Economic Aspects of Information Security

June 27, 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

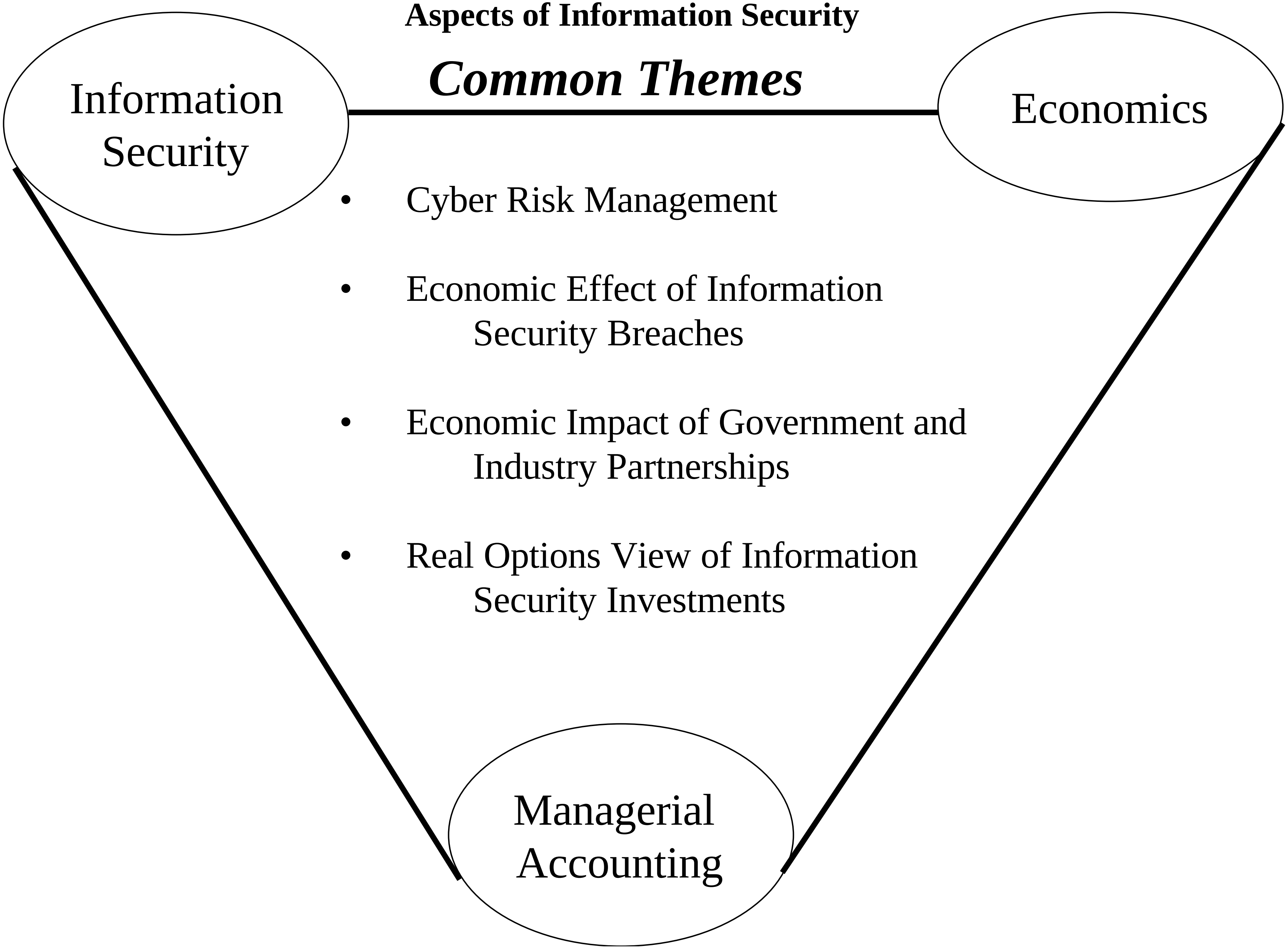
Professor of Accounting and Information Assurance

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



Information Security

Common Themes

Economics

- Cyber Risk Management
- Economic Effect of Information Security Breaches
- Economic Impact of Government and Industry Partnerships
- Real Options View of Information Security Investments

