CYBERSECURITY RISK MANAGEMENT AND INSURANCE

by

Paul J M Klumpes
Professor of Sustainable Finance and Risk Accounting

GIRO Conference September 2014

Authors Brief

- Paul Klumpes
  - Professor of Risk Accounting and Sustainable Finance, Nottingham Trent University
  - PhD LLB BComMCom CPA (Australia)
  - Research specialization is risk reporting, audit and financial institutions, risk management exposure and cost of capital estimation
  - 60 publications including Journal of Business, Journal of Banking and Finance, Journal of Accounting Auditing and Finance, Journal of Accounting Literature
  - 7 years experience in financial services
  - Consultant to Analytics and GLG
  - Has previously been Professor of Risk Accounting at Nottingham University, and Associate Professor at Warwick University and Lancaster University and Lecturer at Australian National University
  - Current research awards include
    - IAAER-KPMG Liabilities and Equities Program: risk management and cost of capital
    - ACCA: derivative reporting by MNCx

Main Objectives

- Briefly Discuss the Concept and Importance of Cybersecurity Risk Management
- Develop proposal toTSB

Basic Concepts

Cybersecurity

Protection of Information Transmitted and Stored over the Internet or any other Computer Network

Objectives of Cybersecurity

Protect Confidentiality of Private Information

Ensure Availability of Information to Authorized Users on a Timely Basis

- Authentication
- Nonrepudiation

Protect the Integrity of Information (i.e., Accuracy, Reliability, and Validity)

Basic Concepts (Cont:)

Cybersecurity Risk

Uncertainty of Potentially Harmful Events Related to Cybersecurity

Cybersecurity Risk Management (CRM)

Process of Managing (Reducing) Potentially Harmful Uncertain Events Due to the Lack of Effective Cybersecurity. CRM is a subset of Enterprise Risk Management

COSO's Definition of Internal Control (1992)

The Committee of Sponsoring Organizations of the Treadway Commission (usually referred to as COSO) defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in the following three categories:

(1) effectiveness and efficiency of operations;

(2) reliability of financial reporting; and

(3) compliance with applicable laws and regulations.

COSO's Enterprise Risk Management – Integrated Framework (2004)

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004).

Entity's Objectives in COSO (2004) are:(1) Strategic high-level goals, (2) Operating, (3) Reporting, and (4) Compliance.

ERM, IFRS and Solvency II

- QIS4 based on IFRS (?)
- Some differences   - oriented towards measurement of liabilities
- Allows for unhedgeable risks to be incorporated
- Entity theory view of reporting
- Solvency II reporting like underwriting year
- Appears to link to EWRM – or does it?
- Different reason for reporting:
  - What assets and liabilities does the insurer have (IFRS)?
  - What assets should an insurer hold (S II)?

2. PWC UK security breach survey

- Security breaches increased in 2011
- Relative to others; insurers:
  - Subject to most external attacks
  - Have significant business exposure
  - Suffer greatest loss

