The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy

Alfredo Garcia and Barry Horowitz
University of Virginia

February 25, 2006

Abstract

With the continuing growth of the use of the Internet for business purposes, the consequences of a possible cyber attack that could create a large scale outage of long time duration becomes a more and more serious economic issue. In this paper, we construct a game-theoretic model that addresses the economic motivations for investment in added Internet security and makes a case for a possible market failure in the form of underinvestment in the provision of Internet security. This result relies on the fact that the social value derived from consumption (which is at least equal to a fraction of the surplus derived from e-commerce) greatly exceeds the revenue at stake associated with the telecommunications companies' and ISP's security levels. If the ratio of social value to revenue at stake to Internet providers continues to grow, the likelihood of underinvestment in security becomes higher and some form of regulation may become necessary. We discuss the difficulties associated with designing and enforcing a regulatory scheme based upon mandatory security standards.

Keywords: Internet Security, Market Failure, Game Theory, Nash Equilibrium, Markov Perfect Equilibrium.

1 Introduction

With the continuing growth of the use of the Internet for business purposes[1], the consequences of a possible cyber attack that could create a large scale outage of long time duration becomes a more and more serious economic issue. Two recent cyber security events have raised concerns about the risks of a large-scale, possibly long lasting cyber attack on the Internet (see Garza (2005) and Zetter (2005)). These events were: 1) CISCO communications router software was stolen, recognizing that CISCO routers constitute 70% of Internet routers, and 2) a subsequent technology demonstration of a cyber attack (based on knowledge of that software) that could tamper with messages going through routers. The possibility of creating an important Internet outage raises the question of how long would it take to restore such an outage. In 1998, ATT had reported an incident involving a software flaw that affected its frame-relay network, causing a service disruption. This event required restoration of a number of switches through a software patch. ATT indicated that complete restoration required 26 hours (see ATT (1998)). While it is speculation, one can readily imagine that restoration of a large segment of the Internet, involving a number of service providers and telecommunications companies, would likely take much longer. This confluence of growing consequences and plausible scenarios of cyber attacks with significant macro-economic consequences raises questions about investment in added cyber security in response to the growing risk, recognizing that the Internet is part of the nation's critical infrastructure.

In 2003, the President's National Strategy to Secure Cyberspace (see White House (2003)) stated that government action is warranted where alleged "market failures result in underinvestment in cyber security". However, there is a lack of empirical evidence and/or theoretical support for such "market failure". While there exists a large body of technical literature on cyber security, research on the economics of cyber security is still on its very early stages (see for instance, Anderson (2001), Cave and Mason (2001), Gordon and Loeb (2002), Kannan and Telang (2005) and Gal-Or and Ghose (2005)).

This paper provides a game-theoretic model that addresses the economic motivations for investment in added Internet security and makes a case for a possible market failure in the form of underinvestment in the provision of Internet security. While investments in security by Internet Service Providers (ISP's) and telecommunications companies are in a sense, "unproductive" (i.e. no new value is created), they have a strategic dimension: a firm that has been subject to successful cyber attacks may see its market share negatively affected, as some customers may switch to another service provider. In our model, an ISP with a higher level of security is able to earn a higher expected revenue. However, the expected revenue gains resulting from investments in security, decrease as

[1] According to the US Census Bureau, for the second quarter of 2005, e-commerce retail sales amounted to $21.1 billion, roughly 2.2% of all retail sales (see US Census Bureau (2005)).

competitors increase their security levels.

Motivated by the economic analysis results presented in this paper, a discussion is presented on the complexities associated with the design of cyber security regulations that might address the economic issues. The paper highlights and discusses particular aspects of the cyber security domain that make the design of regulations especially difficult. These include issues of security measurement, high variability of the cost to satisfy regulations based on variable technical integration complexities, industrial readiness of key providers of Internet components in terms of their technical capability and availability of resources, and the continuous nature of cyber attackers learning how to overcome previously viable defenses.

The structure of the paper is as follows. In section 2 we develop a simple, but illuminating, strategic model for investments in cyber security that are motivated by competition for revenue. In section 3, this model is extended to account for the continuing depreciation of cyber security defenses due to the continuing advancements in exploitation software. In section 4, we identify conditions under which equilibrium investments differ from the socially optimal level of investment. This result relies on the fact that the social value derived from consumption (which is at least equal to a fraction of the surplus derived from e-commerce) greatly exceeds the revenue at stake associated with the telecommunications companies and ISP's security levels. Since investments in Internet security are in the control of the providers and there is little vertical integration in e-commerce, the likelihood of underinvestments in security emerges as public policy issue that may justify some form of regulation. In section 5, the paper concludes by discussing the difficulties associated with designing and enforcing a regulatory scheme based upon mandatory security standards.

2 A Simple Illustrative Game

We consider a setting in which firms plan for long-term security investments taking into account the likelihood of cyber-attacks. We restrict our attention to attacks that may cause significant service disruption and consequently, reductions in a firm's customer base. A firm (i.e. an ISP or telecommunications company) that incurs an added cost F in security has a probability α of successfully protecting itself when attacked. If a firm does not make this added investment, the probability of a vulnerability being exploited is $1 - \beta$ (we assume $\alpha > \beta$). Let us assume the revenue "at stake" is denoted by V. In words, this is the revenue associated with customers that are sensitive to security failures. Under normal operating conditions (i.e. no cyber attacks), in a market with two symmetric firms, firms share V equally. However, when attacked and with only one firm successfully withstanding the attack, all revenue V is accrued by this one firm.

