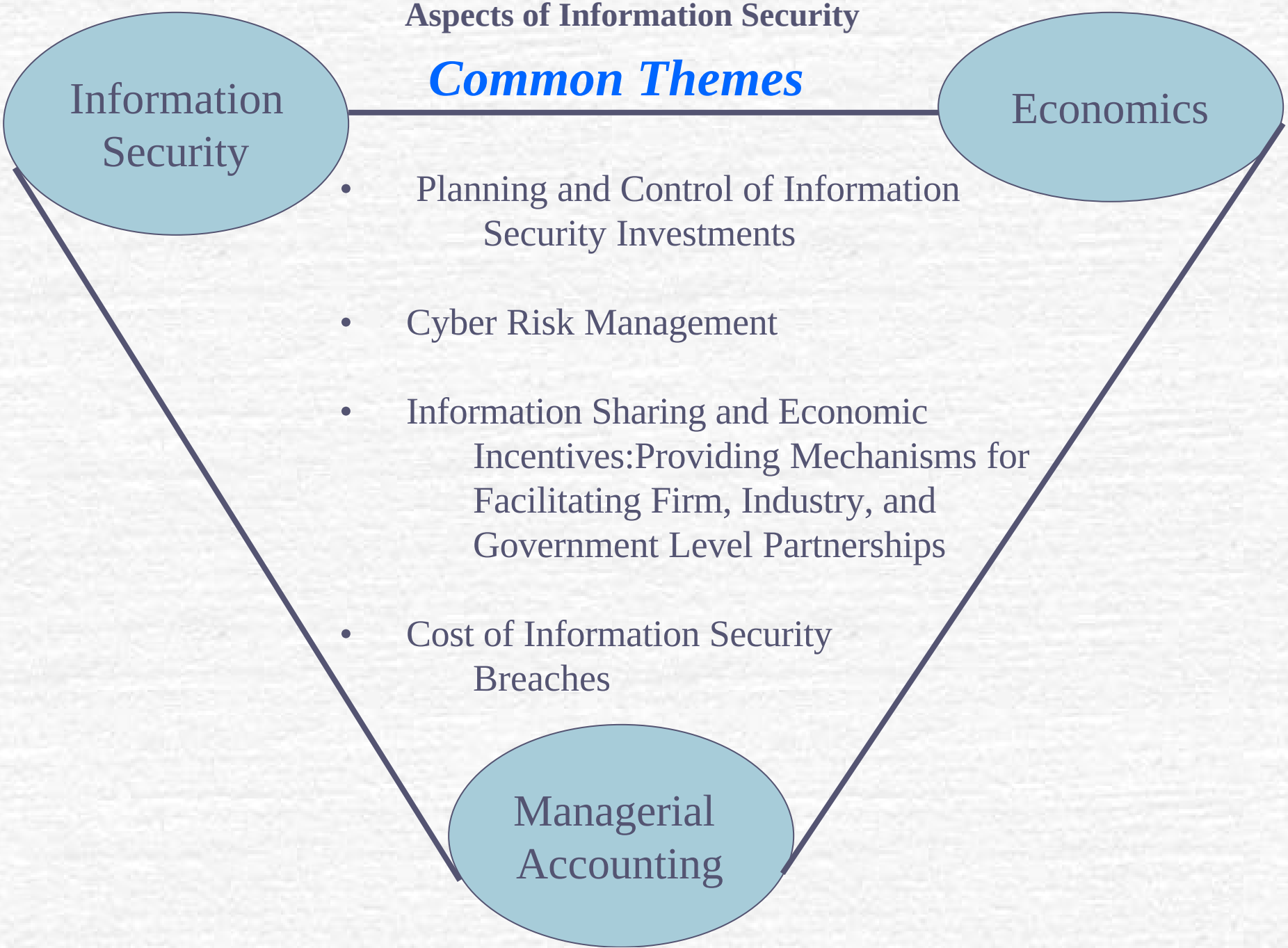
Economic Aspects of Information Security

March 6, 2003

Lawrence A. Gordon
Ernst & Young Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland, College Park

Martin P. Loeb
Professor of Accounting and Information Assurance
Deloitte & Touche Faculty Fellow
Robert H. Smith School of Business
University of Maryland, College Park

Stream of Research by Lawrence A. Gordon and Martin P. Loeb on Economic Aspects of Information Security



Stream of Research by Lawrence A. Gordon and Martin P. Loeb on Economic Aspects of Information Security

- Gordon and Loeb, Fall 2001, "Economic Aspects of Information Security," *Tech Trend Notes.*

- Gordon and Loeb, Sept. 2001, "A Framework for Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM.*

- Gordon, Loeb and Lucyshyn, May 2002, "An Economic Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence," Proc. of the First Workshop on Economics and Information Security, Berkeley.

