MODELING THE LOJACK EFFECT IN THE CYBER SECURITY MARKET – A STUDY OF INCENTIVES

Abstract:

Cyber security has become a pertinent concern among businesses following the increasing digitization of operations. Hacking methods are ever evolving and businesses struggle to detect and respond promptly, as well as develop preventive measures against future attacks. It is widely acknowledged that cooperation is key in an industry's efforts in combating cyber crime, and in my paper, I focus mainly on the financial services sector. There exists a network of collaboration within the sector, such as the Financial Services Information Security Analysis Center (FS-ISAC), which facilitates the sharing of anonymized data about attack information among companies to improve situation awareness. However, in light of the private costs involved in investing in research, companies are reluctant to invest in R&D, preferring to act as free riders. I turn my focus to the LoJack industry within the auto theft market, which faces similar externalities and incentive problems. I model the incentive problems of both markets, analyzing the similarities and differences in network effects. Results show that although the LoJack model has significant positive externalities, excludable private benefits incentivize car owners to invest in a LoJack. However, in the cyber security market, companies have little incentive to invest more than the bare minimum in research due to the contagion effects of both negative and positive externalities. Finally, I draw on the successes of the LoJack in deterring auto theft to apply them to better outline the opportunities for collaboration for cyber security within various industries.

Keywords: cyber security, incentives, modeling, LoJack, contagion effect, network effects, free rider, externalities, financial services

AN HONORS THESIS
SUBMITTED TO THE DEPARTMENT OF ECONOMICS
OF STANFORD UNIVERSITY

PRESENTED BY:
CASATRINA LEE
CYLEE1@STANFORD.EDU
MAY 2014

HONORS ADVISOR:
PROFESSOR TIMOTHY BRESNAHAN

DEPARTMENT OF ECONOMICS

Acknowledgments

I am deeply grateful to my Honors Advisor, Professor Timothy Bresnahan, for his invaluable guidance and patience throughout the completion of the Honors Thesis. Despite his busy schedule, he is always eager to meet for a discussion and guide me through formulating a convincing economic model. I am grateful for his instruction throughout the process of pinning down my thesis topic, pointing me in the direction of relevant literature and ironing out the kinks in my paper.

I am also thankful to Professor Marcelo Clerici-Arias for his continued guidance and support since I embarked on this journey to write an honors thesis. I am grateful that he planted the inspiration in me during the Junior Honors Seminar class I took under him.

Finally, I am thankful to my friends and for their support, without which this honors thesis would not have been possible.

Contents

Chapter 1

Introduction

As the marketplace becomes increasingly digitized, businesses move a greater part of their operations online, and data is increasingly being migrated to the cloud. Naturally, the need to protect data has become more pertinent. Hacking methods have evolved to become more sophisticated, with millions of attacks happening every day. New modes of attack are being developed rapidly, more specifically zero-day attacks,[1] making it difficult to incentivize companies to invest in attack prevention research, or even to respond efficiently to these attacks.

There are numerous existing problems associated with information security. Companies often lack insight into the source and effect of attacks, making it difficult for them to take preventive measures or respond effectively. Companies also acknowledge that research in cyber security is often too time-consuming and cost-inefficient. With the high costs and low returns of research, companies lack incentives to invest in cyber security research.

[1] Zero-day attacks are attacks which exploit a previously unknown vulnerability, such that developers have no time to address and patch

Network effects of the Internet further exacerbate this underprovision of research. The high interconnectivity of firms and networks has resulted in high negative externalities on other members of the network. Once a member of a network has been hacked, other members of the network are more vulnerable as it is now easier for the hacker to infiltrate other members of the network. Positive externalities, however, can also result from these network effects if firms are willing to invest in security measures. A secure network would benefit the network as a whole, and this mutually beneficial relationship provides opportunity for collaboration among members by sharing information. Useful information would include attack sources, attack vectors, as well as effective methods of response and recovery.

The auto theft industry faces similar externalities, and research has demonstrated that the LoJack, despite its private costs, has been successful in overcoming free rider problems, therefore increasing positive externalities, deterring criminals and lowering crime rate. I aim to examine this model in the hopes of applying it to the cyber crime market.

The LoJack is a hidden radio transmitter used to retrieve stolen vehicles and has proven to be very effective in achieving general deterrence among car thieves. LoJacks facilitate cost and time efficient theft detection and recovery of stolen cars as the police are better able to track them. Consequently, a higher arrest rate has been associated with the increased use of LoJacks.

An important feature of the LoJack is that it is invisible to criminals. This feature is key in achieving general deterrence among auto thieves because criminals are unable to distinguish a car with a LoJack installed from a car without a LoJack installed. With a higher probability of being arrested if they happen to steal a car with a LoJack, thieves are reluctant to take the risk of stealing a random car in the first place. Similar to the cyber security market, network effects also come into play here in the form of positive externalities. For example, if LoJacks are popular in a particular neighborhood, residents of that neighborhood benefit from the high incidence of LoJacks and enjoy a lower risk of theft even if they do not install a LoJack themselves. I model this incentive structure in my paper below.