Let $R(\alpha, \beta)$ denote firm 1's expected revenues if only this firm invests in security. Conditional upon

successful protection, firm 1 revenues are given by:

$$E[\,R(\alpha,\beta)|\text{ “firm 1 withstands attack”}] = \begin{cases} V & \text{with prob. } 1-\beta \\ \\ \frac{V}{2} & \text{with prob. } \beta \end{cases}$$

Let us denote by t the probability of a cyber attack. Firm 1's expected revenue is:

$$R(\alpha,\beta) = \alpha t[(1-\beta)V + \beta\frac{V}{2}] + (1-t)\frac{V}{2}$$

Similarly, the expected revenue for firm 1 when only this firm does not invest in security is:

$$R(\beta,\alpha) = \beta t[(1-\alpha)V + \alpha\frac{V}{2}] + (1-t)\frac{V}{2}$$

If both firms invest in security then their expected revenue is

$$R(\alpha,\alpha) = \alpha t[(1-\alpha)V + \alpha\frac{V}{2}] + (1-t)\frac{V}{2}$$

Finally, if no firm invests in software, expected revenues are

$$R(\beta,\beta) = \beta t[(1-\beta)V + \beta\frac{V}{2}] + (1-t)\frac{V}{2}$$

Here, a few words on the structure of the function R are warranted. First, we remark that $R(\alpha,\alpha) > R(\beta,\beta)$, i.e. expected revenues are increasing in symmetrically adopted levels of security. Also, the expected revenue gains resulting from investments in security, i.e. $R(\alpha,\cdot) - R(\beta,\cdot)$ decrease as competitors increase their security levels. That is;

$$R(\alpha,\beta) - R(\beta,\beta) > R(\alpha,\alpha) - R(\beta,\alpha)$$

A similar structure of revenue can also be found in the literature on competition and quality of service (see for instance Shapiro (1983)). The basic premise of this literature is that customers react to low levels of quality of service by switching to other providers. This effect takes place even if quality of service is imperfectly observed, as other observables such as price and customer base, serve as informative signals for quality.

2.1 Nash Equilibrium

After deriving the expected revenue function R, we introduce the investment game (in normal form):

	Invest	Do Not
Invest	$(R(\alpha,\alpha)-F; R(\alpha,\alpha)-F)$	$(R(\alpha,\beta)-F; R(\beta,\alpha))$
Do Not	$(R(\beta,\alpha); R(\alpha,\beta)-F)$	$(R(\beta,\beta); R(\beta,\beta))$

Both firms invest in security in a Nash equilibrium iff $R(\alpha,\alpha) - F \geq R(\beta,\alpha)$. That is,

$$\alpha t[(1-\alpha)V + \alpha\frac{V}{2}] - F \geq \beta t[(1-\alpha)V + \alpha\frac{V}{2}]$$

Or equivalently,

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{V}\frac{1}{\beta t(1-\frac{\alpha}{2})} \tag{1}$$

Condition (1) simply states that the gain in security as measured by $\frac{\alpha}{\beta}$ must compensate the (relative) investment cost, as measured by $\frac{F}{V}$. The required compensation increases exponentially as $\beta t \to 0$. Note also that when β is close to 1, the condition requires that $\frac{\alpha}{\beta} \gtrsim 1 + \frac{2}{t}\frac{F}{V}$.
If $R(\beta,\beta) \geq R(\alpha,\beta) - F$ then in equilibrium *no firm* invests in security. This condition is equivalent to:

$$\frac{\alpha}{\beta} \leq 1 + \frac{F}{V}\frac{1}{\beta t(1-\frac{\beta}{2})}$$

Note that

$$\frac{1}{1-\frac{\beta}{2}} < \frac{1}{1-\frac{\alpha}{2}}$$

since $\alpha > \beta$. This means that whenever

$$1 + \frac{F}{V}\frac{1}{\beta t(1-\frac{\beta}{2})} < \frac{\alpha}{\beta} < 1 + \frac{F}{V}\frac{1}{\beta t(1-\frac{\alpha}{2})}$$

there is a symmetric equilibrium in mixed strategies[2] (see Appendix 6.1). Finally, we note that assuming risk averse players may increase the range of parameters for which a full investment equilibrium applies. However, this effect is negligible for small values of t. For tractability, we leave out this effect in our comparison of private vs. social incentives to invest.

2.2 Numerical Illustration

In order to illustrate the results presented above, an example is provided. Assume that two ISP companies are competing in a geographical region for a common customer base. According to *Factiva* (www.factiva.com) the national ISP market was about $\$50bb$ per year in 2003. Additionally, *ISP Planet* (see www.isp-planet.com) reports that in 2005, 21 companies captured about 70% of the national ISP market. For the example, assume each of the companies has a revenue base of $\$2bb$ (about the average for the top companies). Assume that the revenue at stake, V, is 10% of total revenue, $\$200mm$. Assume that the likelihood of a credible attack, t, for both companies is .95 over a five year period. Assume that there is an increase in cost for security to go from a β level of protection to an alpha level of protection that is spread evenly over a five year period for a total of $\$50mm$ (i.e., $F = \$50mm$). For this example, we introduce a new parameter, $\rho = \frac{1-\alpha}{1-\beta}$, where ρ is the reduction in likelihood of a successful attack due to the increased investment in security, F.

[2] There are also asymmetric equilibria where only one firm invests in security.

