ECONOMIC ASPECTS OF INFORMATION SECURITY

Lawrence A. Gordon, Ph.D.
Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance
The Robert H. Smith School of Business
University of Maryland
Affiliate Professor, UMIACS

Martin P. Loeb, Ph.D.
Professor of Accounting and Information Assurance
Deloite & Touche Faculty Fellow
The Robert H. Smith School of Business
University of Maryland
Affiliate Professor, UMIACS

February 4, 2005

Objectives of Presentation

- Provide overview of our stream of research that relates to the economic aspects of information security
- Discuss the following four specific research projects and implications of these projects

1. Cost of Information Security Breaches
2. Investments in Information Security
3. Information Security Audits and Organizational Value
4. Disclosures of Information Security Activities within Telecommunications Industry

Information Security & the Internet

- Many aspects to this concern:
  - Technical aspects that address such issues as cryptology, access controls, and intrusion detection systems.
  - Behavioral aspects that address the way human actions affect security breaches.

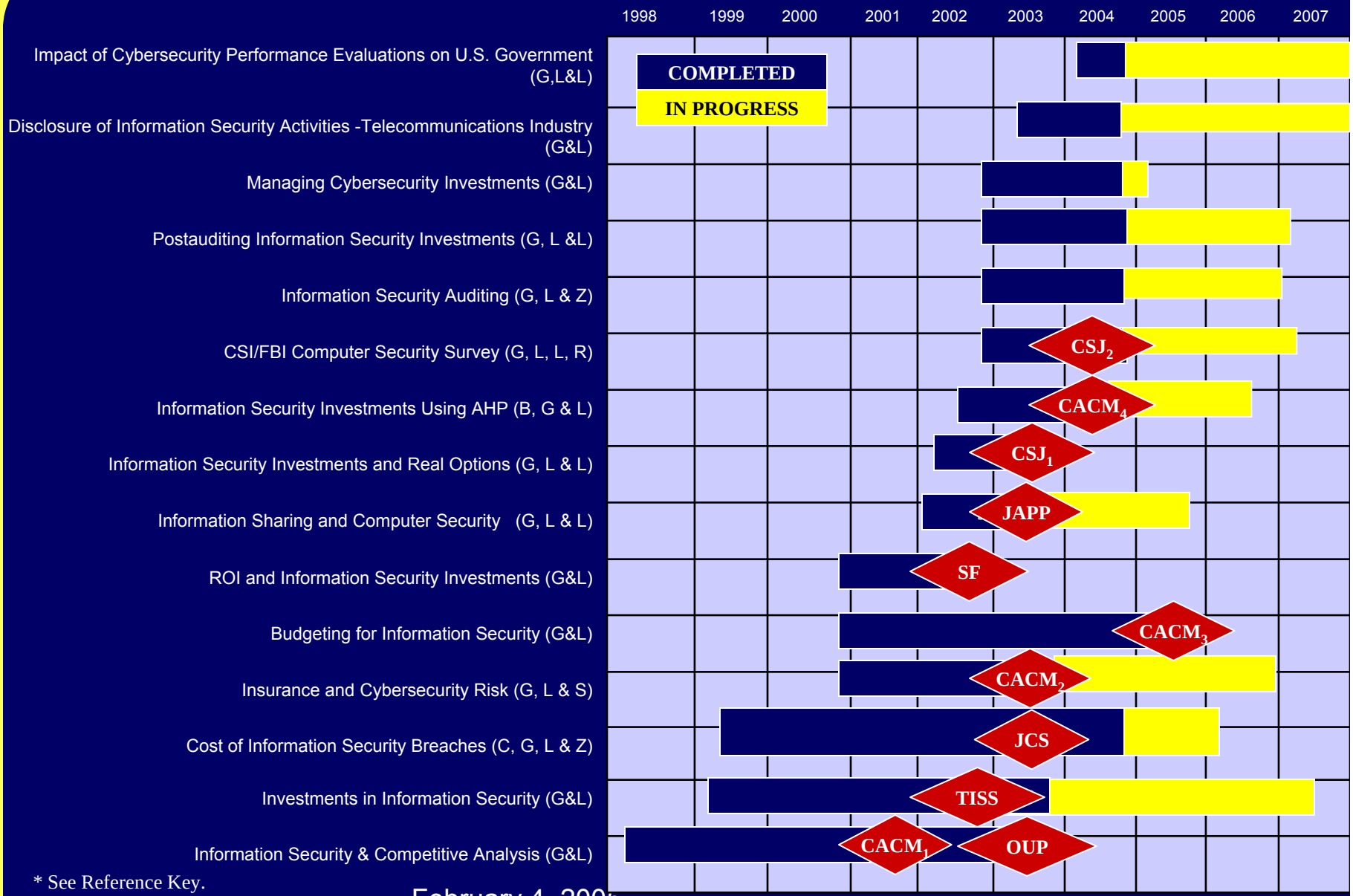
  Economic aspects of information security are also a critical concern to the future of the Internet. Unfortunately, until recently, there has been scant research on the Economic Aspects. The focus of our research is to offset this imbalance. The basic assumption is that the efficient allocation of scarce resources is a fundamental issue.