Given the success of LoJack in deterring crime, I aim to apply a similar model to the market of cyber crime. In both markets, we see a barrier against investment – car owners are reluctant to invest in a LoJack and companies are reluctant to invest in research – because at the time of investment, the marginal benefit to the car owner and company is zero. No attack has taken place yet, and thus they are disincentivized to incur additional costs in investing. However, the benefits of collective investment are amplified with group investment. As investment is increased in both markets, the threat of falling prey to a successful attack is lowered. This implies that the social benefit of investing in crime prevention clearly exceeds the private benefit of investment. However, this result also consequently suggests the clear possibility of free riders in both markets.

Specific to the cyber crime market, the model shows that sharing of information among companies is optimal, assuming that sharing incurs no cost. This is because companies are indifferent between sharing and not sharing information, but the collective pooling of information helps provide better situational awareness of the cyber crime landscape and therefore decreases the risk of falling victim to an attack.

Furthermore, the model showed that the amount that companies are willing to invest in cyber security research is in fact a low constant, independent of the value they place on their information, and independent of the current risk of attack. This suggests again that companies are unwilling to invest beyond that equilibrium constant, resulting in a severe underprovision in the cyber security market.

In my paper, I break down the differences between the auto theft and cyber crime markets, more specifically in terms of the free rider and network effects. While the auto theft market is discrete (ie. breaking into a car does not gain one access into another), the cyber crime market is relatively less discrete due to the high level of interdependence and connectivity. This results in high network effects, which can compound positive externalities of collaborative research, but can also compound negative externalities of a company in the network getting hacked and exposing other members to a higher risk of infiltration.

I aim to draw on the successes of the LoJack in deterring auto theft and apply them in better analyzing the opportunities for collaboration for cyber security among network members. My thesis is outlined as follows. A brief literature review is provided in Chapter 2, followed by my economic models of the auto theft and cyber crime markets in Chapter 3. In Chapter 4, I compare the cyber crime market to the auto theft market and subsequently apply my findings and provide more in-depth analysis and suggestions for the financial industry to better reap the rewards of collaboration in cyber security.

Chapter 2

Literature Review

Companies have thus far failed to develop an effective way to deal with the threat of cyber crime. While they widely acknowledge that prevention is ideal, it is impossible to determine a stock solution or mode of prevention for attacks, given the high rate at which attack vectors evolve. This, on the other hand, has incentivized criminals to persist in their hacking attempts, undeterred by the legal ramifications or the possibility of being caught. In fact, research has shown that the likelihood of detecting cybercrime is so low that the penalty inflicted would have to be of enormous magnitude to deter cyber crime (Grady & Parisi, 2006). As a result, companies have proved to be more inclined to choose "cure" over "prevention" – choosing to tackle attacks by patching the problem, rather than resolving the root vulnerability.

However, in responding to attacks, companies face several challenges. Firstly, the system needs to be able to detect when it has been hacked before response can even begin to take place. Secondly, the system needs to undertake the most effective patch in response to the infiltration – if the attack were a zero-day attack, response becomes even more problematic. Thirdly, the system needs to have adequate resources to deal with the attack; often, small and medium enterprises lack these resources (Bauer & van Eeten, 2008). Due to these factors, response is slow, and damage is rarely mitigated efficiently.

Market failure is present in the cyber security market, manifesting itself in the form of externalities. When a firm is compromised, it passes on the damage to its consumers in the event of a data breach. Financial institutions have chosen to internalize such negative externalities by compensating customers in the event of a security breach, rather than investing in security measures (Bauer & van Eeten 2011). Another form of negative externalities is also present among members of a computer network. Due to the high interconnectivity of computer systems, a breach in a member's system would result in the security of other members being compromised. As explained in a paper by Neil Gandal, large networks are more vulnerable to security breaches, precisely because of the success of the network. In example given by Gandal, in part because of its large installed base, Microsoft's Internet Explorer is likely to be more vulnerable to attack than Mosaic's Firefox Browser. This is because the payoff to hackers from exploiting security vulnerabilities in Internet Explorer is much greater than the payoff to exploiting similar vulnerabilities in Firefox.

On the flip side, positive externalities can be created when companies invest in security measures and research to strengthen their systems. Via the same network effects, the entire network is consequently strengthened. Such mutually dependent relationships offer an opportunity for collaboration among members of a network.

Anderson uses the network effect to better illustrate this in the context of the Internet (2001). The more people use the Internet, the more value it has for its users. In the realm of cyber security, the more companies share information with each other, the larger and more exhaustive the pool of resources, and therefore the more effective it is in preventing security breaches. The sharing of information related to methods for preventing, detecting and correcting security breaches is desirable as it helps prevent organizations from falling prey to security breaches previously experienced (Gordon, Loeb & Lucyshyn, 2003). This knowledge of the cyber security landscape is termed "situational awareness". Additionally, such information helps organizations respond more quickly and efficiently with focused solutions if an actual breach occurs. Threats can be more effectively pre-empted and attacks can be more efficiently patched, therefore alleviating potential damages of the cyber attack. Situational awareness therefore involves achieving visibility of emerging threats, and is key in facilitating the anticipation and management of attacks.