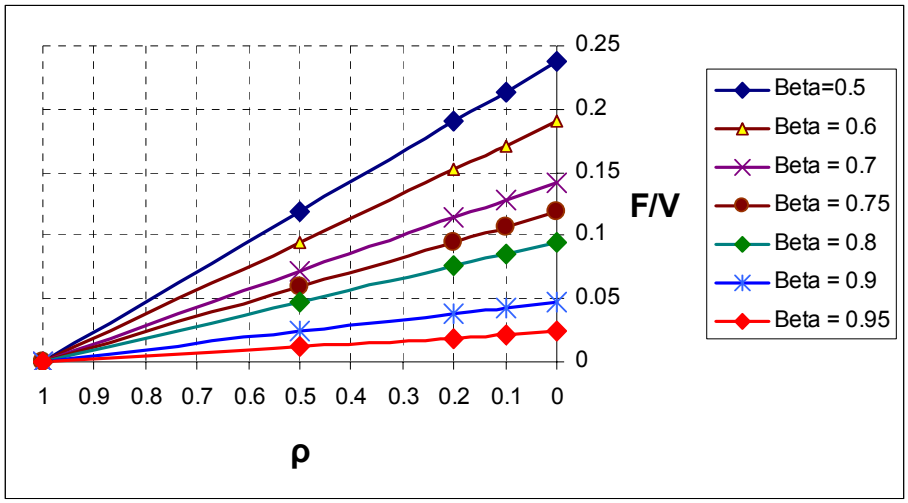

Figure 1: $\frac{F}{V}$ vs. improvement in security

Figure 1 presents the relationship between the decision thresholds for investment in added security ($\frac{F}{V}$) versus the required reduction in the likelihood of a successful attack (ρ), with β as a variable and alpha approaching values close to 1. From Figure 1 it can be seen that if, for example, the increased investment in security, F, is expected to reduce the likelihood of successful attacks by half, and if beta is .75, the decision threshold for investment in security is 6% (i.e., the five year cost of security must be less than 6% of the revenue at stake). For the example, since the revenue at stake is $\$200mm$ for each company, the maximum acceptable incremental cost for added security is $\$12mm$ over 5 years. Since the incremental cost for this example is $\$50mm$, the companies would decline making the added investment. Note from Figure 1 that as β increases, for any given value of improvement, m, the decision threshold decreases, so that there is a lower and lower interest in further improvements as the level of protection increases. For example, from Figure 1, using the example presented above, but changing β to 0.8 results in a decision threshold reduction to 4.75%, or $\$9.5mm$ as the maximum acceptable cost for the five year period.

2.3 The Effect of More Competitors

Let us suppose we have $N+1$ symmetric firms. If all firms invest in software security, a firm's revenue (if successfully protected), are given by

$$E[R(\alpha,N)|\text{ "firm 1 withstands attack"}] = \begin{cases} V & \text{with prob. } (1-\alpha)^N \\ \vdots & \\ \frac{V}{n+1} & \text{with prob. } \left(\begin{array}{c} N \\ n \end{array}\right)\alpha^n(1-\alpha)^{N-n} \\ \vdots & \\ \frac{V}{N+1} & \text{with prob. } \alpha^N \end{cases}$$

where $0 < n < N$. Thus, its expected revenue is

$$R(\alpha,N) = \alpha t E[V(\alpha,N)] + (1-t)\frac{V}{N+1}$$

where

$$E[V(\alpha,N)] = \sum_{n=0}^{N} \frac{V}{n+1}\left(\begin{array}{c} N \\ n \end{array}\right)\alpha^n(1-\alpha)^{N-n}$$

Similarly, if firm 1 does not invest while other firms do, its expected revenue is given by:

$$R(\beta,N) = \beta t[E[V(\alpha,N)] + (1-t)\frac{V}{2}$$

If $R(\alpha,N) - F \geq R(\beta,N)$ investment by all firms is a Nash equilibrium. This condition translates into

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{E[V(\alpha,N)]}\frac{1}{\beta t} \tag{2}$$

Note that $E[V(\alpha,N)]$ is monotonically decreasing in N. Hence, a larger number of competitors *weakens* the incentive to invest and the condition for a Nash equilibrium in which *all* firms invest becomes more stringent. In particular, for $\beta \simeq 1$, $E[V(\alpha,N)] \simeq \frac{V}{N+1}$ and condition (2) requires that $\frac{\alpha}{\beta} \gtrsim 1 + \frac{N+1}{t}\frac{F}{V}$. This leads to the interesting result that should the number of Internet providers rise, the orientation toward Internet security investments would likely decrease.

2.4 Numerical Illustration

In order to illustrate the results of the effects of multiple competing companies, we return to the example of Section 2.1. From the earlier example involving two competitors the threshold $\frac{F}{V}$ was shown to be $\$12mm$ for beta equal to 0.75. When there are four competing companies it can be seen that the decision threshold, $\frac{F}{V}$ reduces by half for the same improvement value of ρ, to about $\$6mm$. This serves to demonstrate that as the ISP market becomes more and more competitive, it would follow that the investment of individual companies in security of the Internet would be reduced.

3 Depreciation and Investment Dynamics

Let us now extend our model to capture some of the dynamic features of investments in security. Specifically, we are interested in studying the effects of depreciation or obsolescence associated with new attacks and/or new vulnerabilities being developed and/or exploited. Depreciation is a very important aspect of cyber security, since software exploitations are continually under development by potential attackers, and results are often posted on the Internet for others to refine into even more enhanced attack capabilities. We shall restrict our attention to investment policies that are a function of the current level of security as measured by the probability of successful protection (e.g. α, in the case of investment and β, the status-quo level). In this sense, we define a "state" variable $s = (x, y)$ with $x, y \in \{\alpha, \beta\}$. If the state of the system is $s = (\alpha, \alpha)$ and firms *do not* invest in cyber security, then with probability $q \in (0, 1)$ the state variable transitions to (β, β). Likewise, with probability $1 - q$ the state remains at (α, α). In words, if firms do not invest, depreciation occurs with probability q, implying that current infrastructure in cyber security becomes outdated (i.e. the probability of a successful attack is $1 - \beta$).