- Gordon and Loeb, Nov. 2002, "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance.**

- Gordon and Loeb, Nov. 2002, "The Economics of Investment in Information in Information Security," *ACM Transactions on Information and System Security.**

- Gordon and Loeb, 2003 forthcoming, "Expenditures on Competitor Analysis and Information Security: A Management Accounting. Perspective," in *Management Accounting in the New Economy*, Oxford University Press.*

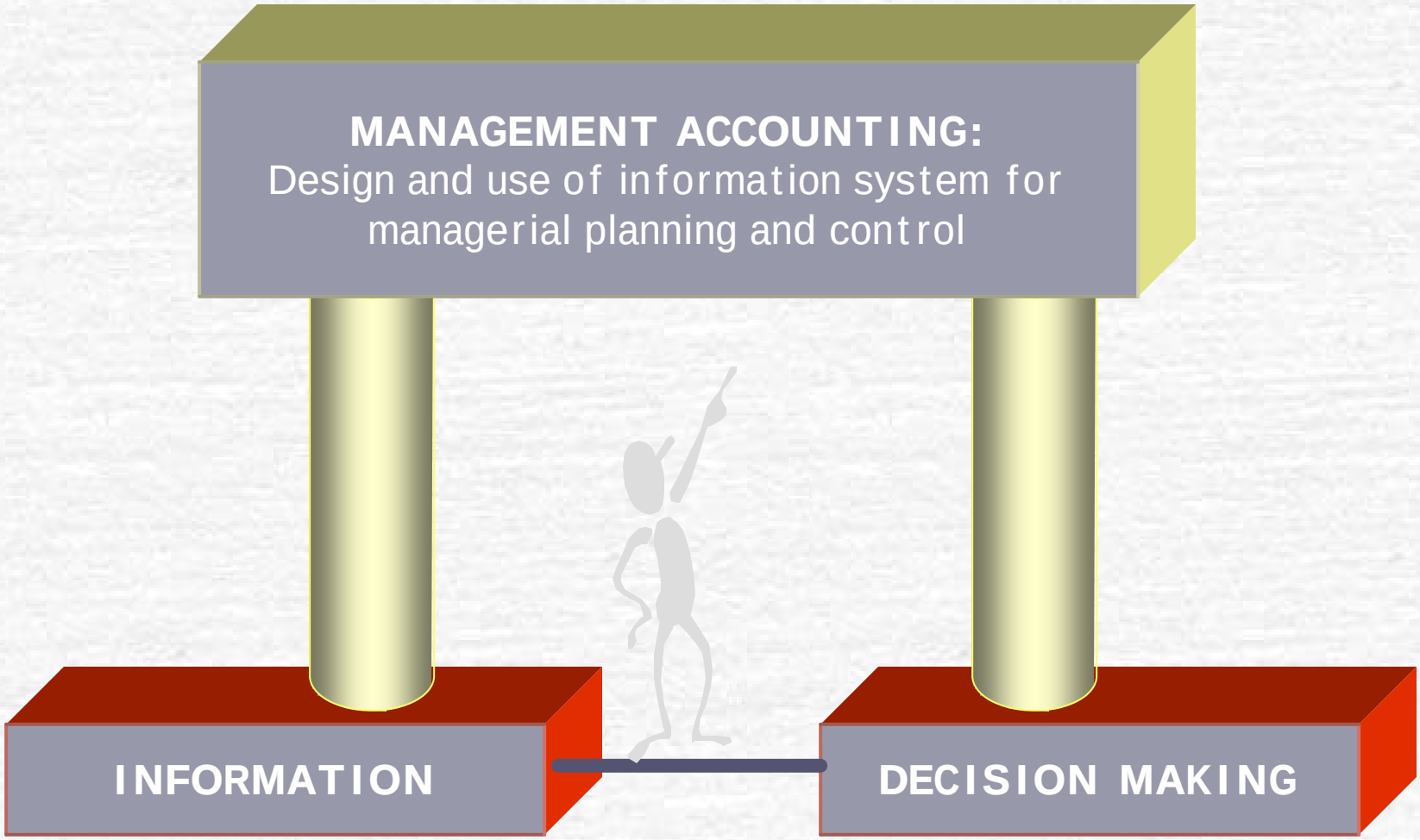
* copies available here for distribution

