CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Cyber Economics

University of Maryland

September 17, 2013

Homeland Security

Science and Technology

Team Profile

- **Dr. Lawrence A. Gordon, R.H. Smith School of Business, University of Maryland, PI**
- **Dr. Martin P. Loeb, R.H. Smith School of Business, University of Maryland, Co-PI**
- **Mr. William Lucyshyn, Maryland School of Public Policy, University of Maryland, Co-PI**
- **Dr. Lei Zhou, R.H. Smith School of Business, University of Maryland, Research Associate**

Customer Need

- **Increasing threats from criminals, hackers, nation states**
  - **Estimates of global losses to firms from cyber crime and espionage range between $300B and $1T.**
- **WSJ notes that global spending for the protection of critical infrastructure cybersecurity threats will rise to $46 billion in 2013, a $4.25 billion increase over 2012.**
- **Need to develop an economic framework (model) to evaluate the appropriate level of cybersecurity investments in critical infrastructure that considers the total costs (i.e., private costs and externalities) from cybersecurity breaches.**
- **Need to develop models to analyze impact of regulations/incentives on level of cybersecurity investments.**
- **Need to determine the most appropriate way to allocate cybersecurity investments.**

Approach: Step 1
Develop Conceptual Model

- **We began by developing a conceptual model/framework for considering the optimal level of cybersecurity investments that includes *externalities,* as well as *private costs* (based on the Gordon-Loeb Model*).**
  - ***Private costs* = costs to individual firms experiencing cybersecurity breaches.**
  - ***Externalities* = spill-over costs to other and the general public.**
  - ***Private costs + Externalities = Social Costs***

*Lawrence A. Gordon and Martin P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol.5, no 4 (2002), pp. 438 – 457.

Approach: Results of Step 1

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

Base Model: Considers only the firm's private costs

Basic Model: $z_1 = argmin[S(z,v)L_P + z]$

GL Result: $z_1 \leq \frac{1}{e} v L_P$

Extended Model: Considers private costs plus externalities

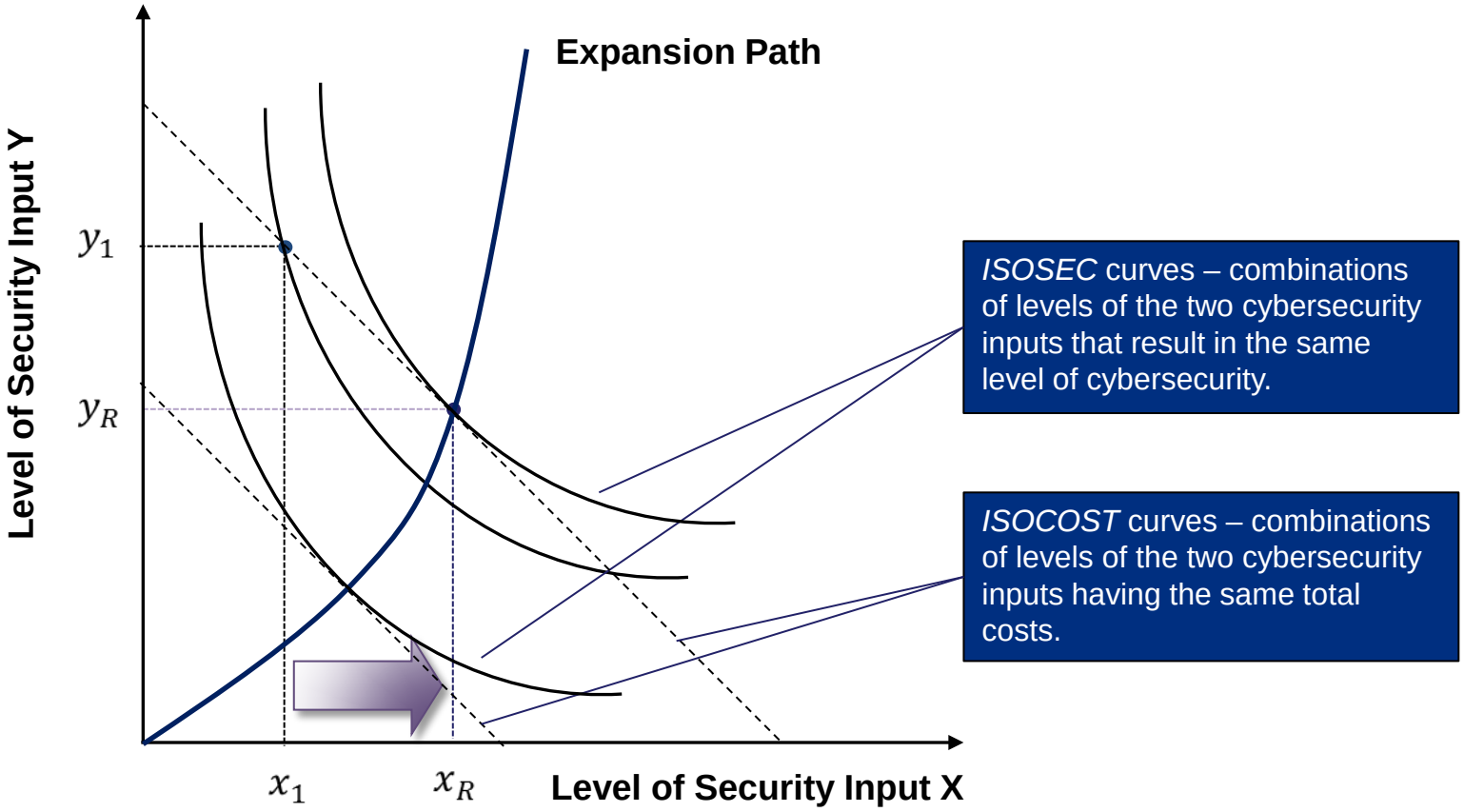
Extended Model: $z_2 = argmin[S(z,v)(L_P + L_E) + z]$