We are interested in Markovian strategy combinations that have the following property: at every time period, for any given state, no firm can do strictly better by choosing a different decision than the one prescribed by the strategy combination under consideration. This concept known as Markov Perfect Equilibrium (MPE) formalizes a notion of recursive rationality, i.e. play prescribed by the strategies from any state off the equilibrium path must also be in equilibrium (see Chapter 13 on Fudenberg and Tirole (1991) and Maskin and Tirole (2001)). As a refinement of Nash equilibrium, this solution concept filters out all "non-credible" Nash equilibria, i.e., those equilibrium strategies supported upon the basis of irrational play off the equilibrium path. A second advantage of MPE pertains to the simplicity of Markovian strategies which substantially reduces the number of parameters to be estimated in dynamic econometric models (see for instance, Ericson and Pakes (1995)). In the analysis that follows, we take an "inverse" approach to equilibrium analysis, that is, we identify sufficient conditions for parameter values that lead to a given equilibrium strategy combination. However, there may be parameter combinations for which multiple equlibria exist.

Let us first analyze the investment strategy in which the firms *constantly* update their cyber security infrastructure (that is, they incur investment cost F at *all* time periods). Let $v(x, y)$ denote firm 1's present value of profits when firms adhere to this strategy. It follows that

$$v(\alpha, \alpha) \quad = \quad R(\alpha, \alpha) - F + \gamma v(\alpha, \alpha) \tag{3}$$

where $\gamma = \frac{1}{1+r}$ is the discount factor and r stands for the cost of capital. Typically for cyber security investments the major cost of capital is opportunity costs; i.e., the use of the capital for purposes of achieving corporate growth. this can take the form of investments in increasing sales

staff, increasing advertising, increasing R&D, etc. To check that the strategy under consideration is an equilibrium, we consider a deviation in which firm 1 abstains from investing. In this situation, with probability q, the state becomes (β, α) and with probability $1-q$, the state becomes (α, α). To ensure that it is not profitable for firm 1 to deviate (not investing) we must ensure the following incentive compatibility constraint holds:

$$\begin{gathered} -F + \gamma v(\alpha, \alpha) \\ \geq \\ \gamma[qv(\beta, \alpha) + (1-q)v(\alpha, \alpha)] \end{gathered}$$

Note that

$$v(\beta, \alpha) \quad = \quad R(\beta, \alpha) - F + \gamma v(\alpha, \alpha) \tag{4}$$

Using (3) and (4) it can be seen that the incentive compatibility constraint is equivalent to:

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{V} \frac{1}{\beta t(1 - \frac{\alpha}{2})} \frac{1+r}{q} \tag{5}$$

Conditions (5) formalizes the interplay between the likelihood of depreciation or obsolescence and the incentives to invest. The lower the likelihood of depreciation, the more stringent the compensation on the relative gain of security as a function of the relative investment cost in order for a strategy of *constant updating* of cyber security to be in equilibrium.

When condition (5) is not satisfied, the firms do not have the incentives to maintain a high level of cyber security at *all* times. Let us consider a more flexible investment strategy under which firms invest (i.e. update their cyber security) only when they are "outdated" (i.e. the probability of a successful attack is $1-\beta$)[3]. The associated "bubble" diagram in shown in Figure 2. The state transitions can be summarized as follows: in state (α, α) firms do not invest and depreciation takes place with probability q leading to state (β, β). With probability $1-q$ the state remains at (α, α). Thus,

$$v(\alpha, \alpha) \quad = \quad R(\alpha, \alpha) + \gamma[qv(\beta, \beta) + (1-q)v(\alpha, \alpha) \tag{6}$$

In state (β, β) firms invest and reach state (α, α) after one period. Thus,

$$v(\beta, \beta) \quad = \quad R(\beta, \beta) - F + \gamma v(\alpha, \alpha) \tag{7}$$

In state (α, β), only firm 2 invests, thus with probability q firm 1's security infrastructure becomes outdated, i.e. the state reached is (β, α). With probability $1-q$, both firms will be "up to date"

[3]Note that investments in security can be seen as "negative" R&D: no new value is created but there is a higher chance of incurring losses if no investment is undertaken. This analogy is limited as equilibrium in R&D can be characterized by "leapfrogging" (see Giovannetti (2001)). This differs from the "invest when outdated" equilibrium analyzed here.