As much as information sharing has been touted a possible solution for cyber security, there is a major inherent problem - companies lack adequate economic incentives to facilitate such sharing. Anderson and Moore indicate misaligned incentives as the main reason for the failure of information sharing (2006). This is corroborated by a paper by van Eeten and Bauer, highlighting the issue of the free rider problem (2009). Individual businesses and users may suffer from the perception that their own risk exposure is low, coupled with the interconnectivity associated with computer networks, when a firm invests in cyber security activities, it bears all the costs but doesn't reap all the benefits. The larger the share of benefits that accrue to other firms, the smaller the incentive for a firm to increase its investments. Companies are therefore disinclined to invest in and share their security solutions because it would allow other companies in the network to benefit freely from it. For example, joining and reporting to Information Security Analysis Centers (ISACs) is voluntary, with no incentives in place to encourage full reporting and discourage free riding. Members may under-invest in the development of information security measures in anticipation of obtaining them for free from other ISAC members (Gordon, Loeb & Lucyshyn, 2003). As a result, the security level of the network is less than ideal.

Zooming in on the financial services sector, there is an existing framework for information sharing under the FS-ISAC (Financial Services Information Sharing & Analysis Center). It is unique in that it seems to have succeeded in creating a successful partnership in information sharing despite the potential pitfalls as mentioned previously. According to the current President and CEO of the FS-ISAC Bill Nelson, most of the information shared comprises of anonymized data about attack vectors and sources. However, little research is done by the ISAC on security measures; without extracting value from the shared information to develop new solutions, the FS-ISAC simply becomes a data collection center.

We first have to distill the factors that have contributed to the success of the LoJack in the auto theft market. With the LoJack, a small radio transmitter is hidden in one of many possible locations within a car. When the car is reported to be stolen, the transmitter is remotely activated by the police, allowing the police to track the stolen car's precise location. LoJack-equipped stolen vehicles have a 90% recovery rate, compared to a 63% recovery rate for vehicles that lack a tracking system. (Helperin, 2009).

In an empirical paper by Ayres and Levitt, it is found that there are strong positive externalities by the LoJack in achieving general deterrence (1998). They further found that each dollar spent on LoJack resulted in a reduction in the costs of auto theft of approximately $10. Because there is no external indication that the LoJack has been installed in a car, it does not directly affect the likelihood that a protected car will be stolen. However, it was found that the availability and adoption of LoJacks in a particular area is associated with a sharp fall in auto theft. More specifically, the introduction of LoJack in a city has been shown to reduce auto theft, even though the initial use may be very small. The reason for this is that while the odds of a stolen car having a LoJack installed are very small, an auto thief may typically steal many cars a year. Once he unknowingly steals a car with a LoJack installed, he is caught, as with the rest of his accomplices (Bankman, 2001).

However, similar to the case of cyber security, there is the phenomenon of underprovision. While it was found that the marginal social benefit of an additional unit of LoJack has been fifteen times greater than the marginal social cost in high crime areas, those who install LoJack, however, obtain less than ten percent of the total social benefits, leading to underprovision by the market (Ayres & Levitt, 1998). In other words, people are inclined to free ride on deterrence phenomenon of the presence of the LoJack in the neighborhood, but are reluctant to personally invest in one. An individual car owner's decision to install the LoJack only trivially affects the likelihood of his or her car being stolen since thieves typically base their theft decisions on mean

LoJack installation rates. As thieves are unable to distinguish cars with LoJacks from cars without, the deterrence effect is very strong, and the extent of positive externalities arising from LoJack usage is very large. It is therefore crucial that one is able to incentivize car owners to invest in a LoJack.

Moving on, we examine the exact mechanism by which the LoJack has achieved its large social benefits. It disrupts the operations of “chop-shops”.[2] In the absence of LoJacks, identifying these chop-shops require operations that are highly time and resource intensive, whereas the installation of the LoJack often leads police directly to the heart of criminal operations. However, it is crucial to note that there is an interesting substitution effect in the form of older vehicles; older vehicles are less likely to have LoJacks installed and are therefore more targeted by criminals. Consequently, while the overall auto theft rate decreases, the theft rate for older vehicles increases.

LoJacks are expensive ($700), and while they have proven very effective in reducing auto theft rates, these reductions are purely an externality from the perspective of the car owner installing a LoJack. The only internalized benefits of installing a LoJack are higher retrieval rates and lower theft damages once a vehicle is stolen (Ayres & Levitt, 1998). In light of these effects, I will compare the externalities and network effects in both markets in greater detail in the following sections.

[2] Where stolen vehicles are disassembled for resale of parts.

Chapter 3

LoJack Model

We define the variables as follows:

$V_i = value\ of\ car\ to\ Person\ i$

$C = fixed\ cost\ of\ installing\ a\ LoJack$

$L_i = dummy\ variable; L_i = 1\ if\ the\ car\ has\ a\ LoJack\ installed, 0\ otherwise$

$T = probability\ that\ a\ car\ is\ broken\ into, where\ T = t\left(\frac{\sum L_i}{n}\right)$

$n = number\ of\ car\ owners\ in\ market$

T is defined as a function of the fraction of the population of car owners in the market who choose to invest in a LoJack.

We define Person *i*'s utility (U_i) as follows:

$$If\ L_i = 0, \qquad U_i = V_i(1 - T)$$

$$If\ L_i = 1, \qquad U_i = V_i - C$$

Without a LoJack, Person *i*'s utility of his car is discounted by the risk of theft. With a LoJack, his utility is unaffected by the risk of theft, and his valuation is only reduced by the fixed cost of buying and installing a LoJack.