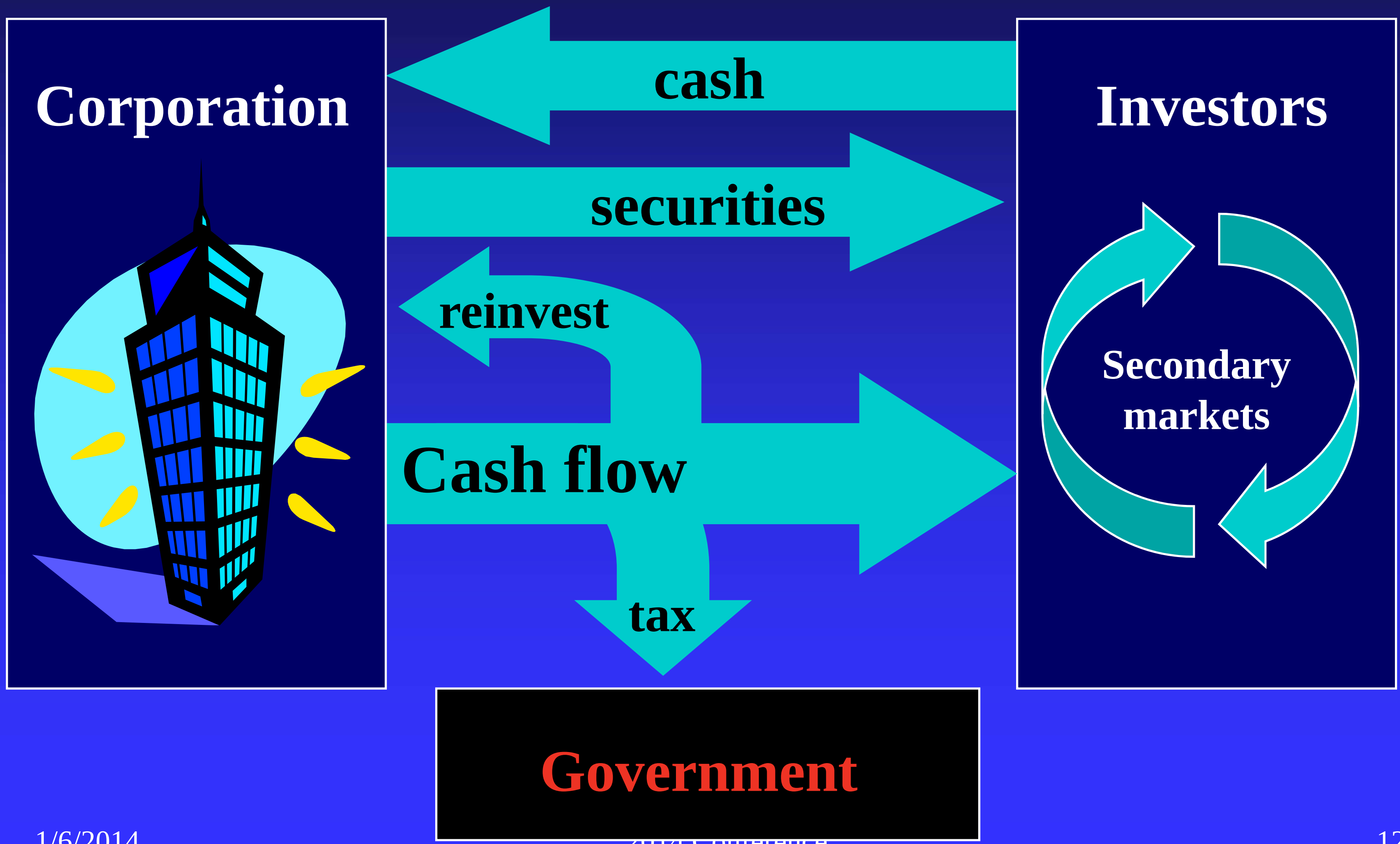
3 Institutional backgound

- Demands for mandatory disclosure of security breaches?
  - SEC 2011 guidance
  - IFRS limited requirements
    - IAS 1
    - IFRS 7
- Voluntary disclosure only?
  - Proprietary theory explanation
  - Guidance from regulators
  - Cloud computing developments?