- Cybersecurity breaches are a critical concern for the future of the Internet:
  - Cybersecurity breaches are rampant and often costly.
  - Dynamic environment
  - Many externalities (e.g., one organization's actions impact the security of other organizations)
  - Benefits of information security activities are cost savings and very difficult to measure.

Economic Aspects Of Information Security

(Research Agenda by Gordon and Loeb)

Stream of Research on Economic Aspects of Information Security by Gordon and Loeb*



* See Reference Key.

February 4, 2005

1. Cost Of Information Security Breaches

- Conventional Wisdom
- Previous Studies of Explicit Costs to Firms
- Hypotheses
  - H1: No stock market reaction to public reports of corporate information security breaches.
  - H2A: No stock market reaction to public reports of corporate information security breaches involving unauthorized access to confidential information.
  - H2B: No stock market reaction to public reports of corporate information security breaches that do not involve unauthorized access to confidential information.
- Research Design
  - Event Study—public announcement of IS Breach
  - 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)—(i.e., Generalized Least Squares (GLS) Methodology)

Research 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;

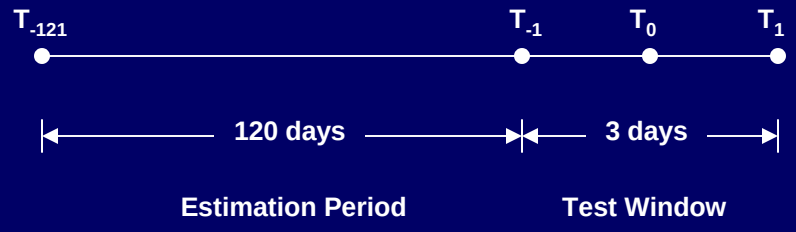
α_i β_i = market model intercept and slope parameters, respectively, for firm i; and

ε_{it} = disturbance term.

The abnormal returns (AR)

$$AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt})$$

- Time Line



- CAR

$$CAR_i = \sum_{t=t1}^{t2} AR_{it}$$

Where: [t1, t2] = the event interval.

The mean announcement effect:

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

Where N = the number of events.

- SUR

$$R_{1t} = \alpha_1 + \beta_1 R_{mt} + \gamma_1 D + e_{1t}$$
$$R_{2t} = \alpha_2 + \beta_2 R_{mt} + \gamma_2 D + e_{2t}$$
$$\vdots$$
$$R_{Nt} = \alpha_N + \beta_N R_{mt} + \gamma_N D + e_{Nt}$$

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

Results, Implications and Extensions

- Results
  - Total Sample
    - Mixed, Results Depend on Methodology
  - Split Sample
    - Confidentiality Breaches Significant (5% of Capitalization)
    - Non-Confidentiality Breaches Not Significant
- Implications
  - Allocation of Resources to Protect Information Needs to be Targeted Based on Type of Breach
- Extensions (in progress)
  - Much Larger Sample
  - Sample Split by: Confidentiality, Viruses, Accounting Profits
  - Market-Value Relevance Analysis

    (e.g., $V_{Eq} = \beta_0 + \beta_1 BV_{Eq} + \beta_2 RI + \beta_3 SB + \varepsilon$)
  - Industry analyses
  - In-depth Analyses of Firms with Breaches

2. Investments In Information Security

- How much should an organization invest?

  (Need to consider Security Breach Function [i.e., vulnerabilities, threats, and productivity of investments] & Potential Loss)
  - How does the optimal level of information security change with changes in vulnerability?
  - How does the optimal level of information security compare with the expected loss from a breach?

