Research Report No. 5, January 2006

I3P Economics Project Workshop Report

Report on the results of an I3P workshop that took place on December 8, 2005 at the Institute for Critical Infrastructure Protection at George Mason University.

Barry Horowitz, University of Virginia

January 11, 2006

This work was supported under grant number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Secuirty or the Science and Technology. The I3P is managed by Dartmouth College.

I3P Workshop Report

1. Introduction

This paper is a report on the results of an I3P workshop that took place on December 8th, 2005 at the Institute for Critical Infrastructure Protection at George Mason University. The purpose of the workshop was to expose participants to work in decision making with respect to intellectual property security risks. The following people participated in the workshop; 7 software company security managers, 10 non-profit security analysis managers, 5 representatives from government agencies, and 8 members of academic institutions. It included a 1 hour presentation on the risks of intellectual property attacks. The presentation is included in the appendix. The next aspect of the workshop was a decision making game wherein players chose between two investment alternatives, revenue enhancement or cyber security enhancement. 23 workshop participants played the game. The rules of the game are shown below in the identical form presented to workshop and game participants. We would like to emphasize that the game was not a controlled experiment. Nonetheless, it provided an opportunity to receive input and feedback from a large number of experienced professionals in an organized setting.

Computer Security Game Instructions

- The purpose of this computer game is to **compare and evaluate cyber security investment decisions made by managers with decisions derived through the application of decision analysis**. The results will be used as part of the design process of a **more general decision support tool for managers**.

The game provides a group of **decision-makers from 20 competing companies** with a set of parameters that surround their cyber security investment decisions related to **the protection of Intellectual Property (IP) theft**. The companies for which the decisions are being made are US-based, each have annual revenue of $2bb, and they are all **expanding their automated supply chain support systems** with non-US based suppliers. Based on history it is generally accepted that with the normal levels of investment in security any individual company faces a likelihood of a successful attack occurring of about once during a 10 year period.

- The game runs for a simulated **5-year period with annual management decisions** and **corresponding annual financial simulation results** corresponding to the players' investments in cyber security.

- Each player (decision-maker), on an annual basis, has a choice between 2 alternative investments of the same dollar amount (five sequential decisions in all). The size of the investment is externally set and displayed at the start of the game (e.g., $2mm).
    - Alternative 1 – **Invest in enhanced cyber security to reduce the likelihood of IP theft.** The normal security budget for your company is $10mm per year. This added investment will reduce the likelihood of your company's IP being stolen. The financial consequences of successful IP theft reduce the revenue of the company for four years by an externally set amount of 2% per year (total of $160mm). The impact of the Alternative 1 investment is to extend the anticipated period for a successful attack by a factor of 2.5; i.e., from 10 years to 25 years)
    - Alternative 2 – **Invest in enhanced sales capability that results in an externally set level of revenue growth** for the next four years. (i.e., $2mm increase in the year of the investment that sustains itself for all of the remaining years in the game).
    - For the simulated year in question, all players decide on which investment alternative to select. A simulation is then run to determine the outcome of IP thefts for each player. The simulation determines the IP theft outcomes for each player's company by using the probabilities that are based on the cyber security investment decisions of the players. Security breaches are probabilistic, so that **those who do not select the cyber security investment alternative will not necessarily experience a breach**. Similarly, **those who invest in the cyber security alternative may experience a breach**. All that can be said is that **those who invest in the cyber security alternative are less likely to experience a breach**.

- After all the players make their decisions, **everyone sees all companies' financial outcomes** for the simulated year of decision-making. In addition, **all players see information about any IP theft** event that occurs during that year through press releases. **No player sees another player's decisions.**

- The decision-making process and corresponding simulations are **conducted 5 consecutive times representing 5 years of decision-making time.**

2. Game Organization

The implementation of the game occurred through the use of the Groove collaboration program and Microsoft Excel. The game was based on a probabilistic decision analysis model that compared expected financial outcomes for investments in cyber security versus other revenue creation opportunities for the same level of investment. The analysis results in a mathematical decision criterion. Appendix 1 presents the analysis. Players were not informed of the criteria, but instead are asked to make investment decisions on whatever basis they choose. The game consisted of three separate decision situations (treatments) each requiring annual decisions on investments for each of five years (each year considered to be a round). One of the treatments was used to calibrate the investment biases of the players. This is accomplished by selecting a set of decision parameters that make the two alternate decisions of security or sales enhancement equally attractive from a mathematical viewpoint and based on player actual decisions, determining what starting decision bias exists. The other two treatments were set up to orient players to different decision selections (i.e., one treatment mathematically favors a security investment strategy and the other a revenue enhancement strategy). Players arrived at their computer station where the game instructions for a particular treatment were already displayed for them. After reading the instructions players clicked a start button and proceeded to the next form to make their first round decision. The Groove tool allows for the creation of forms using a built in design tool, JavaScript, and html. After selecting one of the two alternative decisions, players would click the submit button and advance to a form that allowed the players to record their reasoning. While they completed this form the results were transferred to Excel where the results of the round were calculated. After the results were displayed for all players to see, they moved on to the next round's decision screen. The players would then submit this decision and would have a further form to record their reasoning for this round or they could check that the same reasoning applied as the previous round. Then the decisions would again be transferred to Excel for calculation and display. This process repeated itself for the next three rounds until a total of five rounds had been completed. At the end of the treatment a graph was shown displaying the number of players that invested in each of the alternatives in each round (Figure 1). A second graph was shown that indicated the number of players that had changed their decision once, twice, three, or four times (Figure 2). A final graph showed the integrated

revenue results for completed rounds to that point in the game (Figure 3). This same process was repeated for the other two treatments.