GL Extension Result: $z_2 \leq \left(1 + \frac{L_E}{L_P}\right)\frac{1}{e} v L_P$

Implications of Extended Model: Optimal cybersecurity investment level is clearly higher when total social costs, which include externalities, are considered than when only private costs are considered by a factor of $\frac{L_E}{L_P}$.

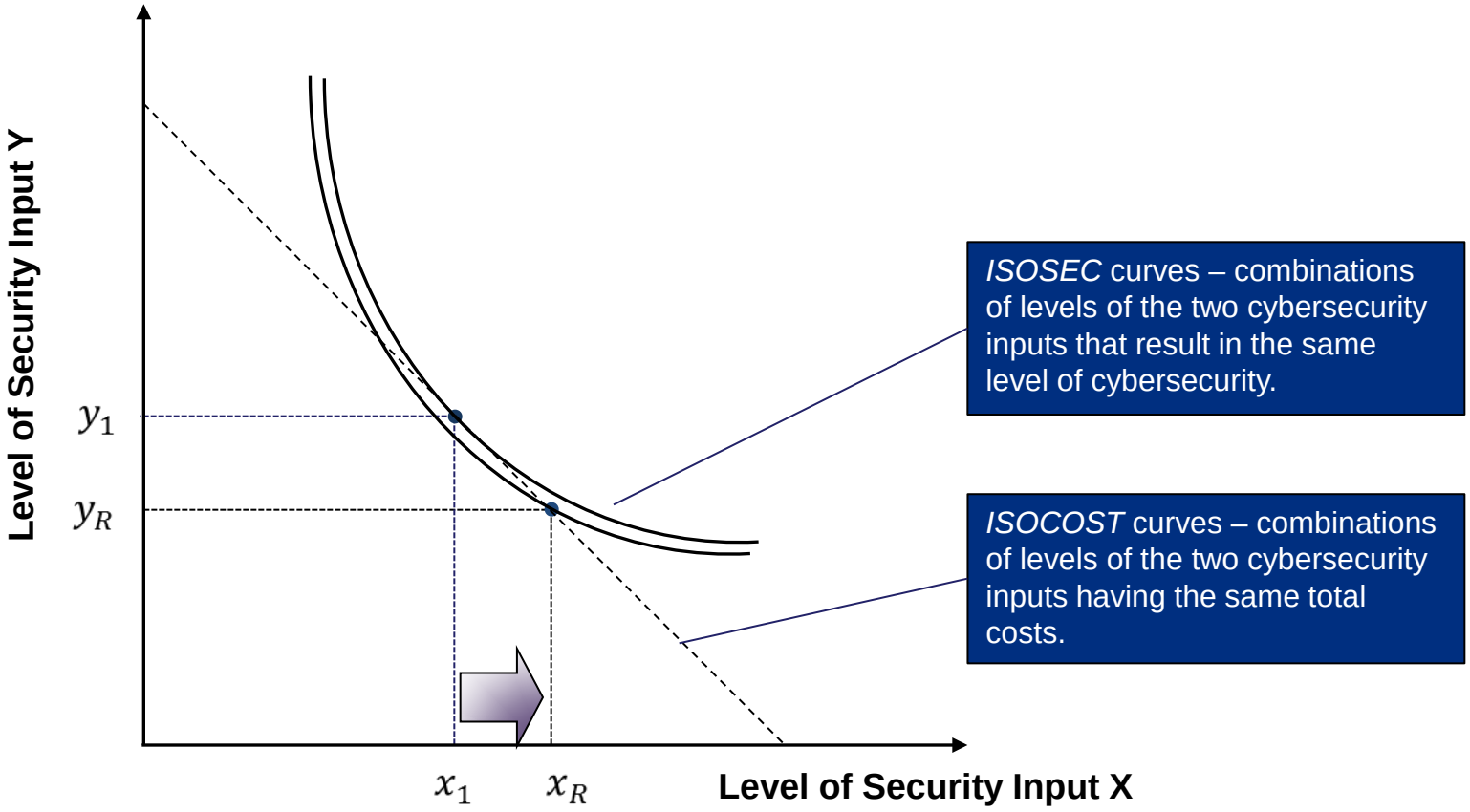
Approach: Step 2
Input-Output Analysis

Moving to expansion path increases level of cybersecurity without additional cost



Approach: Step 2 Continued

Hypothesis: Regulating inputs may cause firms to reduce or increase their overall levels of cybersecurity



ISOSEC curves – combinations of levels of the two cybersecurity inputs that result in the same level of cybersecurity.

ISOCOST curves – combinations of levels of the two cybersecurity inputs having the same total costs.

Approach: Results of Step 2

- **If firms cannot determine the optimal mix of inputs, then government regulations/incentives could cause a reallocation of resources that improve cybersecurity even when cybersecurity expenditures are fixed.**
- **If firms can, and do, determine the optimal mix of inputs, then the only way that government regulations/incentives could increase cybersecurity level is by increasing cybersecurity expenditures by firms.**

Benefits

Improve cybersecurity investment practices in the private sector by:

- **Assisting firms analyze their cybersecurity investment requirements, taking into consideration the benefits, costs, and risks associated with such investments.**
- **Develop methodologies to increase the efficiency of allocating resources to cybersecurity investments.**
- **Assisting in the formulation of policies, regulations, and incentives aimed at ensuring an appropriate level of cybersecurity investments, and the efficient allocation of resources to such investments, by firms in the private sector.**

Current Status

- **Models**
  - **We developed a model to evaluate the appropriate level of cybersecurity investment for a firm that considers the externalities, as well as private costs.**
