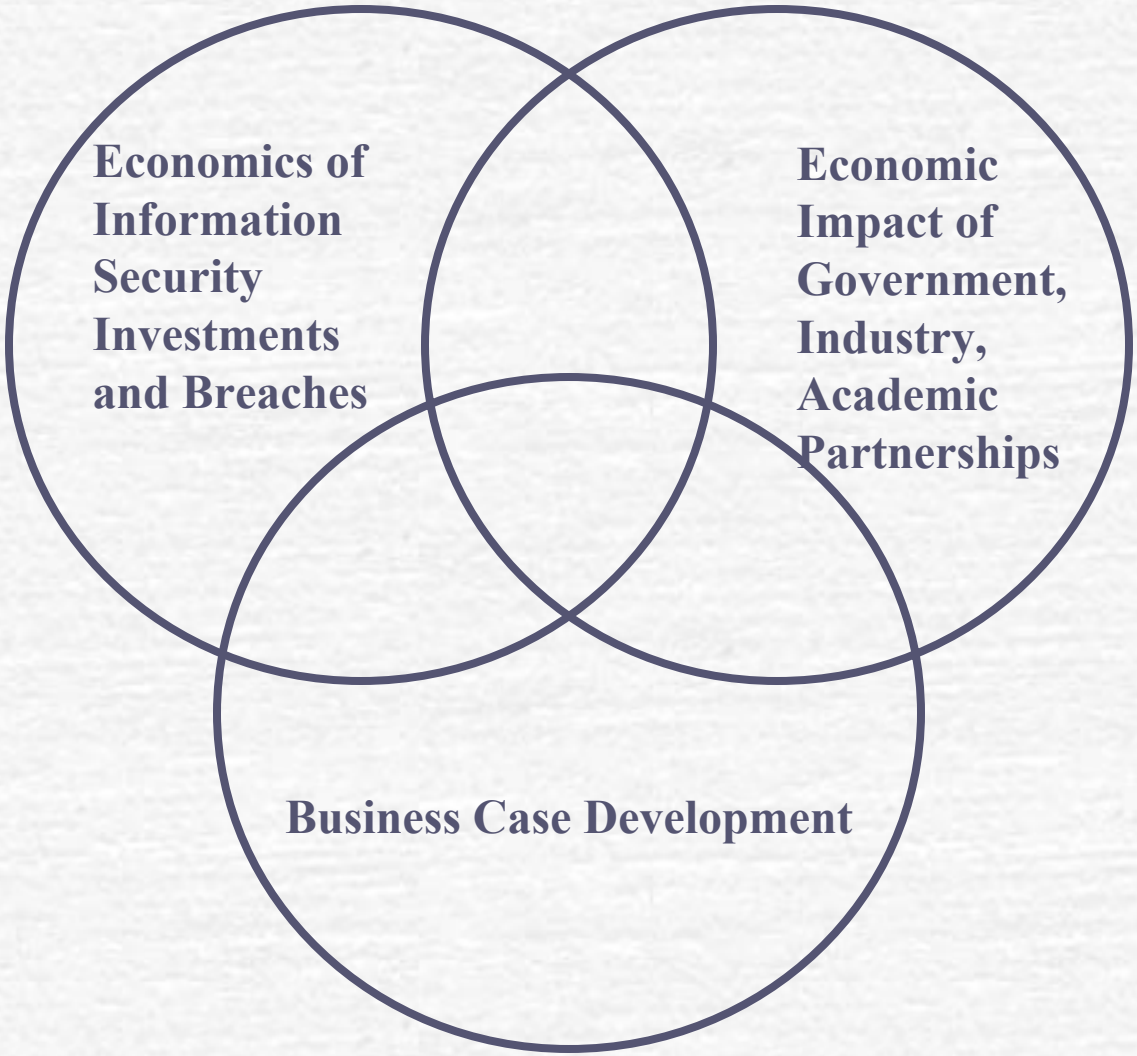
The Economics of Networking and Technology

Lawrence A. Gordon
Ernst & Young Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business
Affiliate Professor in University of Maryland Institute for Advanced Computer Studies
University of Maryland, College Park

