Growth and Sustainability of Managed Security Services Networks:

An Economic Perspective

Alok Gupta
Dmitry Zhdanov
Department of Information and Decision Sciences
University of Minnesota
Minneapolis, MN 55455
(agupta, dzhdanov@csom.umn.edu,)

Abstract

Managed Security Service Provider (MSSP) networks are a form of collaboration where several firms share resources such as diagnostics, prevention tools, and policies to provide security for their computer networks. While decisions to outsource security operations of an organization may seem counterintuitive, there are potential benefits from joining a MSSP network due to pooling of risk and access to more security-enabling resources and expertise. We provide structural results that explain the reasons for firms to join a MSSP network. We also characterize the growth of MSSP network size under different forms of ownership (monopoly vs. consortium). Our results illustrate the need for initial investment in MSSP networks to overcome initial stalling effect and illustrate that while need for initial investment may increase the optimal network size for a consortium, it has no impact on the optimal network size for a profit maximizing monopolist.

KEYWORDS: Information security, Managed security services, Outsourcing, Network Effects, Network growth, Network ownership structure

1. Introduction

Emergence of complex and closely interconnected business-to-business relationships have made security perimeter around a single firm's network disappear (McKenzie, 2003). It is being replaced by a network of protected business relationships. The major challenge in such environments becomes the identification of legitimate partner and potential intruders to protect computing resources and business data from unauthorized access. Enabling, but complex to manage, technologies such as web services further complicate provision of security to enterprise resources. Originally web services were envisioned as a lightweight solution to allow different applications to talk freely; however, it is becoming apparent that for web services to be successful, security issues need to be addressed (Welsh, 2003). Among technical developments on this front, there are initiatives to implement security for such tools as XML and SOAP, but the issue of whom to offer web services to and who to exclude remains a largely non-technical problem. To make matters more complicated, there are now many more technologies that allow making information transfer in and out of a company almost uncontrollable. Use of storage area networks, peer-to-peer communications and instant messaging provide broad opportunities for information transfer and significantly complicate determination of security perimeter. Further, many such technologies are used in telecommuting and telework that are projected to continuously grow as more enabling and collaborative technology evolve. For example, Starner (2003) reported that more than 80% of executives worldwide expect some of their workers to telecommute over the next two years.

Therefore, firms increasingly find that they are unable to manage security of their resources themselves. This has led to one of the most interesting emergent phenomenon - the "spillover" of outsourcing into the area of information security. While counterintuitive, in 2002, 29% of all European enterprises intended to use managed security services (Computerwire, 2002). Outsourcing of security services is an interesting but perplexing phenomenon because firms are often ready to hand over the security of their precious digital assets to outsiders. Estimates report the current number of companies obtaining security from outside providers to be up to 30% and growing. A compound annual growth rate in the market of Managed Security Services Providers (MSSP) is estimated to be at least 17-20% (Kavanagh 2002). The entire market is expected to grow from $140 million in 2000 to 1.2-1.7 billion in 2005-07 (Yasin 2001, Van Mien and Praveen 2003, Sturgeon 2004a). In addition, there is significant consolidation in the MSSP market with the number of providers getting smaller while increasing their range of services (Phifer 2004).

The cost/benefit tradeoffs for MSSP arrangements are still not well understood. The risks of working with MSSP include issues of trust, dependence on outside entity for support of critical functions, and ownership of systems (Allen et al.,2003). However, as Allen and Gabbard (2003) point out, there are multiple benefits that individual firms can derive by using MSSPs:

- Cost savings: cost of managed security service is usually lower than hiring in-house full-time experts. MSSPs are able to spread their investment in infrastructure and people across several clients.
- Staffing: shortage of qualified security personnel (a trend that is expected to continue through at least 2006) puts big pressure on companies to recruit, train and retain their security staff.
- Skills and security awareness: MSSPs have better insight into evolving security threats directly and indirectly because of their focus and wider install base.
- MSSPs can provide objectivity, independence, liability protection, dedicated facilities,

and round-the-clock service.

While current MSSPs focus on their relationships with government entities and large companies, benefits of managed security services are also appealing for small and medium size companies due to relative amount of resources that they have to commit to security operations (Sturgeon 2004b). Thus, MSSP service offering is attractive to a wide range of organizations and study of MSSP markets has real practical value.