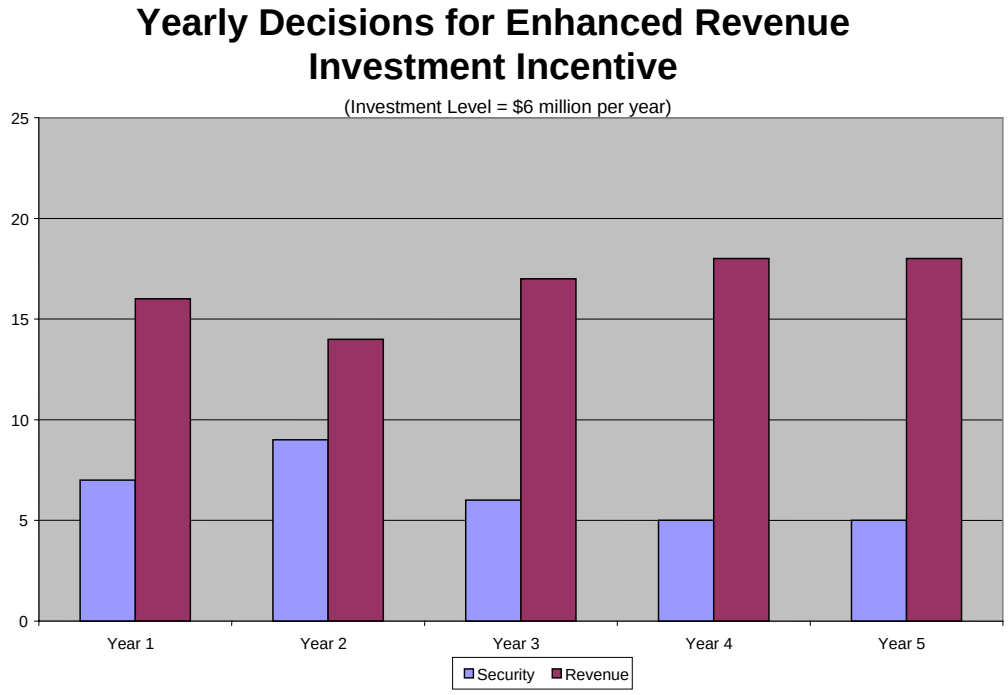


Figure 1

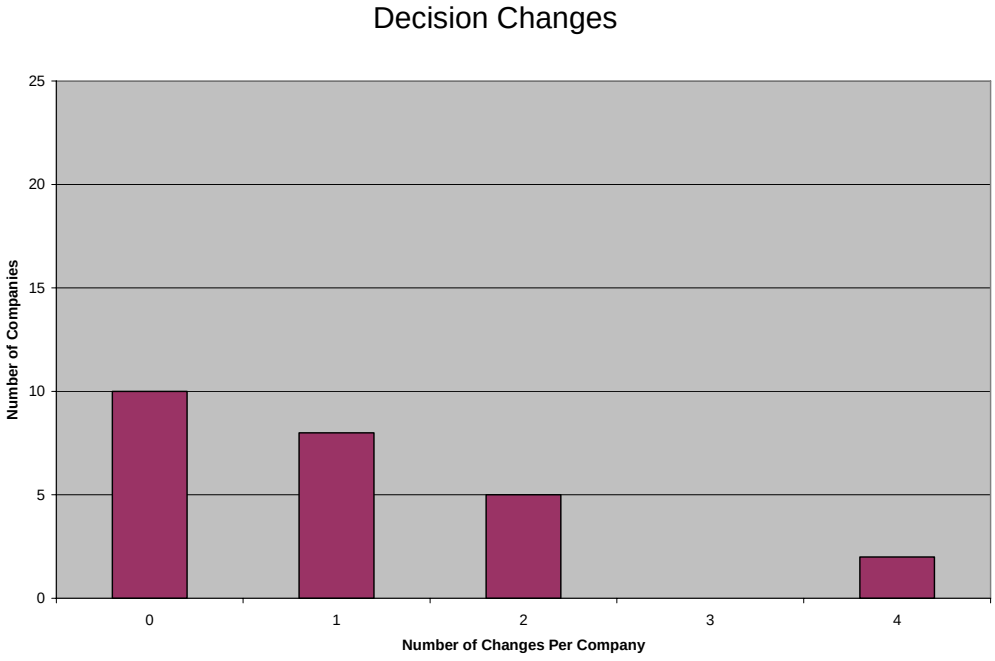


Figure 2

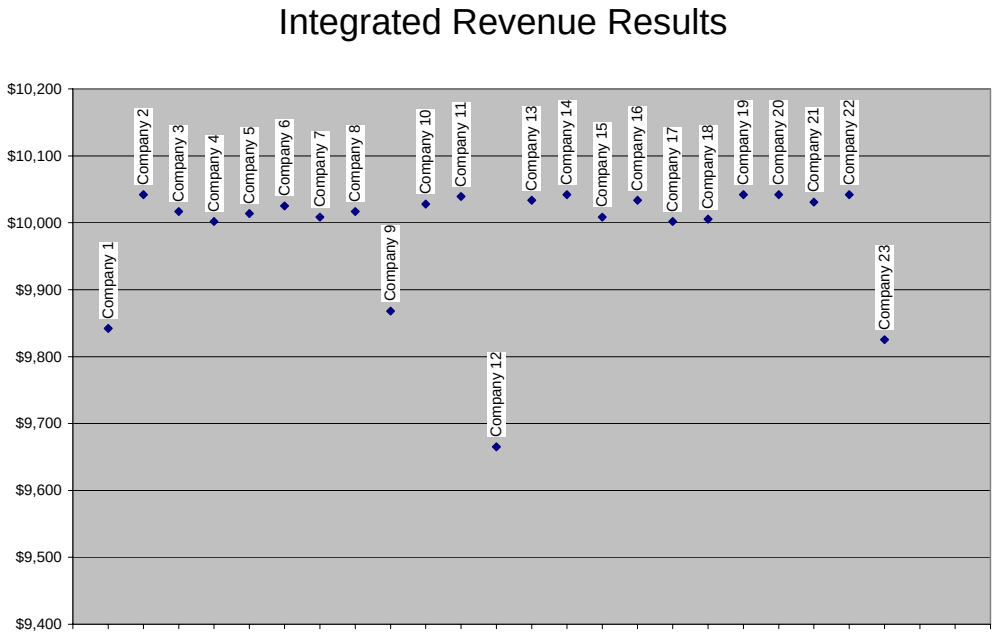

Integrated Revenue Results
$10,200
$10,100
$10,000
$9,900
$9,800
$9,700
$9,600
$9,500
$9,400
Company 1
Company 2
Company 3
Company 4
Company 5
Company 6
Company 7
Company 8
Company 9
Company 10
Company 11
Company 12
Company 13
Company 14
Company 15
Company 16
Company 17
Company 18
Company 19
Company 20
Company 21
Company 22
Company 23

Figure 3

3. Results

As indicated above, the workshop consisted of three treatments of the game. In one of the treatments the expected return on the revenue investment was the same as the expected return on the security investment. The result of this indifference treatment was a 3 to 1 bias towards investing in developing short term increases in company revenue rather than enhanced security (Figure 4).