Martin P. Loeb
Professor of Accounting and Information Assurance
Deloitte & Touche Faculty Fellow
Robert H. Smith School of Business
Affiliate Professor in University of Maryland Institute for Advanced Computer Studies
University of Maryland, College Park

June 18, 2004

Gordon and Loeb Tasks



Overall Goals and Approach

Goals

- Analyze the economic cost of security breaches
- Determine the optimal amount to invest in information security
- Determine how to allocate information security expenditures
- Provide an economic analysis of partnerships designed for information sharing related to computer security (e.g., ISACS)
- Address issues related to the business case for research
- Address issues related to the business case for information security expenditures

Research Approach:

- Building Economic Models (Theory Development)
- Statistical Analysis of Archival Data
- Simulated Case Analysis

Milestones – last 12 months

Milestones – last 12 months	Gordon and Loeb Tasks		
	Security Investments and Breaches	Government and Industry Partnerships	Business Case Development
Revised model and rewrote analysis of information sharing paper for publication purposes: **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***		X	
Prepared 2002 *ACM Transactions on Information and System Security* paper for reprinting: **Gordon, L.A. and M.P. Loeb, 2004. "Economics of Information Security Investment" *Economics of Information Security* , Camp (Harvard) and Lewis (Cambridge), eds.**	X		
Revised and resubmitted paper (paper accepted for publication) **Bodin, L., Gordon, L.A., and M.P. Loeb, forthcoming. "Evaluating Information Security Investments Using the Analytic Hierarchy Process, " *Communications of the ACM***	X		
Developed a framework for the Business Case for Research			X
Prepared Annotated Bibliography (see Appendix)	X	X	

Research Results

The annotated bibliography (Appendix) summarizes research results of all our papers.

Example: Information Sharing

- Game theoretic model
- 2 firms, each minimize their expected information security cost - the expected costs due a breach plus the costs of information security investments

$$\min_{x_i} \; [P^i(x_i, \theta_j x_j) L_i + x_i]$$

- At (Nash) equilibrium, each firm spends no more (and often less) on information sharing than it does in the absence of sharing (i.e., when $\theta=0$).
- For most cases, information sharing will increase the overall level of information security, i.e., the probability of a breach goes down
- For all cases, information sharing increases social welfare (more security for less $)
- For all cases, firms' underinvest in information security –they get all the costs but not all the benefits.
- If level of information sharing, (θ_1, θ_2), is endogenous, then each firm has incentives to free-ride and not share, i.e., to set $\theta_i=0$,

Significance of Research Results

Influence related to academic community

- Publications in academic journals (see Appendix)
- Invited to participate in University level discussions, at the request of special assistant to the Provost (Dr. William Destler), on the desirability of an interdisciplinary MS in information security program at the University of Maryland, College Park. Other participants have been from Computer Science, Engineering, School of Public Policy and Communications.
- Invited as founding program committee members of the Workshop on Economics of Information Security (WEIS), Workshops at Berkeley (2002), Maryland (2003), Minnesota (2004), and next year at Harvard
- Reviewed NSF proposals related to economics of information security and manuscripts for premier academic journals

Significance of Research Results

Influence related to academic community (continued)

- Chaired dissertation committee for Maryland Accounting and information Assurance student

- Served on dissertation committee for Harvard computer science Ph.D. student

- Co-Coordinated the Forum on *Financial Systems and Cybersecurity: A Public Policy Perspective*

- Contacted about our stream of research by individuals from such Universities as: MIT, Harvard, Cambridge, Minnesota, Georgia Tech., Singapore Management Univ., Penn State, Berkeley, Carnegie Mellon, London School of Economics, Michigan and Dartmouth

Significance of Research Results (continued)

Public Policy related meetings during past 12 months:

- Department of Homeland Security
  - -Assistant Secretary for Infrastructure Protection
  - -Director of Cybersecurity
- National Security Council
  - -Director of Cyberspace Security
- Presentation at Committee on National Security Systems

Significance of Research Results (continued)