To incentivize Person *i* to invest in a LoJack,

$$U_i \colon L_i = 1 > U_i \colon L_i = 0$$

$$V_i - C > V_i(1 - T)$$

$$C < V_i T \tag{1}$$

Let us assume that m is the number of people who choose to invest in a LoJack (ie. m people have $C < V_i T$). In this model, we seek to find equilibrium values of $\tilde{V}$, $\widetilde{m}$ and $\tilde{T}$ such that they fulfill the following conditions:

1. $\tilde{V} = \frac{C}{\tilde{\tilde{T}}}$
2. $\widetilde{m} = \ number\ of\ people\ where \{V_i \geq \tilde{V}\}$
3. $\tilde{T} = t\left(\frac{\widetilde{m}}{n}\right)$

Utilizing these equations, we can derive the equilibrium values of an individual's value of his car ($\tilde{V}$), the equilibrium risk of car theft ($\tilde{T}$), as well as the number of people who would install a LoJack ($\widetilde{m}$).

When Person i chooses to install a LoJack, his private benefit is 0, since no theft has occurred yet. However, the probability of a theft occurring (T) decreases as the number of LoJacks installed increases (ie. m increases). This is clearly a social benefit and indicates positive externalities of LoJack usage. We express the social value of a higher fraction of LoJack adoption (higher $\frac{\widetilde{m}}{n}$) on the market as a whole as follows:

Social benefit = total private value

+ social benefit of decreased risk of theft

$$= 0m + \int_{\{all\ i\}} V_i \cdot \left(-t'\left(\frac{\widetilde{m}}{n}\right)\right) di \qquad (2)$$

Note the term $0m$ is obtained from the zero marginal benefit that a LoJack adopter experiences after installing a LoJack because no theft has occurred and therefore, no tangible benefit can be felt. The second term $\int_{\{all\ i\}} V_i \cdot \left(-t'\left(\frac{\widetilde{m}}{n}\right)\right) di$ represents the sum of social benefits over each car owner. The first derivative of t is negative because the theft rate decreases with an increased fraction of LoJack adoption. This benefit is not exclusive only to those people who have installed the LoJack since the overall theft rate for both LoJack adopters and non-adopters decreases alike. The benefit is thus represented by the product of their individual valuation of the car (V_i) and the marginal decrease in risk of theft on society as a whole borne out of a greater fraction of LoJack adoption among car owners in the region $\left(-t'\left(\frac{\widetilde{m}}{n}\right)\right)$.

Here, we can see that because the general decrease in theft rate benefits the entire car owner population, the excess of social benefits as compared to individual marginal benefit has encouraged free riding and resulted in underprovision in the market for LoJacks.

Cyber Security Model

We examine the financial industry with respect to the market for cyber security, specifically because the financial industry is the most developed in the realm of cyber security, and because cyber security is at the forefront of companies' priorities. The financial industry has an existing organization, the Financial Services Information Sharing and Analysis Center (FS-ISAC), in which banks cooperate and share anonymized data on cyber attacks.

We define the variables as follows:

$V_i = value\ of\ protected\ information\ to\ bank$

$S_i = dummy\ variable;\ S_i = 1\ if\ company\ shares\ information, 0\ otherwise$

$r = cost\ of\ engaging\ in\ research$

$R_i = dummy\ variable;\ R_i = 1\ if\ company\ engages\ in\ research, 0\ otherwise$

$T = probability\ of\ getting\ hacked, where\ T = t\left(\frac{\sum s_i}{n}, \sum r_i\right), t_1', t_2' < 0$

$n = number\ of\ banks\ in\ market$

T is defined as a function of the fraction of banks that chose to share attack information and the cumulative amount of money invested in research. This assumes that the sharing of attack information and research have valuable payoffs.

We first consider the issue of sharing information within the organization. We can assume that the cost of sharing information is 0, since companies are not engaging in additional efforts in the course of sharing information with other companies in the organization. Since the cost of sharing information is 0, companies would be indifferent between choosing to share ($S_i = 1$) and not to share information ($S_i = 0$). Given that T is dependent on S and $t_1' < 0$ (ie. the greater the number of companies who share information, the lower the risk of being hacked), companies are incentivized to share (ie. $S_i = 1$).

Therefore, sharing of information (S) is assumed to be efficiently provided in this model, given that all banks share at zero cost. This assumption is supported by the FS-ISAC, which confirms that all banks contribute anonymized data to the organization voluntarily. This is attributed to the fact that sharing of data incurs little time or monetary cost to individual banks as long as sufficient infrastructure to collect relevant data was already in place.

If Bank *i* chooses not to engage in research ($R_i = 0$),

$$\text{Payoff} = V_i(1 - T_1), r_i = 0,$$

$$(T_1 = theft\ rate\ without\ Bank\ i's\ contribution)$$

Consequently, there is no contribution by Bank *i* to the reduction of crime rate.

If Bank *i* chooses to engage in research ($R_i = 1$),

$$\text{Payoff} = V_i(1 - T_2) - r_i, r_i \neq 0,$$

$$(T_2 = theft\ rate\ with\ Bank\ i's\ contribution)$$

Consequently, this increases $\sum r_i$ and reduces T, as a social benefit, much like the case in the LoJack model above. This implies that $T_2 < T_1$. It is important to note that r_i is a wholly private cost chosen solely by the bank, and can be perceived as the bank's contribution to group research (assuming the bank does not engage in any research on its own using its own resources). Clearly, the socially preferred option would be for $R_i = 1$.

