INVESTING IN CYBERSECURITY

Lawrence A. Gordon

EY Alumni Professor of Managerial Accounting & Information Assurance
Affiliate Professor in University of Maryland Institute for Advanced Computer Studies
The Robert H. Smith School of Business
http://scholar.rhsmith.umd.edu/lgordon

January 2016

© lgordon@rhsmith.umd.edu
Basic Facts

Cybersecurity Breaches are Growing at an Alarming Rate

100% Security Is Not Possible

Investments in Cybersecurity Involve Resource Allocation Decisions (i.e., Cost-Benefit Decisions or Making the Business Case)

Large Share of Infrastructure Assets Owned by Private Sector Corporations
Costs of Cybersecurity Breaches to Corporations

Explicit Costs (e.g., Detecting and Correcting Breaches)
Implicit Costs (e.g., Reputation Effect, Potential Liability)

Impact of Breaches on Corporations*

• Breaches Impact Annual Earnings of Corporations
• Large % of Breaches Do Not Have a Significant Impact on Stock Market Returns of Firms -- *but Some Do!*
• Firms Have Strengthened Remediation Strategies
• Stockholders Have Become Tolerant of Breaches

*See Appendix A for Methodology.
Why Are Cybersecurity Investments So Difficult to Justify?

Cybersecurity Investments are Largely Cost Savings Projects Rather Than Revenue Generating Projects (and Among the Most Difficult Cost Savings Projects to Justify)

Benefits and Risk Factor are Impossible to Measure Precisely (Wait-and-see approach is often rational from an economics perspective due to real deferment option)

Externalities are Rarely Considered
$vL = (v - S[z,v])L$

$v = \text{Vulnerability/Threat}$
$L = \text{Potential Loss}$
$vL = \text{Expected Loss}$
$z = \text{Level of Investment}$

Benefits are Increasing at a Decreasing Rate

100% Security is Not Possible

Expected Benefits of Investment

Cost of Investment

Level of investment in information security

*Adapted from Gordon and Loeb, 2002a (see Appendix B).
Results of Gordon-Loeb Model*

Key Components of Optimal Amount to Invest:
- Potential Losses (Cost Savings)
- Vulnerabilities/Threats
- Productivity of Investments

Optimal Level of Cybersecurity Investments Does Not Always Increase with Level of Vulnerability

Firms should generally Invest ≤ 37% of Expected Loss (i.e., Invest, but Invest Wisely)

*Economic models should be viewed as a complement to, not as a substitute for, sound business judgment!
How Can Executives Use the Gordon-Loeb Model?*

**Step 1.** Estimate the Potential Loss (L) from a Security Breach for each Set of Information

**Step 2.** Estimate the Likelihood that an Information Set will be Breached, by examining its Vulnerability/Threat (v) to Attack

**Step 3.** Create a Grid with all the Possible Combinations of the First Two Steps, from Low Value, Low Vulnerability/Threat to High Value, High Vulnerability/Threat.

**Step 4.** Focus Spending where it Should Reap the Largest Net Benefits Based on Productivity of Investments (Conduct a Simulation by Changing Key Parameters)

*Adapted from Gordon and Loeb, 2011 (article in *WSJ*).
**Figure 2 (Example): Potential Loss from Information Security Breach**

Value of Information Sets (in $M)*

<table>
<thead>
<tr>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>20%</td>
<td>30%</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>20</td>
<td>40</td>
<td>50</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>70</td>
</tr>
<tr>
<td>40</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>50</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

*Value of Information = Potential Loss (L)