- ROI and Security Investments
- Option Value of Investments
- Risk Management Concepts (e.g., Insurance)
- Making the Business Case

How Much Should An Organization Invest?

Expected benefits of an investment in information security, denoted as EBIS, are equal to the reduction in the firm's expected loss attributable to the extra security. That is:

$$\mathbf{EBIS(z) = [v- S(z,v)] L} \qquad [1]$$

EBIS is written above as a function of z, since the investment in information security is the firm's only decision variable (v and L are parameters of the information set). The expected net benefits from an investment in information security, denoted ENBIS equal EBIS less the cost of the investment, or:

$$\mathbf{ENBIS(z) = [v -S(z,v)]L -z} \qquad [2]$$

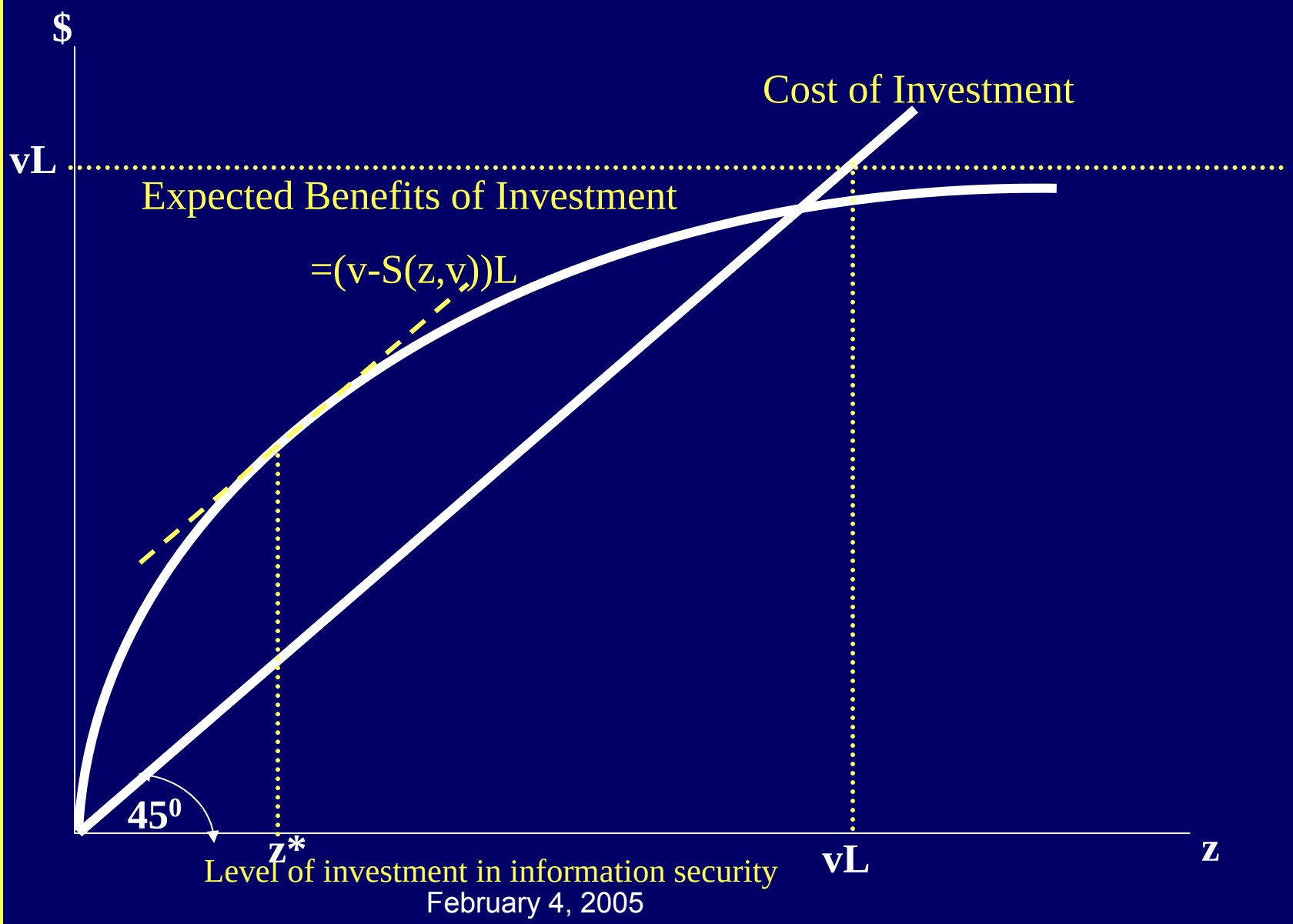
Maximizing [2] is equivalent to minimizing:

$$\mathbf{s(z,v)]L +z} \qquad [3]$$

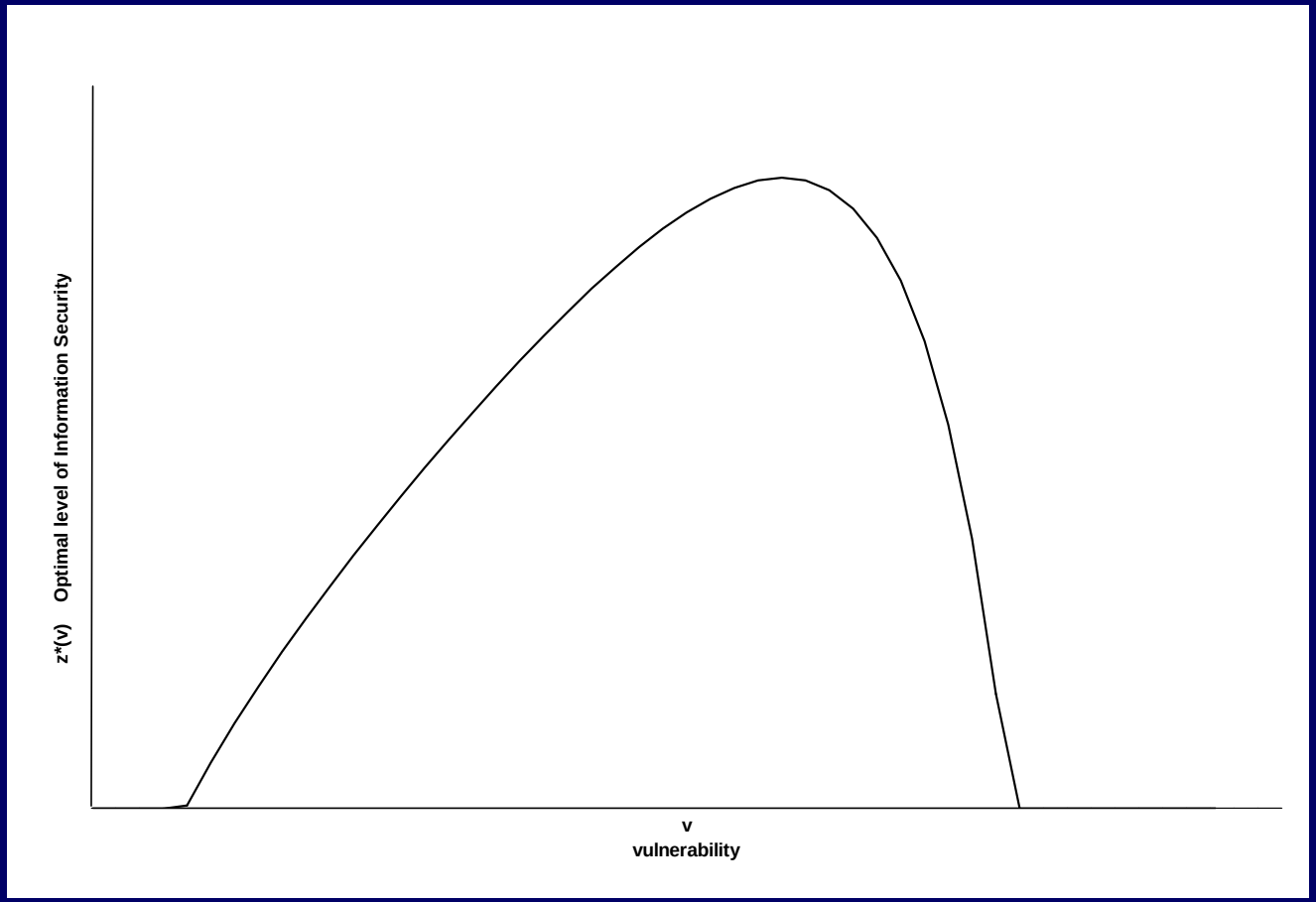
Interior maximum z*>0 is characterized by the first-order condition for maximizing [2] (or minimizing [3]) :