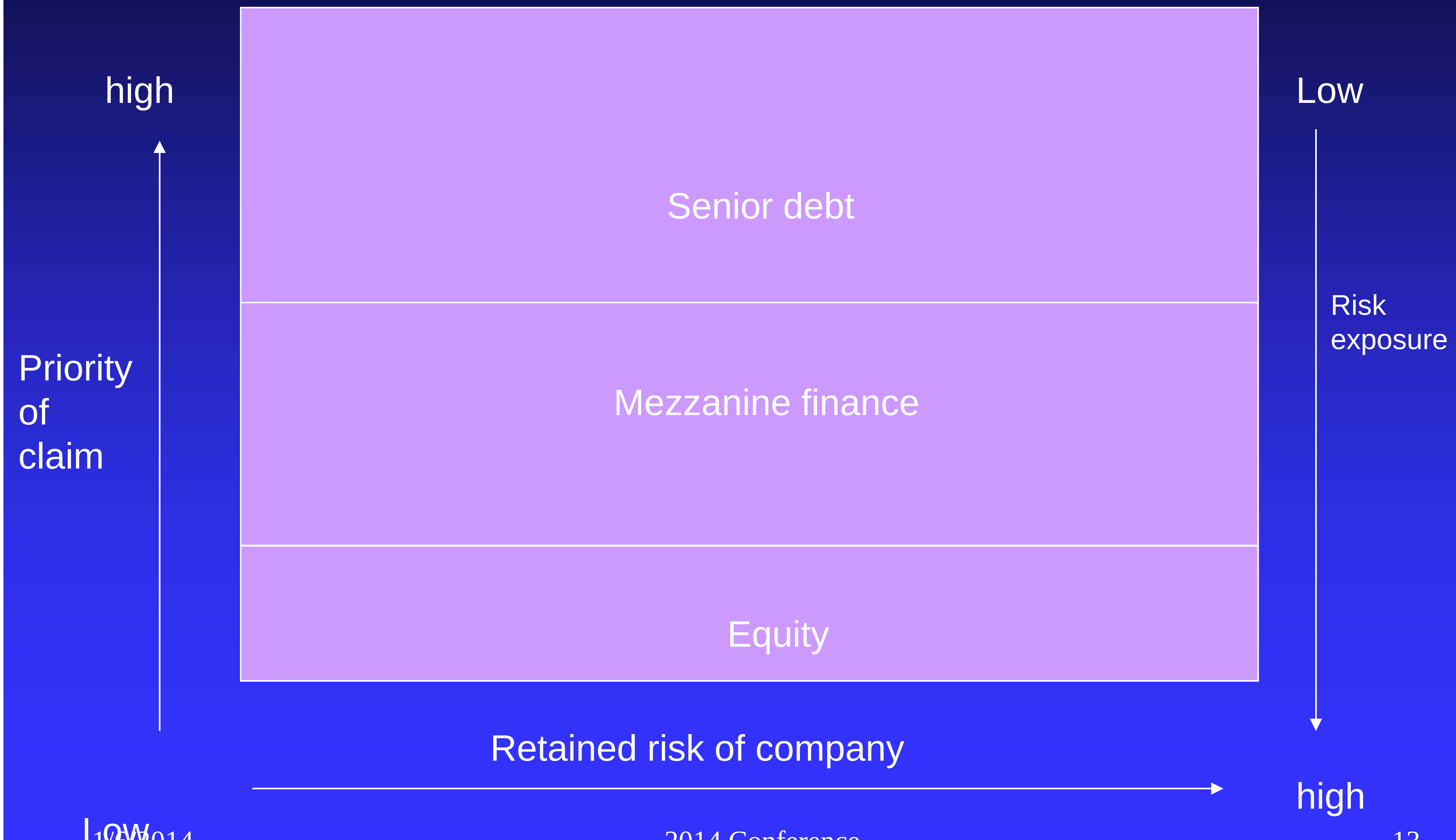
Current Example of Legal Compliance 2 – Cybersecurity risks in the EU?

- http://www.bbc.co.uk/news/uk-politics-26046720
- Worldwide problems
  - UN conventions?
  - EU legislation
  - UK Legislation
    - Data Protection Act 1998
    - Freedom of Information Act 2002
    - Human Rights Act 1998 and right to privacy?
  - Patents infringement
  - Criminal law; state monitoring of www?