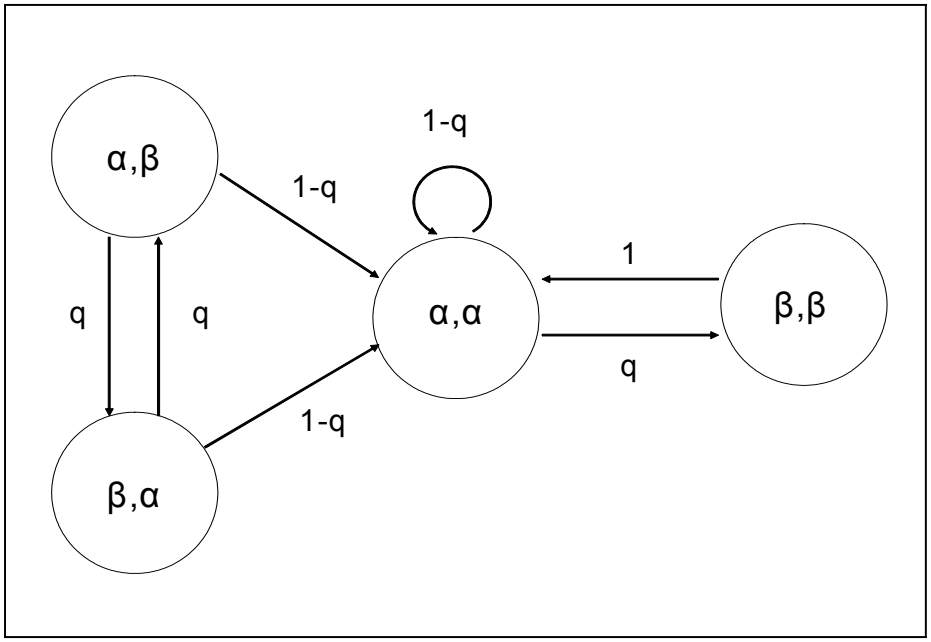

Figure 2: State-transition diagram under the strategy combination in which players invest only if cyber security infrastructure is "outdated"

at the beginning of next period. Thus,

$$v(\alpha,\beta) \quad = \quad R(\alpha,\beta) + \gamma[qv(\beta,\alpha) + (1-q)v(\alpha,\alpha)] \tag{8}$$

and:

$$v(\beta,\alpha) \quad = \quad R(\beta,\alpha) - F + \gamma[qv(\alpha,\beta) + (1-q)v(\alpha,\alpha)] \tag{9}$$

For this strategy to be in equilibrium we must check that there are no incentives to deviate. First, when in state (α,β), we must check that there is no incentive for firm 1 to invest, that is,

$$-F + \gamma v(\alpha,\alpha) \leq \gamma[qv(\beta,\alpha) + (1-q)v(\alpha,\alpha)]$$

As shown in the Appendix 6.2, this is equivalent to:

$$\frac{\alpha}{\beta} \leq 1 + \frac{F}{V}\frac{1}{\beta[1-\frac{\alpha}{2}-\gamma q(1-\frac{\beta}{2})]}\frac{1+r}{qt} \tag{10}$$

This condition is sufficient to ensure that investment in state (α,α) is also not profitable as long as $\beta > \frac{1}{2}$ (see Appendix 6.3). We finalize by checking that abstaining from investing when in state (β,β) does not constitute a profitable deviation from the investment strategy under consideration. The associated condition is:

$$\gamma v(\beta,\alpha) \leq -F + \gamma v(\alpha,\alpha)$$

which translates into (see Appendix 6.4)

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{V} \frac{1}{\beta[1 - \frac{\alpha}{2} - \gamma q(1 - \frac{\beta}{2})]} \frac{1+r}{\theta t} \tag{11}$$

where $\theta = [1 - \gamma + \gamma(q(1-q)]^{-1} > 1$.

Note that as $q \to 0$, conditions (10) becomes less stringent. Intuitively, as the prospect of depreciation diminishes the incentive to invest also weakens. Conversely, as $q \to 0$, condition (11) captures that fact that the relative gain in security afforded by investing must increase.

4 Socially Optimal Investments

In the above analysis, we have focused on the investment incentives faced by Internet Service Providers (ISP's) and telecommunication companies, whose combined technology components constitute the Internet. In this section, we explore optimal investments from a social standpoint. That is, investment that maximize the difference between the expected social surplus (derived from businesses and consumers that make use of the Internet as a channel for commerce) and investment costs.

4.1 The Simple Illustrative Game Again

Let us denote by S, the social value derived from Internet usage. Let $W(N)$ denote the expected social welfare (S + the ISP's surplus) when a total of N ISP's have invested in security and $N \in \{0, 1, 2\}$. Under normal operating conditions (i.e. no cyber attacks) a transfer V from consumers to the Internet Service Providers takes place. If a cyber attack takes place, this transfer does not occur if the two firms fail.

Let $p(N)$ denote the probability that the transfer V from consumers to producers takes place, when N firms have invested in cyber security. Conditional upon an attack taking place, we have:

$$E[p(N)|\text{ “firms under attack”}] = [1 - (1-\alpha)^N (1-\beta)^{2-N}]$$

It follows that

$$p(N) = t[1 - (1-\alpha)^N (1-\beta)^{2-N}] + (1-t)$$

and

$$W(N) = S \times p(N) - F \times N$$

If $W(2) \geq W(1)$, investment by both firms is optimal from a social standpoint. This is equivalent to

$$S[p(2) - p(1)] \geq F \tag{12}$$

Since $p(2) - p(1) = t(1-\alpha)(\alpha - \beta)$ this is equivalent to:

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{S}\frac{1}{\beta t(1-\alpha)} \tag{13}$$

After comparing conditions (1) and (13), we conclude whenever $S(1-\alpha) > V(1-\frac{\alpha}{2})$, or equivalently

$$\frac{S}{V} > 1 + \frac{1}{2}\frac{\alpha}{1-\alpha} \tag{14}$$

condition (1) is more restrictive than (13). Thus, a situation may arise under which investment by both firms is socially optimal yet it is not undertaken by both firms in equilibrium (i.e. there may be *under*-investment in cyber security). In other words, *under*-investment in cyber security is more likely in industries where the social value derived from consumption substantially exceeds industry revenue and the protection probability α is not high enough. Conversely, whenever

$$\frac{S}{V} < 1 + \frac{1}{2}\frac{\alpha}{1-\alpha}$$

condition (13) is more restrictive than (1). In other words, in equilibrium there may be *over*-investment in cyber security.