Increased public awareness

- Presentation at I-4 Meeting
- Presentation at BizNet Conference
- Have had significant impact on research direction of AIA Department within Robert H. Smith School of Business
- Invited as part of academic team to assist with 2004 CSI/FBI Computer Crime and Security Survey
- Interviews with Maryland Public Television
- Stories in Print Media , e.g. *Washington Business Journal, InformationWeek*
- Meeting with representatives from Cyber Security Industry Alliance
- Meeting with representatives from Corporate Executive Board

Interaction with LTS

- Summer 03 meeting with Bill Semancik and Gary Hayward
- Spring 04 Presentation of Business Case for Research to Bill Semancik, Dan Foerter, and Justin McCann
- Participation in LTS-UMIACS seminars

Plans and Projected Milestones for Next 12 Months

Business Case for Research

- **Objective**—Investigate how decisions on whether research should be accomplished in-house or outsourced
- **Goal**—Develop an economics based methodology to evaluate the make/buy research alternatives
- **Plan**
  - Conduct a literature review (completed)
  - Develop methodology (completed)
  - Review and evaluate (completed)
  - Draft paper and submit to *TechTrends (in progress)*

Plans and Projected Milestones for Next 12 Months (Continued)

Cost of Information Security Beaches

- **Objective**—Extend *Journal of Computer Security* study to investigate the total (explicit and implicit) economic costs of security breaches using larger sample, new empirical model, and incorporating LTS feedback.

- **Goal**—Estimate the economic cost of breaches to a firm and determine which types of breaches are most costly. Provide guidance to organizations in allocating their scarce information security resources.

- **Plan**
  - Conduct a literature review (completed)
  - Develop methodology (completed)
  - Collect data (completed)
  - Perform Analysis (in progress – to be completed by 8/21/ 2004)
  - Draft paper and submit to research journal (to be done – target date of completion 1/31/05)

Plans and Projected Milestones for Next 12 Months (Continued)

Business Case for Information Security Expenditures Research (focus on critical infrastructure industries).

- **Objective**—Analyze how to make the best case internally for funding of information security activities and projects.
- **Goal**—Develop framework that information security officers can use to effectively compete for internal funds.
- **Plan**
  - Conduct a literature review (completed)
  - Develop methodology (in progress, target completion – 12/31/04)
  - Propose draft and circulate for comments (to be completed by 2/15/05)
  - Draft paper (to be completed 5/30/05).

Plans and Projected Milestones for Next 12 Months (Continued)

Financial Reporting of Information Security Expenditures by Telecommunications Firms

- **Objective**—Investigate the current state of financial reporting of information security expenditures by telecommunications firms and determine the economic impact of these reports.

- **Goal**—Provide evidence that encourages further voluntary information security reporting

- **Plan**
  - Conduct a search of 10Ks (expected completion date 7/31/04)
  - If search produces sufficient disclosures, collect archival data for econometric analysis and draft paper for comments

Appendix: Annotated Bibliography
Economics Aspects of Information Security by Gordon and Loeb

PUBLISHED (OR FORTHCOMING) ARTICLES

Bodin, L., L. A. Gordon and M. P. Loeb, "Evaluating Information Security Investments Using the Analytic Hierarchy Process," *Communications of the ACM*, forthcoming. The Analytic Hierarchy Process (AHP) is a tool for analyzing multi-criteria decision problems involving quantitative and qualitative criteria. This paper shows how a Chief Information Security Officer can apply the AHP to determine the best way to spend a limited information security budget and to make a case to the organization's Chief Financial Officer for an increase in funds to further enhance the organization's information security.

Gordon, L. A., M. P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003. The U.S. federal government has fostered a movement toward sharing information concerning computer security, with particular emphasis on protecting critical infrastructure assets that are largely owned by the private sector. This paper presents a model to examine the welfare economic implications of this movement. It is shown that, since information sharing lowers the cost of each firm attaining any given level of information security, there are potential benefits for individual firms and society at large from sharing. However, it is also shown that in the absence of appropriate economic incentive mechanisms, each firm will attempt to free ride on the security expenditures of other firms (i.e., renege from the sharing agreement and refuse to share information).