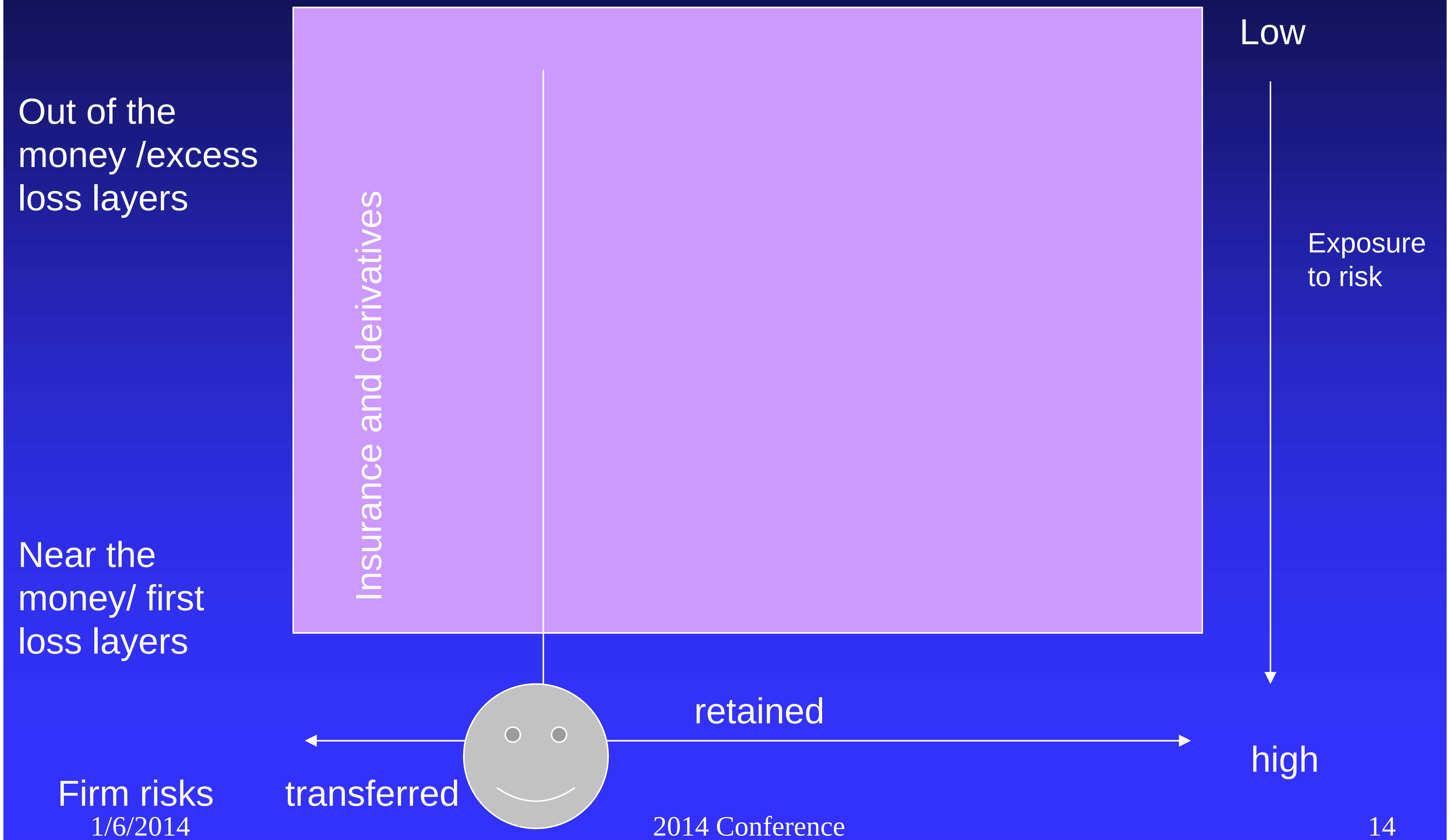
3. Sources of breaches



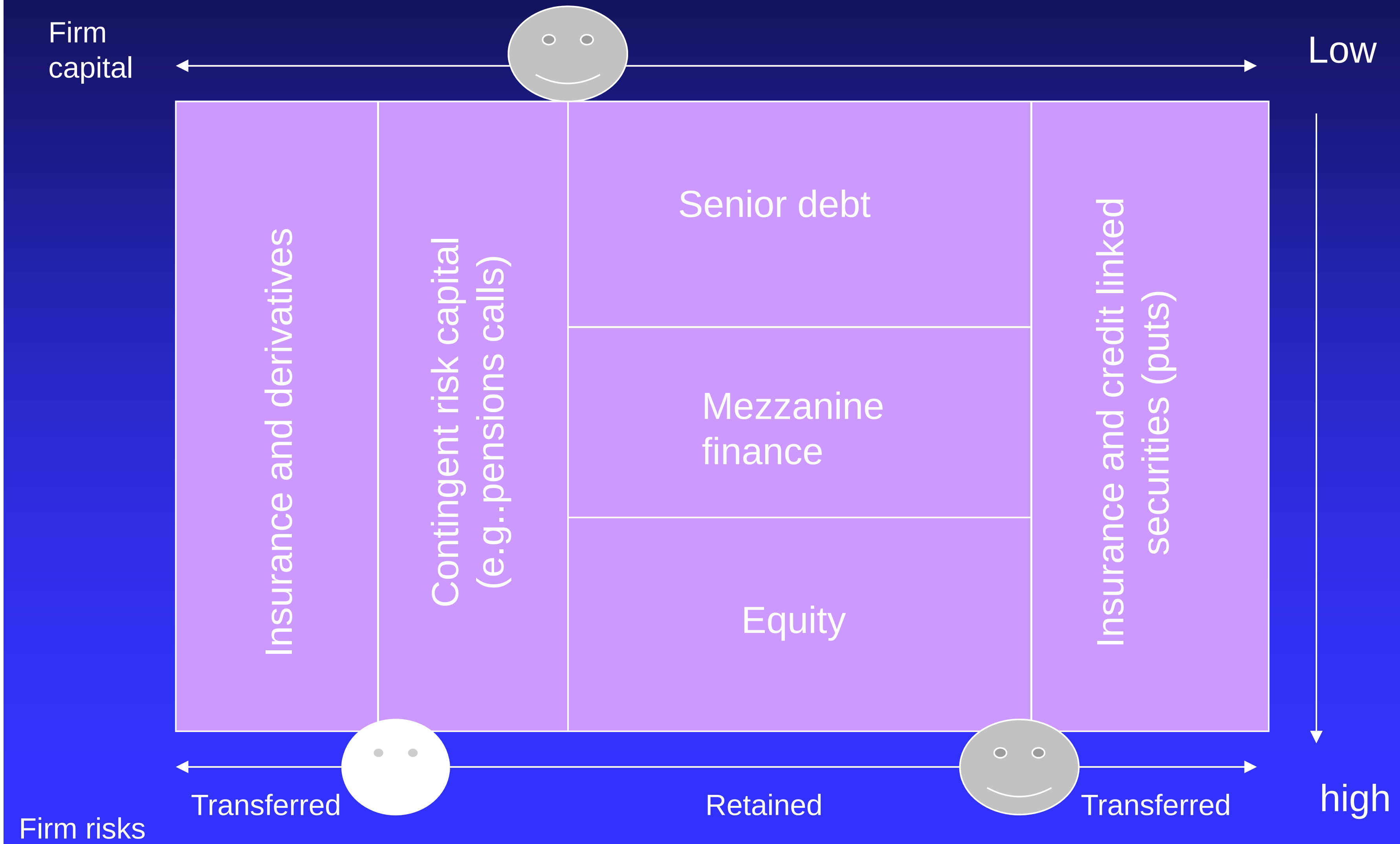
4. Capital structure: standard view



IFRS model of corporation



“Insurative” SII model of the firm



ENTERPRISE RISK MANAGEMENT and ENTERPRISE RESILIENCE

Enterprise risk management (ERM) is the "overall process of managing an organization's exposure to uncertainty with particular emphasis on identifying the events that could potentially prevent the organization from achieving its objectives" ('Gordon and Loeb, 2006, p.175).

However, no matter how well managed, organizations may experience major disruptions (e.g., theft of an entire database that contains confidential information on customers).

Enterprise resilience represents an organization's ability to adapt to such disruptions, and even grow in the face of such adversity.

Popular Myths

1. RISK CONCEPT IS WELL UNDERSTOOD*
2. APPLYING COST-BENEFIT ANALYSIS TO CYBERSECURITY THREATS IS VOODOO ECONOMICS*
3. ALL CYBERSECURITY BREACHES HAVE A SIGNIFICANT IMPACT ON ORGANIZATIONS*
4. INFORMATION SHARING REDUCES CYBERSECURITY RELATED PROBLEMS*
