UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

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

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

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.

© lgordon@rhsmith.umd.edu

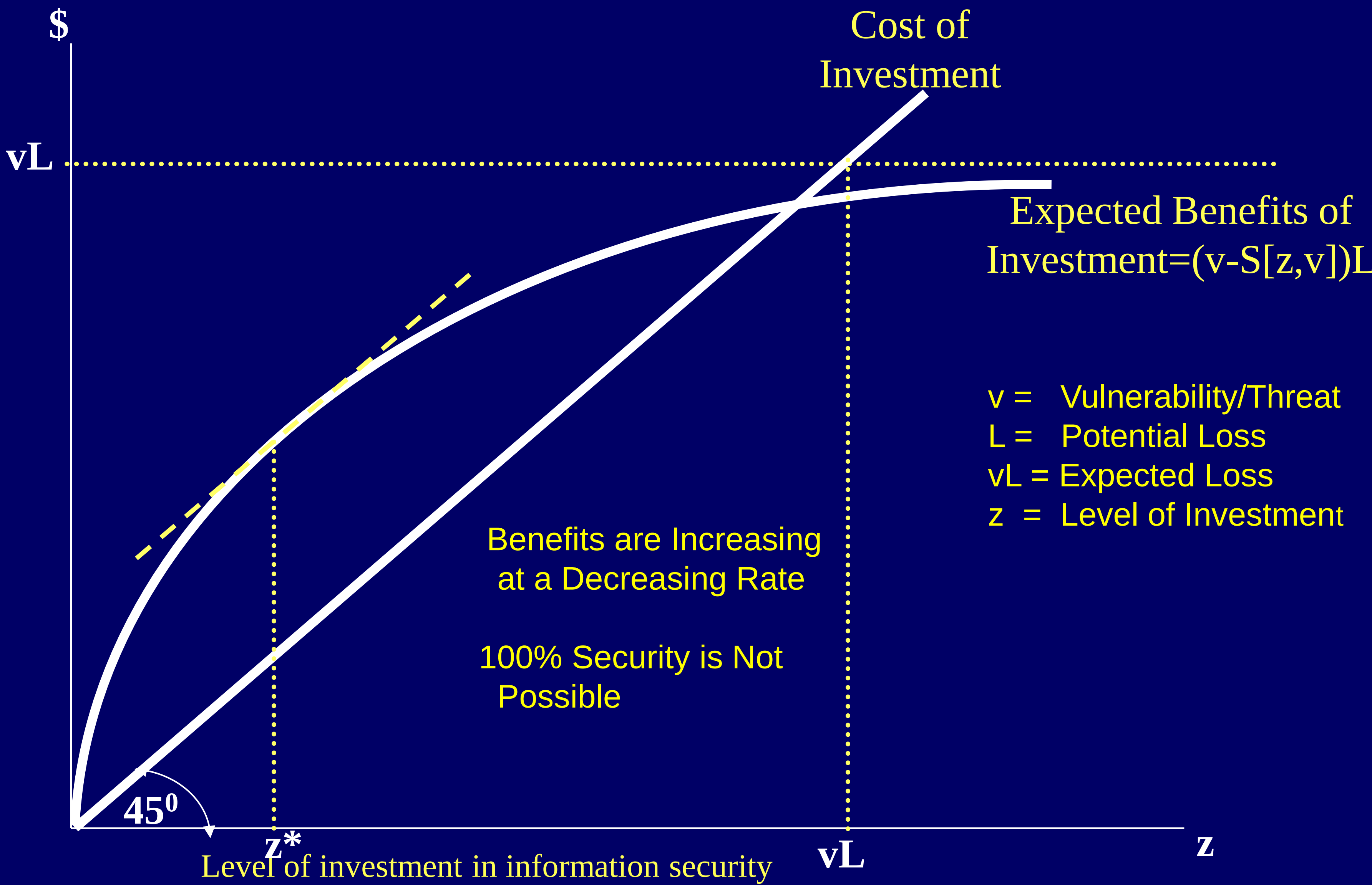
Why Are Cybersecurity Investments So Difficult to Justify?

- 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

Figure 1: Benefits and Cost of an Investment in Cyber/Information Security*



*Adapted from Gordon and Loeb, 2002a (see Appendix B).

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

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!