4.2 Numerical Illustration

In order to illustrate the potential for under investment in Internet security by ISP's when considered through the economic perspectives of e-commerce and other e-businesses, consider the potential for a substantial Internet failure of the sort inspired by the discussion in Section 1 pertaining to stolen Cisco router software. Using equation (14) above, the value of V would be the lost revenue to ISP's due to a substantial Internet outage. Using the Section 2.1 annual revenue assumption for ISP's of \$50*bb*, an assumed Internet outage of one week, and a policy of making refunds for downtime to customers (assumed to be $\frac{1}{52}$ of annual revenue, i.e. one week out of 52), the resulting integrated revenue loss to all ISP's would roughly be \$1*bb*. If for the same incident, one assumes that there was an average 6 month loss of 1% of the Internet business market including retail sales, business-to-business sales, advertising, etc. (total market of \$1.7 tt/year for 2003 according to US Census Bureau) due to consumer shifts to brick and mortar companies, and other lost revenue opportunities (e.g., one week's loss of advertising banner revenue), S would equal \$8.5*bb*. Accordingly, $\frac{S}{V}$ would equal 8.5. From equation (14), for α equal to 0.9 the ratio of $\frac{S}{V}$ where one could start to expect under investment from ISP's would be 5.5. As a result, for the scenario portrayed above, one could anticipate that security investments would be less than the e-business community would desire.

The result clearly depends on the assumptions of duration of outage, shifts in market, temporary losses of markets and other difficult to predict or validate factors. Nonetheless, it seems clear that

as e-business continues to grow (e.g., according to the US Census Bureau e-commerce retail sales have tripled over the five year period between 2000 -2005), the potential for underinvestment is likely to grow with it, indicating that a better understanding of the elusive parameters needs to be developed. In fact, if one accepts the premise that the Internet provides an economy of scale, then the ratio of e-business to provider revenues will continue to grow and the liklihood of eventually arriving at a point of security underinvestment becomes more and more likely.

4.3 Optimal Investment Dynamics

Let us assume we start from the (α, α) state. From a social standpoint, a strategy of constant updating of cyber security infrastructure yields a expected social surplus of

$$W(2) + \gamma W(2) + \gamma^2 W(2) + \ldots = \frac{W(2)}{1-\gamma} \tag{15}$$

In a more flexible strategy, in which firms invest (i.e. update their cyber security) only when they are "outdated". Let us denote by W_α and W_β, the welfare under the flexible strategy when the initial state is (α, α) and (β, β). It follows that

$$\begin{bmatrix} W_\alpha \\ W_\beta \end{bmatrix} = \begin{bmatrix} W(2) \\ W(0) \end{bmatrix} + \gamma \begin{bmatrix} 1-q & q \\ 1 & 0 \end{bmatrix} \begin{bmatrix} W_\alpha \\ W_\beta \end{bmatrix}$$

After solving this system of equations, we obtain

$$W_\alpha = \frac{W(2) + \gamma q W(0)}{1 - \gamma(1 - q(1-\gamma)} \tag{16}$$

Thus, a policy of constant updating is socially optimal whenever the value in (15) is at least equal to the value in (16). The reader can verify that this is equivalent to $W(0) \leq W(2)$. A sufficient condition for this condition is (see Appendix 6.5):

$$\frac{\alpha}{\beta} \geq 1 + \frac{F}{S} \frac{1}{\alpha t (1-\alpha)} \tag{17}$$

Let us now compare conditions (17) and (5). Note that if

$$\frac{S}{V} > \frac{\beta}{\alpha} \frac{1 - \frac{\alpha}{2}}{1-\alpha} \frac{q}{1+r}$$

the condition (5) is more stringent. Hence, for a wide range of parameters *both* firms will not invest in equilibrium, while this is optimal from a social standpoint. Note also that while the condition for social optimality of constant updating (i.e. (17)) is independent of depreciation (i.e. the probability q), the condition for constant updating in equilibrium (i.e. (5)) is highly sensitive to depreciation. It is therefore possible that for low values of q, both firms do not invest in equilibrium while

they should do under the socially optimal investment strategy. Another parameter that affects individual firms' decisions is the cost of capital r. A strategy of constant updating is less likely to be in equilibrium, the higher the cost of capital r. This parameter does not play a role in determining whether such an investment strategy is optimal from a social standpoint.

5 Implications for Regulatory Policy

We have presented a game-theoretic model of investments in security by Internet Service Providers. The model sheds light on the conditions for a "market failure" in the sense of under-investment in equilibrium. On the one hand, as shown through the examples, plausible parameter values lead to a conclusion of underinvestment by Internet providers. On the other hand, these parameters can be adjusted so that the conclusion is that Internet providers adequately invest in security. Thus, further empirical research is necessary at this point to be able to ascertain the validity of our model. However, if the internet provides an economy of scale, the ratio of social value to revenue at stake will continue to grow and underinvestment in security becomes more and more likely. Consequently, some form of regulation may eventually become necessary.

However, the choice of the most appropriate regulatory scheme in this setting is by no means a straightforward task. Typically, regulatory instruments can be classified in two camps: "technology-based" or "performance-based" (see Breyer (1982) and Viscusi (1983)). In the former, regulators mandate specific technologies and/or practices while in the latter they require that firms achieve (or avoid) certain outcomes. Sometimes the actual regulatory framework is a hybrid. For example, the Occupational Safety and Health Administration (OSHA) regulates businesses that operate toxic, reactive, and flammable chemicals by undertaking extensive risk analysis[4] and evaluation of operational procedures aimed at mitigating risks. The U.S. Environmental Protection Agency (EPA) has implemented a similar scheme designed to protect the public from the accidental release of hazardous chemicals (see Chinander, Kleindorfer and Kunreuther (1998)). In strict sense, it appears as if neither a technology-based nor a performance-based scheme can be used for regulating the provision of Internet security. This is due essentially to the following unique features associated with Internet security: 1) the inability to measure levels of security (which makes it impossible to define quantitative standards), 2) evolving potential for cyber attackers to identify weaknesses in existing security, 3) the potentially high costs for implementing security that are related to integration with existing systems that vary from company to company, 4) the ranking of security risks that are dependent on the system designs that vary from company to company, 5) the wide

[4]Risk analysts (see for instance, Haimes (2005)) point to the fundamental measurements of risk being identified by the following three questions that serve to measure risk: 1) What can go wrong?, 2) What are the consequences?, and 3) What are the likelihoods?

variation in the technical and financial readiness to financially support security of companies that support the Internet infrastructure.