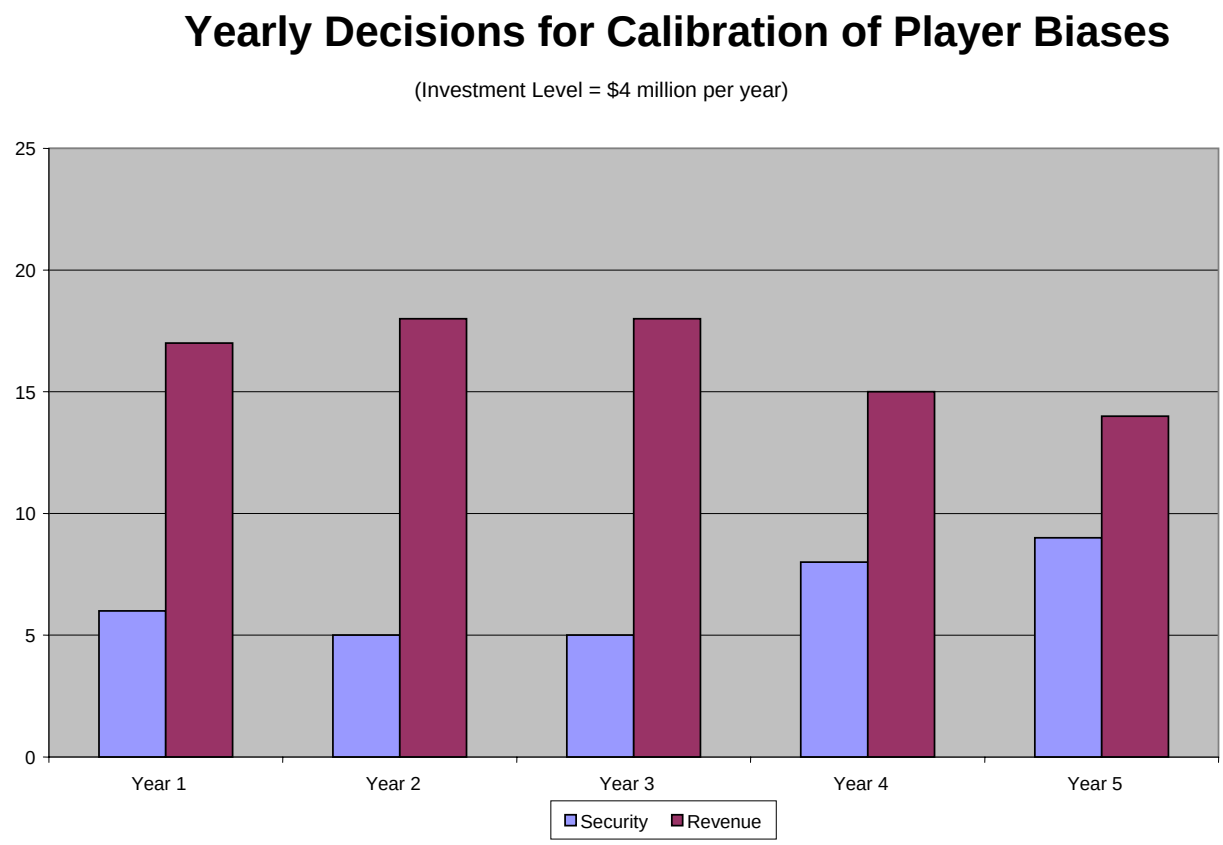


Figure 4

Another treatment was set with the expected value of the security investment higher than the expected return on the revenue investment. The instance of security investments doubled compared to the

indifference round (Figure 5).