$$-S_z(z^*, v)L = 1 \qquad [4]$$

Benefits and Cost of an Investment in Information Security



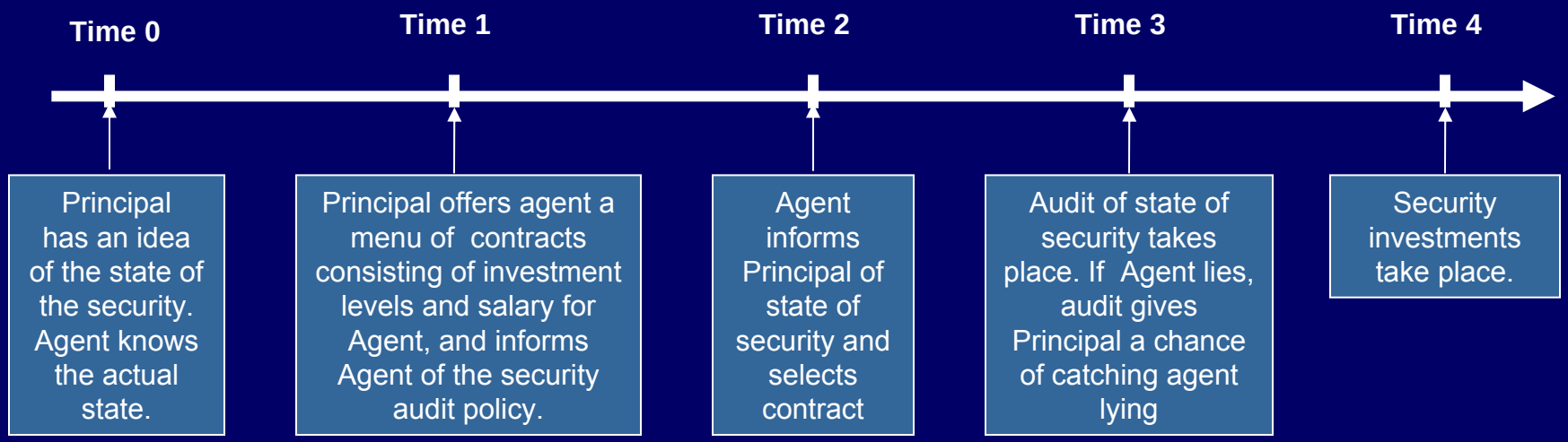
Optimal Value of Security versus Vulnerability, z*(v) for Class II (for a given L)



Results, Implications and Extensions

- Results
  - Under a wide range of circumstances, firm should spend substantially less than the expected loss (i.e., no more than 37% [1/e]).
  - Optimal level of information security investment does not always increase with the level of vulnerability (i.e., relation between vulnerability and marginal productivity of information security investments is critical).
- Implications
  - Spend Wisely: The relation between the efficient level of information security investments and expected losses is more complicated than conventional wisdom suggests.
  - The appropriate level of investments in information security should not always increase as the vulnerability increases.
- Extensions
  - Use above framework to investigate how information sharing affects optimal levels of information security investment
  - Applying to Making the Business Case (in progress).
  - Consider different notions of risk management and their impact on appropriate levels of information security investments.

3. Information Security Audits And Organizational Value



Additional Assumptions:

- Both Principal and Agent can observe breaches ex post
- Agent prefers more investment to reduce breaches
- Costless communications and security audits (optimization results indicate the maximum one should pay for security audit)
- Incentive mechanisms based on truthful revelation principle

Results, Implications and Extensions

- Results
  - Without security auditing Principal has to pay Agent much more, in terms of investments and salary, than with security auditing.
  - The higher the degree of information asymmetry between Principal and Agent concerning state of security (ex ante): (1) the more Principal is willing to spend on auditing, (2) the more Principal is willing to pay Agent in terms of investments and salary
- Implications
  - Auditing standards (intensity) should vary across organizations/agencies based on the degree of information asymmetry.
- Extension (in progress)
  - Empirical study to assess the value of information security auditing within U.S. government agencies.