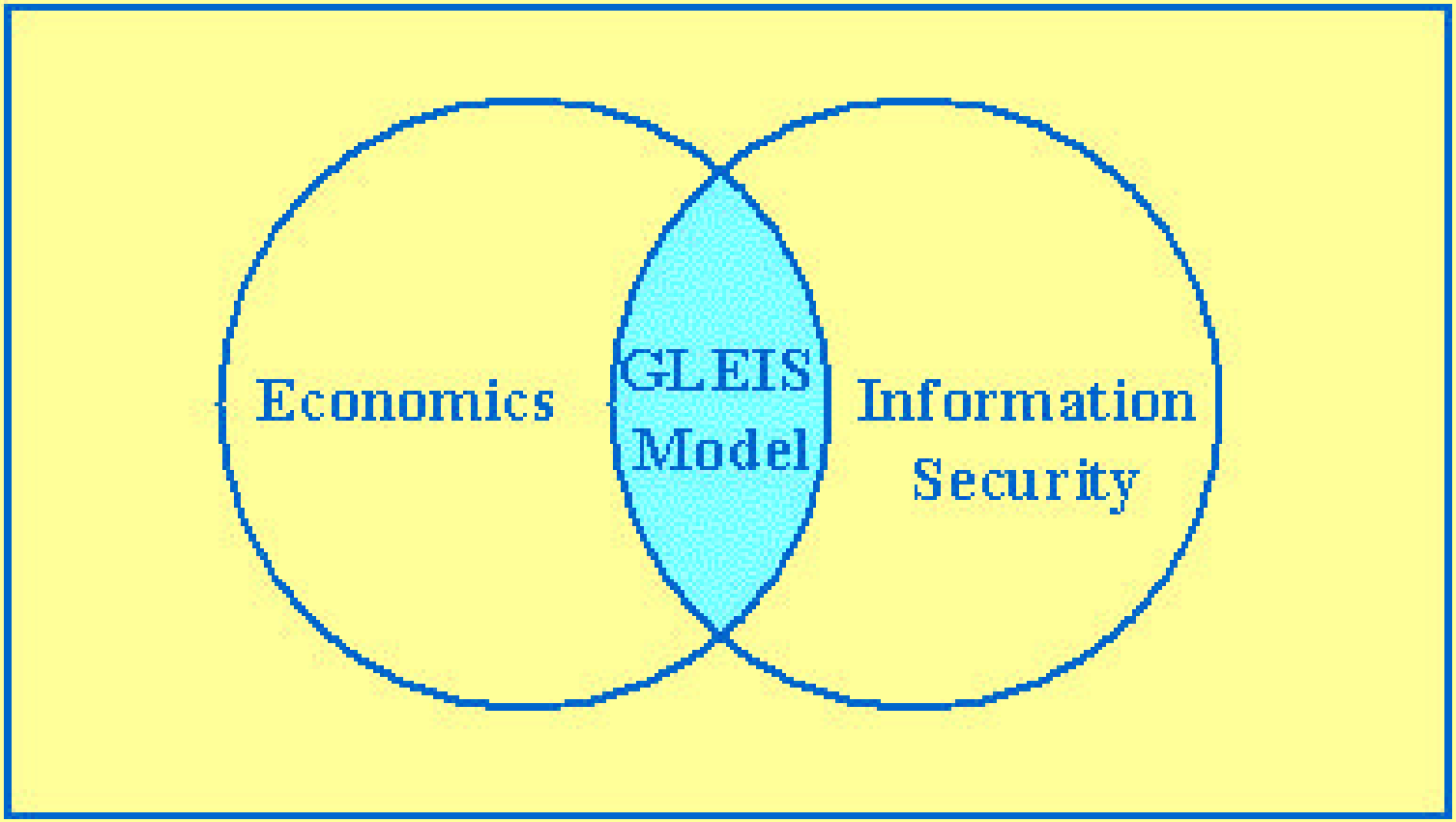
Stream of Research by Lawrence A. Gordon and Martin P. Loeb on Economic Aspects of Information Security (continued)

- Gordon, Loeb, and Sohail , Mar. 2003, "A Framework for Using Insurance for Cyber Risk Management," *Communications of the ACM*.*
- Campbell, Gordon, Loeb and Zhou, 2003 forthcoming "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*.
- Gordon, Loeb and Lucyshyn, under review, "Information Security Expenditures and Real Options: A Wait-and-See Approach."
- Gordon, Loeb and Lucyshyn, Jan. 2003, "Sharing Information on Computer Systems Security: An Economic Analysis," Working Paper.
- Gordon and Loeb, Feb. 2003, "Budgeting Process for Information Security Expenditures:Empirical Evidence," Working Paper.