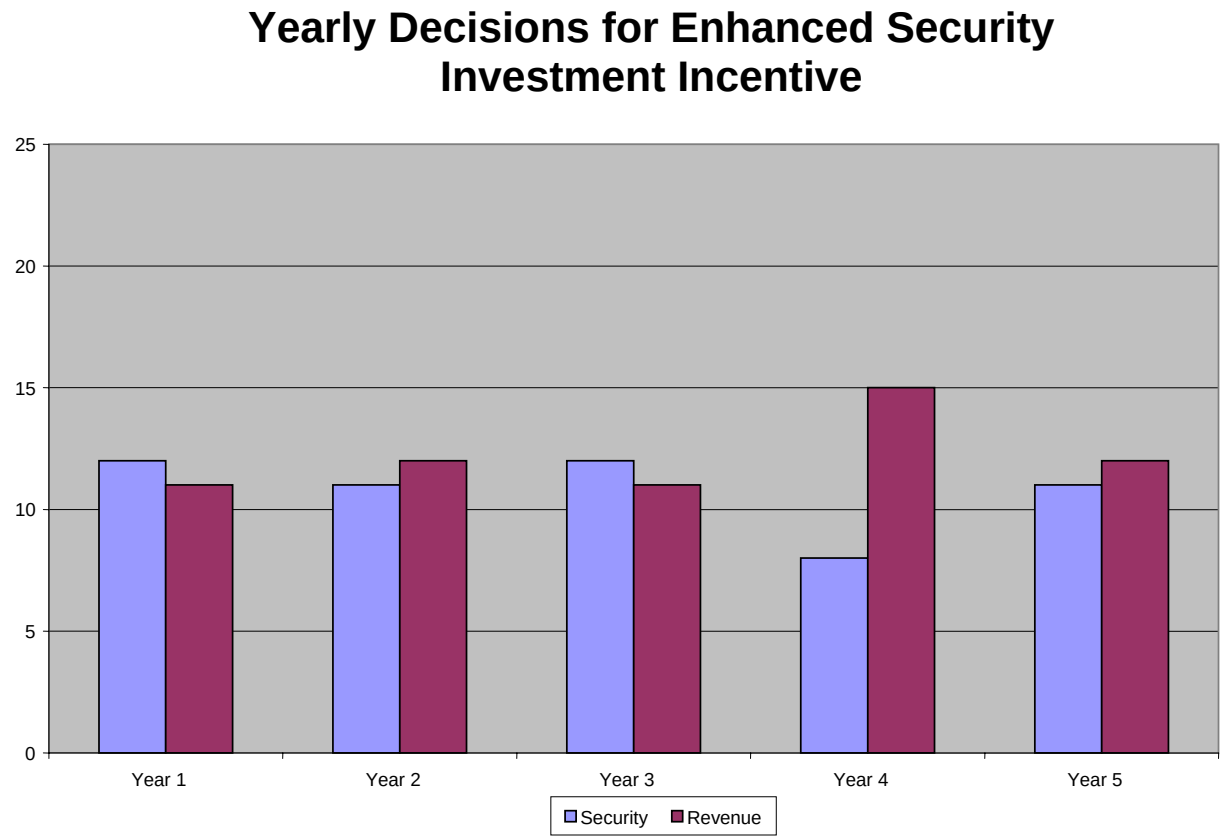


Figure 5

The other treatment was configured with the expected value of the revenue investment greater than the expected value of the security investment. The investment decisions for this treatment did not significantly differ from the indifference round (Figure 1).

The players in the game received a total of 25 successful cyber attacks for the 23 players through 15 rounds (years) of play (a total of 345 rounds and a successful security attack rate of about one in 14 years per company). Of those attacks 6 resulted in players changing their decisions from the revenue to security investment. Two of the attacks caused players to shift from the security to revenue investment based on a presumption that they were not likely to be successfully attacked more than once. The other 17 attacks did not result in players changing their decisions or occurred in one of the last rounds of a treatment.

4. Player Provided Reasons for Decisions

The provided reasons for investment decisions varied widely among the various players in the game. The reasons fall into two categories, revenue enhancement investment rationale and cyber security investment rational. The cyber security investment rationale includes the following reasons.

1) the expected value comparison between the two alternatives,

2) the perceived probability difference between the two alternative security decisions,

3) the concern for the potential loss of revenue from a successful attack,

4) the return on investment comparison between the two alternatives,

5) successful direct attacks or attacks on other players and

6) players wanted to protect their prior revenue gains in the five year window of a treatment

The provided reasons for revenue enhancement investments were:

1) willingness to take the cyber attack risk and invest in revenue enhancement,

2) the certainty of the revenue investment superseded the unlikely chance of a successful cyber attack,

3) the advantage of the way in which revenue gains accumulate over the five year treatment period,

4) the need to compete with other players in terms of advancing revenues, and

5) expected value of return on investment calculations.

5. Expected Value of Winner and Loser

We defined the "winner" as the player (company) that accumulated the most annual revenue over the integrated 15 year set of games. Correspondingly, we defined the "loser" as the player (company) that accumulated the least revenue over the integrated 15 year period. We recognize that this biases players towards investing in revenue, but judged that this mirrored the that companies face in the real world. After analyzing all results for the three treatments, it was determined that the "winner's" strategy was to invest in revenue for all rounds. Expected value of this strategy was $29,868mm; the winner received $30,108mm (Figure 6). The probability of maximizing revenue following this strategy is 20.6%. This is determined by computing the probability of no successful attacks in fifteen annual opportunities with a 10% likelihood of successful attack per year, assuming independent outcomes from year to year. (See Figure 7).

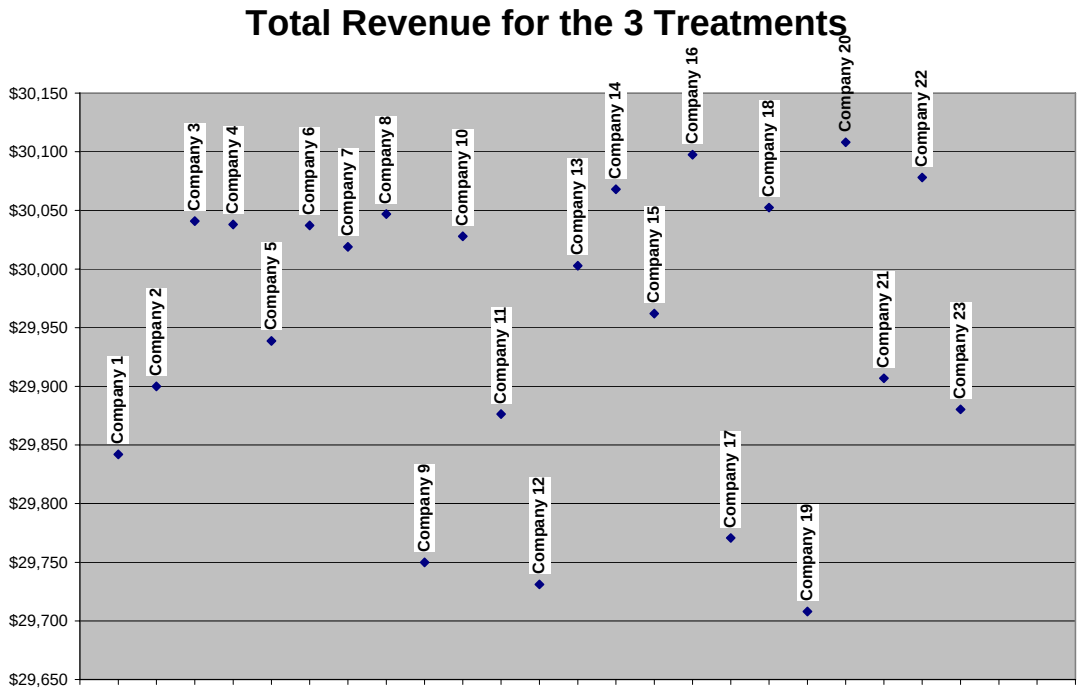


Figure 6

An analysis of game results interestingly showed that the "loser's" strategy was also to invest in revenue in each round. The resulting total for this player was $29,708mm. This player was hit three times during the

games and the probability that the player would have been attacked three times was 12.9% (Figure 7).