**Vulnerability/Threat = v**

Low: vL < 30
Medium: 69 ≥ VL ≥ 30
High: vL ≥ 70

© lgordon@rhsmith.umd.edu
PRODUCTIVITY OF INVESTMENTS IN CYBERSECURITY

<table>
<thead>
<tr>
<th>z</th>
<th>S(z,Low v)</th>
<th>S'</th>
<th>S(z,Medium v)</th>
<th>S'</th>
<th>S(z,High v)</th>
<th>S'</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.500</td>
<td>0.500</td>
<td>0.250</td>
<td>0.750</td>
<td>0.125</td>
<td>0.875</td>
</tr>
<tr>
<td>2</td>
<td>0.333</td>
<td>0.167</td>
<td>0.111</td>
<td>0.139</td>
<td>0.037</td>
<td>0.088</td>
</tr>
<tr>
<td>3</td>
<td>0.250</td>
<td>0.083</td>
<td>0.063</td>
<td>0.049</td>
<td>0.016</td>
<td>0.021</td>
</tr>
<tr>
<td>4</td>
<td>0.200</td>
<td>0.050</td>
<td>0.040</td>
<td>0.023</td>
<td>0.008</td>
<td>0.008</td>
</tr>
<tr>
<td>5</td>
<td>0.167</td>
<td>0.033</td>
<td>0.028</td>
<td>0.012</td>
<td>0.005</td>
<td>0.003</td>
</tr>
<tr>
<td>6</td>
<td>0.143</td>
<td>0.024</td>
<td>0.020</td>
<td>0.007</td>
<td>0.003</td>
<td>0.002</td>
</tr>
</tbody>
</table>

Low Productivity = v/(1+z) for Low Vulnerability/Threat
Medium Productivity = v/(1+z)^2 for Medium Vulnerability/Threat
High Productivity = v/(1+z)^3 for High Vulnerability/Threat
Figure 7: Investment Amounts

Value of Information Sets (in $M)

Low | Medium | High
---|---|---
10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100

- 10%: <1M, 1M, <2M, <2M, 2M, <3M, <3M, <3M, <3M, <3M
- 20%: 1M, <2M, 2M, <3M, <3M, 3M, <4M, <4M, <4M, 4M
- 30%: <2M, 2M, <3M, 3M, <4M, <4M, >4M, >4M, >4M, >4M
- 40%: <2M, <3M, <3M, <3M, <4M, <4M, <4M, <4M, <4M, <4M
- 50%: <2M, <3M, <3M, <3M, <4M, <4M, <4M, <4M, <4M, >4M
- 60%: <2M, <3M, <3M, <4M, <4M, <4M, <4M, <4M, >4M, >4M
- 70%: <2M, <3M, <4M, <4M, <4M, <4M, >4M, >4M, >4M, >4M
- 80%: <2M, <3M, <3M, <3M, <3M, <4M, <4M, <4M, <4M, <4M
- 90%: <2M, <3M, <3M, <3M, <3M, <4M, <4M, <4M, <4M, <4M
- 100%: <2M, <3M, <3M, <3M, <4M, <4M, <4M, <4M, <4M
Concluding Comments

I. Cybersecurity Investments Are Hard To Justify
   They are Cost Savings, Not Revenue Generating, Projects
   You Can’t See Savings
   Most Breaches Do Not Have Significant Effect on Stock Prices

II. Invest, but Invest Wisely
    Conduct Cost-Benefit Analysis (Making the Business Case)
    On Average, Invest \leq 37\% of Expected Loss
    Wait-n-See Approach is Rational from Economics Perspective
    Key Investment Factors: Potential Loss,
       Vulnerabilities/Threats,
       Productivity of Investments
    Conduct Simulation

III. Optimal Level of Investment Does Not Always
     Increase With The Level of Vulnerability/Threat
     Best Payoff Often Comes from Mid-level Vulnerability/Threat

© lgordon@rhsmith.umd.edu


*The Gordon-Loeb Model was originally published in this article.
Appendix A: Research Methodology for Studying Cybersecurity Breaches

One-factor Model (Basic CAPM)

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

Abnormal Returns:

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

Cumulative Abnormal Returns:

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

Average CAR across Firms:

\[ \overline{CAR} = \frac{1}{N} \sum_{i=1}^{N} CAR_i \]

- \( R_{it} \): 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 called the firm’s beta)
Appendix B: 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.

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

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]) :

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

*Adapted from Gordon and Loeb, 2002a.