* copies available here for distribution

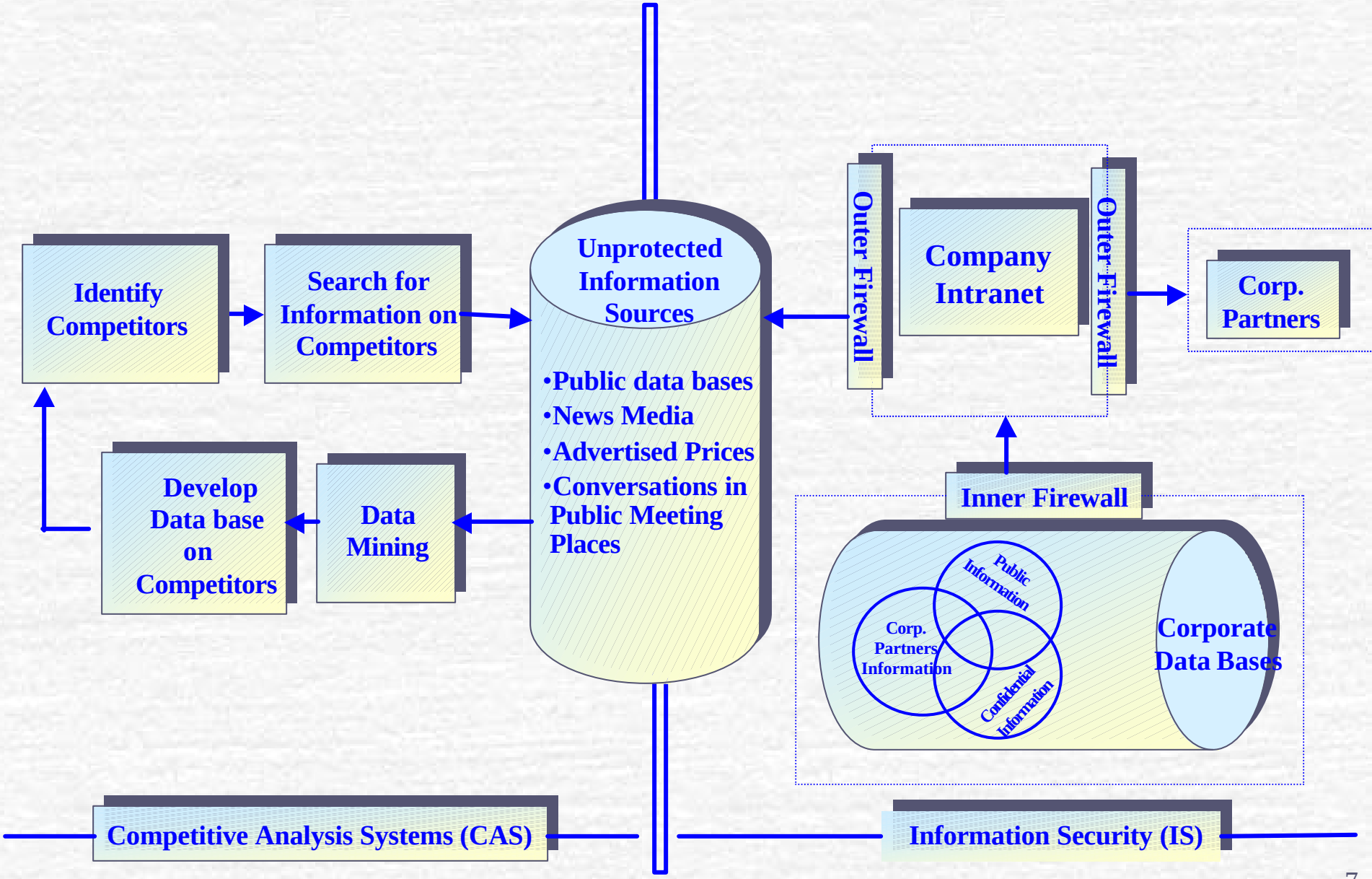
Definition: Management Accounting





The GLEIS™ model provides an economic framework for deriving the appropriate level of investments in information security.

