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

December 2010        L. A. Gordon ©
OBJECTIVES

A. Define Basic Concept of Cybersecurity

B. 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

C. Framework for Cybersecurity Risk Management
   (Cybersecurity Risk Management is a Subset of ERM)
A. Basic Concept of Cybersecurity

Cybersecurity

— Protection of Information Transmitted and Stored over the Internet or any other Computer Network

Objectives of Cybersecurity

— Protect Confidentiality of Private Information
— Ensure Availability of Information to Authorized Users on a Timely Basis
  — Authentication
  — Nonrepudiation
— Protect the Integrity of Information (i.e., Accuracy, Reliability, and Validity)
B1. 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)
B1: Research Methodology

One-factor Model (Basic CAPM)

\[ R_{it} - RF_t = a_i + b_i (RM_t - RF_t) + \epsilon_{it} \]

Fama and French (F&F) 3-Factor Model

\[ R_{it} - RF_t = a_i + b_i (RM_t - RF_t) + s_i SMB_t + h_i HML_t + \epsilon_{it} \]

- \( R_{it} \): firm’s return, \( RF_t \): risk-free rate, \( RM_t \): market’s return
- \( b_i \) = the CAPM market model’s slope parameter (i.e., the systematic risk of the return for firm \( i \), relative to the return of the entire market place, and often call the firm’s beta)
- \( SMB_t \): the difference between the return on a portfolio of small stocks and the return on a portfolio of large stocks
- \( HML_t \): the difference between the return on a portfolio of high-book-to-market stocks and the return on a portfolio of low-book-to-market stocks
Abnormal Returns:

\[
AR_{it} = (R_{it} - RF_t) - [\hat{a}_i + \hat{b}_t (RM_t - RF_t)]
\]

or

\[
AR_{it} = (R_{it} - RF_t) - [\hat{a}_i + \hat{b}_t (RM_t - RF_t) + \hat{s}_i SMB_i + \hat{h}_i HML_i]
\]

Cumulative Abnormal Returns:

\[
CAR_i = \sum_{t=t_i}^{t_2} AR_{it},
\]

Average CAR across Firms:

\[
\overline{CAR} = \frac{1}{N} \sum_{i=1}^{N} CAR_i
\]
Large Percentages of Breaches Do Not Have Significant Impact on SMR of Firm

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

Note: Economic Models Should be Used as Complement to, and Not as a Substitute for, Sound Business Judgment!!!
B2. 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!!!
1. Specify Organizational Cybersecurity Objectives

2. Identify Alternatives for Achieving Cybersecurity Objectives

3. Acquire Data and Analyze Each Alternative Identified

4. Conduct Cost-Benefit Analysis and Rank Order the Alternatives Identified – Select Alternative

5. Control (Postauditing)

Source: Gordon and Loeb, 2006a, pp. 116 and 131.
The NPV model, shown below in Eq. 1, gives rise to a simple decision rule for accepting or rejecting incremental information security investments.

\[
NPV = \frac{(B_t - C_t)}{(1+K)^t}
\]

where \( B \)=Benefits, \( C \)=Costs, \( K \)=Discount Rate, \( t \)=Time and \( n \)=Number of Time Periods. Biggest Challenge is estimating \( B \).
B2: Optimal Amount to Invest in Cybersecurity (Gordon-Loeb Model)

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:

$$EBIS(z) = [v - S(z,v)] L$$  \[1\]

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:

$$ENBIS(z) = [v - S(z,v)] L - z$$  \[2\]

Maximizing [2] is equivalent to minimizing:

$$s(z,v)L + z$$  \[3\]

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

$$-S_z(z^*, v) L = 1$$  \[4\]
— Optimal level of Information Security Investment Does Not Always Increase with the Level of Vulnerability

— For a Wide Range of Circumstances, Firms should Invest $\leq 37\%$ of Expected Loss

— Wait-and-see approach is often Rational from An Economics Perspective due to Real Options
B3. Impact of Sarbanes Oxley Act of 2002 on Information Security

CEO Certification

Mandatory Disclosures
- Financial Reports
- Internal Controls Reports

CFO CIO/CSO/CISO

Financial Systems

Information System Security

SOX

Legend
- Mandatory
- Voluntary

Voluntary Disclosures of Security Activities

B3: The Impact of SOX on Voluntarily Disclosing Cybersecurity Activities

B4. Impact of Voluntary Disclosures of Cybersecurity Activities on Firm Value

METHODOLOGY: Pooled Stock Price Regression by Industry on Disclosure Proxies

PRC-3M_{it} = b_0 + b_1 \cdot \text{Dis}_{it} + b_2 \cdot \text{BVPS}_{it} + b_3 \cdot \text{EPS}_{it} + b_4 \cdot \text{LnAst}_{it} + b_5 \cdot \text{NEG}_{it} + \sum b_k \cdot \text{Year}_{it} + e_{it}

Results: 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.