A bank will choose to invest in research if:

$$V_i(1 - T_1) < V_i(1 - T_2) - r_i$$

$$(1 - T_1) < (1 - T_2) - \frac{r_i}{V_i}$$

$$-T_1 < (-T_2) - \frac{r_i}{V_i}$$

$$\frac{r_i}{V_i} < T_1 - T_2$$

$$V_i < \frac{r_i}{(T_2 - T_1)} = \frac{r_i}{(-t_2')} \qquad (3)$$

We seek to find equilibrium values of $\tilde{V}$, $\tilde{r}$ and $\tilde{T}$ such that they fulfill the following conditions:

1. $\tilde{V} = \frac{\tilde{r}}{\widetilde{(-t_2')}}$
2. $\tilde{T} = t\left(\frac{\sum s_i}{n}, \sum \tilde{r}\right)$
3. $maximize\ \tilde{V}\left(1 - \tilde{T}\right) - \tilde{r}\ wrt\ \tilde{r}$

Utilizing these equations, we can derive the equilibrium values of an individual bank's value of protecting its information ($\tilde{V}$), the equilibrium risk of cyber crime ($\tilde{T}$), as well as the optimal amount that a bank should invest in research ($\tilde{r}$).

Focusing on conditions 2 and 3,

$$Maximize\ \tilde{V}\left(1 - \tilde{T}\right) - \tilde{r}$$

$$= \frac{d}{d\tilde{r}}\left[\tilde{V}\left(1 - t\left(\frac{\sum S_i}{n}, \sum \tilde{r}\right)\right) - \tilde{r}\right]$$

$$= -\tilde{V}\widetilde{t_2'} - 1$$

$$= 0$$

$$\therefore \widetilde{t_2'} = -\frac{1}{\tilde{V}} \tag{4}$$

Substituting this result into $\tilde{V} = \frac{\tilde{r}}{(\widetilde{-t_2'})}$, we obtain:

$$\tilde{V} = \tilde{r}(\tilde{V})$$

$$\tilde{r} = 1 \tag{5}$$

We see here that the optimal amount that a bank should invest in research is 1. This is a constant, independent of the bank's value it places on protecting its information, and independent of the current risk of crime. This can be attributed to the fact that each bank is reluctant to invest in more than the minimum to contribute to lowering the risk of crime, preferring to spread out the responsibility and put the onus equally on every member of the organization. They are choosing to sacrifice the long-term rewards of engaging in research and the compounding benefits of network effects in a strengthened network in favor of short-term cost savings.

Clearly, this is a myopic approach, but is unfortunately rampant in the current market. Research has also shown that, rather than invest in research and prevention, banks and financial institutions have chosen to internalize the costs of being hacked by compensating companies. In their opinion, the benefits of research fail to outweigh the time and monetary costs. As more banks adopt this mindset, the lack of a credible research team and foundation is perpetuated. Knowing that their counterparts have adopted this mindset, individual banks are less likely to be the sole member in the network investing in research. In this case, network effects and the potential benefits of increased research investment are not tapped.

To quantify such benefits, we look at the social value of increasing r_i:

Social benefit = private value for marginal bank

+ social benefit of decreased risk of theft

$$= 0 + \int_{\{all\ i\}} V_i \cdot \left(-t_2'\left(\frac{\sum s_i}{n}, \sum \tilde{r}\right)\right) di \qquad (6)$$

Note the private value for the marginal bank is 0, regardless of whether it chooses to invest in research or not. This is because research has a time lag, whether in conducting the research or the utility of research results, and the benefit at a time where no hacking has occurred is 0.

The second term $\int_{\{all\ i\}} V_i \cdot \left(-t_2'\left(\frac{\sum s_i}{n}, \sum \tilde{r}\right)\right) di$ represents the sum of social benefits over everyone in the community. The first derivative of t with respect to $\tilde{r}$ is negative given that the crime rate decreases with an increased overall investment in research. Like in the LoJack model above, this benefit is not exclusive to those banks that have chosen to invest in research, but benefits every member of the organization as a whole by decreasing the probability of an effective hacking attempt. The benefit is thus represented by the product of their individual valuations of their information V_i and the marginal decrease in risk of hacking on the community as a whole borne out of a greater cumulative investment in research.

Given that the research is collaborative, and there is no private research done by banks, the social benefit is shared among all the banks equally. Therein lies the problem of incentives – since all benefit is shared but all cost is private, there is an incentive to become a free rider, resulting in underprovision of security research, similar to the case of LoJacks above.

We found that $\tilde{r} = 1$ for all banks. This seems to be a unanimous decision, with no bank choosing to invest more than the equilibrium. This equilibrium, however, is not optimal, as the risk of hacking can be further decreased with increased investment in research. Yet if any bank chooses to invest more than the perceived equilibrium, it is unlikely that other banks will follow suit. Given that the research is non-rivalrous and non-excludable within the FS-ISAC, the problem of free riders arises.

Chapter 4

Comparative Analysis

While we can draw similarities between the cyber security and LoJack markets in terms of underprovision, there are numerous differences that need to be highlighted, specifically in the structure of its respective externalities.

1 – Differing structures of network effects

For the LoJack market, the skills and tools required to steal a car is directly transferrable from car to car. In other words, once a criminal is equipped with the knowledge and tools of how to steal a car, there is no economic barrier preventing him from stealing another car. However, stealing one car does not automatically gain him access to another car (ie. the auto theft market is discrete).