5. SOX HAS NO IMPACT ON CYBERSECURITY ACTIVITIES*
6. CYBERSECURITY INSURANCE IS TAKING OFF*

1. RISK CONCEPT IS NOT WELL UNDERSTOOD*

RISK METRICS

Expected Loss

Most Popular in Information Security Literature

= (Probability of Loss) X (Amount of Loss)

Probability of No Loss

Probability of Largest Loss

Variance (or Standard Deviation) of Losses

Most Popular Metric in Management Accounting, Economics & Finance

Figure 1: Different Risk Metrics

(1)	(2)	(3) = (1) x (2)	(4)	(5) = (1) x (4)	(6)	(7) = (1) x (6)
Possible Losses	Probability of Losses	Expected Value of the given loss	Probability of Losses	Expected Value of the given loss	Probability of Losses	Expected Value of the given loss
	Investment A		Investment B		Investment C	
$0	0.40	$0	0.60	$0	0.15	$0
$1,000,000	0	$0	0	$0	0.60	$600,000
$2,000,000	0.60	$1,200,000	0	$0	0.15	$300,000
$3,000,000	0	$0	0.40	$1,200,000	0.10	$300,000

Expected Value of Losses

Investment A=sum of column (3)	$1,200,000		
Investment B=sum of column (5)		$1,200,000	
Investment C=sum of column (7)			$1,200,000

Investment A, B and C are Equal Amounts

Equal Expected Value of Loss

Source: Gordon and Loeb, 2006a, p. 98.