Managerial Accounting

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.*

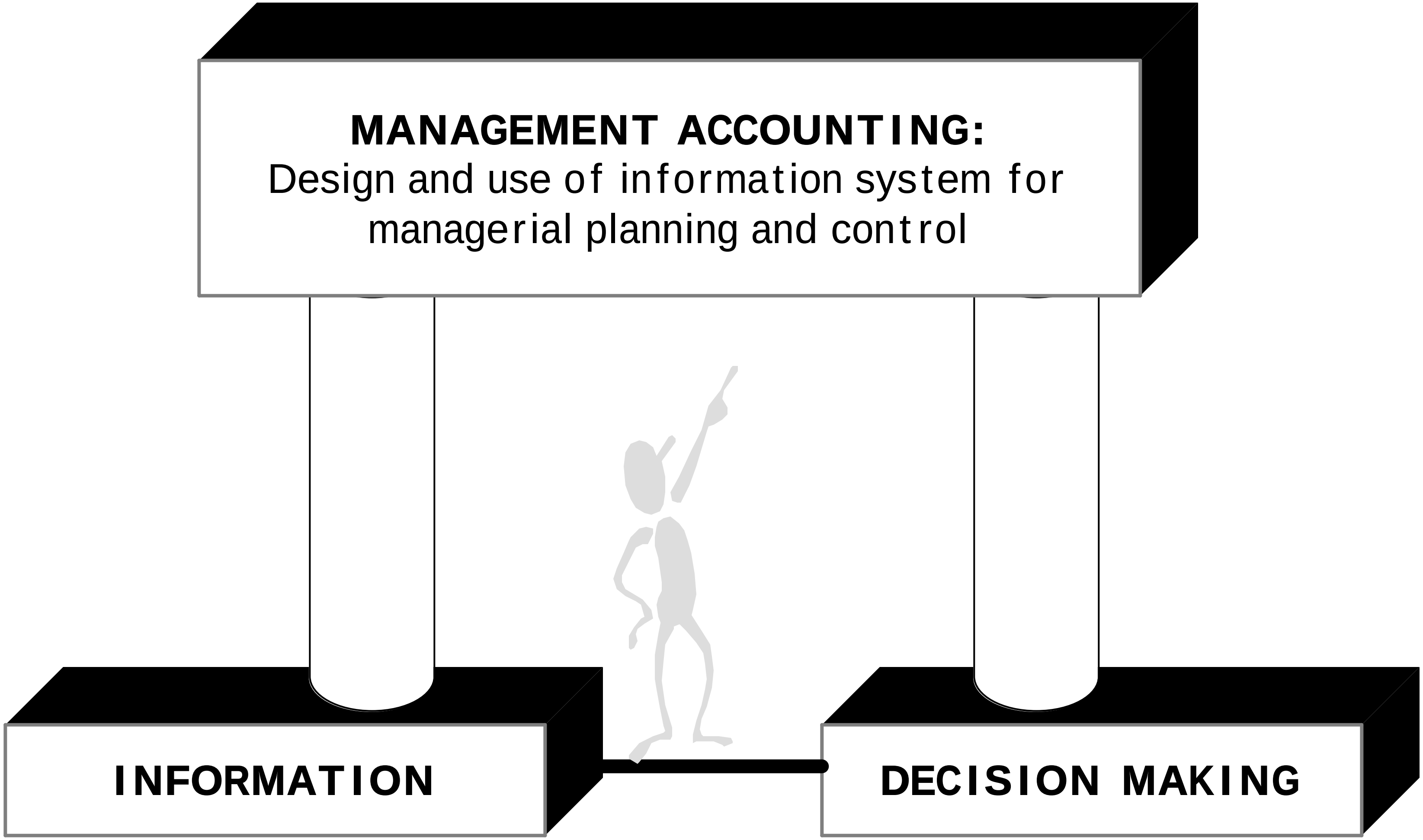
- Gordon and Loeb, Nov. 2002, "The Economics of Investment in Information in Information Security," *ACM Transactions on Information and System Security*.