In this paper we explore the structure of the MSSP market as well as its formation process and stability. We primarily try to identify whether there are indeed economic benefits for firms to hire external entities to manage their security. We look at the economic incentives that lead to particular choices in security outsourcing. For example, we show that it may be beneficial for firms to join larger groups (MSSP networks) just to hide themselves from potential attacks among other targets. We compare two different types of ownership structures for MSSP: i) a consortium based approach where several companies join hands to pool their resources to collectively provide security for their computing resources; and ii) when a MSSP is a for-profit provider who manages security for a group of firms.

We look at the dynamics of growth for these MSSP networks where the network may start with a small group of firms and grow over time. One of the key concerns in such networks is that below a certain size, the networks are not economically viable. In network externality literature this phenomenon is called "critical mass" (e.g. Oren and Smith, 1981; Economides 1996). We define optimal growth rules with respect to the viability and network size. In the network effects literature, the issues of growth and optimal size of networks are not nearly as extensively explored as the issues of standards, coordination and choice of networks (Liebowitz and Margolis 1998). Weitzel et al. (2000) call for reconsideration and new work in the area of network effects in application to modern-day IT markets, emphasizing evolutionary system dynamics as one potential direction of development. Walden and Kauffman (2001) call for research of whether network externalities exist in specific e-commerce settings and how they affect behavior of actors involved.

Another related issue concerns the form of ownership of a MSSP network. Given the B2B relationships that companies have with each other it would seem that a consortium based approach may be appealing. However, we show that firms may have better incentives for joining a for-profit MSSP, especially initially when network size is small. We also identify conditions under which profit-oriented proprietary MSSPs may have larger size than consortium operated MSSPs.

The paper is organized as follows. In the next section we review relevant literature and reasons for analytical work in MSSP networks field. In section 3 we provide conceptual basis for our analysis including the definitions of constructs used to analyze the market structure for MSSPs. In section 4, we present some structural results that indicate why individual firms may prefer to share resources for security purposes. Then in section 5, we analyze the MSSP networks under the two ownership structures discussed earlier. We also discuss the implication of theoretical results in this section. Finally, we conclude in section 6 with a summary of contributions and directions of future research.

2. Background

We conceptualize a MSSP network as a collection of interconnected companies that share common security resources and have access to the same information on potential attacks. We consider two forms of market organization. One possibility is where a set of core firms with common interests join their security efforts and create a consortium. In this case, efforts and benefits are likely to be similar among participants. On another hand, a MSSP network may be created by a for-profit organization (e.g., a telecommunications company) that provides security services as its business offering. In this case, pricing and membership decisions will be controlled by a single firm acting as a monopolistic owner of its network. Our objective is to analyze the feasibility of such market organizations and derive structural results regarding the growth of these networks. We will also explore whether the ownership structure makes a difference in potential network size.

The problem of MSSP network formation is related to two general perspectives: alliance formation and incentive analysis for information security decisions. Researchers in the theory of collective actions has looked at the efficiency of defense alliances such as NATO and found that due to public good nature of security, smaller members tend to exploit larger ones (Olson and Zeckhauser 1966, Oneal 1990, Sandler 1993, 1999). However, the process of alliance evolution is generally not studied. In the context of information security decision analysis, the recent tendency is to consider a number of economic-based approaches to these problems. For example, the effects of information disclosure are studied from the perspective of econometric analysis (Campbell et al 2003, Schechter 2005, Cavusoglu et al 2004) or from the perspective of formal analysis of economic threats and markets for sharing of security information (Ozment 2004, Schechter and Smith 2003, Kannan and Telang 2004). Many of these works do not look at the issue of formation and growth of information sharing entities; this is the issue that we are trying to address.

More specifically, our work fits under the general paradigm of network effects while it provides a new and interesting perspective to the problem of network growth. Leibowitz and Margolis (1998) provide several classification dimensions of network effects. First, not all network effects are externalities, but only those which are not internalized. In our case, we describe pricing mechanisms that allow network effects in MSSP market to be internalized. Further, there is a distinction between direct and indirect network effects. Direct effects occur as an immediate result of participation in a network, while indirect effects are due to emergence of complimentary products and services. In our case, the network effects are direct, as they result instantly from MSSP network membership. Finally, network effects may be positive or negative. While most research focuses only on one type of network effect, our approach considers both positive and negative effects that arise from use of MSSP networks.