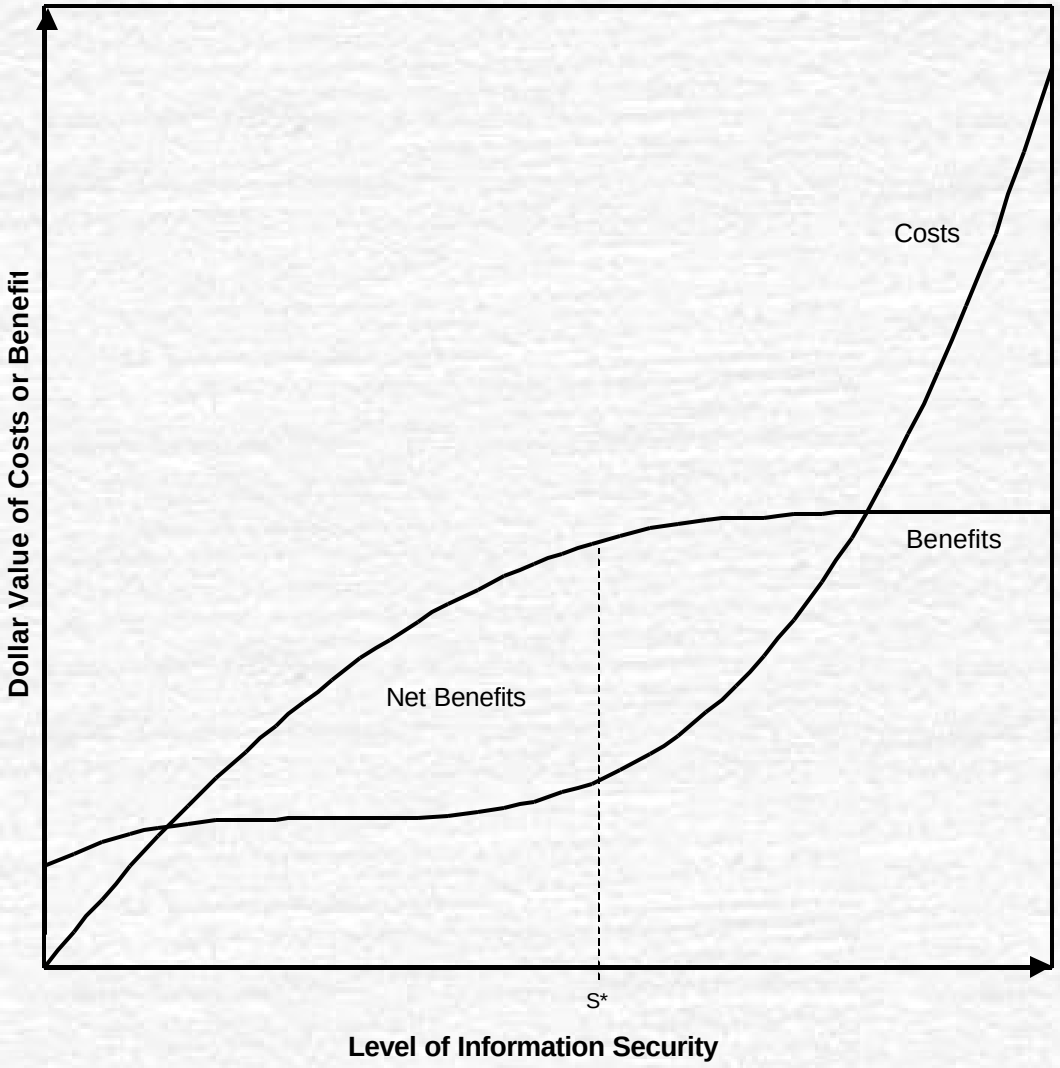
Competitor Analysis Systems Vs. Information Security