4. Disclosures Of Information Security Activities Within Telecommunications Industry

- Telecommunication industry SIC code: 4800-4899
- Time coverage: filing date is between January 1, 2003 and June 30, 2004.
- Database source: 10K reports in Lexis-Nexis Database
- Keywords: information security, security breach, security monitoring, intrusion, cybersecurity, internet security

Disclosures Of Information Security Activities Within Telecommunications Industry

Procedure	No. of firms
Use of keywords (no hits for keyword of cybersecurity)	100
With keyword “security breach” but has nothing to do with cybersecurity (they provide products/services that prevent security breach)	(3)
With keyword “information security” but has nothing to do with cybersecurity (39 describe “the information with the SEC”; 2 provide information security products; 2 discuss the adoption of new regulation about information security).	(43)
With keyword “security monitoring” but has nothing to do with cybersecurity (3 provide information monitoring products/services; 1 relates to security system in executives’ home; 1 relates to landlord’s contractual agreement to maintain security; 1 relates to an executive’s former position; 1 relates to an alarm system)	(7)
With keyword “intrusion” but has nothing to do with cybersecurity	(6)
With keyword “internet security” but has nothing to do with cybersecurity (e.g., mentions that employees are supposed to report internet security misconduct)	(5)
Final sample	36

Results, Implications and Extensions

- Results
  - Most of the 36 firms have information on security activities related to at least two of the following four items: Risk of Security Breaches, Specific Security Measures, Expenditures on Cybersecurity, Security Breaches.
  - The information disclosed is largely nonquantitative in nature.
- Implications
  - Disclosure is occurring, but Impact is Limited (Sarbanes-Oxley Act of 2002 may change things)
- Extensions (in Progress)
  - Sarbanes-Oxley Act of 2002 (Section 404)
  - Market-Value Relevance Analysis

Impact/Contacts Resulting from Research

Government Related Contacts:

Department of Homeland Security (met with Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection; also met with Mr. Amit Yoran, while he was the Director of Cyber Security; the above meetings also included several other individuals from DHS who attended one of two separate meetings).

National Security Council (meeting with Dr. Gregory Rattray, Director for Cyberspace Security, concerning ways of using our research to help set national policy related to cyberspace security).

National Institute of Standards and Technology (met with Ms. Kathy Lyons-Burke, Director, Computer Security Expert Assist Team based on recommendation from Mr. Ed Roback, Chief of the Computer Security Division, NIST concerning NIST's project on return on investment [ROI] for computer security).

Federal Trade Commission (met with Ms Maureen Ohlhausen, Ms. Toby Levin, and Mr. Mark Nance from the FTC's Office of Policy Planning in April 2003).

Impact/Contacts Resulting from Research

Government Related Contacts (continued):

DARPA (Mr. Bill Lucyshyn, Director at DARPA and currently a visiting senio research scholar at the Maryland's School of Public Policy. Bill currently reports directly to the Honorable Dr. Jacques Gansler [Under Secretary of Defense for Acquisition, Technology and Logistics from 1997-2001], who is now the Vice President for Research at UMCP).

CSI/FBI Computer Crime and Security Survey (as of 2004, we became two of the three academic advisors for this annual survey [which is probably the oldest and most widely referenced of all such related surveys]).

National Science Foundation (have served as a reviewer for numerous NSF proposals related to cybersecurity, for Dr. Carl Landwehr, Director - Cyber Trust Program).

Department of Energy (Dr. Thomas Dnousse, Director, High-Performance Network Research).

Federal Reserve Board (numerous meetings with Ms. Marianne Emerson, Director of IT for FRB).

Impact/Contacts Resulting from Research

Government Related Contacts (continued):

Committee on National Security Systems (invited to present an overview of our research at annual meeting in April 2004 - approximately 200 people attended the presentation). "Under Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, the President has re-designated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS). The Department of Defense continues to chair the committee under the authorities established by NSD-42. As a standing committee of the President's Critical Infrastructure Protection Board, the CNSS reports fully and regularly on its activities to the Board."

National Security Agency/West Point Military Academy (in September 2004, met with Dr. Aaron Ferguson, visiting professor at West Point while on loan from NSA).

2004 State of Maryland Information Technology Security and Privacy Conference (invited to present an overview of our research at annual meeting by a Mr. Rick O'Donnel, representative for the Assistant Director of Security for the State's Department of Budget and Management).