In contrast, in the cyber security market, more often than not, criminals require specific insider knowledge in order to gain access to the system on top of general hacking skills. This knowledge is unique to individual companies and is less transferrable to other companies. That said, however, once a criminal gains access to a company's system, the barrier to gaining access to systems of other companies in the network is lowered (ie. the cyber crime market is less discrete). While the LoJack criminal is not bound by geographical or regional restrictions in applying his knowledge, the cyber criminal is bound by the network of companies he is trying to infiltrate (ie. This knowledge may not be applicable to another network such as the food and beverage industry).

2 – Differing free rider effects

In the LoJack market, there are little to no free rider effects. A car owner installing a LoJack has no direct impact on the probability of his immediate neighbor's car getting stolen. Therefore, the LoJack is excludable. The free rider effect only kicks in when the installation of LoJacks in a specific region exceeds a particular threshold such that the general theft rate decreases. Even so, while car owners who choose not to install LoJacks may benefit from the general decrease in theft rate, they reap no benefits when their cars without LoJacks are stolen. Here, we see that the incentive to be a free rider is low.

In the cyber security market however, it is acknowledged that there is an infinite number of ways that a company's system could fail, both on the individual company and collective (network) levels. Investment in research, therefore, does not, in any way, guarantee a return. Given the high monetary costs of research, coupled with the time-intensive efforts and contrasted with the fast pace at which attack vectors evolve and develop, research is expensive and may not present itself as an economically rational decision for companies at first glance. In fact, banks have shown that they prefer to compensate customers for any security breaches their network may suffer rather than invest in research (Bauer & Van Eeten, 2011). Therein lies the incentive for companies to free ride on research carried out by other companies in the network. Like in the LoJack model, companies who do not carry out research benefit from the general increase in protection of the network. In the event of infiltration, they experience a negative payoff, but so do the other companies in their network, who may have invested in research. I elaborate on these network effects below. In light of this, the incentive to free ride is drastically higher in the cyber crime market than that of the market for LoJacks.

Contagion Effect

Due to the high interconnectivity of networks within the financial industry, the probability of a bank getting hacked is no longer only dependent on simply sharing information and engaging in research. When a bank in the network gets hacked, other members of the network are subsequently more susceptible to getting hacked as well. This contagion effect therefore changes the payoff of each individual bank. We assume that the threat function is unchanged.

Taking into account the contagion effect,

$$\text{Bank } i\text{'s payoff} = V_i(1 - T_i - \alpha T_{other}) \ - r_i \tag{7}$$

Here, T_i is the probability that Bank *i* is hacked, α is the network effect coefficient, and T_{other} is the probability that another bank in the network is hacked, and affects Bank *i* via network effects.

We see here that the contagion effect has lowered Bank *i*'s payoff. Therefore, the contagion effect serves as a motivating factor for banks to share information within the network, as mentioned above, particularly since the cost of sharing information is zero. It also motivates banks to engage in research to contribute to the overall security of the network to maximize their security.

This is an important result and distinguishes the cyber security market from the LoJack market. The investment in a LoJack is very much individual. As long as Person *i* invests in a LoJack, the general rate of LoJack investment in Person *i*'s region does not affect him. On the other hand, a collectively high rate of LoJack investment in a region without Person *i* investing in one may result in a lower probability of Person *i*'s car getting stolen, but does nothing to aid recovery of Person i's car if it gets stolen.

In contrast, companies' research efforts are individual responsibilities. They contribute to securing the network as a whole as they invest in the collective research done by the network. It also better secures their individual system from being hacked, therefore indirectly securing the network at the same time. They should, therefore, theoretically be more interested in contributing to improving the overall security level of their network. Based on our last model, we see that collective efforts are key in cyber security to amplify network effects and correspondingly amplify the positive externalities over the negative externalities.

Chapter 5

Discussion & Analysis

As proven by the models above, collaboration is definitely advantageous in tackling the problem of cyber security. The financial services sector already has the FS-ISAC in place; one would naturally hope to put in place similar organizations in other industries to promote cooperation in other sectors. However, as much as information sharing has been touted a possible solution for cyber security, there is a major inherent problem - companies lack adequate economic incentives to facilitate such sharing in industries other than the financial services sector. Instead, market failure and externalities come into play.

First and foremost, companies are unwilling to share information with other companies, because it may mean losing their competitive edge, particularly in industries where systems are part of the company's winning moves. For example, Amazon.com prides itself on its efficient retail system and supply chain, with secure payment options and short turnover times. They would be reluctant to share intimate information about their systems and its vulnerabilities to their competitors in the same space who are looking to optimize their respective systems to compete in the ecommerce market.

Also, companies are reluctant to admit whenever their network has been breached, because of the public backlash that could occur when their customers learn that their information has been leaked. This could have negative ramifications on the hacked company's reputation. In 2011, Sony was the victim of a massive data breach and had naturally been reluctant to share the crime with the public. It was heavily criticized when it finally admitted to having been hacked, which only served to amplify the public backlash. One can only imagine that other retail companies like Target would be cautious in revealing its network security flaws.

Furthermore, as we have shown above, information sharing brings with it the problem of free riders. The problem of free riders simply serves to increase the barriers against encouraging collaboration in other industries against cyber crime. To date, the most effective effort in combating cyber crime has been in the financial services industry, in setting up the FS-ISAC. We can attribute several reasons to its collaborative success as opposed to other industries.