Figure 1: Different Risk Metrics

(1)	(2)	(3) = (1) x (2)	(4)	(5) = (1) x (4)	(6)	(7) = (1) x (6)
	Probability of Losses	Expected Value of the given loss	Probability of Losses	Expected Value of the given loss	Probability of Losses	Expected Value of the given loss
Possible Losses	Investment A		Investment B		Investment C	
$0	0.40	$0	0.60	$0	0.15	$0
$1,000,000	0	$0	0	$0	0.60	$600,000
$2,000,000	0.60	$1,200,000	0	$0	0.15	$300,000
$3,000,000	0	$0	0.40	$1,200,000	0.10	$300,000
Expected Value of Losses						
Investment A=sum of column (3)		$1,200,000				
Investment B=sum of column (5)				$1,200,000		
Investment C=sum of column (7)						$1,200,000
Investment A, B and C are Equal Amounts						

Smallest Probability of Largest Loss

Largest Probability of No Loss

Smallest Variance of Losses

Source: Gordon and Loeb, 2006a, p. 98.

2. APPLYING COST-BENEFIT ANALYSIS TO CYBERSECURITY THREATS IS NOT VOODOO ECONOMICS *

Planning and Control of Cybersecurity Investments

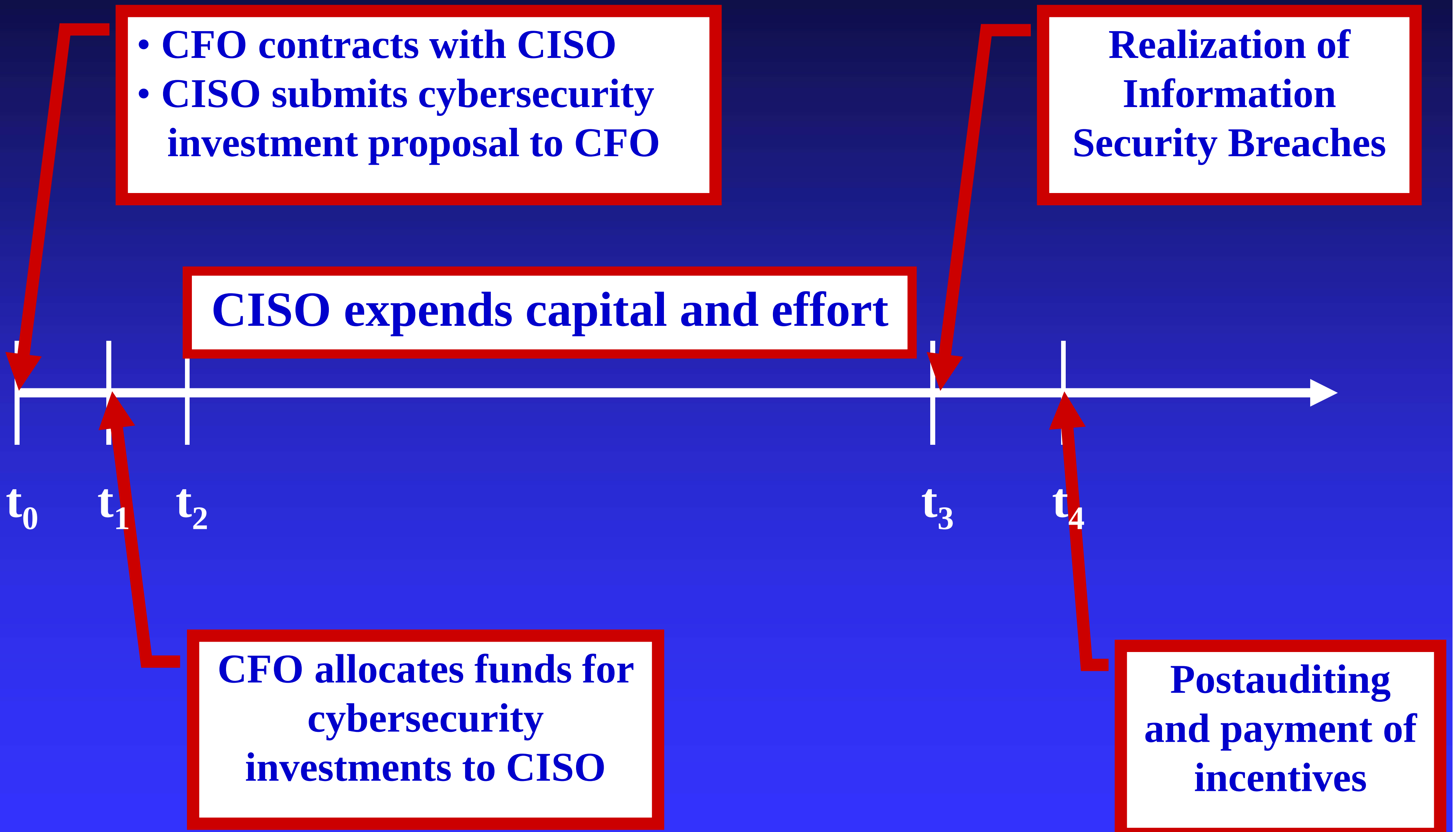
- The Business Case
- Postauditing

Figure 2: The Business Case for Cybersecurity Investments

1. Specify Organizational Cybersecurity Objectives
2. Identify Alternatives for Achieving Cybersecurity Objectives
3. Acquire Data and Analyze Each Alternative Identified
4. Conduct Cost-Benefit Analysis and Rank Order the Alternatives Identified
5. Control (Postauditing)

Source: Gordon and Loeb, 2006a, pp. 116 and 131.

Figure 3: Postauditing Cybersecurity Investment Timeline



Source: Gordon and Loeb, 2006a.

3. MOST CYBERSECURITY BREACHES DO NOT SIGNIFICANTLY IMPACT ORGANIZATIONS*

Empirical Evidence

Surveys (e.g., CSI/FBI Survey)