Impact/Contacts Resulting from Research

Government Related Contacts (continued):

2003 Netcentricity Conference (invited to present an overview of our research at the annual Netcentricity Conference held at the University of Maryland - approximately 120 participants attended, a large number of whom were CIOs from organizations within the Public and Private Sectors).

2002, 2003, and 2004 Workshop on Economics and Information Security (presented papers and/or chaired sessions; 2002 held at University of California, Berkeley, 2003 held at University of Maryland, 2004 held at University of Minnesota; each Workshop attended by approximately 65 participants from academia, business [e.g., Microsoft], and government [e.g., Naval Research Labs, Los Alamos National Laboratory]).

Assistant U.S. Attorney, District of New Jersey (Mr. Elliot Turrini).

Two Professors at the University of Tokyo (Dr. Kanta Matsuura and Dr. Hideyuki Tanaka) have been in touch with us about applying our model (what we affectionately call the GLEIS Model) for determining information security investments to E-Government activities. Their work is being supported by Japan's Ministry of Economy, Trade and Industry.

Impact/Contacts Resulting from Research

Non-Government Related Contacts:

Microsoft
Hewlett-Packard
Shell
Computer Security Institute (CSI)
Corporate Executive Board
McConnell International
Sun Microsystems
Coca-Cola
Cyber Security Industry Alliance
Red Siren
Booze Allen Hamilton
PriceWaterhouseCoopers
IBM
I-4 Corporate Members (gave a talk to about 80

Popular Press/Trade Magazines:

Business Week
Government Enterprise
Washington Business Journal
Network Computing
Maryland Public Television
Information Week
Optimize
Network Magazine
Secure Enterprise
Business Finance Magazine

Universities:

Harvard
UC-Berkeley
Penn State
University of Colorado
University of Minnesota
Georgia Institute of Technology
George Mason University
State Univ. of NY - Buffalo
University of Toronto
University of Rochester
Yale
Cambridge
Carnegie Mellon
Indiana University
London School of Economics
Michigan
Johns Hopkins
Dartmouth
Singapore Management University

Concluding Comments

- Information (Cyber) Security is a fundamental concern to Public and Private Organizations operating in the Digital Economy
- The area of research related to "Economic Aspects of Information (Cyber) Security" is emerging as a critical component of the Cybersecurity landscape
- Research opportunities are abundant

REFERENCE KEY

CACM$_1$ Gordon, Lawrence A. and Martin P. Loeb, "A Framework for Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM*, September, 2001, pp.70-75.

CACM$_2$ Gordon, L.A., M.P. Loeb, and T. Sohail, 2003. "A Framework for Using Insurance for Cyber-Risk Management," *Communications of the ACM* (March), pp. 81-85.

CACM$_3$ Bodin,.L, L. A. Gordon, and M.P. Loeb, "Evaluating Information Security Investments Using the Analytic Hierarchy Process," *Communications of the ACM* , forthcoming.

CACM$_4$ Gordon, L. A. & M. P. Loeb, "Information Security Budgeting Process: An Empirical Study," *Communications of the ACM*, forthcoming.

CSJ$_1$ Gordon, L.A., M.P. Loeb, and W. Lucyshyn, 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal* (Vol. 19, No. 2), pp. 1-7.

CSJ$_2$ Gordon, L.A., M.P Loeb, W. Lucyshyn, and R. Richardson, 2004, "CSI/FBI Computer Crime and Security Survey," *Computer Security Journal*, Summer.

JAPP Gordon, L.A., M.P. Loeb, and W. Lucyshyn, 2003. "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy* (Vol. 22, No. 6), pp. 461-485.

JCS Campbell, K., L.A. Gordon, M.P. Loeb, and L. Zhou, 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (Vol. 11, No.3), pp. 431-448.

OUP Gordon, Lawrence A. and Martin P. Loeb, "Expenditures on Competitor Analysis and Information Security: A Management Accounting Perspective," Chapter in Management Accounting in the Digital Economy (Oxford University Press), A. Bhimini (ed), 2003, pp. 95-111.

SF Gordon, L.A. and M.P. Loeb, November 2002. "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance* (November), pp. 26-31.

TISS Gordon, L.A. and M.P. Loeb, 2002, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* (November), pp. 438-457. (reprinted in Economics of Information Security, 2004).