Risk Management/Information Security and Cyber Insurance

Benefits and Costs of Information Security

Figure 1: Benefits and Costs of Information Security



The value S^* that maximizes $G(S) = B(S) - C(S)$ is characterized by

$$\frac{dG}{dS} = \frac{dB}{dS} - \frac{dC}{dS} = 0$$

$$\frac{dB}{dS} = \frac{dB}{dS}$$

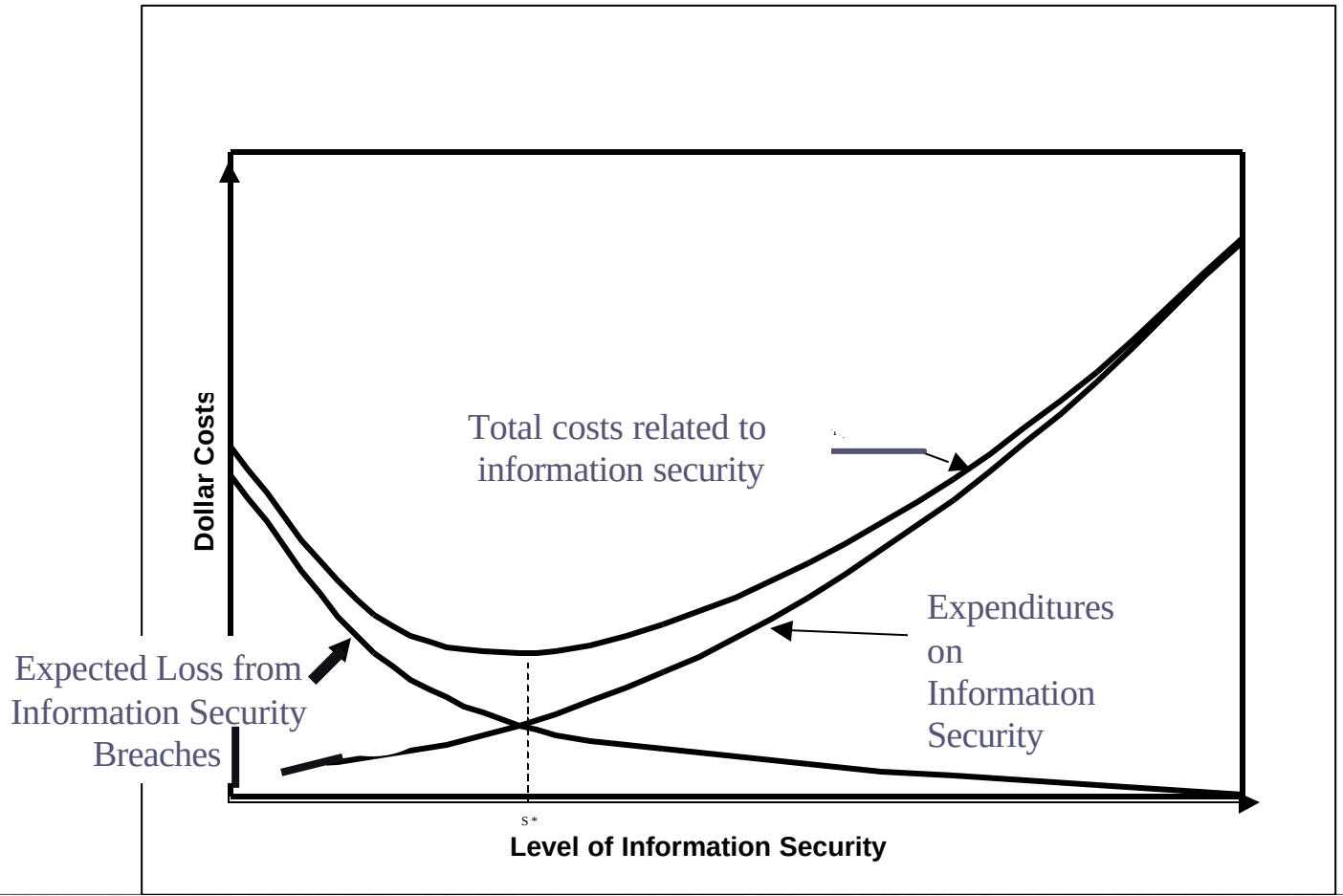
i.e., marginal benefits = marginal costs

Incremental Security Investments

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+k)^t} - Cost$$

Minimization of Total Expected Loss

Total Expected Loss = Expenditures on Information Security + Expected Loss from Information Security Breaches



The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*

Katherine Campbell
Assistant Professor of Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland, College Park

Lawrence A. Gordon
Ernst & Young Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland, College Park

Martin P. Loeb
Professor of Accounting and Information Assurance
Deloitte & Touche Faculty Fellow
Robert H. Smith School of Business
University of Maryland, College Park

Lei Zhou
Ph.D. Candidate, Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland, College Park

*The study reported in this paper was partially supported by the DOD, Laboratory for Telecommunications sciences (LTS), through a contract with the University of Maryland Institute for Advanced Computer Studies (UMIACS). Preliminary results of some data analyses reported in this paper were included in a working paper by Gordon et al. (2001) and presented at the LTS May 2001 workshop.

MOTIVATION

- Information Security (IS) Breaches are Ubiquitous (e.g., Love Bug, Denial of Service)
- Conflicting Views about Economic Impact of Such Breaches
  - Significant losses (e.g., Kedrosky, 2000; Power 2002)
  - Nuisance (e.g., Anders, 2000; Smith, 2000) especially in terms of long-run impact – i.e., firms protect their most significant information assets

Empirical research on Economic Impact is largely descriptive in nature (i.e., primarily surveys and some case studies) and has focused on "direct" financial cost of IS Breaches

HYPOTHESES

$H1_0$: There is no stock market reaction to public reports of corporate information security breaches.

$H2_A$: There is no stock market reaction to public reports of corporate information security breaches involving unauthorized access to confidential information.

$H2_B$: There is no stock market reaction to public reports of corporate information security breaches that do not involve unauthorized access to confidential information.