The majority of work in network effects area concerns with the question of choice among competing networks. This vast body of literature touches upon several issues that are relevant to the formation and growth of MSSP networks. One such issue is the question of growth and optimal size of the network. From the perspective of competition between two product standards, Farell and Saloner (1986) consider the effects of installed base on choice between two competing standards and discuss effect of pre-announcements on shifting the market balance. Katz and Shapiro (1985) study the effects of compatibility between standards on adoption dynamics. Different forms of obstacles to the organic network growth are possible in such cases – for example, excess inertia or momentum, tipping, lock-in, insufficient waiting etc. (as summarized in Stango 2004; Farrell and Klemperer 2006). In addition, such dynamics lead to suboptimal network size and welfare distribution by market mechanism (e.g., Church et al., 2002). To overcome such effects, a variety of tools may be used - pre-announcements, expectation management and other forms of coordination (e.g. Farrell and Klemperer, op. cit., Shapiro and Varian 1999). In our setting, we do not consider competition between standards, but look at the evolution of the same standard. Still, we find obstacles to organic growth of MSSP network in terms of “critical mass” problem; we also propose a way to overcome such problem by using the investment mechanism. Such investment serves as a signal of confidence from the network owners to customers and allows for further organic growth.

Next issue considers the ownership of networks. While work in competition between standards usually assumes monopolistic sellers or service providers, McAndrews and Rob (1996) find that in situations like ownership of ATM networks by banks, a consortium market structure may bring greater benefits to its members, thus achieving greater size and social benefits than monopoly-owned networks. We also compare the consortium and monopoly market structures for MSSP networks and find that in information security settings, consortium-owned network is sometimes easier to start up, but the monopoly-owned network can reach larger size.

Another related issue is the question of pricing the service provided in a network industry. When network effects are present, then even a monopolist will often deviate from the pricing discrimination strategy and will adopt some form of introductory pricing (Shapiro and Varian 1999; Cabral et al. 1999); sometimes below marginal cost (Grajek 2004). In the MSSP problem that we consider, we show that for a consortium owner an equal sharing pricing scheme is optimal. For the monopoly owner, there are incentives to offer zero prices at startup of the network.

Finally, there is a consideration for the direction of the network effect. Majority of the literature looks at the network effects that are positive, i.e. larger network size lead to the greater benefits to consumers (Matutes and Regibeau 1995; Gandal 2002). Economides and Flyer (1997) analyze the opposing incentives of firms to choose compatible or differentiated products and illustrate frequent domination of network industries by a few (one or two) firms. Issues of lock-in and path dependence often arise in these settings (e.g., Liebowitz and Margolis 1995). However, there are also negative networks effects, where addition of new users deteriorates the value received by those already on the network. Examples of such negative effects are congestion and information overload (MacKie-Mason and Varian 1994; David and Steinmueller 1994). In our work, we explicitly model the trade-offs between positive and negative effects that individual firms face while being on the MSSP network; we also study how these effects impact the dynamics of network growth.

Compared to competition between standards, work on the network size and network formation process is much less explored in the modern information systems literature. One example is the work of Riggins et al (1994), studying the growth of interorganizational systems with negative externalities, leading to "stalling" of growth. We believe that our model fills a gap in the literature on the growth of networks and provides a perspective that considers both positive and negative network effects in the process in the context of MSSP networks.

Furthermore, Weitzel, et al (2000) suggest to reconsider some of the common assumptions of network effects theory to address the issues occurring in today's IT markets. In particular, they question the following assumptions: exclusion principle (goods may be in unique possession only), consumption paradigm (consumption of a good leads to it destruction) and separation of consumers and producers. We are looking at information security, which is a good that is usually non-excludable, i.e., it is not being used up while "consumed" and may be "produced" by the ultimate "consumers" of security. Information security displays properties of a public good (Varian 2004) as well as an externality (Camp and Wolfram 2000). As an externality, security (or the lack thereof) of a system affects other entities involved in a business transaction. Thus, it is important to explicitly consider such effects and attempt to internalize those. In the later sections we suggest pricing schemes that help to internalize security externalities resulting from increased network sizes.

Information security also partially possesses common attributes of public goods: non-excludability and non-rivalrous consumption (Cowen 2005). For example, use of particular antivirus software by one company does not prevent others from using the same software. However, companies that choose not to subscribe for updates exclude themselves from enjoying the benefits of protection against most recent viruses. Similarly, if a MSSP provider offers spam filter as part of its offering, its use to filter one client email does not exhaust its functionality to filter email for any other client, though it does create conflicts in allocation of computing resources to different clients. Thus, we can approach information security as a “near-public” good, as it frequently exhibits public good properties. Thus, we are studying a previously unexplored area of network effects field while considering important properties of the information good such as security.

