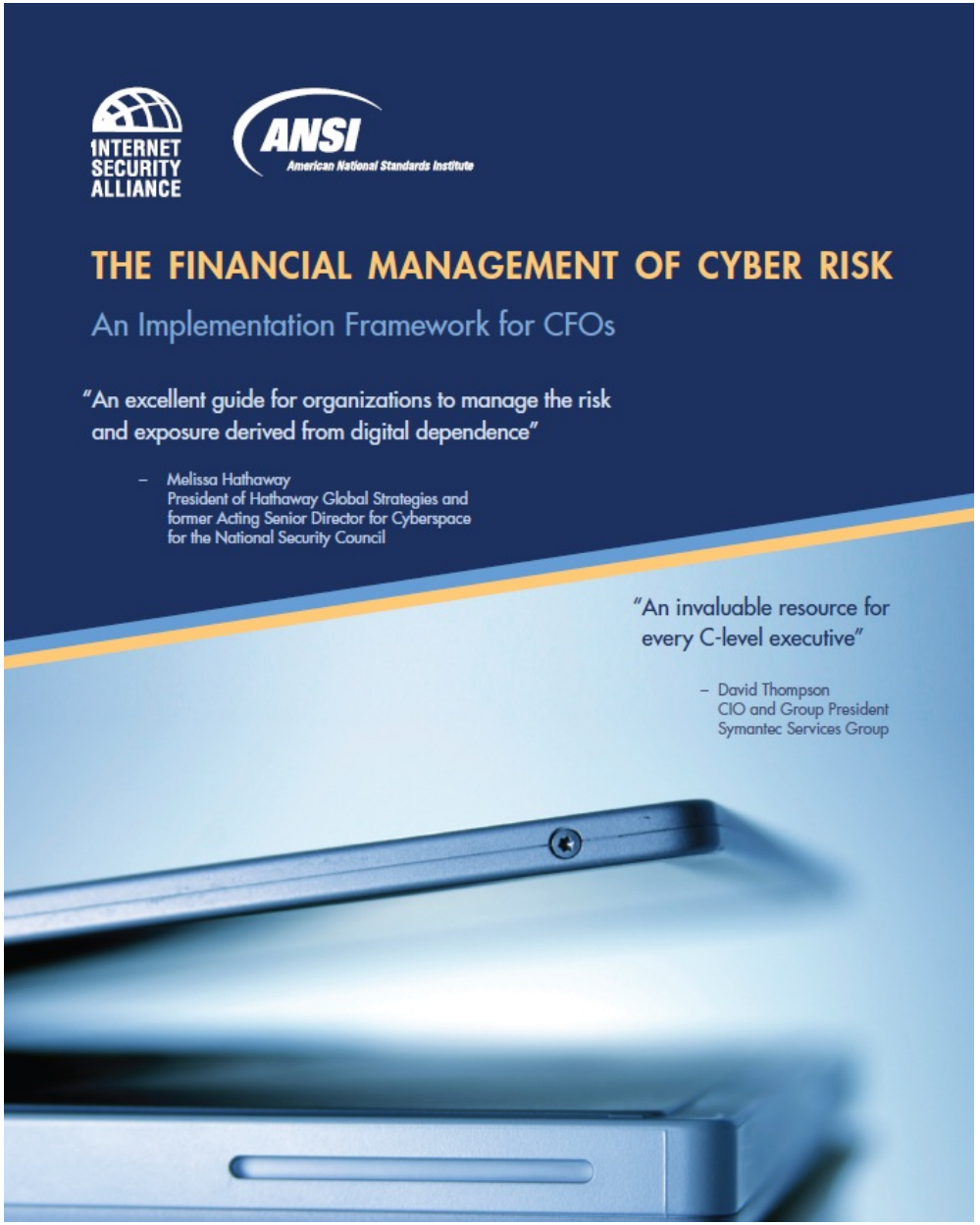
President's Cyber Space Policy Review May 30, 2009 page 15

