Incentivizing Cybersecurity in Business

April 25, 2018

Famous Data Breaches

Review: Why Do Hacks Occur?

Lax Security

- “One firewall and 148 routers, switches, and web servers were left unwatched for months”
- Sony’s network was most likely breached through spear phishing

Hacker Ingenuity

- A la Stuxnet
- “Against a sufficiently skilled, funded, and motivated attacker, all networks are vulnerable”

Review: Costs of Cybersecurity

To Customers

- Target: “theft of 40 million payment cards and 70 million other records”
- Home Depot: ~ 50 million credit card numbers and 70 million other records

To Companies

- Target: “0.1% of 2014 sales”
- Sony: “I will not invest $10 million to avoid a possible $1 million loss”

$57 -$109 bil

Estimated Cost of Malicious Cyber Activity for the US Economy in 2016

Project Objective

Survey the existing regulatory landscape regarding private cybersecurity practices and propose a National Cybersecurity Safety Board

RoadMap

- Current State of Industry
- Economic Theory
- Possible Solutions
  - NCSB

Current Regulatory State

Private Industry Self-Regulation

- 2006: American Express, Discover, JCB, MasterCard, and Visa
- Universal PCI Data Security Standard
- Case Law:
  - Breach of contract lawsuits
  - Target settled

State Regulation

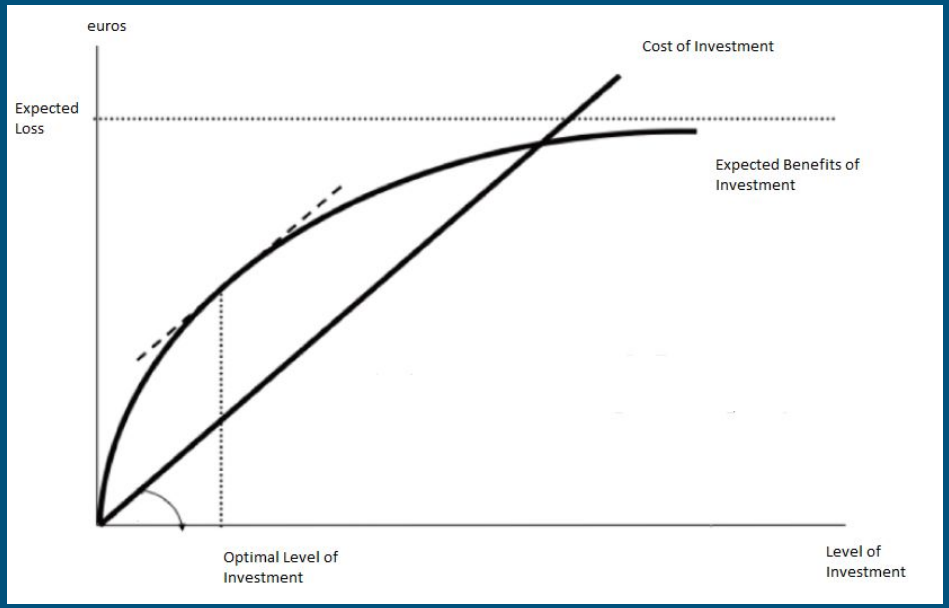
- New York Financial Industry
- Mandated Risk Assessment
- Fines for Non-Compliance
- Specific to:
  - Financial Industry => not applicable
  - State => fragmented?

NIST Framework

- National Institute of Safety and Technology
- Extensible for Most Situations
- Not Mandatory
- Risk-Based - possibly too flexible?
- Dependent on Lawsuits for Compliance

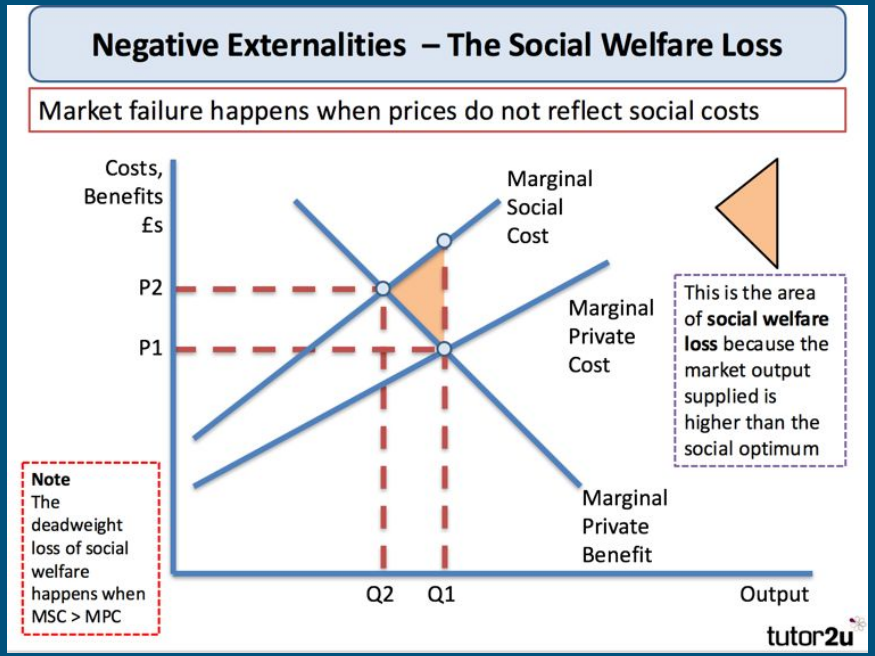
Microeconomic Theory

Gordon - Loeb Model: Introduction



- Theoretical model that assumes:
  - Perfect information
- S(z, v)
  - v: probability of successful cyber-attack with no investment
  - Z: investment quantity
- Max_z [v - S(z, v)]L_p - z
- Invest no more than 37% of expected loss

Gordon - Loeb Model: Externalities



- Examples of Cyber Security Externalities
  - Costs for Consumers When Data Lost
  - Hacked Computer used in DDOS Attack
- F: percent externality cost => optimal investment as % of private expected loss

Return on Security Investment

ALE= Single Loss Expectancy (SLE) (total cost)* Annual Rate of Occurrence (ARO)(probability of risk).

$$\text{ROSI} = \frac{(\text{ALE} * \%\text{risk mitigated}) - \text{cost of security}}{\text{cost of security}}$$

Gordon - Loeb vs. ROSI

Gordon - Loeb

- Given the probabilities of cyber attack and expected loss, how much do I invest?
- Theoretical: assumes perfect information

ROSI

- Is this particular security measure worth it for me?
- More Applied

Proposed Solution

National CyberSecurity Safety Board

Key Benefits

- Transparent Regulatory Structure
- Mandated Risk Assessment
- Investigations into Noteworthy Data Breaches
  - Practices
  - Culture
- Allocations of Social Cost

Bibliography

https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/

https://www.wired.com/story/equifax-breach-no-excuse/

https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html

http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/