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

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, Jun. 2003, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," J*ournal of Computer Security*.
- Gordon, Loeb and Lucyshyn, 2003 forthcoming, "Information Security Expenditures and Real Options: A Wait-and-See Approach." *Computer Security Journal.*
- Bodin, Gordon, and Loeb, 2003 "Information Security Investments using the Analytic Hierarchy Approach." (Under review).
- Gordon and Loeb, 2003, "Budgeting Process for Information Security Expenditures:Empirical Evidence," (Under review).
- Gordon, Loeb and Lucyshyn, 2003, "Sharing Information on Computer Systems Security: An Economic Analysis," Working Paper.

Definition: Management Accounting

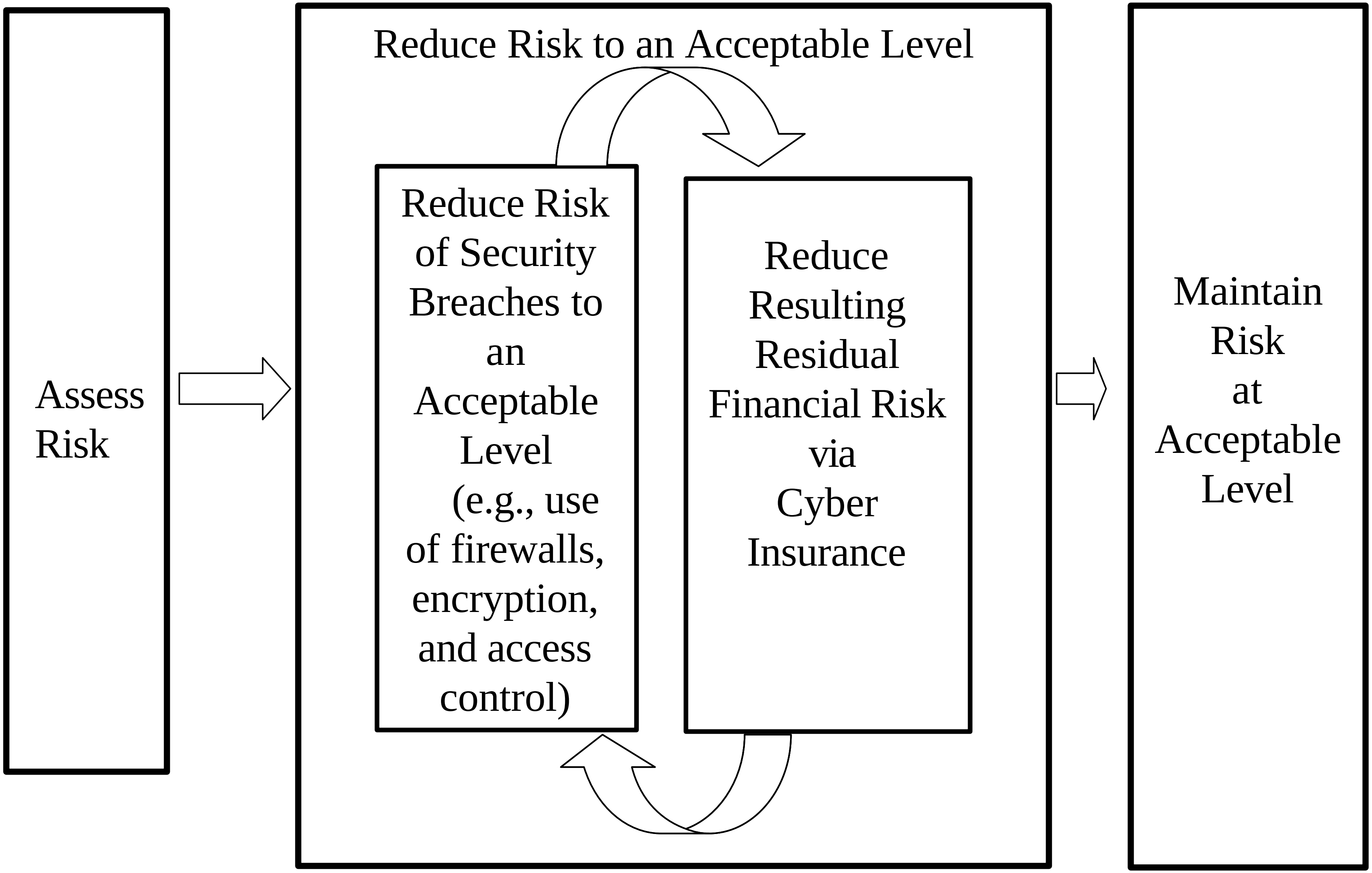


MANAGEMENT ACCOUNTING:
Design and use of information system for managerial planning and control