- large absolute dollar amounts of losses

Campbell et al., 2003 Study

- most breaches are not statistically significant

- exception relates to breaches of confidentiality

4. INFORMATION SHARING REQUIRES ECONOMIC INCENTIVES TO BE EFFECTIVE*

Potentially Valuable

Free-Rider Problem

- Need Economic Incentives

(see Gordon et al., 2003b)

5. SOX DOES IMPACT CYBERSECURITY ACTIVITIES

Sarbanes-Oxley (SOX) Act of 2002

Section 302, entitled "Corporate Responsibility for Financial Reports", requires the CEO and the CFO to take personal responsibility for establishing and maintaining the corporation's internal controls and for certifying that the financial statements provide an accurate representation of a corporation's financial condition.

Section 404, entitled "Management Assessment of Internal Controls", requires corporations to include internal control report with SEC filing

SOX & Information Security Activities

Although not Explicit in SOX or SEC Rules, a Widely Held View is that Information and System Security is an Implicit Requirement of the Internal Control Structure and Procedures Mandated by Sections 302 and 404 of SOX (see Figure 4)

Cybersecurity Risk Management and Firm Value

A. Empirical Evidence

Voluntary Disclosure of Information Security Activities (including Investments and Internal Control)

⇨ Increased Firm Value (Gordon, Loeb and Sohail, 2006)

B. Analytical Model

Auditing Cybersecurity Investments

⇨ Enhanced Firm Value (Gordon, Loeb, and Zhou, 2006)

6. CYBERSECRITY INSURANCE IS SLOW TO TAKE OFF*

Organization's Perspective:

- Assess if Cybersecurity is Needed
- Evaluate Available Insurance Policies
- Select Appropriate Policy

