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

Sr. Management & Cyber Security—Good News!!!

- Pricewaterhouse Coopers survey of 9,000 executives published September 2011
- “Executives were confident in their ability to secure their information systems and bullish about cyber security spending”
- 43% had confidence in their security protocals
- 50% expected their companies to spend increasing amounts of money on cyber security”

Now… the Harsh Reality

- Only 13% of the Executives polled by PWC actually had done what is considered to be “adequate” security.
- Most executives didn’t have an overall security strategy, had not reviewed the effectivness of their strategy or knew what types of breaches had hit them in the past 12 months.
- Only 1 in 3 said their companies had a policy for dealing with employee use of social media

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 Study, July 2006*

Digital Defense ------ Not So Much

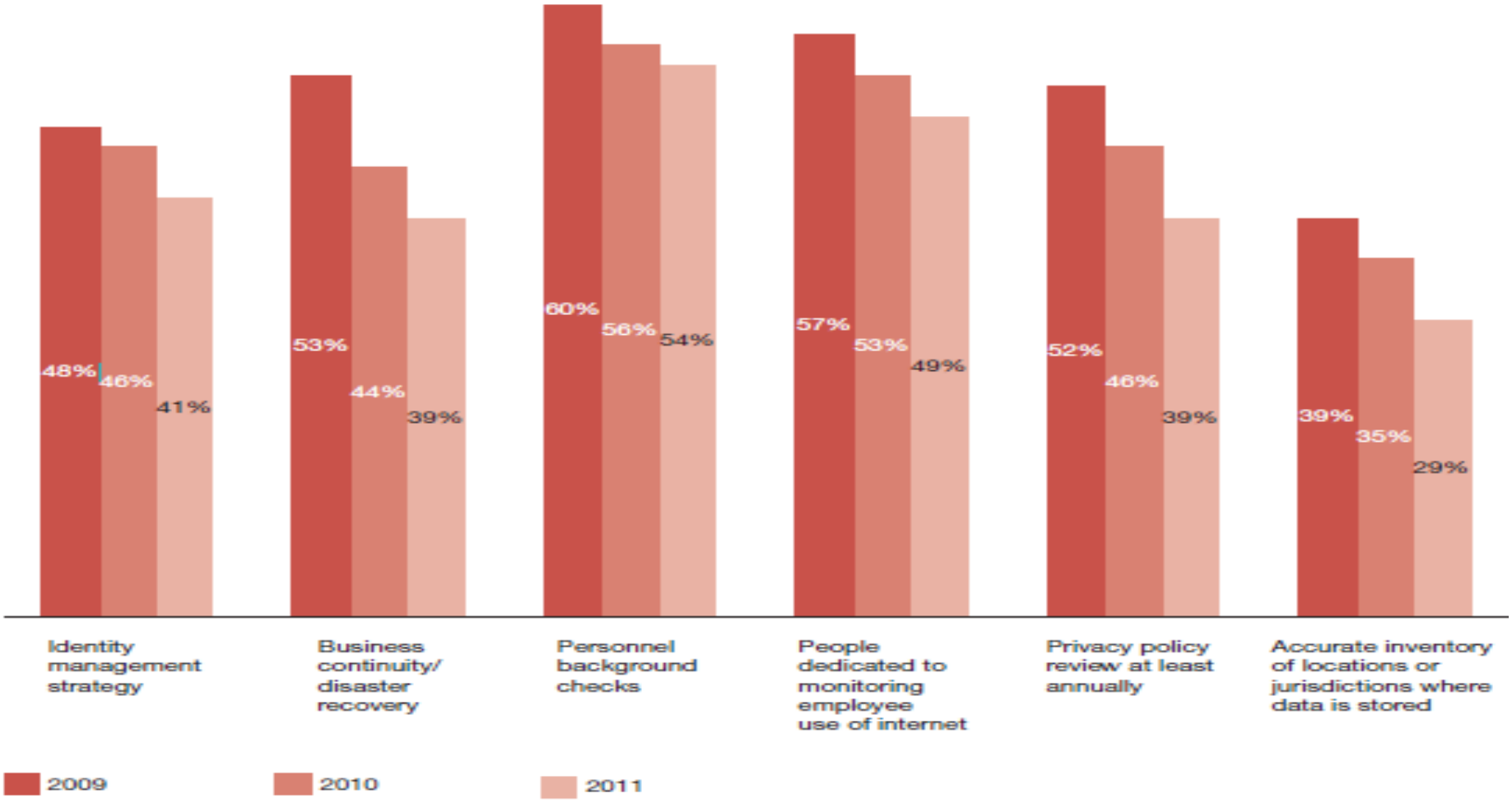
- 23% of CTOs did not know if cyber losses were covered by insurance.
- 34% of CTOs thought cyber losses would be covered by insurance----and were wrong.
- SONY v Zurich insurance---when comprehensive doesn't mean comprehensive (CGL policies)
- "The biggest network vulnerability in American corporations are extra connections added for senior executives without proper security."
- *---Source: DHS Chief Economist Scott Borg*

INTERNET SECURITY ALLIANCE

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
- In 2010 50%-66% of US Companies are deferring or reducing investment in cyber security

Corp Cyber Practices Are Degrading



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

Why is this the case?

- The vast majority of Sr management---and the majority of all employees---are digital immigrants
- Cyber Security is not, just, an “IT” problem
- “Insiders” (including lawyers and PR/sales Execs) are the single biggest cyber security vulnerability
- Most children learns their cyber behavior from their parents who learn it at work
- The enterprise space is a key educational space

INTERNET SECURITY ALLIANCE

Why is this important?