INFORMATION

DECISION MAKING

Risk Management/Information Security and Cyber Insurance



Assess Risk

Reduce Risk to an Acceptable Level

Reduce Risk of Security Breaches to an Acceptable Level (e.g., use of firewalls, encryption, and access control)

Reduce Resulting Residual Financial Risk via Cyber Insurance

Maintain Risk at Acceptable Level

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)

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;

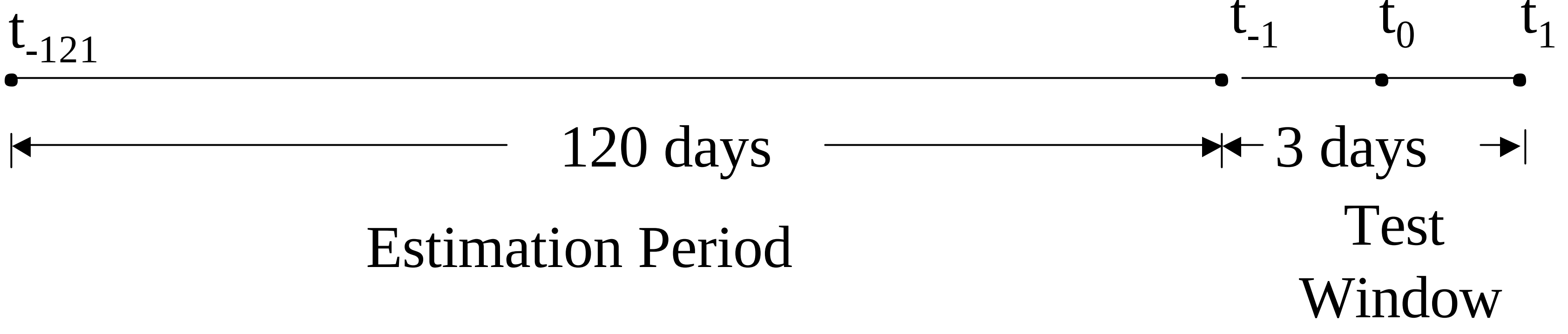
$a_{i,}\ b_i$ = market model intercept and slope parameters, respectively, for firm i; and

e_{it} = disturbance term.

The abnormal retuens (AR)

$$\mathrm{AR}_{\mathrm{it}} = \mathrm{R}_{\mathrm{it}} - (\hat{a}_{\mathrm{i}} + \hat{b}_i R_{mt})$$