METHODOLOGY

Sample Selection

- Public announcements in highly visible newspaper – WSJ, NY Times, Washington Post, FT &USA Today
  - We wanted a powerful test for a stock market reaction
  - 1/1995 to 12/2000
  - 43 events affecting 38 firms

    (Search Terms: IS Breach, Computer System Security, Hacker, Cyber Attack, Computer Attack and Computer Virus)
- Sample partitioned by confidentiality of event as: Confidential (11) or Non-Confidential (32)

Table 1
Sample Selection Criteria

Criterion	Impact on Sample Size	Firms Remaining
Initial set of corporate information security breaches reported in major newspapers	84	84
CRSP data availability	(28)	56
Merger	(2)	54
Sufficient returns data for estimation period computations	(4)	50
Overlapping multiple information security breaches	(7)	43

Table 2

Sample Information Security Breach Events

Company name	Source	Date	Confidentiality of Event	Event Description
Egghead.com	Washington Post	12/23/00	Confidential	Unauthorized access to credit card data
Disney	USA Today	09/27/00	Confidential	Unauthorized access to Disney World guest data
First Data Corp (Western Union)	Wall Street Journal	09/11/00	Confidential	Unauthorized access to credit card data
Sabre Holdings Corp	Wall Street Journal	06/27/00	Confidential	Unauthorized access to proprietary data
Nike Inc	Wall Street Journal	06/22/00	Non-confidential	Unauthorized traffic re-direction
Ford Motor Co.	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Microsoft Corp	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Estee Lauder Cos	Wall Street Journal	05/05/00	Non-confidential	Love bug virus
Bear Stearns Cos	USA Today	05/05/00	Non-confidential	Love bug virus
Trans World Airlines Inc	USA Today	05/05/00	Non-confidential	Love bug virus
National Discount Brokers	Wall Street Journal	02/25/00	Non-confidential	Service interruption
McGraw-Hill Cos	Wall Street Journal	02/22/00	Confidential	Unauthorized access to confidential info facilitated by employee
Aastrom Biosciences Inc.	Wall Street Journal	02/18/00	Non-confidential	Unauthorized website entry & alteration
ZDNet	Wall Street Journal	02/10/00	Non-confidential	Denial of service attack
About.com	Wall Street Journal	02/10/00	Non-confidential	Denial of service attack
Time Warner Inc (CNN)	Washington Post	02/09/00	Non-confidential	Denial of service attack
Amazon.com Inc	Wall Street Journal	02/09/00	Non-confidential	Denial of service attack
eBay Inc	USA Today	02/08/00	Non-confidential	Denial of service attack
Lycos	Financial Times	02/08/00	Non-confidential	Denial of service attack
E-Trade Group	USA Today	02/08/00	Non-confidential	Denial of service attack
Yahoo!	Wall Street Journal	02/08/00	Non-confidential	Denial of service attack
Drug Emporium Inc	Wall Street Journal	01/31/00	Confidential	Unauthorized access to credit card data
America Online	Wall Street Journal	01/27/00	Non-confidential	Flaw in email system

Table 2
Sample Information Security Breach Events (Continued)

Company name	Source	Date	Confidentiality of Event	Event Description
Northwest Airline	Wall Street Journal	01/10/00	Confidential	Unauthorized access to credit card data
Dell Computer Corp	Financial Times	11/19/99	Non-confidential	Production interruption by virus
Critical Path Inc	Wall Street Journal	09/22/99	Non-confidential	Flaw in email system
Symantec Corp	Wall Street Journal	08/09/99	Non-confidential	Unauthorized website entry & alteration
Network Solutions Inc	Washington Post	07/03/99	Non-confidential	Unauthorized website entry & traffic re-direction
AT&T Corp	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Lehman Brothers Holdings Inc	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Boeing Co	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
General Electric Co	Financial Times	06/12/99	Non-confidential	Worm.ExploreZip virus
Raytheon Co	Wall Street Journal	04/05/99	Confidential	Unauthorized employee posting of confidential information
Merrill Lynch & Co Inc	USA Today	03/30/99	Non-confidential	Melissa virus
Intel Corp	USA Today	03/30/99	Non-confidential	Melissa virus
Compaq Computer Corp	USA Today	03/30/99	Non-confidential	Melissa virus
Lockheed Martin Corp	USA Today	03/30/99	Non-confidential	Melissa virus
Microsoft Corp	Wall Street Journal	10/27/98	Confidential	Unauthorized access to subscriber data
America Online	Wall Street Journal	10/19/98	Non-confidential	Unauthorized alteration of services address
New York Times Co	Wall Street Journal	09/14/98	Non-confidential	Unauthorized website entry & alteration
America Online	Wall Street Journal	01/05/98	Confidential	Unauthorized access to passwords/credit card data
America Online	Washington Post	06/28/97	Confidential	Unauthorized access to users' accounts
Microsoft Corp	Wall Street Journal	06/23/97	Non-confidential	Unauthorized service interruptions