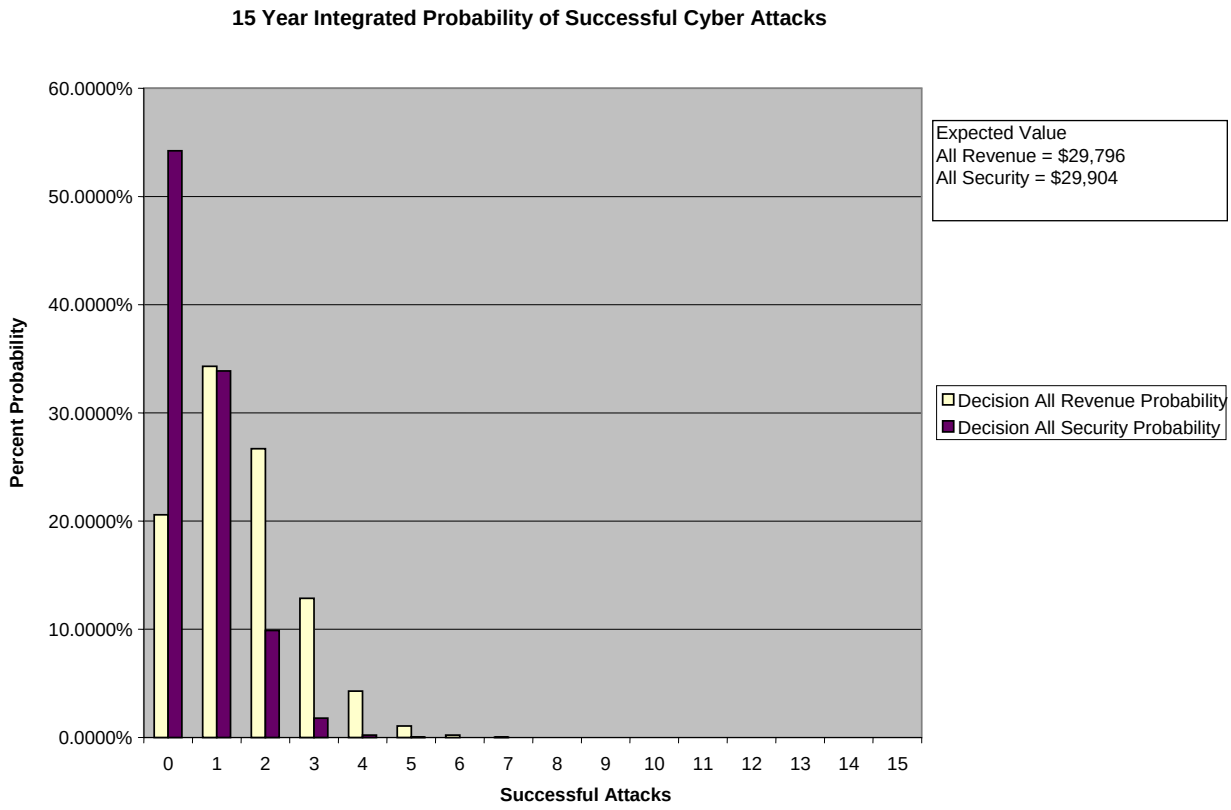


Figure 7

The probability of a player winning who followed a strategy of always investing in enhanced cyber security while every other player invested in enhanced revenue is only 0.34%.

6. Conclusions

Before discussing conclusions, it is important to emphasize that the workshop was not a controlled experiment from which statistically justified conclusions could be drawn. However, it was a unique opportunity to obtain inputs from seasoned people who regularly get involved in cyber security investment decision-making. The first conclusion that can be drawn from the results of the workshop is that players have **a bias towards investing in revenue**. We recognize that the real world aspects of the game biases players towards revenue enhancement, but this conclusion is especially interesting given that the workshop was organized for people expected to have a tendency to be interested in cyber security enhancement. A second conclusion is that **even in the face of the initial bias, players behaved rationally (acted in a consistent manner with the mathematical analysis results) when the expected value of the security investment exceeded the revenue investment.** In fact, the number choosing the security investment doubled. Finally, **the bias toward enhancing revenue opportunities did not rise with the scenario that favored a revenue investment.**

7. Discussion of Recommendations

The workshop resulted in many recommendations from the participants. Players reported great interest in the opportunity-cost oriented framework for decision analysis. For traceability in decision-making, players also liked the notion of assumption-driven decision making, even when the assumptions are "best guesses". Players asserted that adding cost side details with regards to particular solution options and costs should be incorporated into the game. Participants also suggested adding conditional probabilities about attack likelihoods based on competitor decision-making. Another suggestion was to add emphasis to security expertise being integrated with business expertise to achieve decisions through a decision support tool. Finally, there were suggestions to eventually account for all of the kinds of cyber risks in one game.

7. Appendix 1

Derivation of Decision Criterion

$\alpha =$ Probability of Successful Defense with ADDED Investment

$\beta =$ Probability of Successful defense with NO ADDED Investment

S = Added Security Investment under Consideration (Also Alternative Sales Investment)

O = 4 Year Return on Sales Sacrificed with Security Investment

V = 4 Year Market that will be lost if successfully attacked

X = 4 year Market that is not at risk

$$\alpha * (X + V) + (1 - \alpha) * X - (S + O) \geq \beta * (X + V) + (1 - \beta) * X$$

$$\alpha * X + \alpha * V + X - \alpha * X - (S + O) \geq \beta * X + \beta * V + X - \beta * X$$

$$\alpha * V + X - (S + O) \geq \beta * V + X$$

$$\alpha * V - (S + O) \geq \beta * V$$

$$\alpha * V \geq \beta * V + (S + O)$$

$$\alpha \geq \beta + \frac{(S + O)}{V}$$

$$\frac{\alpha}{\beta} \geq 1 + \frac{(S + O)}{\beta * V}$$

$$1 + \frac{(S + O)}{\beta * V} \leq \frac{\alpha}{\beta}$$

$$(S + O) \leq (\frac{\alpha}{\beta} - 1) * \beta * V$$

$$S \leq \left[(\frac{\alpha}{\beta} - 1) * \beta * V \right] - O$$

8. Appendix 2

Economics of Cyber Security

Barry M. Horowitz
I3P Research Team
University of Virginia
December 8, 2005

UVa Team

Faculty: Alfredo Garcia
Barry Horowitz
Students: Eva Andrujcic
Jonathan Crawford
Francis Teo