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



ANSI-ISA Program

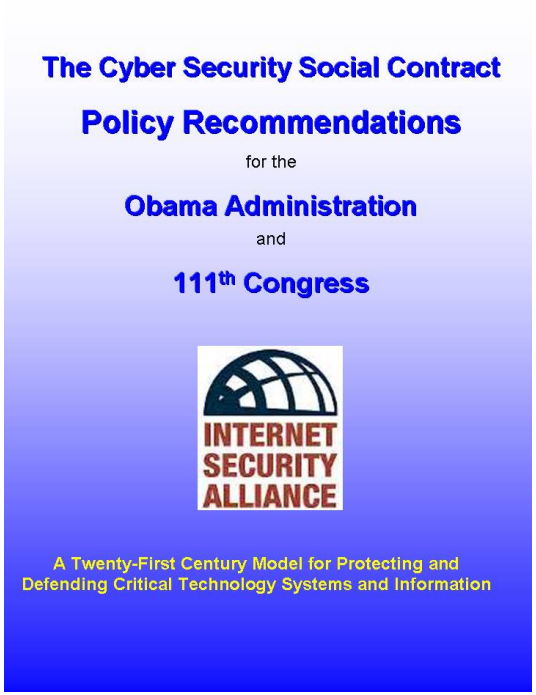
- Outlines an enterprise wide process to attack cyber security broadly and economically
- CFO strategies
- HR strategies
- Legal/compliance strategies
- Operations/technology strategies
- Communications strategies
- Risk Management/insurance strategies

What CFO needs to do

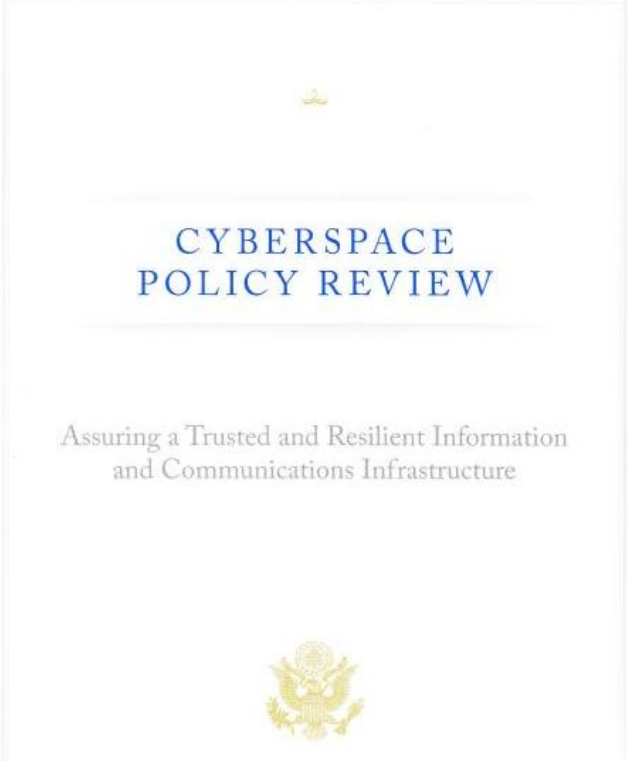
- Own the problem
- Appoint an enterprise wide cyber risk team
- Meet regularly
- Develop an enterprise wide cyber risk management plan
- Develop an enterprise wide cyber risk budget
- Implement the plan, analyze it regularly, test and reform based on EW feedback

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



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

Social Contract II

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

INTERNET SECURITY ALLIANCE

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)

Chapter 2: Partnership at the Business Plan Level

- Obama personally rejected regulation of Private Sector for cyber security
- Gov role to evaluate & create incentives for adopting good cyber secure policies practices and technologies just as in other areas of economy
- Market incentives endorsed by Obama Cyber Space Policy Review used as menu for voluntary compliance

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 111th Congress

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

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

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

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