Firstly, the personal information that customers provide to financial services companies are much more sensitive and important (ie. Social Security Numbers, personally identifiable information, bank account numbers) than those provided to retailers (eg. Shopping preferences). Entrusted with such information, financial services companies are held responsible in ensuring that the information is secure. The importance of having a secure network is therefore much higher in the financial sector than in other industries.

The reluctance of other industries to share information with their competitors is also less conspicuous in the financial sector because such information is not the edge by which financial services companies compete in the market. Financial institutions are, in fact, highly mutually dependent and the bulk of their revenue comes from large investments, rather than the precise mechanisms of their systems and customer preferences. Their high mutual dependence also necessarily implies a higher contagion effect, which would pose a greater threat in the event of a network breach. These factors therefore uniquely incentivize financial institutions to partake in collaborative efforts to combat cyber crime.

We do know, from our above analysis, that such collaboration and research is a high-cost and high-time investment. However, cooperation can collectively strengthen the network and have a net positive effect. These positive effects include increased situational awareness of the cyber crime landscape, as well as more efficient detection of network breaches given the myriad ways that a network can be infiltrated. Information sharing is clearly incentive-compatible, while research action seems to be incentive-incompatible.

Given that research is time and cost-intensive, the use of honeypots could be a plausible alternative, as they are relatively low cost, but yet contribute to the database of knowledge as a precursor to research. Honeypots are traps set to counteract attempts at unauthorized use of information systems. They involve computers that seem part of the network but are actually isolated and monitored. These computers seem to contain information or resources of value to attackers, baiting hackers, from which the FS-ISAC can learn valuable information on the criminals' *modus operandi* and techniques. This is a collective, yet active mechanism, as it builds on the collective strength of the organization, is able to glean useful findings, but requires less active participation on the part of individual companies.

Research could be outsourced with stipulated individual investments in research expenditure. This way, the research process would be more coherent and equitable. While the above analysis only takes into account collaborative research, companies may be incentivized to conduct private research on top of that. This, while clearly serving to strengthen the individual company's system, also benefits the network as a whole, by virtue of the strong network effects in the cyber security market. A possible example of outsourced research includes the Interpol Global Complex for Innovation (IGCI), which is set to become operational in Singapore in 2014. This would definitely prove highly effective given that the IGCI would have access to information beyond industry and geographical borders. Research would allow threats to be pre-empted, and response and recovery facilitated.

Chapter 6

Conclusion

Modeling the respective markets in the LoJack and cyber crime markets have illuminated several key similarities. The incentive structures of both models are similar, with emphasis on contrasting marginal private benefits of investing in a LoJack and cyber security research respectively with the social benefits. Due to the fact that the risk of falling victim to an attack decreases with increased buy-in for both the LoJack and cyber security markets, both models demonstrate social benefits that far outweigh private benefits.

There is a clear disincentive for individuals in both markets to invest in the LoJack and cyber security research respectively. This is because of the private cost incurred to the individual – monetary cost of the LoJack and time and monetary costs of cyber security research – but yet zero marginal private gains since no attack has taken place yet. There is therefore a barrier against the initial investment.

However, we know that with each individual's investment in the market reduces the respective risks of crime, resulting in positive externalities. In the LoJack market, while an individual who chooses not to invest in a LoJack may reap the benefits of a lowered theft rate, he reaps no benefit if his car is targeted since it cannot be recovered easily without a LoJack. This itself serves as motivation for individuals to invest in a LoJack. On the other hand, companies who do not invest in cyber security research benefit from the lowered threat, and also reap the rewards of research conducted by other members of the network without needing to spend a single cent. Successful research by other companies help to strengthen the network as a whole, and members of the network who choose not to invest in research benefit from the increased security, effectively becoming free riders. Therefore, due to differences in the structure of externalities and network effects of the two models, the incentive effects are different.

Specific to the cyber crime market, assuming that sharing of information within the network incurs no cost, the model also shows that sharing of information among companies is optimal. The pooling of information helps improve situational awareness of the cyber crime landscape and therefore decreases the risk of falling victim to an attack. Furthermore, the model showed that the amount that companies are willing to invest in cyber security research is in fact a low constant, independent of the value they place on their information and of the current risk of attack. This again refers to the rampant existence of free riders within the market.

Applying these findings to the cyber crime market, we must acknowledge first and foremost that, although the sharing of information seems to be feasible and beneficial in the financial services industry, this is not easily transferrable to other industries, such as retail. Other industries lack economic incentives to cooperate and fear public backlash if information about their security breaches are leaked. In contrast, information security is such a key facet of the operations of financial institutions that their mutual interdependence forces them to cooperate.

On the research front, a possible alternative would be the use of honeypots. These honeypots can glean valuable information on attack vectors by posing as traps. This requires a collective contribution from each member of the FS-ISAC, but is owned by no one member, therefore alleviating the free rider and underprovision phenomena. Another plausible alternative would be to outsource research to international bodies, therefore allowing research contributions by each member to be more equitable.

In all, in modeling the market for cyber crime, it is evident that both sharing and investment in research is key for effective improvement in security. To combat the problem of free riders, it is important for the organization to set contractual terms such that members are bound to contribute to research in order to reap the full benefits of increased security. International bodies are also well-positioned to alleviate the free rider problem because not only are they impartial and less susceptible to incentive problems, they possess greater resources that can increase the effectiveness and holistic nature of their research.