5.1 Measuring Security

For cyber attacks, the information technology community has developed and matured techniques for identifying system vulnerabilities that can potentially be exploited by attackers. However, little data is available to help in the determination of the likelihoods of a particular attack, both with and without additional security measures. Furthermore, these likelihoods vary with time, as potential attackers learn about protective technologies and eventually may be able to exploit existing weaknesses. With regard to consequences of cyber attacks, the cyber security community recognizes that they can take on many dimensions whose values vary from company to company. For example loss of reputation, loss of money, legal liabilities, loss of intellectual property, etc. can all be consequences of an attack, and different companies place different values on these consequences. As a result, regulation would need to be built upon approaches that deal with these complexities.

5.2 Learning Curve for Cyber Attacks

Cyber attackers typically derive exploiting software through trial and error based developments. As a result, one can expect the answers to the risk analysis questions presented above to vary with time. However, existing data does not support the derivation of depreciation factors for protection software, resulting in an important uncertainty in decisions related to selection of security solutions. In addition, the possibility of insider attacks can include insiders from the software provider companies as well as the companies seeking protection, resulting in significant uncertainty in decision-making about security. Section 4 above discusses depreciation rate for security technology as a important variable. It can be seen that an error in knowing the depreciation rate can lead to significant errors in cost estimation. While in some cases the security vendors suffer the costs, if errors in predicting depreciation are large, one can reasonably expect a less aggressive activity by them in response to problems, and ultimately expected price increases.

5.3 Security Integration into Systems

The risks of a cyber attack discussed above depend on the design of the information system being attacked as well as the security solutions that are a part of the system. When one combines the system design variations that exist from company to company with the variable costs for integration of security solutions with the varying measurement parameters that are part of security, it becomes clear that there would be great difficulty in finding universally agreed upon security needs that

would be preemptive. As a result one can expect that the regulations would likely be driven toward being responsive to historical attacks as opposed to focusing on future high risk possibilities.

5.4 Industrial Readiness

The Internet is provided by a wide range of companies when measured by size or technical capability. For example the companies that are Internet registrars under the Internet Corporation for Assigned Names and Numbers (ICANN) can be very small compared to the largest ISP's that are multi-billion dollar companies. This size variation typically brings with it less of an internal staff with the required skills and experience to focus on cyber security as a special area of business concern, as well as less of a budget to focus on the implementation of security solutions. This issue of size differences is highlighted in a scoping study conducted by the National Research Council of the National Academies (2003) as a major factor in considering possible regulation of cyber security in the freight transportation area.

6 Conclusions

We have presented a game-theoretic model that addresses the economic motivations for investment in added Internet security and makes a case for a possible market failure in the form of underinvestment in the provision of Internet security. This result relies on the fact that the social value derived from Internet use (which is at least equal to a fraction of the surplus derived from e-commerce) greatly exceeds the revenue at stake associated with the telecommunications companies' and ISP's security levels. While further empirical research is necessary at this point to be able to ascertain the validity of our model and given the scant level of vertical integration in e-commerce, it seems plausible that the ratio of social value of Internet use to revenue at stake to Internet providers will continue to grow. Thus, underinvestment in security becomes more and more likely. Consequently, if in the near future, vertical integration in e-commerce does not take place, some form of regulation may eventually become necessary and will very likely be "process oriented": i.e., Internet provider companies would need to produce a standardized analysis of security risks that identifies and ranks risks from their users' perspective and propose investment plans to mitigate these risks. While we can not predict the future needs for such regulation, this paper points to the pressing need and direction for more research on these issues.

7 Appendix

7.1 Derivation of Mixed-strategy equilibrium

Let p the probability with which a player is to invest in equilibrium. Indifference requires:

$$pR(\alpha,\alpha) + (1-p)R(\alpha,\beta) - F$$
$$=$$
$$pR(\beta,\alpha) + (1-p)R(\beta,\beta)$$

After algebraic manipulation, the reader can verify that $p \in (0,1)$ is such that

$$\frac{\alpha}{\beta} = 1 + \frac{F}{V}\frac{1}{\beta t[p(1-\frac{\alpha}{2}) + (1-p)(1-\frac{\beta}{2})]}$$

7.2 Derivation of (10)

The required condition can be rewritten as:

$$\gamma q[v(\alpha,\alpha) - v(\beta,\alpha)] \leq F \tag{A.1}$$

Using (6) and (9) we obtain

$$v(\alpha,\alpha) - v(\beta,\alpha) = t(\alpha-\beta)(1-\frac{\alpha}{2})V + F + \gamma q[v(\beta,\beta) - v(\alpha,\beta)]$$

Similarly, using (7) and (9)

$$v(\beta,\beta) - v(\alpha,\beta) = t(\beta-\alpha)(1-\frac{\beta}{2})V - F + \gamma q[v(\alpha,\alpha) - v(\beta,\alpha)]$$

