How to Assess the Financial Impact of Cyber Risk

MODERATOR:

Justin Somaini
Symantec Corporation

PANELISTS:

Ty Sagalow
Zurich North America

Tom Jackson
Phillips Nizer

Larry Clinton
Internet Security Alliance

Session ID: BUS-203
Session Classification: Intermediate

RSA CONFERENCE 2011

ISA-ANSI Project

- DHS Assistant Secetary Garcia asks ISA-ANSI to develop a program on enterprise financial analysis of cyber risk 2007
- ISA-ANSI conduct 6 workshops publish “50 Questions Every CFO Should be asking @ Cyber Security” 2008 (Phase I)
- ISA –ANSI- Symantec conduct workshops on “responses” to Phase I & Publish “Financial Aspects of Cyber Risk” 2010 (Phase II)
- Currently developing Phase III targeted to CEO & Board levels

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

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

Problem: Industry is not cyber structured

- In 95% of companies the CFO is not directly involved in information security
  Deloitte, *Information Security & Enterprise Risk 2008*
- 2/3 of companies don't have a risk plan
  Deloitte, *Information Security & Enterprise Risk 2008*
- 83% of companies don't have a cross organizational privacy/security team
  Deloitte, *Information Security & Enterprise Risk 2008*
- Less than ½ have a formal risk management plan—1/3 of the ones who do don't consider cyber in the plan CyLab, *Governance of Enterprise Security Study*, December 2008
- In 2010 50%-66% of US Companies are deferring or reducing investment in cyber security
  PricewaterhouseCoopers, *Trial by Fire*, 2009

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

ISA-ANSI Phase I Produces Model of Gross Financial Risk OF Cyber Events

THREAT		CONSEQUENCE		VULNERABILITY				
FREQUENCY of Risk Event	X	SEVERITY of Risk Event	X	LIKELIHOOD Or % of Damage	−	RISK TRANSFERRED	=	NET FINANCIAL RISK
Probable number of events in a year		Possible loss from an individual event		Given the risk mitigation actions taken				

GROSS FINANCIAL RISK

(Annualized Expected Loss)

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

ANSI-ISA Phase II 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

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

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

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

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?

Apply

Complete the "equation" for attendees:

Educate + Learn = Apply

Illustrate that cyber security is more than a technical issue, it is an enterprise wide risk management issue.

Appreciate how organization changes with respect to analyzing cyber security can lead to increased investment and greater protection.

How to Apply – see slide

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Appoint an enterprise wide cyber risk team
  - Develop an enterprise wide cyber risk management plan
  - Develop an enterprise wide cyber risk budget

- Within six months you should:
  - Implement the plan, begin analyzing it regularly, test and reform based on enterprise wide (all departments) feedback

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE

Internet Security Alliance

www.isalliance.org

(703)907-7090

Larry Clinton, President

RSA 2011 CONFERENCE

INTERNET SECURITY ALLIANCE