An Executive View of Cyber Risk Management

Presented By

Ty R. Sagalow

President

Innovation Insurance Group, LLC

September 18, 2013

ISSA Conference

New York, NY

President Obama

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

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

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

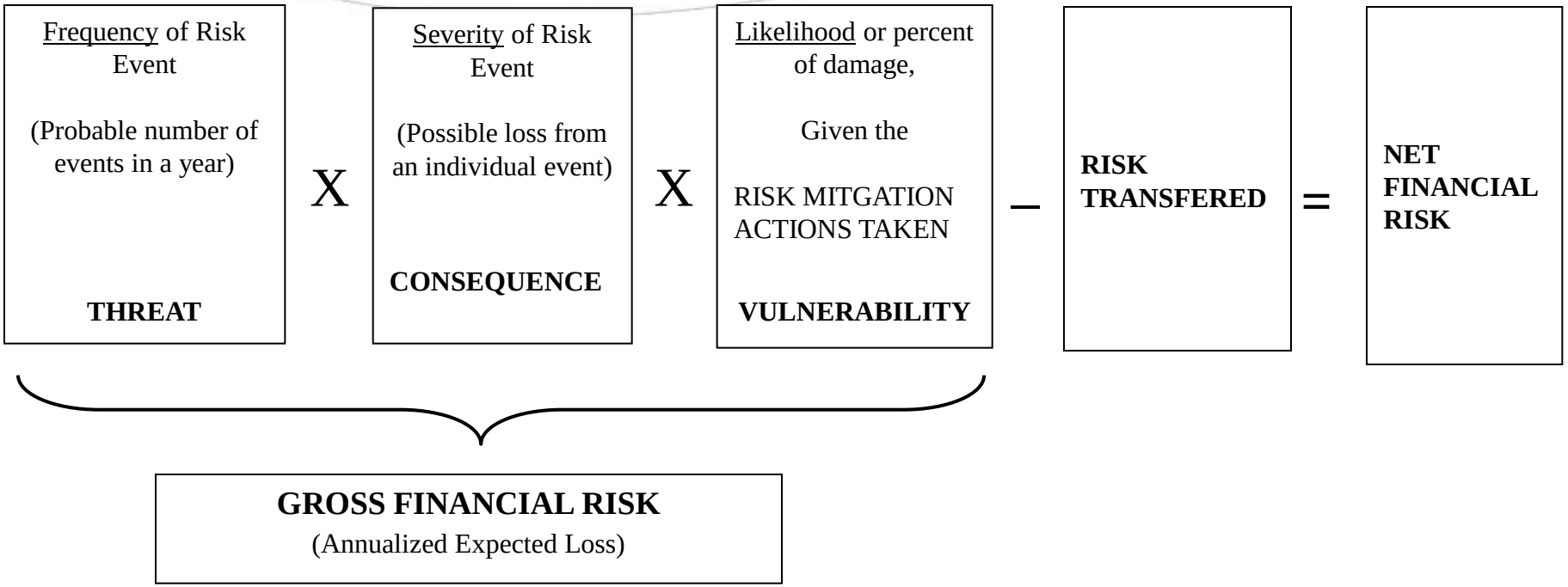
We have to shift our focus from considering cybersecurity as a technical-operational issue to a economic-strategic issue

Follow the money – Part 2

Overall, cost is most frequently cited as "the biggest obstacle to ensuring the security of critical networks.

- Making the business case for cybersecurity remains a major challenge, because "management often does not understand either the scale of the threat or the requirements for a solutions
- The number one barrier is the security folks who haven't been able to communicate the urgency well enough and they haven't actually been able to persuade the decision makers of the reality of the threat.

A Financial Perspective



The Result: We are not cyber structured

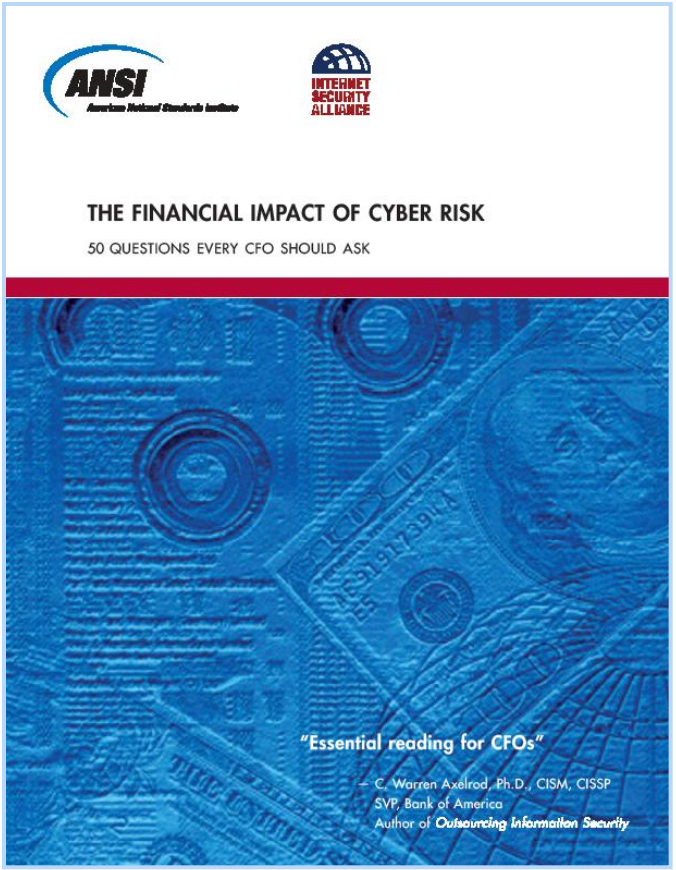
- In 95% of companies the CFO is not directly involved in information security
- 2/3 of companies don't have a risk plan
- Less than ½ have a formal risk management plan—1/3 of the ones who do don't consider cyber in the plan
- In recent years most US Companies are deferring or reducing investment in cyber security
- **More than 80% of companies don't have a cross organizational privacy/security team**