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

Source: Gordon, Loeb and Sohail, 2010.
B5. Cybersecurity Insurance is Slowly Gaining Momentum

— Organization’s Perspective:
  — Assess if Cybersecurity Insurance is Needed
  — Evaluate Available Insurance Policies
  — Select Appropriate Policy

— Insurance Company’s Perspective
  — Pricing Decisions Require More Actuarial Data
  — Adverse Selection
  — Moral Hazard

— Executive Office of the President is Currently Involved in this Issue
B5. 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
C. Risk Metrics

- **Expected Loss**
  - Most Popular in Information Security Literature
  - \( = (\text{Probability of Loss}) \times (\text{Amount of Loss}) \)

- **Probability of No Loss**

- **Probability of Largest Loss**

- **Variance (or Standard Deviation) of Losses**
  - Most Popular Metric in Management Accounting, Economics & Finance
## C. Different Risk Metrics

<table>
<thead>
<tr>
<th>Possible Losses</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>0.40</td>
<td>$0</td>
<td>0.60</td>
<td>$0</td>
<td>0.15</td>
<td>$0</td>
</tr>
<tr>
<td>$1,000,000</td>
<td>0</td>
<td>$0</td>
<td>0</td>
<td>$0</td>
<td>0.60</td>
<td>$600,000</td>
</tr>
<tr>
<td>$2,000,000</td>
<td>0.60</td>
<td>$1,200,000</td>
<td>0</td>
<td>$0</td>
<td>0.15</td>
<td>$300,000</td>
</tr>
<tr>
<td>$3,000,000</td>
<td>0</td>
<td>$0</td>
<td>0.40</td>
<td>$1,200,000</td>
<td>0.10</td>
<td>$300,000</td>
</tr>
</tbody>
</table>

**Expected Value of Losses**

- Investment A = sum of column (3) = $1,200,000
- Investment B = sum of column (5) = $1,200,000
- Investment C = sum of column (7) = $1,200,000

Investment A, B and C are Equal Amounts

Source: Gordon and Loeb, 2006a, p. 98.
C. Different Risk Metrics

<table>
<thead>
<tr>
<th>Possible Losses</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
<th>Probability of Losses</th>
<th>Expected Value of the given loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>0.40</td>
<td>$0</td>
<td>0.60</td>
<td>$0</td>
<td>0.15</td>
<td>$0</td>
</tr>
<tr>
<td>$1,000,000</td>
<td>0</td>
<td>$0</td>
<td>0</td>
<td>$0</td>
<td>0.60</td>
<td>$600,000</td>
</tr>
<tr>
<td>$2,000,000</td>
<td>0.60</td>
<td>$1,200,000</td>
<td>0</td>
<td>$0</td>
<td>0.15</td>
<td>$300,000</td>
</tr>
<tr>
<td>$3,000,000</td>
<td>0</td>
<td>$0</td>
<td>0.40</td>
<td>$1,200,000</td>
<td>0.10</td>
<td>$300,000</td>
</tr>
</tbody>
</table>

Expected Value of Losses

Investment A = sum of column (3) $1,200,000
Investment B = sum of column (5) $1,200,000
Investment C = sum of column (7) $1,200,000
Investment A, B and C are Equal Amounts

Source: Gordon and Loeb, 2006a, p. 98.
C. Cybersecurity Risk Management Assessment and Control Framework

Organizational Objectives

Identifying Cybersecurity Risk

Is Risk Level Acceptable?

No

Manage Cybersecurity Risk via
- Efficient Use of Resources (Investments)
- Internal Controls
- Voluntary Disclosures
- Information Sharing
- Technical Improvements
- Behavioral/Organizational Improvements

Yes

Estimate Residual Risk

Further Reduce Risk via Insurance?

No

Cybersecurity Risk Control and Response (e.g., intrusion detection systems, cybersecurity auditing, corrective actions)

Yes

Cybersecurity Insurance
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 Slowly Gaining Momentum.
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 NOTED IN GANTT CHART


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, and Instituto de Empresa. 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 (e.g., IBM) and public (e.g. U.S. Government Accountability Office) 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, etc.).