Larry Clinton

President & CEO
Internet Security Alliance

lclinton@ISAlliance.org

703-907-7028

202-236-0001

INTERNET SECURITY ALLIANCE

Overview

- Defining the cybersecurity problem
- What does this mean for public policy
- How does the ANSI-ISA Financial Risk Management program help address the cyber security problem

Cyber Security and the Economy

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

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

We have to shift our focus from considering cybersecurity as a technical-operational issue to a economic-strategic issue

INTERNET SECURITY ALLIANCE

The Insider Threat

This year marks the first time "employees" beat out "hackers" as the most likely source of a security incident. Executives in the security field, with the most visibility into incidents, were even more likely to name employees as the source.

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

INTERNET SECURITY ALLIANCE

Follow the money

- We have –and will continue to have cyber attacks because of the economic incentives
- Attacks are easy/cheap/very profitable
- Defense is hard---successful prosecution 1%
- Perimeter to defend is endless
- Extremely hard to show ROI because enterprises don't analyze their cyber risk correctly

INTERNET SECURITY ALLIANCE

Structural / economic misalignment

- Symantec: attacks up 500% between 2006-07 & 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

Obama: What We Need to Do

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.

Obama Administration Cyber Space Policy Review
May 30, 2009 page 15

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

INTERNET SECURITY ALLIANCE

What to do…

- Good News: We know a lot about how to solve this problem--80-90% can be solved by using best practices and standards—most don't due to cost
- Focus on Enterprise Education so companies understand total financial cyber risk
- ISA-ANSI program (which is free) provides a pathway to do this

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

Human Resources

- Recruitment
- Awareness
- Remote Access
- Compensate for cyber security
- Discipline for bad behavior
- Manage social networking
- Beware of vulnerability especially from IT and former employees

Legal/Compliance Cyber Issues

- What rules/regulations apply to us and partners?
- Exposure to theft of our trade secrets?
- Exposure to shareholder and class action suits?
- Are we prepared for govt. investigations?
- Are we prepared for suits by customers and suppliers?
- Are our contracts up to date and protecting us?

Operations/IT

- What are our biggest vulnerabilities? Re-evaluate?
- What is the maturity of our information classification systems?
- Are we complying with best practices/standards
- How good is our physical security?
- Do we have an incident response plan?
- How long till we are back up?---do we want that?
- Continuity Plan? Vendors/partners/providers plan?

Communications

- Do we have a plan for multiple audiences?

--general public

--shareholders

--Govt./regulators

--affected clients

--employees

---press

Insurance—Risk Management

- Are we covered?----Are we sure?????????
- What can be covered
- How do we measure cyber losses?
- D and O exposure?
- Who sells cyber insurance & what does it cost?
- How do we evaluate insurance coverage?

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