Thus, $A.1$ can be rewritten as

$$\frac{\gamma q t(\alpha-\beta)[(1-\frac{\alpha}{2}) - \gamma q(1-\frac{\beta}{2})]V}{1-\gamma^2 q^2} \leq \frac{F}{1+\gamma q}$$

This equivalent to

$$\frac{\gamma q t(\alpha-\beta)[(1-\frac{\alpha}{2}) - \gamma q(1-\frac{\beta}{2})]V}{1-\gamma q} \leq F$$

7.3 Sufficiency of (10) when in (α,α)

We must check that

$$-F + \gamma v(\alpha,\alpha) \leq \gamma[qv(\beta,\beta) + (1-q)v(\alpha,\alpha)]$$

Since

$$v(\alpha,\alpha) - v(\beta,\beta) = \frac{t(\alpha-\beta)(1-\frac{\alpha+\beta}{2})V + F}{1+\gamma q}$$

the above condition is thus equivalent to

$$\frac{\alpha}{\beta} \leq 1 + \frac{F}{V} \frac{1}{\beta[1 - \frac{\alpha+\beta}{2})]} \frac{1+r}{qt}$$

Hence, condition (10) is more restrictive provided $\beta > \frac{1}{2}$.

7.4 Derivation of (11)

The condition $\gamma v(\beta, \alpha) \leq -F + \gamma v(\alpha, \alpha)$ is equivalent to:

$$\gamma \left[v(\alpha, \alpha) - v(\beta, \alpha) \right] \geq F$$

From before we know

$$\gamma \left[v(\alpha, \alpha) - v(\beta, \alpha) \right] = \frac{\gamma t(\alpha - \beta)[(1 - \frac{\alpha}{2}) - \gamma q(1 - \frac{\beta}{2})]V}{1 - \gamma^2 q^2} + \frac{\gamma F}{1 + \gamma q}$$

7.5 Derivation of (16)

The condition $W(0) \leq W(2)$ is equivalent to

$$p(0) \leq p(2) - \frac{2F}{S} \tag{A.2}$$

which in turn is equivalent to:

$$t[1 - (1 - \beta)^2] + \frac{2F}{S} \leq t[1 - (1 - \alpha)^2]$$

We now use the fact that for $f(x) = x^2$, convexity implies

$$f(y) \geq f(x) + f'(x)(y - x)$$

Let $y = 1 - \beta$ and $x = 1 - \alpha$, thus

$$(1 - \beta)^2 \geq (1 - \alpha)^2 + 2(1 - \alpha)(\alpha - \beta)$$

It follows that a sufficient condition for $(A.2)$ to hold is

$$t[1 - (1 - \beta)^2] + \frac{2F}{S} \leq t[1 - (1 - \beta)^2] + 2t(1 - \alpha)(\alpha - \beta)$$

After some algebraic manipulation, condition (16) is obtained.

References

[1] Anderson R. "Why Information Security is Hard-An Economic Perspective", Proceedings of 17^{th} Annual Computer Security Applications Conference (ACSAC) (2001) pp 10-14.

[2] AT&T News Release. "AT&T announces cause of frame-relay network outage", (1998) in *http://www.att.com/news/0498/980422.bsb.html*

[3] Breyer, S. "Regulation and Its Reform" (1982) Harvard University Press, Cambridge MA.

[4] Cave M. and Mason R. "The Economics of the Internet: Infrastructure and Regulation" Oxford Review of Economic Policy (2001) Vol. 17 pp 188-201

[5] Chinander, K., Kleindorfer P. and Kunreuther H. "Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks", (1998) Risk Analysis Vol 18, pp.135-144.

[6] Ericson, R. and Pakes. A. "Markov-Perfect Industry Dynamics: A Framework for Empirical Work" Review of Economic Studies (1995) Vol. 62, pp. 53–82.

[7] Fudenberg D. and Tirole J. (1991) "Game Theory", MIT Press.

[8] Gal-Or, E., Ghose. A. "The Economic Incentives for Sharing Security Information", Information Systems Research (2005), Vol 16 No (2), pp. 86-208.

[9] Garza V. "Security Researcher Causes Furor by Releasing Flaw in Cisco Systems IOS" in *www.SearchSecurity.com* (28 July, 2005).

[10] Giovannetti E. "Perpetual Leapfrogging in Bertrand Duopoly" International Economic Review (2001), Vol. 42 (3) pp 671-682

[11] Gordon L. and Loeb M. "The Economics of Information Security Investment", ACM Transactions on Informations and System Security (2002), Vol 5 No. 4 pp. 438-457.

[12] Haimes Y. "Risk Modeling, Assessment, and Management" (2004) Wiley-Interscience; 2 edition.

[13] Kannan K., Telang R. "Market For Software Vulnerabilities? Think Again", Management Science, (2005) Vol 51 No. (5) pp. 726-740.

[14] Maskin E. and Tirole J., "Markov Perfect Equilibrium I. Observable Actions". Journal of Economic Theory, (2001) Vol. 100 (2) pp.191-219.

[15] National Research Council. "Cyber Security of Freight Information Systems", Special Report 274, Transportation Research Board, 2003

[16] Shapiro, C. "Premiums for High Quality Products as Returns to Reputations", Quarterly Journal of Economics, (1983) Vol 98 pp. 659-680.

[17] White House, "National Strategy to Secure Cyberspace" (2003) available at *http://www.whitehouse.gov/pcipb/*

[18] US Census Bureau, "Quarterly Retail E-Commerce Sales", March (2005).

[19] Viscusi, K, "Risk by Choice: Regulating Health and Safety in the Workplace" (1983) Harvard University Press, Cambridge MA.

[20] Zetter K. "Cisco Security Hole a Whopper" in *www.wired.com* (27 July, 2005)