ECONOMIC ASPECTS OF CYBER/INFORMATION SECURITY

Lawrence A. Gordon

Ernst & Young Alumni Professor of Managerial Accounting & Information Assurance

The Robert H. Smith School of Business

University of Maryland

Affiliate Professor in UMIACS

Researcher in Maryland Cybersecurity Center

Objectives of Presentation

A. Discuss a Few Issues Related to Cybersecurity Economics:
   1. Economic Impact of Cybersecurity Breaches on Corporations
   2. Making Cybersecurity Investment Decisions
   3. The Effect of SOX on Disclosing Cybersecurity Activities
   4. The Effect of Voluntarily Disclosing Cybersecurity Activities on Firm Value
   5. Cybersecurity Insurance as a Mechanism to Transfer Risk

B. Present Framework for Cybersecurity Risk Management

Note: Economic Models Should be Used as Complement to, and Not as a Substitute for, Sound Business Judgment!!!

A1. Impact of Cybersecurity Breaches on Corporations

Cybersecurity Breaches are a Key Concern to Private and Public Sector Organizations

President Obama's Initiatives

Economic Costs of Cybersecurity Breaches

- Conventional Wisdom
- Need to Consider Implicit and Explicit Costs
- Key Studies have Looked at Impact of Breaches on Stock Market Returns (SMR)

A1: Results of Studies Looking at Impact of Cybersecurity Breaches on SMR

Large Percentages of Breaches Do Not Have Significant Impact on Firms

a. Stockholders have Become Tolerant of Breaches

b. Many Firms have Strengthened their Remediation Plans, thereby Substantially Reducing the Cost of an Average Breach

– Breaches that Do Have a Significant Impact on SMR can Threaten Firm's Survival

A2. Making Cybersecurity Investments

- Making the Business Case
- Net Present Value (NPV) Model
- Optimal Amounts to Invest (Need to Consider Security Breach Function [i.e., Vulnerabilities, Threats, and Productivity of Investments] & Potential Loss)
- Option Value of Investments

Note: Economic Models Should be Used as a Complement to, and Not as a Substitute for, Sound Business Judgment!!!