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

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)*

Columns grouped: Low (10–30), Medium (40–70), High (80–100)

Rows grouped (Vulnerability/Threat**): Low (10%–30%), Medium (40%–70%), High (80%–100%)

	10	20	30	40	50	60	70	80	90	100
10%	1	2	3	4	5	6	7	8	9	10
20%	2	4	6	8	10	12	14	16	18	20
30%	3	6	9	12	15	18	21	24	27	30
40%	4	8	12	16	20	24	28	32	36	40
50%	5	10	15	20	25	30	35	40	45	50
60%	6	12	18	24	30	36	42	48	54	60
70%	7	14	21	28	35	42	49	56	63	70
80%	8	16	24	32	40	48	56	64	72	80
90%	9	18	27	36	45	54	63	72	81	90
100%	10	20	30	40	50	60	70	80	90	100

*Value of Information = Potential Loss (L)
** Vulnerability/Threat = v

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

PRODUCTIVITY OF INVESTMENTS IN CYBERSECURITY

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

Low Prodcutivity = $v/(1+z)$ for Low Vulnerability/Threat
Medium Productivity = $v/(1+z)^2$ for Medium Vulnerability/Threat
High Productivity = $v/(1+z)^3$ for High Vulnerability/Threat

University of Maryland Robert H. Smith School of Business

Figure 7: Investment Amounts

Value of Information Sets (in $M): Low (10–30), Medium (40–70), High (80–100)

Vulnerability Threat: Low (10%–30%), Medium (40%–70%), High (80%–100%)

Vulnerability Threat		10	20	30	40	50	60	70	80	90	100
Low	10%	<1M	1M	<2M	<2M	<2M	2M	<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
Medium	40%	<2M	<3M	<3M	<3M	<3M	<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
High	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	<4M

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

Concluding Comments

I. Cybersecurity Investments Are Hard To Justify

They are Cost Savings, Not Revennue 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 ≤ 37% of Expected Loss
Wait-n-See Approach is Rational from Economics Perspective
Key Investment Factors: Potential Loss,
Vulnerabilites/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

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SELECTED REFERENCES

Gordon, L.A. and M.P. Loeb. 2011,"You May Be Fighting the Wrong Security Battles: How IT executives can determine the right amount to spend—and where to spend it," *The Wall Street Journal*, September 26, 2011.

Gordon, L.A. and M.P. Loeb. 2006. MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis (McGraw-Hill).

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

Gordon, L.A., M.P. Loeb. 2006. "Economic Aspects of Information Security: An Emerging Field of Research," *Information System Frontiers.*

Gordon, L.A. and M.P. Loeb. 2002a. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security.**

Gordon, L.A. and M.P. Loeb. 2002b. "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance.*

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.*

Gordon, L.A., M.P. Loeb, and W. Lucyshyn. 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal.*

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

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou. 2015. "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," *Journal of Information Security*.

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

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

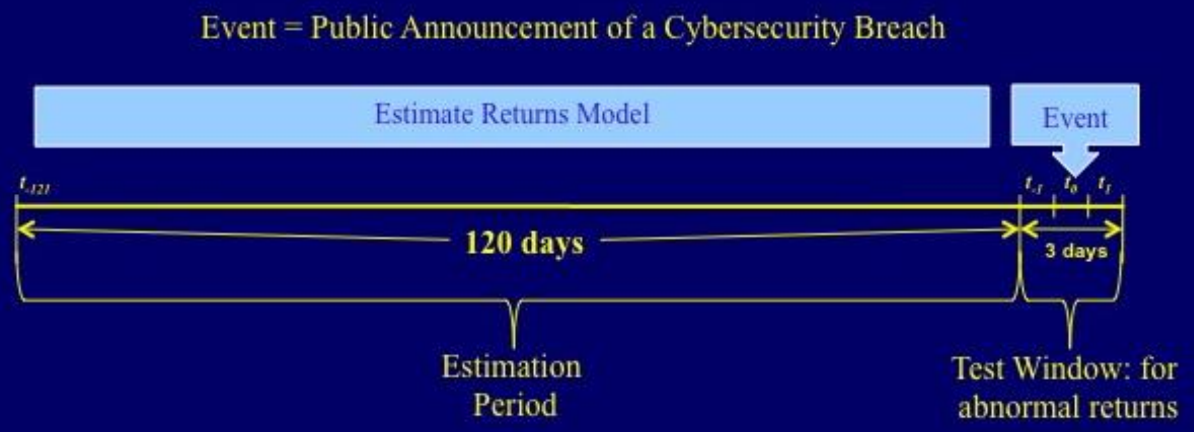
Gordon, L.A., M.P. Loeb, T. Sohail. C-Y Tseng and L. Zhou. 2008. "Cybersecurity Capital Allocation and Management Control Systems," *European Accounting Review.*

Gordon, L.A., M.P. Loeb, and L. Zhou. 2011. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security.*

Lelarge, M. 2012. "Coordination in network security games: A monotone comparative statics approach. Selected Areas in Communications, *IEEE Journal on Selected Areas in Communications* .

*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: $CAR_i = \sum_{t=t_1}^{t_2} AR_{it},$

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 call the firm's *beta*)

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

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.

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

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]) :

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

*Adapted from Gordon and Loeb, 2002a.