As illustrated before, access to additional information about security incidents is one of the benefits of joining an MSSP network. Several studies has looked at the problems of sharing security information among different entities. Gordon et al (2003) consider a case when two firms form security information sharing alliance and show that sharing of security information can either increase or decrease the level of security, as member firms attempt to free ride. Along the same lines, Gal-Or and Ghose (2005) show that sharing security information may impact market shares of competing companies; they also show that such benefits increase with firm size. Both of the above models are developed in a game-theoretic setting between two parties. Hausken (2006) models security investment as a way to offset the varying levels of threats by an external agent and shows that increased interdependence between firms causes free riding, to the detriment of the defenders. In our work, we are not making assumptions about whether firms joining the MSSP network are competitors or collaborators; we study the security impact of network growth rather than particular interdependencies between companies on the network.[1] In addition, the issue of free riding does not occur in our setting, as all effects are internalized using the pricing scheme. Next, we describe the properties of modeling constructs before presenting the formal model in Section 4.

3. Model Preliminaries

Suppose there are multiple identical firms that are considering joining a network of other such firms. Let *N* denote the size of such network. Without loss of generality, a single firm may be then considered as a network of size 1. All networks are continuously exposed to a number of external threats. When these threats can be carried out successfully, the systems on the network may suffer some degree of damage. Firms are seeking to estimate this damage and counter it with their security efforts. We may quantify the damage that may be inflicted to the entire network by a given attack as:

$$D(N) = P_a(N) \times P_s(N) \times N \tag{1}$$

Where:

D(N) -- is the estimate of damage to the network of size N (amount of assets affected by an attack);

$P_a(N)$ -- is the probability of an attack taking place; and

$P_s(N)$ -- is the probability of success for a given attack.

Note that both probabilities of attack taking place and being successful are dependent on the size of network N. We assume that $P_a(N)$ is increasing in N and $P_s(N)$ is decreasing in N, i.e.

$$dP_a/dN > 0 \tag{2}$$

[1] Our discussions with MSSP providers lead us to believe that rarely do a group of companies approach them to provide security for an alliance. Typically, security is still looked at as an issue of a single enterprise's governance.

$$dP_s / dN < 0 \tag{3}$$

Note that these assumptions are realistic and reasonable[2]. For example, larger networks are more likely to be attacked just because they attract more attention while likelihood of a random attack also increases with a larger network. Since firms are physically sharing the security technology, a failure in one of the infrastructure component (e.g., server-based anti-virus) will affect all of them, which is not the case if each firm maintains its own security infrastructure. Furthermore, even though the membership information of MSSP networks in not likely to be publicly available, attacks on different networks that are served by the same MSSP provider are still more likely to occur due to topological proximity of these networks (e.g., being on the same range of IP address if MSSP also acts as an ISP for its network members). However, while larger networks are susceptible to more attacks (Germain 2004), any potential remedy when applied to the network also protects a larger network. In addition, a successful attack allows development and deployment of countermeasures for a larger group of clients. Larger networks also have more resources to negate sophisticated attacks and benefit from a knowledge and solution sharing between the members of the network. Thus, as Sturgeon (2004) notes, attacks on larger systems are less likely to be successful due to accumulation of knowledge and expertise – a key benefit of MSSPs.

To see whether the assumptions about the model parameters are justified, we ran a simulation experiment based on the network traffic data used in KDD Cup 1999[3]. The original dataset consists of data on over four million connections each described by 42 attributes (e.g.,

---

[2] It may be argued that probability of attack success, P_s, is also a function of investment in security, S, and should decrease as this investment increases. Then, an individual firm decision becomes whether to invest S alone or as part of the network. However, MSSPs make security solutions available for those firms whose individual cost of security investment is prohibitively high. Therefore, the effects of investment are captured through the size of the network and there is no need to introduce a separate investment parameter.

[3] KDD Cup is organized by ACM's Special Interest Group on Knowledge Discovery in Data (SIG KDD). The 1999 dataset is available at http://www.acm.org/sigs/sigkdd/kddcup/index.php?section=1999&method=data

duration, protocol, etc.) and identified either as normal traffic or one of 24 attack types. Our simulation proceeded as follows:

1. 20,000 connections were randomly selected from the original dataset to form simulation training set. 16 attack types were represented in the simulation set.
2. Simulation training set was duplicated to represent simulation test set with the same distribution of attacks as in the training set
3. 20,000 connections in training set were randomly split into 20 groups of 1,000. These groups represent "firms". It is assumed that each firm can independently observe 1,000 connections.
4. One firm was chosen to start the "network" (network size = 1, pool of connections =1,000).
5. Proportion of attack connections in the connection pool was computed and provided the probability of attack, P_a.
6. Based on the pool of connections, the decision tree was built to classify the attacks using C4.5 algorithm.
7. The output of C4.5 algorithm was tested against a random subset of attacks from testing set. The testing subset is half the size of the training subset. The proportion of misclassified attacks in testing subset was computed and provided the probability of attack success, P_s (on the assumption that if attack was not identified correctly, then no appropriate defense would be activated).
8. Network size was incremented by 1 (until it reached 20). (e.g., after first iteration, network size = 2, pool of connections = 2,000.). Return to step 5.