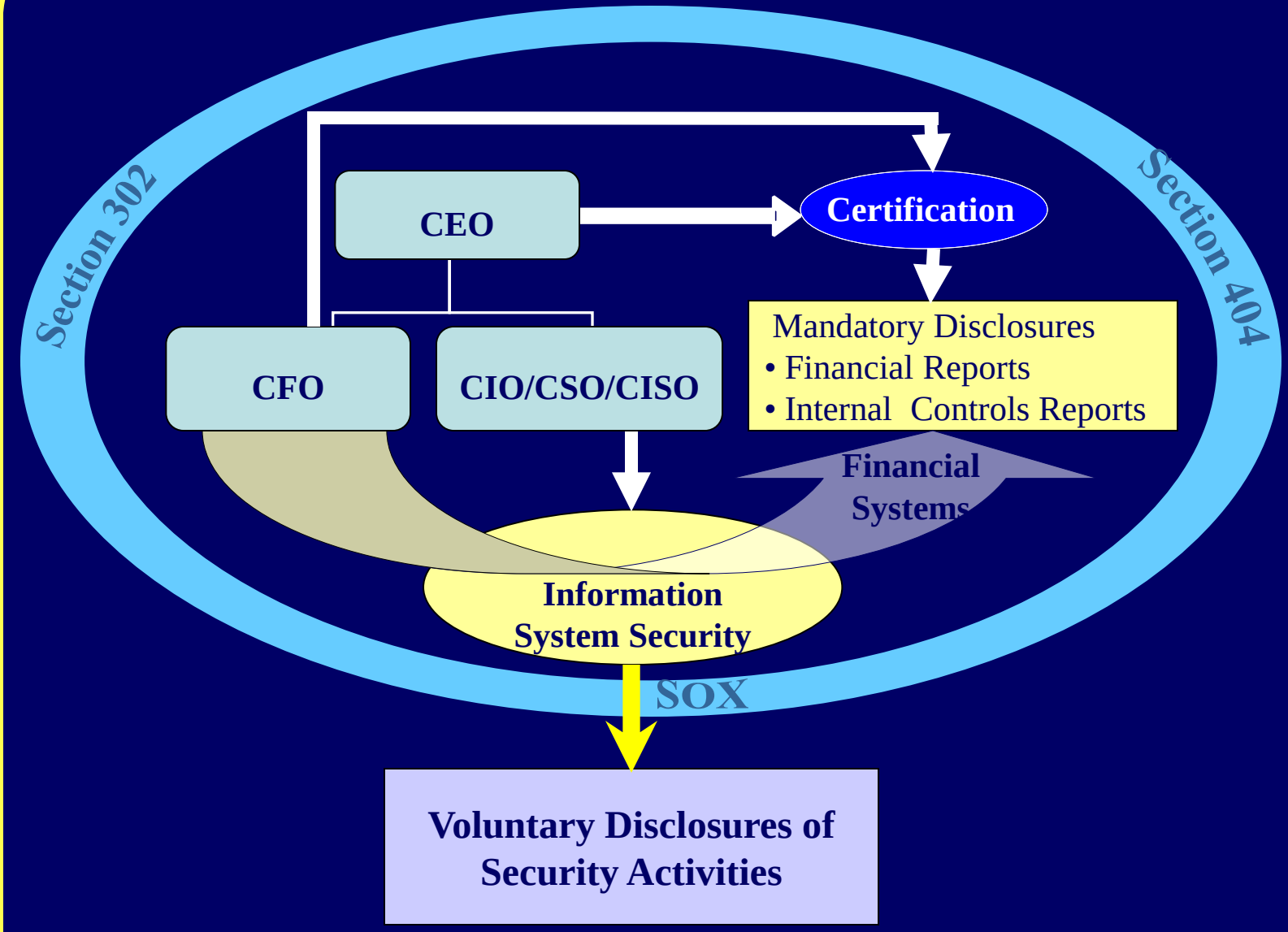
A2 : The Business Case Process for Cybersecurity Investments