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.

INTERNET SECURITY ALLIANCE

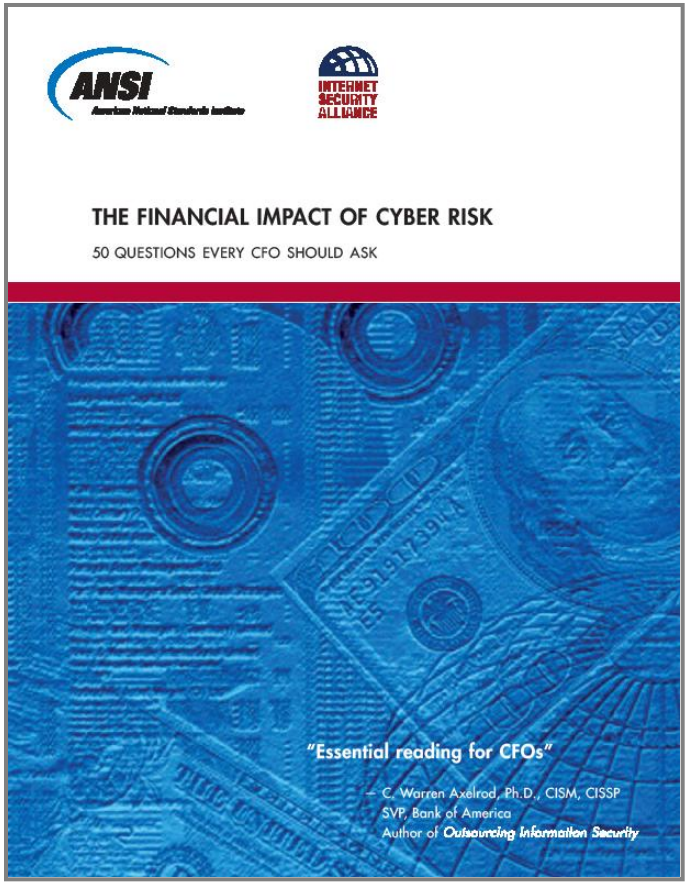
What to do…

- 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

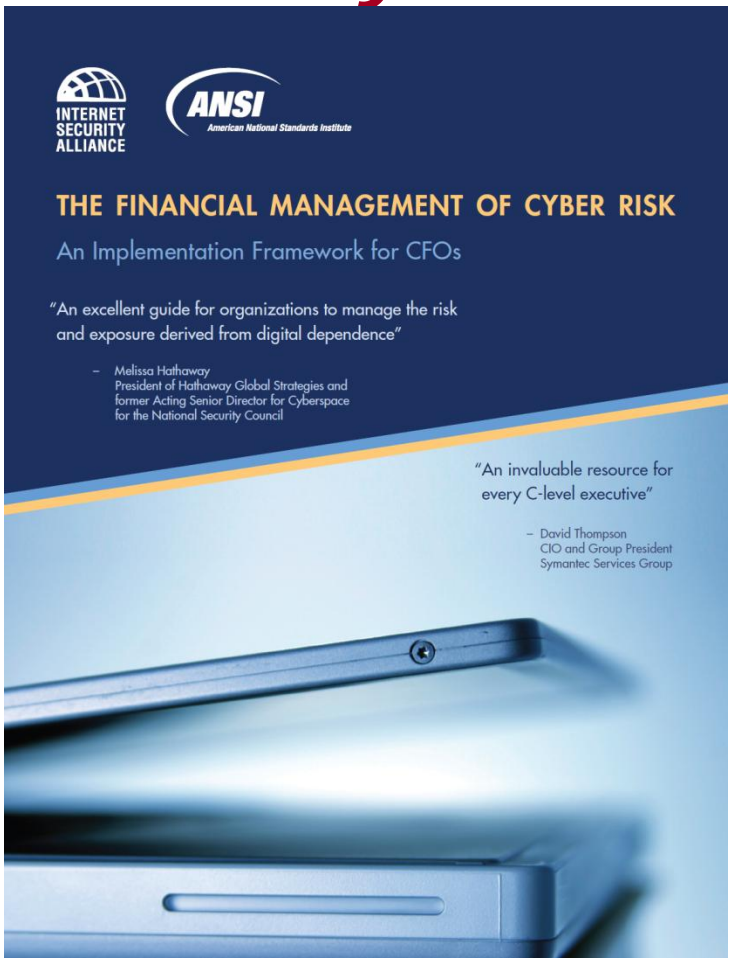
50 Questions Every CFO Should Ask (2008)

It is not enough for the information technology workforce to understand the importance of cyber security; 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

ISA-ANSI Project on Financial Risk Management of Cyber Events: "50 Questions Every CFO should Ask ----including what they ought to be asking their General Counsel and outside counsel. Also, HR, Bus Ops, Public and Investor Communications & Compliance



Financial Management of Cyber Rick (2010)



INTERNET SECURITY ALLIANCE

Government Participants

NIST

U.S. DEPARTMENT OF HOMELAND SECURITY

U.S. SECURITIES AND EXCHANGE COMMISSION · MCMXXXIV ·

DEPARTMENT OF JUSTICE · QUI PRO DOMINA JUSTITIA SEQUITUR

NATIONAL CREDIT UNION ADMINISTRATION

DEPARTMENT OF TRANSPORTATION · UNITED STATES OF AMERICA

THE UNITED STATES CYBER CONSEQUENCES UNIT

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

PEACE CORPS

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

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