Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

Homeland Security
Science and Technology

Cyber Security Division
2012 Principal Investigators' Meeting
TTA: Cyber Economics

PI - Dr. Lawrence A. Gordon* (lgordon@rhsmith.umd.edu), (301) 405 - 4072
Co-PI Dr. Martin P. Loeb* (mloeb@rhsmith.umd.edu), (301) 405 - 4072
Co-PI Mr. William Lucyshyn (lucyshyn@umd.edu), (301) 405 - 8257**

***Smith School of Business, Accounting and Information Assurance Department, University of Maryland**
****School of Public Policy, Center for Public Policy and Private Enterprise, University of Maryland**

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

- Primary Objective: to understand more fully the challenges associated with making cybersecurity investments in the private sector and to recommend policies for facilitating the appropriate level of such investments (emphasis will be given to firms that own and/or operate assets critical to the national infrastructure).

- In pursuing this objective, we begin by developing a conceptual framework for making cybersecurity investments. In other words, since cybersecurity investments compete with other investment opportunities available to firms, they need to be justified by showing that the benefits exceed the costs, in terms of NPV.

$$PV = -C_0 + \sum_{t=1}^{n} \frac{\mathrm{B}_t - \mathrm{C}_t}{(1+k)^t}$$

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

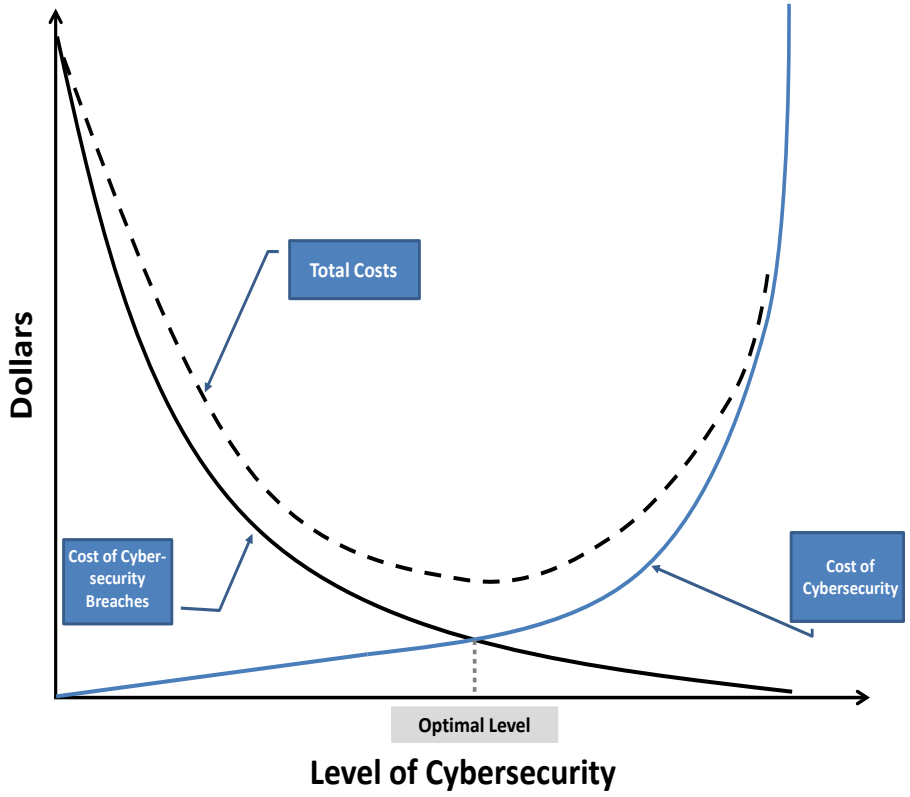
Homeland Security
Science and Technology

Technical Approach:

- **Examine Existing Literature**
- **Develop Model(s) for Investing in Cybersecurity**
- **Conduct In-Depth Interviews with CFOs & CIOs from major firms**
- **Conduct Survey and Analyze Data**
- **Develop Recommendations for Policies and Procedures that Incentivize Appropriate Level of Private Sector Cybersecurity Investment**

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

The Business Case for Cybersecurity Investments



Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

Conceptual View of Costs of Security Breaches

	Direct Costs	Indirect Costs
Explicit Costs		
Implicit Costs		

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

- *H1: The uncertainties associated with measuring the benefits from cybersecurity have created a situation such that it is more difficult for managers to get funds for cybersecurity investments than for investments related to traditional revenue generating projects*.

- *H2: The risk associated with cybersecurity investments is poorly understood by most individuals involved in making cybersecurity investments.*

- *H3: Due to externalities, when firms only consider private profits they tend to under-invest in cybersecurity*.

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

Homeland Security
Science and Technology

Research Design

1. Provide Conceptual Framework for Making Cybersecurity Investments

$$Z_1 = \text{argmin } [P(z)L + z]$$

$$Z_2 = \text{argmin } [P(z)L + z + CS(z)]$$

2. Conduct 4-6 in-depth case studies of the cybersecurity investment activities of organizations operating in critical infrastructure industries, based on interviews with the CFOs and CSOs. The case studies will be viewed as a series of mini-experiments.