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

A2 : Results of Studies Looking at Making Investments in Cybersecurity

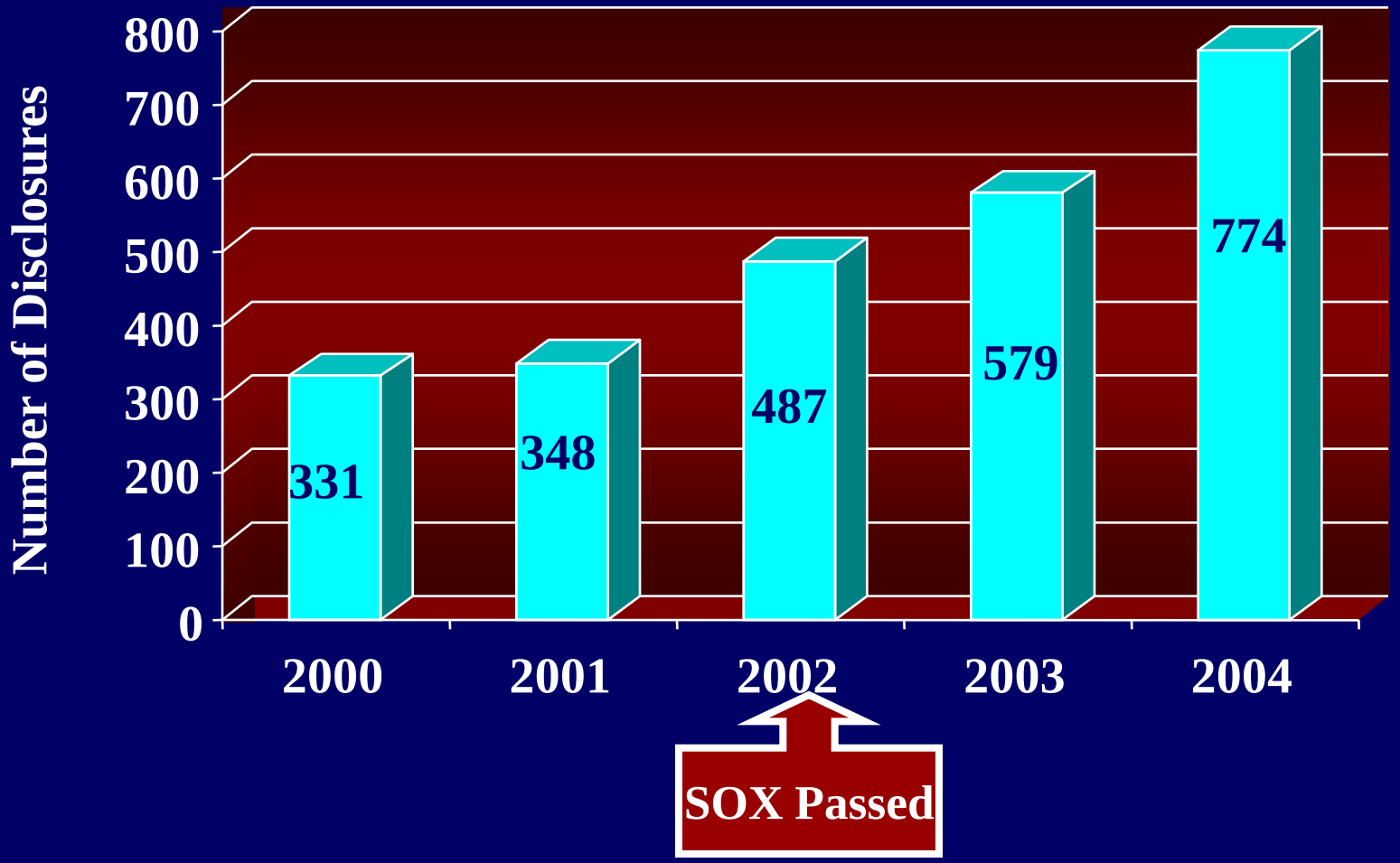
- Optimal level of Information Security Investment Does Not Always Increase with the Level of Vulnerability
- For a Wide Range of Circumstances, Firms should Invest ≤ 37% of Expected Loss
- Wait-and-see approach is often Rational from An Economics Perspective due to Real Options

A3. Impact of Sarbanes Oxley Act of 2002 (SOX) on Information Security



Source: Gordon, Loeb, Lucyshyn, and Sohail, 2006.

A3: The Impact of SOX on Voluntarily Disclosing Cybersecurity Activities



Source: Gordon, Loeb, Lucyshyn, and Sohail, 2006.

A4. Impact of Voluntary Disclosures of Cybersecurity Activities on Firm Value

Voluntary Disclosures Concerning Information Security, in Annual Reports Filed with the SEC, were found to be Positively Associated with Increases in the Stock Market Value of Firms.

Source: Gordon, Loeb and Sohail, 2010.

A5. Cybersecurity Insurance: A Risk Transfer Mechanism

- Organization's Perspective:
  - Assess if Cybersecurity Insurance is Needed
  - Evaluate Available Insurance Policies
  - Select Appropriate Policy and Transfer Risk
- Insurance Company's Perspective
  - Pricing Decisions Require More Actuarial Data
  - Adverse Selection
  - Moral Hazard
  - Slow to Gain Momentum
- Executive Office of the President is Currently Involved in this Issue

B. Cybersecurity Risk Management (CRM)

Cybersecurity Risk

- Uncertainty of Potentially Harmful Events Related to Cybersecurity

Cybersecurity Risk Management

- Process of Managing (Reducing) Potentially Harmful Uncertain Events Due to the Lack of Effective Cybersecurity

B. Risk Metrics (Different Strokes for Different Folks)

- **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

B . Cybersecurity Risk Management Assessment and Control Framework

Concluding Comments

1. Cybersecurity Economics Is Not Voodoo Economics
2. Many Cybersecurity Breaches do not have a Significant Impact on Firms, but some can Threaten the Survival of a Firm
3. SOX has Increased Voluntary Disclosures of Cybersecurity Activities and such Disclosures are Associated with Increasing Firm Value.
4. Cybersecurity Insurance is a Mechanism for Transferring Risk
5. There are Different Ways to View Risk
6. CRM provides a Framework for Viewing Many Economic Issues Associated with Cybersecurity
7. A Catastrophic Cybersecurity Breach May Occur

SELECTED REFERENCES RELATED TO STREAM OF RESEARCH

Bodin, L., L.A. Gordon and M.P. Loeb, "Information Security and Risk Management," *Communication of the ACM*, Vol. 51, No. 4, 2008, pp. 64-68.