Chapter 7

Bibliography

Abbas, Haider, Hemani, Ahmed, Magnusson, Christer & Louise Yngstrom. “A Structured Approach for Internalizing Externalities Caused by IT Security Mechanisms.” *2nd International Workshop on Education Technology & Computer Science* (2010).

Acquisti, Alessandro & Sasha Romanosky. “Privacy Costs & Personal Data Protection: Economic & Legal Perspectives.” *Berkeley Technology Law Journal.* Vol 24. No. 3. (2009)

Anderson, Ross. "Why information security is hard-an economic perspective."*Computer Security Applications Conference.* 358-365 (2003)

Anderson, Ross & Shailendra Fuloria. “Security Economics & Critical National Infrastructure.” *Economics of Information Security & Privacy.* (2010)

Anderson, Ross & Tyler Moore. “Economics & Internet Security: A Survey of Recent Analytical, Empirical & Behavioral Research.” *The Oxford Handbook of the Digital Economy, Oxford University Press.* (2011)

Anderson, Ross & Tyler Moore. "The Economics of Information Security." *Science*. Vol 314. (2006)

Anderson, Ross, Clayton, Richard & Tyler Moore. "The Economics of Online Crime." *Journal of Economic Perspectives.* Vol 23. No. 3. 3-20. (2009).

Andrijcic, Eva & Barry Horowitz. "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property" *Risk Analysis.* Vol 26. No. 4. (2006).

Arora, Ashish, Nandkumar, Anand & Rahul Telang. "Does Information Security Attack Frequency Increase With Vulnerability Disclosure? An Empirical Analysis." *Information Systems Frontiers.* Vol 8, No. 5. 350-362 (2006)

Aviram, Amitai & Avishalom Tor. "Overcoming Impediments to Information Sharing." *Harvard John M Olin Discussion Paper Series.* No. 427. (2003)

Ayres, Ian & Steven Levitt. "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack" *The Quarterly Journal of Economics.* Vol 113. No. 43-77(1998)

Bauer, Johannes & Michel van Eeten. "Cybersecurity: Stakeholder Incentives, Externalities & Policy Options." *Telecommunications Policy.* Vol 33. 706-719 (2009).

Bauer, Johannes & Michel van Eeten. "Economics of Malware: Security Decisions, Incentives & Externalities." *STI Working Paper* (2008).

Bauer, Johannes & Michel van Eeten. "Emerging Threats to Internet Security – Incentives, Externalities and Policy Implications." *Journal of Contingencies & Crisis Management*, Vol 17, No. 4. (2009).

Bauer, Johannes & Michel van Eeten. "Introduction to the Economics of Cyber Security." *Communication & Strategies.* No. 81 (2011)

Bolot, Jean & Marc Lelarge. "Cyber Insurance as an Incentive for Internet Security." *7th Workshop on the Economics of Information Security.* (2008)

Cook, Phillip. "Coproduction in Deterring Crime." *American Society of Criminology.* Vol 10. Issue 1. (2011)

Cordes, Joseph. "An Overview of the Economics of Cybersecurity & Cybersecurity Policy." *The George Washington University Cyber Security Policy & Research Institute.* (2011).

Gandal, Neil. "An Introduction to Key Themes in Cyber Security." *Tel Aviv University & CEPR.* (2006).

Gordon, Lawrence, Loeb, Martin & William Lucyshyn. "Sharing information on computer systems security: An economic analysis." *Journal of Accounting & Public Policy*. (2003) 461-485

Gorden, Lawrence & Loeb, Martin. "The Economics of Information Security Investment." *ACM Transactions on Information & System Security.* Vol 5, No. 4. (2002)

Grady, Mark & Francesco Parisi. "The Law and Economics of Cybersecurity: An Introduction." *The Law and Economics of Cybersecurity*. (2006)

Johnsen, Bruce & Supriya Sarnikar. "Cyber Security in the National Market System." *Rutgers Business Law Journal.* Vol 6. No 1. (2009)

Katz, Michael & Carl Shapiro. "Technology Adoption in the Presence of Network Externalities." *Journal of Political Economy.* Vol 94, No 4. (1986)

Kobayashi, Bruce. "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods." *Supreme Court Economic Review*. (2005)

Li, Xinghan. "Cybersecurity as a Relative Concept." *An International Journal.* Vol 18. 11-24 (2006)

Locke, Gary. "Cybersecurity, Innovation & the Internet Economy." *The Department of Commerce Internet Policy Task Force.* (2011)

Moore, Tyler. "Introducing the Economics of Cybersecurity" *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies & Developing Options for US Policy.*

Mulligan, Deirdre & Fred Schneider. "Doctrine for Cybersecurity." *Cornell University, University of California, Berkeley.* (2011)

Ozment, Andy & Stuart Schechter. "Bootstrapping the Adoption of Internet Security Protocols." *5th Workshop on the Economics of Information Security.* (2006)

Picker, Randal. "Cyber Security: Of Heterogeneity & Autarky." *The Law School of The University of Chicago.* (2004).

Powell, Benjamin. "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry" *Journal of Law, Economics & Policy.* Vol 1. No. 2 (2005)

Swire, Peter. "A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?" *Journal on Telecommunications and High Technology Law.* Vol 2. (2004)