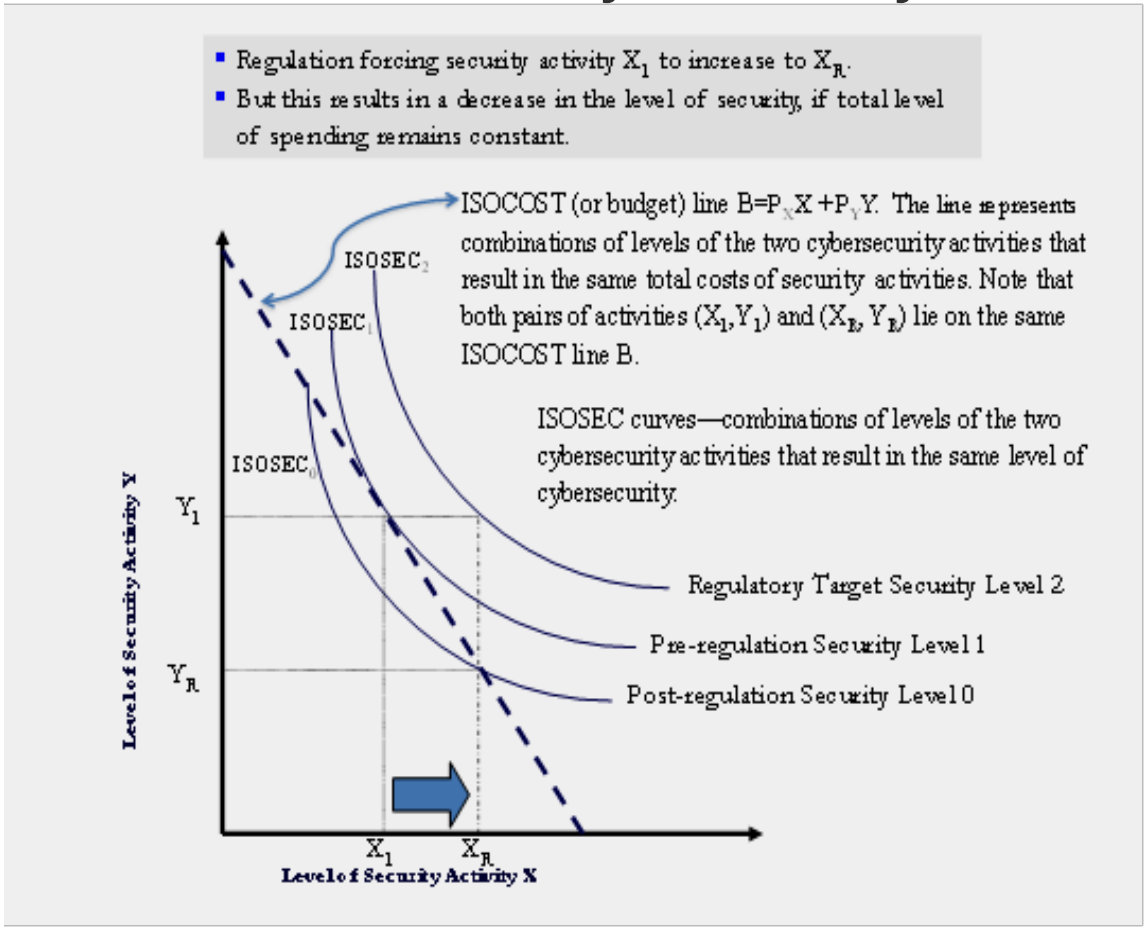
3. Design questionnaire for conducting a large empirical survey. The data collected from the survey will be used to statistically test the hypotheses underlying the study. The questionnaire will be sent to the CFOs and CSOs of approximately 300 major organizations from a variety of critical structure industries.

4. Analyze survey data via statistical and econometric procedures.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \sum_{i=1}^{n} \alpha_i C_i$$

Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

Inappropriate regulatory strategies can cause firms to reduce their overall levels of cybersecurity



Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

Homeland Security
Science and Technology

Deliverables

- **Monthly Progress Reports**
- **Interim Report after the first 12 months.**
- **Final Report after the 24 months that will summarize the entire research project, including: (a) survey of private sector firms, (b) case studies, (c) cyber security investment models, and (d) policy recommendations.**
- **Preparation of Articles for submission to major Research Journals**
- **Presentations at Academic and Professional Conferences**

Application of research

- Inform the formulation of policies and regulations aimed at incentivizing an appropriate level of investment in cybersecurity measures by the private sector

- Assist firms as they analyze their cybersecurity requirements, and work to determine the appropriate level of investment

Selected References

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.

Gansler, J. S. and W. Lucyshyn, "Improving the Security of Financial Management Systems: What Are We to Do?" *Journal of Accounting and Public Policy*, Vol. 24, No.1, pp. 1-9.

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, 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," *Computer 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," *Communications 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.