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, pp. 431-448.

Gordon, L.A. and M.P. Loeb, Managing Cybersecurity Resources: A Cost-Benefit Perspective (McGraw-Hill), 2006.

Gordon, L.A. and M.P. Loeb, "Information Security Budgeting Process: An Empirical Study," *Communications of the ACM* , Jan. 2006, pp. 121-125.

Gordon, L.A., M.P. Loeb, "Economic Aspects of Information security: An Emerging Field of Research," *Information System Frontiers*, Vol. 8, No. 5, 2006, pp. 335-337.

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

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

Gordon, L.A., M.P. Loeb, W. Lucyshyn, "Private Sector Investments in Cybersecurity," in progress.

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, pp. 461-485,

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, pp. 1-7.

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

Gordon, L.A., M.P. Loeb and T. Sohail, "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, September 2010, pp. 567-594.

Gordon, L.A., M.P. Loeb, and T. Sohail, "A Framework for Using Insurance for Cyber-Risk Management," C*ommunications of the ACM*, March 2003, pp. 81-85.

Gordon, L.A., M.P. Loeb, T. Sohail, C-Y Tseng and L. Zhou, "Cybersecurity Capital Allocation and Management Control Systems," *European Accounting Review*, Vol. 17, No. 2, 2008, pp. 215-241.

Gordon, L.A., M.P. Loeb, and L. Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* Vol. 19, No. 1, 2011, pp. 33-56.

Biography of Dr. Lawrence A. Gordon

Dr. Lawrence A. Gordon is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance at the University of Maryland's Robert H. Smith School of Business. He is also an Affiliate Professor in the University of Maryland Institute for Advanced Computer Studies. Dr. Gordon earned his Ph.D. in Managerial Economics from Rensselaer Polytechnic Institute. His research focuses on corporate performance measures, economic aspects of cyber and information security, cost management systems, and capital investments. He is the author of more than 90 articles that have been published in the accounting and computer/information security journals, and is considered to be one of the pioneers in the emerging field of cybersecurity economics. Dr. Gordon is also the coauthor or author of several books, including MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis and Managerial Accounting: Concepts and Empirical Evidence (6th Edition). In addition, he is the Editor-in-Chief of the *Journal of Accounting and Public Policy* and serves on the editorial boards of several other academic journals. In two authoritative studies, Dr. Gordon was cited as being among the world's most influential/productive accounting researchers.

An award-winning teacher, Dr. Gordon has been an invited speaker at numerous universities around the world, including: Columbia University, Harvard University, London School of Economics, London Business School, University of Manchester, University of Toronto, Carnegie Mellon University, Instituto de Empresa. and UC-Berkeley. Dr. Gordon's Ph.D. students (i.e., those students for whom he has served as the Chair or Co-Chair of their dissertation) have had initial placements as an Assistant Professor of Accounting at the Business Schools of such universities as: Northwestern University, University of Southern California, Purdue University, Rensselaer Polytechnic Institute, Instituto de Empresa, McGill University, National Taiwan University, College of William & Mary, and Michigan State University.

Dr. Gordon has served as a consultant to several private and public organizations. He is also a frequent speaker at various professional meetings of corporate and government executives. In October 2007, Dr. Gordon was invited to provide formal Congressional Testimony concerning his research on cybersecurity economics before a Subcommittee of the U.S. House Committee on Homeland Security. He has also been a frequent contributor to the popular press (e.g., Wall Street Journal, Washington Post, Business Week, Baltimore Sun, Washington Business Journal, etc.).