Macro-Economics of Cyber Security

- Objective: To develop analytical models, supported with reliable financial data, to better understand the financial risks and risk management responses related to cyber attacks.
- Prospective 2 Year Activity Initiated in May,2005
- To-date – Models and results for
  - Phishing Attacks
  - Attacks that bring down substantial parts of Internet
  - Intellectual Property (IP) cyber theft

Macro-Economics of Cyber Security

- Objective: To develop analytical models, supported with reliable financial data, to better understand the financial risks and risk management responses related to cyber attacks.
- Prospective 2 year Activity Initiated in May,2005
- To-date – Models and results for
  - Phishing Attacks
  - Attacks that bring down substantial parts of Internet
  - Intellectual Property (IP) cyber theft
- Recently submitted 2 papers for publication review

Purposes of Workshop

- Introduce participants to what we are doing in order to get early feedback
- Run an experiment related to IP theft risk management to gain specific feedback for this part of the effort

UVa's Input-Output Inoperability Model
IIM

Background – Input-Output Analysis

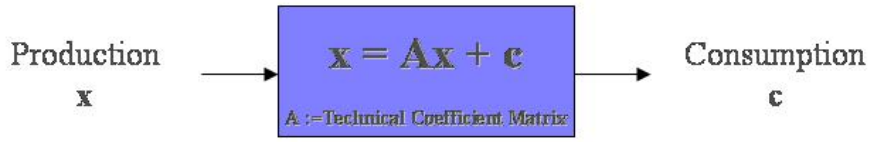
- First Input-Output table was developed in 1750s. (Le Tableau Economique)
- Wassily Leontief developed the Input-Output Model for the U.S. Economy, for which he won the Nobel prize in 1973.
- Leontief's model describes economic interdependencies.
- Many I-O analyses have been performed based on Leontiefs I-O structure
  - Energy
  - Environment
  - Regional water resources
- Many frontiers are being explored to enhance I-O modeling and assessment.

Inoperability Input-Output Model (IIM)

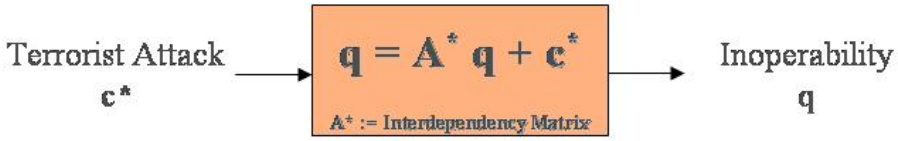
- General analytic framework to quantify and address risks from the intra- and interconnectedness of large-scale complex infrastructures [Haimes and Jiang 2001].
- Data from US Department of Commerce provide information on economic interdependencies (nearly 500 economic sectors).
- Computer-based model for analysis of how perturbations (e.g., demand shocks due to willful attacks, accidental events, or natural disasters) to selected groups of sectors can impose direct and indirect impacts on the operation of other sectors, due to inherent interdependencies [Santos and Haimes 2004].

Model Components

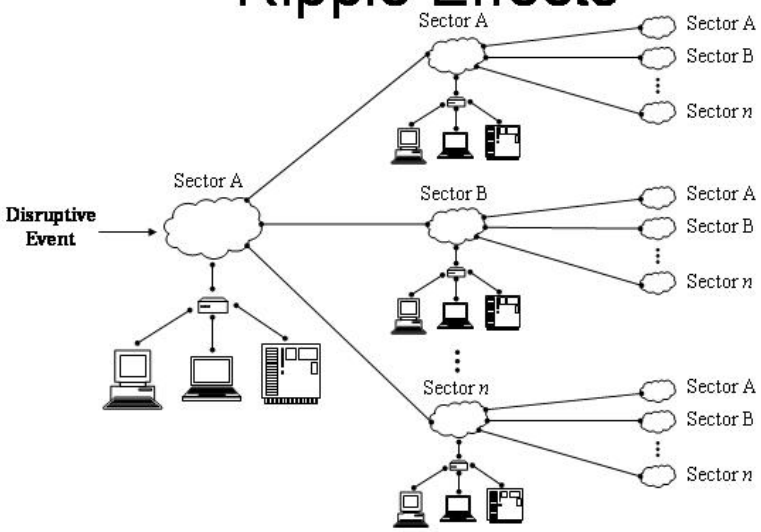
Leontief Model



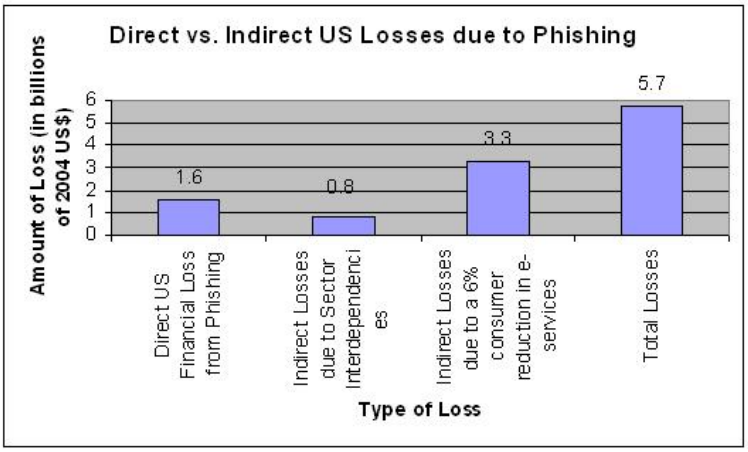
Inoperability I-O Model (IIM)



Ripple Effects



Direct vs. Indirect US Losses due to Phishing



Ratio of indirect to direct monetary losses due to phishing is 2.6!