Campbell, K., L.A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11, No. 3, 2003. This study examines the economic effect of information security breaches on the stock market value of corporations. This approach takes into account the indirect costs, as well as the direct costs, to the firm. The analysis shows that cyber security breaches in which confidential private information is compromised (e.g., the release of customer credit card numbers, bank account numbers, or medical records to unauthorized parties) have a significant negative effect on the stock market value of the attacked firm. However, security breaches not related to confidentiality (e.g., a temporary shut down of a corporate website) involve costs that are transitory and are unlikely to significantly affect shareholder value. Thus, market participants appear to discriminate across types of breaches and economically rational investment strategies should focus on protecting the firms' most valuable information assets.

Gordon, L A., M. P. Loeb and W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal*, Vol. 19, No. 2, 2003. Empirical evidence suggests that security breaches are an important driver of actual expenditures on information security activities. Although this wait-and-see approach toward information security expenditures may seem unwise on the surface, there is a rational economic explanation for such an approach under the appropriate conditions. Indeed, as shown in this paper, this approach toward information security expenditures may be consistent with the real option (in particular, the deferment option) view of capital budgeting.

Appendix: Annotated Bibliography (p. 2)
Economics Aspects of Information Security by Gordon and Loeb

Gordon, L. A., M. P. Loeb and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management," *Communications of the ACM*, March 2003. Insurance companies, designing new policies to deal with the cyber risks of information breaches, have had to address issues related to pricing, adverse selection, and moral hazard. While these issues are common to all forms of insurance, this paper examines the unique aspects associated with cyber risk and presents a framework for using insurance as a tool for helping to manage information security risk. This framework is based on the risk management process and includes a four-step cyber risk insurance decision plan.

Gordon, L. A. and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, November 2002. (Reprinted in *The Economics of Information Security,* Camp and Lewis, eds.) This paper presents an economic model that characterizes the optimal monetary investment to protect a given set of information. It is shown that, for a given potential loss, the optimal amount to spend to protect an information set does not always increase with increases in the information set's vulnerability. Protecting highly vulnerable information sets may be inordinately expensive, and a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities. Moreover, the paper shows that the amount the firm should spend to protect information sets should generally be only a small fraction of the expected loss.

Gordon, L. A. and M. P. Loeb, "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance*, November 2002. Although measures of return on investment have gained increased attention as a financial tool to evaluate information security projects, conceptual and practical problems of these measures have been largely ignored. This paper highlights several of these problems. The paper shows that the common accounting measure of return on investment is different from the economic measure of return on investment, and that the accounting measure is inappropriate for both the ex ante and ex post evaluation of information security projects. The paper also recommends focusing on selecting a profit maximizing level of information security investment as opposed to the investment level that maximizes a measure of return on investment.

Gordon, L. A. and M. P. Loeb, "Economic Aspects of Information Security," *Tech Trends Notes,* Fall 2001. This paper provides an economic framework for looking at the allocation of resources to information security activities. A major argument of this paper is that expenditures on information security need to be considered in cost-benefit terms, in a similar fashion to the way organizations allocate resources to other activities.

Appendix: Annotated Bibliography (p. 3)
Economics Aspects of Information Security by Gordon and Loeb

Gordon, L. A. and M. P. Loeb, "A Framework for Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM*, September 2001. Information security is an appropriate response to rivals' development of competitor analysis systems. This paper provides a framework for using information security in such a fashion. The paper also provides a five-step approach toward allocating information security funds in an effort to protect a firm from becoming a meaningful part of the competition's competitor analysis system.

Gordon, L. A. and M. P. Loeb, "Expenditures on Competitor Analysis and Information Security: A Management Accounting Perspective," in Management Accounting in the Digital Economy (Oxford University Press), A. Bhimini (ed.), 2003. An underlying premise for both expenditures on competitor analysis and expenditures on information security is that information is an economic good with strategic value. In this paper, a game theoretic model of a market shared by two rivals is presented and analyzed in order to shed light on how expenditures on competitor analysis affect, and are affected by, expenditures on information security. The paper also discusses the importance of these information economy based issues for management accounting.