Table 3
Descriptive Statistics

: Financial Variables at FYE 1999

Variable	No. Obs.	Mean	Median	Minimum	Maximum	Std. Dev.
Total Assets ($mill.)	38	49,884.82	4,668.25	9.54	405,200.00	97,959.27
Book Value ($mill.)	38	8,670.74	1,570.07	-171.03	78,927.00	15,644.46
Sales ($mill.)	38	18,676.64	4,384.50	0.88	162,558.00	32,907.26
Net Income/Loss ($mill.)	38	1,379.02	393.00	-719.97	10,717.00	2,581.81
Market Value of Equity ($mill.)	38	64,468.57	8,775.77	13.28	602,432.92	131,966.17
Market to Book	38	12.81	5.96	-36.14	97.43	24.65

Sample Industry Distribution

SIC	Industry Description	Number of Firms
2700	Printing, Publishing & Allied	2
2800	Chemicals & Allied Prods	2
3000	Rubber & Misc. Plastic Prods	1
3500	Ind, Comm Mch, Computer Equip	1
3600	Electrical, Other Elec Equip	2
3700	Transportation Equipment	3
3800	Meas Instr, Photo Gds, Watches	1
4500	Transportation By Air	2
4800	Communications	1
5900	Misc. Retailers	1
6200	Security & Commodity Brokers	5
7300	Business Services	14
7800	Motion Pictures	3
	Total	38

RESEARCH DESIGN

- Event Study, where event is public announcement of IS Breach
- Standard Ordinary Least Squares (OLS) Methodology based on CAR
  - OLS assumes error terms are independent, normally distributed, zero-mean and homoskedastic. However, IS Breaches cluster by day/industry and some contemporaneous cross-sectional correlation and/or heteroskedaticity.
- Seemingly Unrelated Regressions (SUR) Methodology, which is a form of Generalized Least Squares (GLS) Methodology

Standard Market Model

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

Where: R_{it} = return for firm *i*'s stock on day t, net of the risk-free rate;
R_{mt} = return for the market on day t, net of the risk-free rate;
a_i, b_i = market model intercept and slope parameters, respectively, for firm i; and
e_{it} = disturbance term.

The abnormal retuens (AR)

$$AR_{it} = R_{it} - (\hat{a}_i + \hat{b}_i R_{mt})$$

Time Line

CAR

$$CAR_i = \sum_{t=t_1}^{t_2} AR_{it}$$

Where: $[t_1,t_2]$ = the event interval.
The mean announcement effect:

$$CAR = \frac{1}{N} \sum_{i=1}^{N} CAR_i$$

Where: N=the number of events.

SUR

$$R_{1t} = a_1 + b_1 R_{mt} + g_1 D + e_{1t},$$
$$R_{2t} = a_2 + b_2 R_{mt} + g_2 D + e_{2t},$$
$$\vdots$$
$$R_{Nt} = a_N + b_N R_{mt} + g_N D + e_{Nt},$$

Where: D = 1 if within the 3 day event period [-1,+1], and 0 otherwise.

Table 4

CAR Results
3 day window [-1,+1]

	N	Mean CAR	Z-stat	p-value	% negative CARs
Panel A (full sample)					
Full Sample	43	-0.0188	-1.4783	0.1393	46.52
Panel B (sample partitions)					
Confidential Events	11	-0.0546	-2.7830	0.0053	63.64
Non-Confidential Events	32	-0.0065	-0.4142	0.6787	40.63

Table 5

SUR Results
Joint and Average Tests

	Jt. Hypothesis (all coeff = 0)	Avg. Hypothesis (avg. coeff = 0)
Panel A (Full Sample)		
F-value	1.48	1.51
Pr>F	0.0226	0.2192
D.F.	43	1
	5160	5160
Panel B (Confidential Event Sub-Sample)		
F-value	3.68	12.40
Pr>F	0.0001	0.0004
D.F.	11	1
	5160	5160
Panel (Non-Confidential Event Sub-Sample)		
F-value	0.34	0.03
Pr>F	0.9998	0.8744
D.F.	32	1
	5160	5160

Concluding Comments

- Overall negative stock market reactions to IS Breaches
- Partitioned Sample
  - Highly significant reaction for confidentiality breaches
  - Non-significant reaction for non-confidentiality breaches

Future Research

- Extend Cost of Security Breach Study
- Information Sharing
  - Among Companies in an Industry
  - Public- Private Information Sharing Partnerships
- Building the Business Case