Data sources – Tower Group, Denver Post, TRUSTe (Privacy), NACHA (Electronic Payments), Amazon, BEA, US Census Bureau

Internet Security

- ISP's as Internet Protectors - $50bb Industry
- E-biz/E-Com as at risk community – $1.3tt Industry
- Develop Nash Equilibrium Equations to determine logical investment strategy equilibrium points
  - With ISP's competing for market share
  - With E-biz players competing for market share with Brick and Mortar counterparts
- Derived decision variables – Probability of successful attacks vs level of investment, Cost of security, Market at risk due to attacks, opportunity cost for security investment, etc.
- Conclusions
  - Investment formulas
  - If Internet provides an economy of scale (i.e., the E-biz/ISP ratio keeps growing), then the amount that E-Biz would want to see invested in security will eventually outstrip the amount that ISP's will actually invest
  - Illustrative example shows that we already may be at the point of under investment

Cyber Theft of Intellectual Property

Risk Analysis Perspective*

- Risk
  - What can go wrong?
  - What are consequences?
  - What is likelihood?
- Risk Management
  - What are possible solutions?
  - What are costs/benefits
  - How do short term decisions impact long term options?

* Garrick, Kaplin, Haimes

Motivating Example

- One hour outage of all ISP's might cost that industry as much as $5.7mm
- One of the 21 major ISP's (68% of market) losing 10% of its business for one year to a competitor due to a security event loses $163mm
- Equivalently – Every major ISP would have to be down for about 27 hours each year to equal a substantial business loss suffered by one ISP

General Inferences

- Cyber attacks with long-lasting economic consequences or very wide spread consequences are the most worrisome
  - Reputation loss
  - Loss of IP
  - Big legal liabilities
  - Wide-spread Internet outage
  - Long-term productivity loss
  - Costly Regulation-Creating
  - Physical Damage
- Individual DNS attacks are not as significant until they impact the above list of consequences

Why Start with Cyber-based IP Attacks?

- Among the family of potentially most significant consequences due to Cyber attacks
- Globalization is leading to more integrated IT systems that could inadvertently provide access to IP
- Most recent CSI survey puts cyber IP theft high on list of concerns

Risk Analyses of IP Attacks

- **Consequence Analysis**
  - What are the financial impacts, direct and indirect, to the US economy of successful IP attacks from abroad(i.e., converting stolen IP into stolen market share)?
- Likelihood Analysis
  - What sectors are setting up supply chains with what countries as suppliers?
  - What is the non-cyber IP theft track record for those countries?
  - What computer skills exist in those countries?
- **Prevention Analysis**
  - What factors provide the basis for sectors increasing their investments in cyber security?
  - What are current levels of investment in IP related security on a sector by sector basis?
  - What are the costs of various solutions?
  - How do increases in sector investment levels relate to increases in cyber security and reductions in economic losses?

Risk Analyses of IP Attacks

- **Consequence Analysis**
  - What are the financial impacts, direct and indirect, to the US economy of successful IP attacks from abroad(i.e., converting stolen IP into stolen market share)?
- Liklihood Analysis
  - What sectors are setting up supply chains with what countries as suppliers?
  - What is the non-cyber IP theft track record for those countries?
  - What computer skills exist in those countries?
- **Prevention Analysis**
  - What factors provide the basis for sectors increasing their investments in cyber security?
  - What are current levels of investment in IP related security on a sector by sector basis?
  - What are the costs of various solutions?
  - How do increases in sector investment levels relate to increases in cyber security and reductions in economic losses?

Foreign vs. Domestic Electronic Industrial Espionage

- From a macro economic viewpoint shifts in supply chains and consumer markets to foreign sources would be expected to have a much greater macro economic impact than domestic shifts.
- White House Office on Science and Technology estimates the cost of espionage by America's competitors to be around $100bb annually.*
- According to the 2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, economic espionage and loss of critical information cost American companies more than $300bb a year.
- According to Penenberg and Barry**, repeat corporate espionage offenders are located in:
  - China, Japan, South Korea, Taiwan
  - France, UK
  - Russia
  - Mexico, Israel

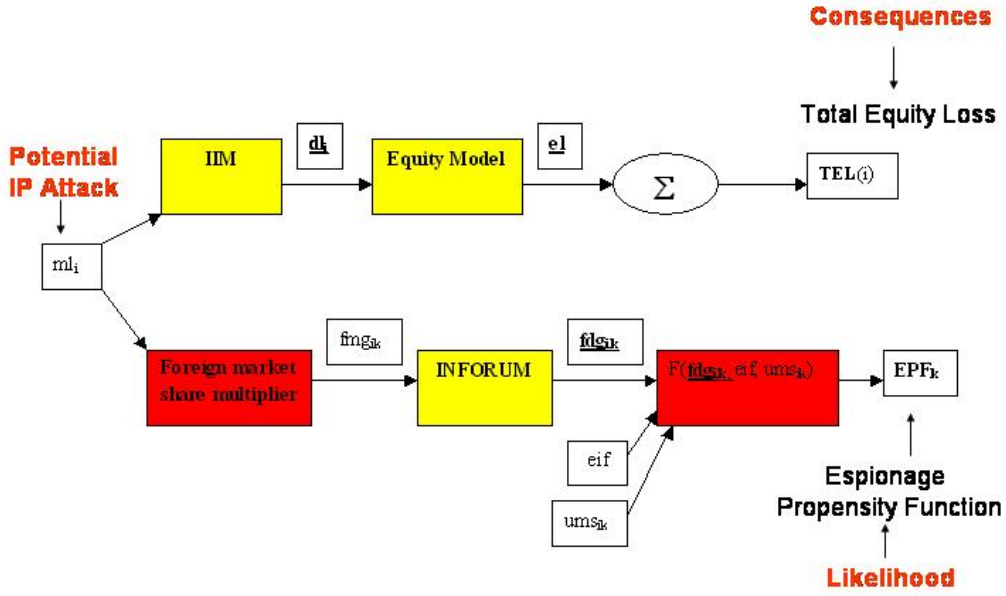
* Schweizer, Peter. Friendly Spies. Jan, 1993.