Time Line



t_{-121}

t_{-1}

t_0

t_1

120 days

3 days

Estimation Period

Test Window

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

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

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

Summarized Results of Study

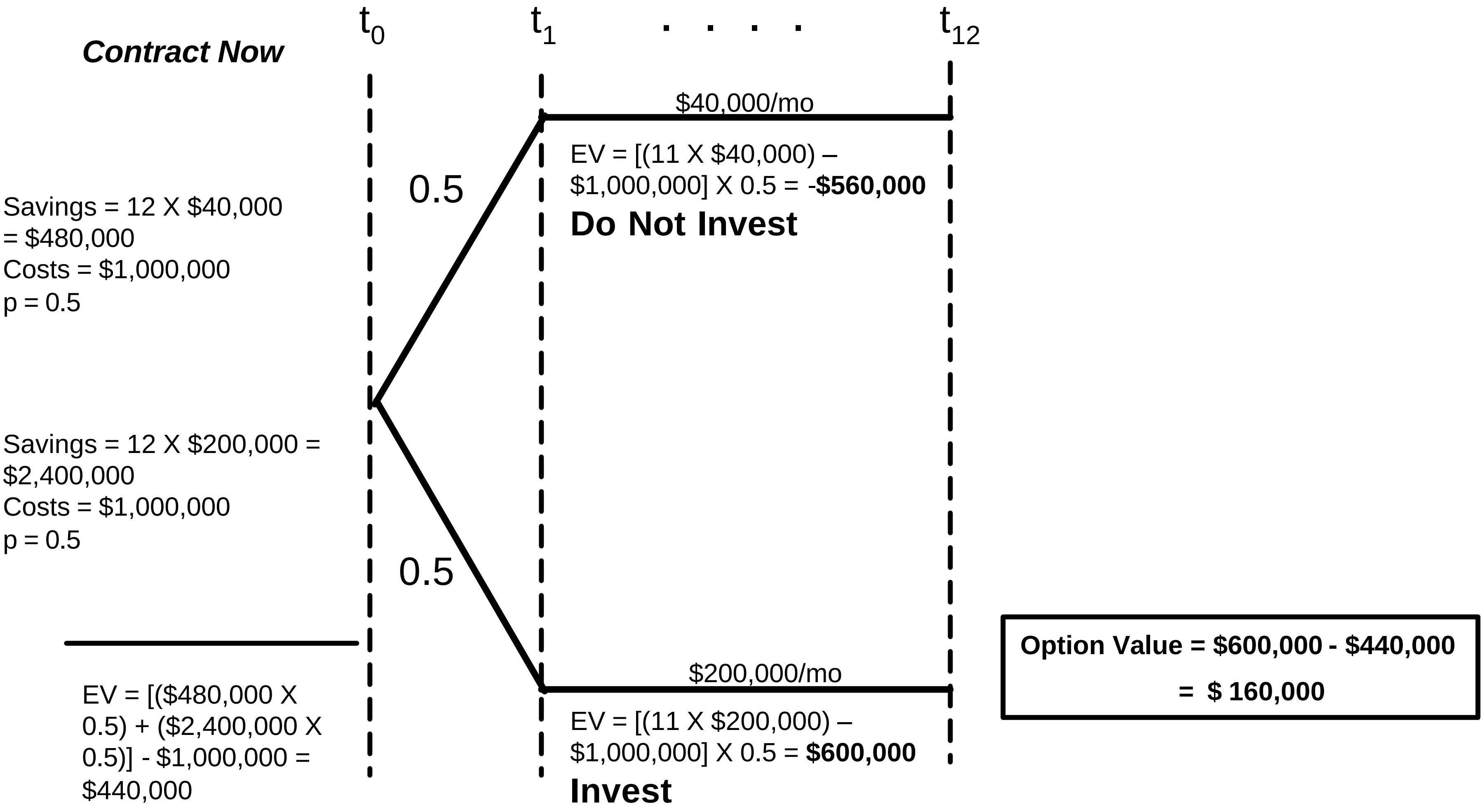
- Overall negative stock market reactions to IS Breaches
- Partitioned Sample
  - Highly significant reaction for confidentiality breaches
  - Non-significant reaction for non-confidentiality breaches

Real Options and Security:
The "wait-and-see-approach"

An Example

- Firm has tentatively budgeted next year's expenditures for information security in the amount of $2,500,000.
  - First $1.5 million is earmarked for basic information security activities (e.g., basic access controls, firewalls and physical protection of the firm's computers).
  - CSO is already authorized to use these funds for this purpose.
  - The remaining $1 million is considered discretionary, and needs the firm's CFO's approval before any final commitments can be made to spend this money.
  - Most likely use of the remaining $1 million is to hire an outside firm that specializes in enhancing the information security operations of major organizations.
  - The outside company's policy is to contract for one fiscal year, or any part thereof, at a cost of $1 million. In addition, once the contract is signed, it is not reversible for the remainder of the year (or part thereof).

Option Value Example



t_0 t_1 . . . . t_{12}

Contract Now

Savings = 12 X $40,000
= $480,000
Costs = $1,000,000
p = 0.5

0.5

$40,000/mo

EV = [(11 X $40,000) –
$1,000,000] X 0.5 = -**$560,000**

Do Not Invest

Savings = 12 X $200,000 =
$2,400,000
Costs = $1,000,000
p = 0.5

0.5

$200,000/mo

EV = [(11 X $200,000) –
$1,000,000] X 0.5 = **$600,000**

Invest

EV = [($480,000 X
0.5) + ($2,400,000 X
0.5)] - $1,000,000 =
$440,000

Option Value = $600,000 - $440,000

= $ 160,000

Current Research

- Information Sharing
- Business Case Development