ECONOMIC ASPECTS OF CYBERSECURITY

Objective:
Provide an overview of stream of research by Gordon and Loeb on the economics of cybersecurity.

Martin P. Loeb
Professor of Accounting & Information Assurance, and Deloitte Faculty Fellow

The Robert H. Smith School of Business
University of Maryland
Affiliate Professor in UMIACS
Researcher in Maryland Cybersecurity Center

June 10, 2014

ECONOMIC ASPECTS OF INFORMATION SECURITY
(Research Agenda by Gordon, Loeb and others at the RH Smith School, UMD)

A. What is the impact of cybersecurity breaches on corporations?
B. How much should a firm invest in cybersecurity (and how should those funds be allocated) ?
****
C. Information sharing
D. Economic incentives for cybersecurity investments in the private sector
E. Disclosure of cybersecurity activities on 10K reports filed with the SEC
F. Cybersecurity insurance
G. Information security audits

A. What is the impact of cybersecurity breaches on corporations?

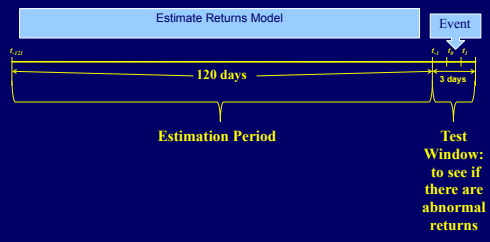
Cybersecurity Breaches are a Key Concern to Private and Public Sector Organizations

Economic Costs of Cybersecurity Breaches

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

A: Research Methodology (Event Study)

Event = Public Announcement of a Cybersecruity Breach



A: Research Methodology

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*)

A: What is the impact of cybersecurity breaches on corporations? Results of our stock market returns studies

Large percentage of breaches do not have significant impact on stock market return 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

B. How much to invest in cybersecurity?

Characteristics of cybersecurity investments:

–Cybersecurity investments are cost savings projects as opposed to a revenue generating project

–Benefits impossible to measure precisely: one would need to know what losses would have been without the cybersecurity investment

–Externalities: a firm's cyber investments affects the cybersecurity of other firms, and vice versa

–Game theoretic aspects: attackers and defenders

Optimal amount to invest (Gordon-Loeb Model)

- Vulnerabilities
- Productivity of investments
- Potential loss

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.

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

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:

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

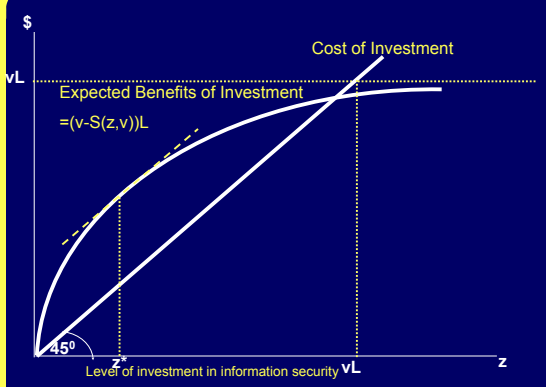
Maximizing [2] is equivalent to minimizing:

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

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

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

Benefits and Cost of an Investment in Information Security



B: Results of Gordon-Loeb Model*

- 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

*Model has been generalized by mathematicians in papers by Lelarge and a paper by Barishnikov

Gordon-Loeb model has been featured in the *Wall Street Journal* and the *Financial Times*

THE WALL STREET JOURNAL.

Monday, September 26, 2011

Home · World · U.S. · New York · Business · Tech · Markets · Market Data · Opinion · Life & Culture · Real Estate

Digits · Personal Technology · What They Know · All Things Digital · CIO Journal

TOP STORIES IN WSJ

1 of 12 — Mort Zuckerman: A Jobless Recovery Is a Phony Recovery

2 of 12 — Holder Criticizes Stand-Your-Ground Laws

3 of 12 — Google Pitches Online TV Service

September 26, 2011, 4:03 p.m. ET

You May Be Fighting the Wrong Security Battles

How IT executives can determine the right amount to spend—and where to spend it

Article · Comments (0)

Email · Print · Save

By LAWRENCE A. GORDON AND MARTIN P. LOEB

More in Leadership in Information Security

- What to Do if You've Been Hacked
- The Dangers of Remote Access
- Heading Off Privacy Problems—Before They Arise
- The Government's Cybersecurity Model Is in Demand
- Security Experts Pick the Best Hacker Movies
- Read the complete report .

A recent wave of information-security breaches at high-profile companies has many executives on heightened alert. They're trying to figure out everything they can do to prevent breaches, limit the damage if one occurs, and be prepared to rebound quickly from whatever harm is done.

As they consider their options, two questions loom large: How much should they spend to protect their companies' information? And how can they get the most for their money?

Our research suggests they should spend substantially less than the expected loss from a breach, and perhaps spend it differently than many might think.

The One-Third Mark

We developed a model to help executives determine the optimal level of investment to protect a given set of

PLUG INTO AN AUDIOBOOK ON YOUR NEXT BUSINESS TRIP

RANDOM HOUSE AUDIO

THE NEW PORTFOLI… THE ULTIMATE INV… AVAILABLE EXCLUSIV…

Don't Miss

FINANCIAL TIMES

ft.com > management >

Business Education

Home · World · Companies · Markets · Global Economy · Lex

Business Education ▾ · Entrepreneurship ▾ · Business Books ▾ · Business Travel · Recruitment · The Co

May 20, 2013 4:17 pm

Maryland professors weigh up cyber risks

By Adam Palin

How much should companies spend on bolstering their cyber defences? Lawrence Gordon and Martin Loeb, both professors of accounting at the University of Maryland's Smith School, are co-authors of an established model that helps companies to evaluate the best way to allocate their financial resources.

Concluding Comments

1. Many cybersecurity breaches do not have a significant impact on firms, but some can threaten the survival of a firm.
2. Under a wide range of circumstances, do not invest more than 37% of expected loss.
3. Cybersecurity solutions should be viewed in the context of economic decision-making.

SELECTED REFERENCES

Baryshnikov, Y. 2012. IT security investment and Gordon-Loeb's 1/e rule. 2012 Workshop on Economics and Information Security, Berlin, available at http://weis2012.econinfosec.org/papers

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

Campbell, K., L.A. Gordon, M.P. Loeb and L. Zhou. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11, No.3, pp. 431-448.

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

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

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

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

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

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*, Vol. 22, No. 6, pp. 461-485,

Gordon, L.A., M.P. Loeb, and W. Lucyshyn. 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal* , Vol. 19, No. 2, pp. 1-7.

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

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

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

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*, Vol. 17, No. 2, pp. 215-241.

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*, 19(1), 33-56.

Lelarge, M. 2012. "Coordination in network security games: A monotone comparative statics approach. Selected Areas in Communications, *IEE Journal* on 30(11), 2210 – 2219.