The need for a interdepartmental approach

- Cyber risk management is 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

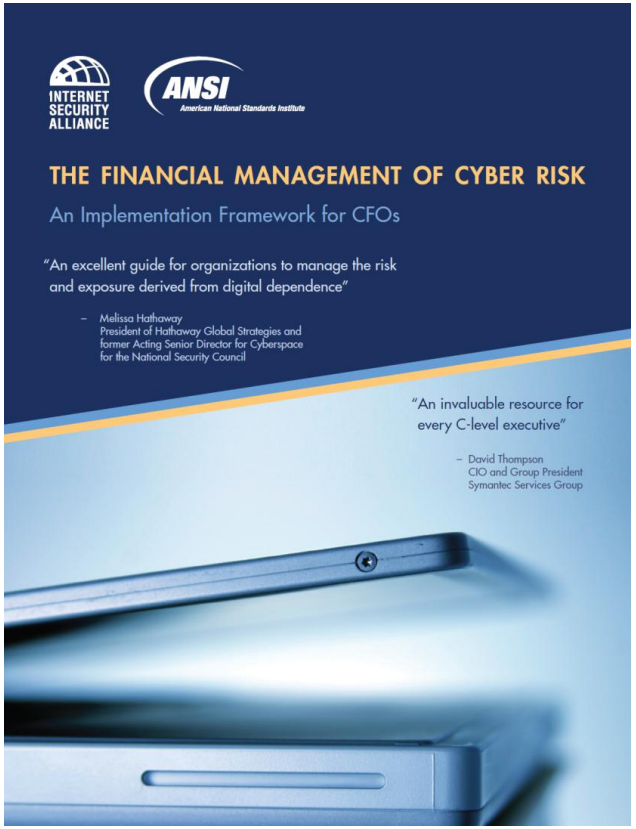
The Financial Impact of Cyber Risk (2008)

In 2008, the Internet Security Alliance in cooperation with the American National Standards Association organized a join Project on **Financial Risk Management of Cyber Events: "50 Questions Every CFO should Ask.**



Financial Management of Cyber Risk (2011)

In 2011, the same group produced a follow-up to their 2008 publication setting for the questions and answers to the top 50 questions from the point of view the a company's top security officer, lawyer, financial executive, risk manager, human resources manager and communications executive.



Government Participants

Cyber Insurance: A Brief History

- **Traditional Insurance Policies to Cover Business Loss** –
  - (1) Business Personal Insurance Policies (first-party loss)
  - (2) Business Interruption Policies
  - (3) Commercial General Liability (CGL) or Umbrella Liability Policies (for damage to third parties)
  - (4) Errors and Omissions Insurance (for Corp. Officers)

- **1970s** – Development of specialized policies that typically extended crime insurance to cover against outsider gaining physical access to computer systems

- **1998** – Advent of Hacker Insurance Policies

- **2000** – Early Forms of Cyber Insurance (1st and 3rd Party) Appear

State of the Market Today

- Number of Carriers – Betterly Report survey finds an increase of Cyber Insurers from 19 in 2010 to 39 in 2012
- **Annual U.S. Gross Written Premiums (GWP) – Betterly Report estimates a total cyber market now past $1 Billion!**

Cyber Risk Insurance Providers

Ace	Admiral
Allied World	Arch
Axis	Beazley
Brit	CFC
Chartis	Chubb
CNA	Crum & Forster
Digital Risk	Euclid
The Hartford	Hiscox
Ironshore	Liberty International
Markel	NAS
Navigators	OneBeacon
Philadelphia	RLI
Safeonline	ThinkRisk
Travelers	XL
Zurich	

Betterly, Richard. "Cyber/Privacy/Media Liability Market Survey – 2011." The Betterly Report (2011): Web. http://betterley.com/samples/CyberRisk11_nt.pdf

Armin, Jart. "Hackers Take Notice: Cyber-Insurance is on the Rise." internet evolution. 27 June 2011: Web. http://www.internetevolution.com/author.asp?section_id=717&doc_id=230782

So, What Can Cyber Policy Cover?

- Third-Party Liability—Defense/Indemnity relating to:
  - Media Liability/Website Media Content
    - Internet-related defamation, intellectual property violation
  - Information, Security, and Privacy—
    - Theft, loss, unauthorized disclosure of personally identifiable information ("PII");
    - Alterations, corruption, destruction, deletion, or damage to data
  - Network Security—breach of network security
- Regulatory Action—Defense and penalties relating to breach of laws associated with control and use of PII
- Notification and Credit Monitoring Costs—Reimburse insured for costs of notification or for credit monitoring for injured people after insured's loss of their PII

So, What Can Cyber Policy Cover?

- First-Party Business Interruption Loss—Relating to a network attack (often excluded from property policy)
- Cyber/Network Extortion—Reimburse insured amounts paid to avert a credible threat to commit or continue a network attack against the insured or to disclose PII for the purpose of obtaining payment
- Crisis Event Management—Public relations costs in dealing with restoring public confidence in insured following material covered event
- Data Forensic/Privacy Breach Response Expenses—Reimburse insured for the expenses to determine the cause, source, and extent of a network attack following a data breach and possibly fix it

How do these guys underwrite this stuff?

- See Slide 1 (Ok, slide 7)
- The importance of service providers – managing the PII risk
  - Forestics
  - Lawyers
- Industry factor
- Size Factor
- Underwriting the *Process* not the *Technology*

Appendix

Q&A

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?