  - **We developed models to analyze impact of regulations/incentives on level of cybersecurity investments.**
  - **We prepared initial draft of paper that incorporates the above noted models.**
- **Case Studies**
  - **We developed the methodology and interview questions for our case studies.**
- **Survey**
  - **We have an initial draft of the survey instrument.**

Next Steps

- **Conduct case studies of the cybersecurity investment activities of a few organizations operating in critical infrastructure industries.**
- **Conduct a large empirical survey.**
- **Analyze survey data via statistical and econometric procedures.**
- **Our Hypotheses underlying case studies and survey:**
  1. **It is more difficult for managers to get funds for cybersecurity investments than for traditional revenue generating projects.**
  2. **The risk associated with cybersecurity investments is poorly understood by most individuals making those investments.**

Next Steps – Transition Activities

1. Present study results at various conferences, universities, corporations and government agencies.
2. Publish articles on study results in publicly available journals.
3. Meet with firms to discuss ways of improving their economic analyses of cybersecurity investments
   - That is, initiate a test bed for assisting firms in making appropriate level of cybersecurity investments.
4. Organize Cybersecurity Forum at UMD in January 2014.
5. Cover results of study in various UMD courses, including:
   - The Honors College's new Cybersecurity program (called ACES).
   - Smith Business School's MBA Accounting and Information Assurance Courses.

Contact Information

Dr. Lawrence A. Gordon
EY Alumni Professor of Managerial Accounting and Information Assurance
University of Maryland
Robert H. Smith School of Business
College Park, Maryland 20742
E-mail: lgordon@rhsmith.umd.edu
Phone: 301- 405- 4072 (Adm. Coordinator, Ms. Diane Hall)