Insurance Company's Perspective

- Pricing – Need More Actuarial Data
- Adverse Selection
- Moral Hazard

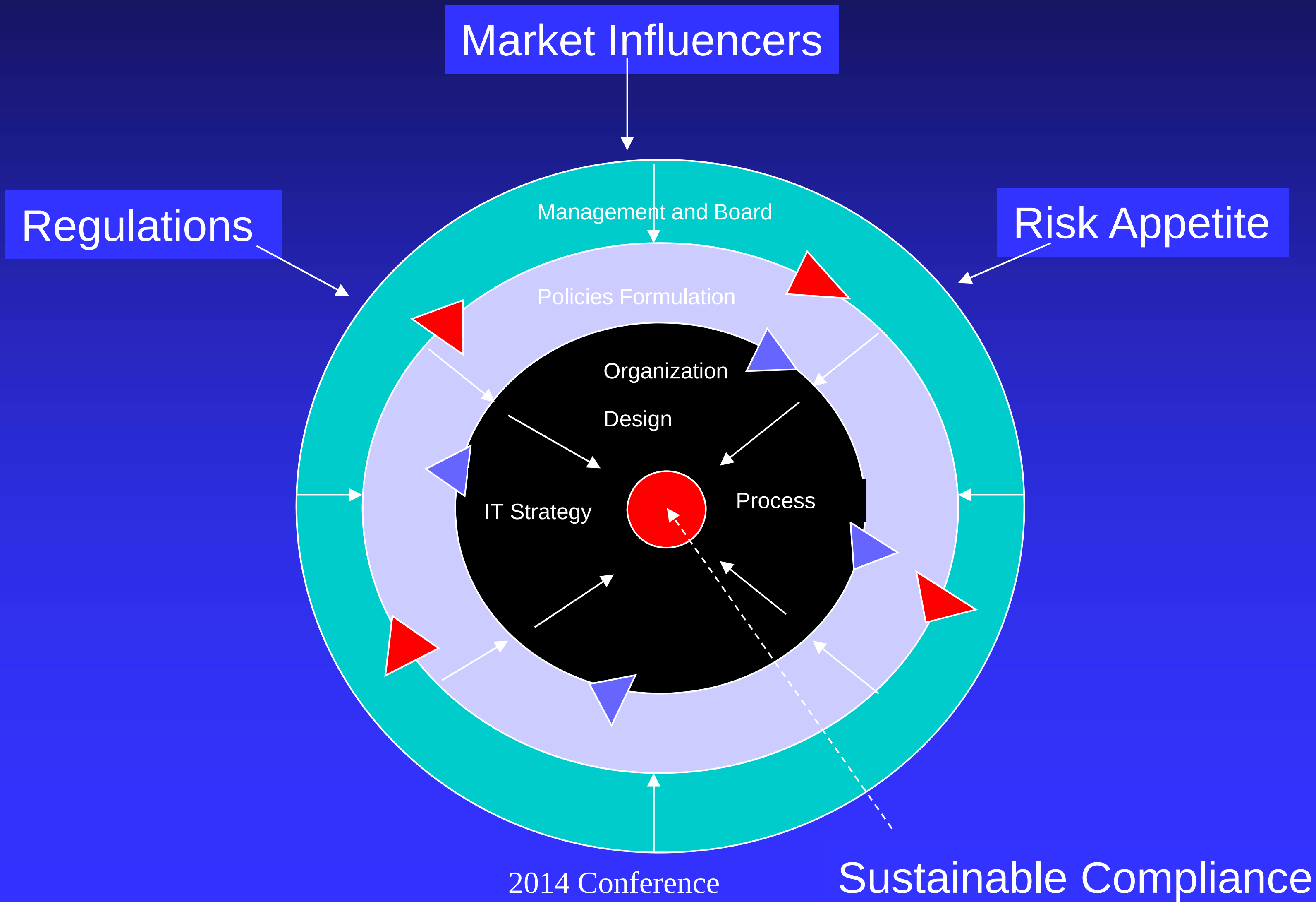
Empirical Evidence

- CSI/FBI Survey

Source: Gordon, Loeb and Sohail, 2003.

Figure 6: Cybersecurity Risk Management Assessment and Control Framework

Proposed Framework



Benefits

- Consolidate reputation as original thinker and contributor to TSB aspirations
- Link to and develop existing ‘technical’ solutions to CRM , connect to operational risk issues arising from compliance with Solvency II
- Provide visibility and leading edge thinking
- Initiate new programmes and packages to show ‘best practice’ internal models & compliance

Research/Business Opportunities

- Study “Best Practices” to help Derive the Right Amount to Spend on Cybersecurity.
- Develop Models and Study “Best Practices” for Assessing the Appropriate Use of Cybersecurity
- Apply the Contingency View of Cybersecurity Risk Management to Solvency II implementation.
- Examine the Broader Relation Among Cybersecurity Budgeting, Performance, Compliance and Managerial Incentives.
- Penetration Testing

Concluding Comments

Cybersecurity Risk Management and insurance is a Concern to all Organizations in a Digital Economy and is an Important Subset of Enterprise Risk Management.

Economics Analysis can, and should, play an important role in Cybersecurity Risk Managing (CRM). Uncertainty needs to be built into these models, and not used as an excuse for avoiding careful economic analysis (i.e., this is not Voodoo Economics). However, applying economic analysis is best viewed as a complement to, rather than a substitute for, other approaches (e.g., technical and behavioral solutions) for CRM.