** Penenberg, Adam and Marc Barry. Spooked: Espionage in Corporate America. Nov, 2000.

Consequence Analysis of International Industrial Espionage – Espionage Propensity Factor (EPF)

- Which US sectors have the most foreign competition?
  - analysis of BEA data
- Do these competitors come from countries with a history of industrial espionage?
  - US Chamber of Commerce
- Which foreign governments receive most financial advantage from a benign neglect policy towards the industrial espionage carried out by their industries?
  - University of Maryland INFORUM model which supports input-output economic models comparable to the BEA model that we use
    - INFORUM (Interindustry, international, input-output model)
    - 12 foreign country models
    - includes interaction features between country models

Risk Analysis Model



Risk Analysis Overview

- For the purpose of initial analysis we will focus on IP attacks on the following ten sectors which might have valuable IP that would be of interest to foreign competitors:
  - Computer and electronic product manufacturing
  - Motor vehicle, body, trailer, and parts manufacturing
  - Chemical manufacturing
  - Machinery manufacturing
  - Fabricated metal product manufacturing
  - Publishing including software
  - Plastics and rubber products manufacturing
  - Primary metal manufacturing
  - Nonmetallic mineral product manufacturing
  - Wood product manufacturing

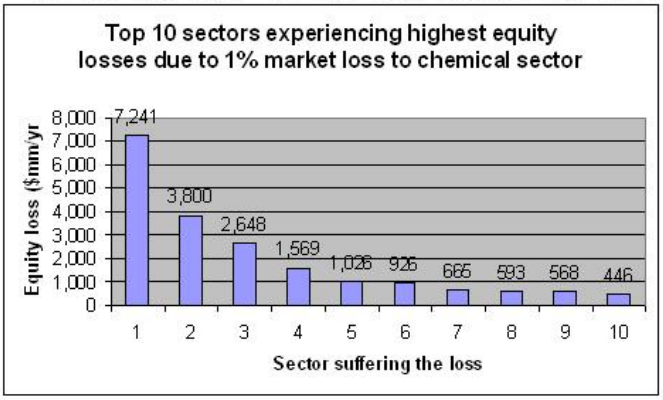
Risk Analysis Results (1)

- **Total equity loss (Direct and Indirect Losses due to 1% direct market loss to sector i)**

1. Computer and electronic product manufacturing
2. Motor vehicle, body, trailer, and parts manufacturing
3. Chemical manufacturing
4. Machinery manufacturing
5. Fabricated metal product manufacturing
6. Publishing including software
7. Plastics and rubber products manufacturing
8. Primary metal manufacturing
9. Nonmetallic mineral product manufacturing
10. Wood product manufacturing

Risk Analysis Results (2)

- **Top 10 highest equity losses to sectors due to 1% market loss to sector i**



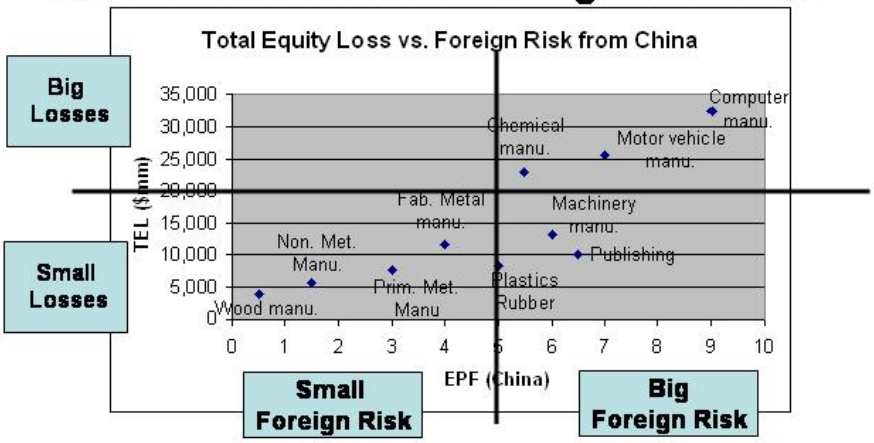
1. Chemical manufacturing
2. Professional, scientific, and technical services
3. Petroleum and coal products manufacturing
4. Oil and gas extraction
5. Real estate
6. Management of companies and enterprises
7. Federal Reserve banks, credit intermediation and related services
8. Other services*
9. Broadcasting and telecommunications
10. Wholesale trade

Risk Analysis Results (3)

- **Rank of top 10 greatest indirect sufferers (given attack on any of the pre-selected 10 sectors)**
  - Other services
  - Professional, scientific, and technical services
  - Wholesale trade
  - Chemical manufacturing
  - Management of companies and enterprises
  - Fabricated metal product manufacturing
  - Utilities
  - Truck transportation
  - Computer and electronic product manufacturing
  - Real estate

Risk Analysis Results (4)

- **Which sectors have the greatest equity losses and are most at risk for foreign IP attacks?**



Risk Management

Collaborative Computing Game

- We have completed a financial decision analysis for decisions on investing in cyber security to protect IP
- We have set up a computer game to see how decision makers' results compare to derived decisions
  - Similar or not?
  - Why?
- Use as a step in developing decision support tool that combines inputs from technology oriented and business oriented staff

Game Rules

- Game 1
  - **Decision**
    - **$6 million investment in security enhancement to protect $40 million a year**
    - **$6 million investment in sales enhancement to return $2.8 million per year**
- Game 2
  - **Decision**
    - **$4 million investment in security enhancement to protect $40 million a year**
    - **$4 million investment in sales enhancement to return $2.4 million per year**
- Game 3
  - **Decision**
    - **$2 million investment in security enhancement to protect $40 million a year**
    - **$2 million investment in sales enhancement to return $2 million per year**

Risk Management Equations

α = Probability of Successful Defense with ADDED Investment

β = Probability of Successful defense with NO ADDED Investment

S = Added Security Investment under Consideration (Also Alternative Sales Investment)

O = 4 Year Return on Sales Sacrificed with Security Investment

V = 4 Year Market that will be lost if successfully attacked

$$S \leq [(\frac{\alpha}{\beta} - 1)\beta * V] - O$$

All Cases: $\alpha = 0.96, \beta = 0.90, V = \$160\text{mm}$

$$S \leq \$9.65 - O$$

Case 1: S = \$6mm; O = \$5.2mm; Conclusion = Don't Invest

Case 2: S = \$4mm; O = \$5.6mm; Conclusion = Indifferent

Case 3: S = \$2mm; O = \$6mm; Conclusion = Invest