The data was averaged over ten simulation runs. Figures 1 and 2 below represent the experimental findings about probability of attack taking place and probability of attack success, respectively. Figure 1 approximates P_a as a ratio of attack types visible to the network of a given size to a total number of attack types possible (due to randomization, the probability in terms of pure volume of attacks without distinction between attack types remains stable at 0.81). Figure 2 represents P_s as classification error as described above. We see that $P_a(N)$ is increasing in N and $P_s(N)$ is decreasing in N, as we assumed before.

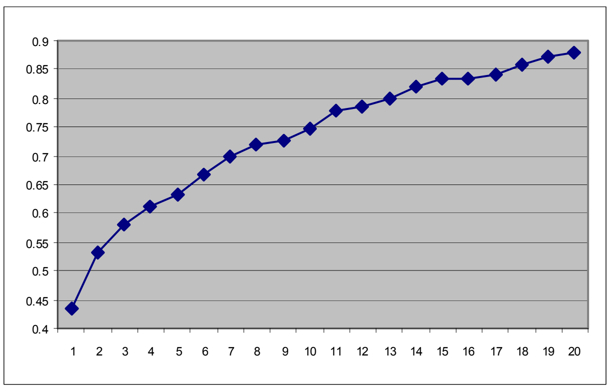	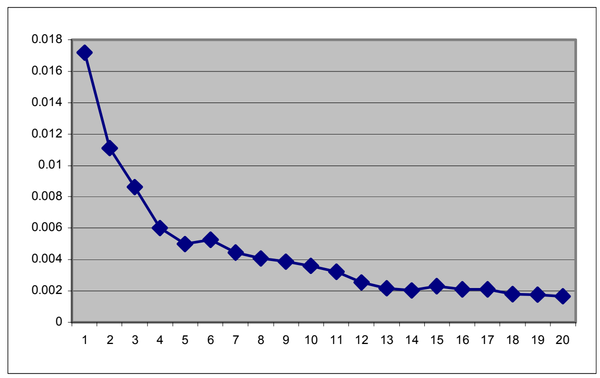
Figure 1. Probability of attack in a network of given size	Figure 2. Probability of attack success in a network of given size

The value of the MSSP network comes from its ability to reduce potential damage to its members through superior technology and larger amount of attack information. Figure 3 below represents an approximation of such benefits by plotting unit expected risk of being on the network vs being alone. ($P_a(1)P_s(1) - P_a(N)P_s(N)$). Based on these observations, we assume that the value of the MSSP network, *V(N),* can be represented by an increasing, concave function.

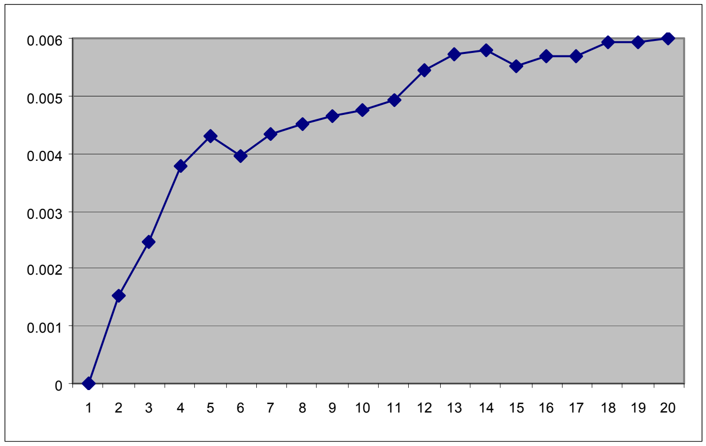

Figure 3. Approximation of network value from simulation data

Once the potential value of the MSSP network has been estimated, it is necessary to understand the costs of maintaining such networks. Let *R(N)* be an input requirement function that describes the amount of resources that are needed to provide the level of information security associated with the size of MSSP network. As a recent Gartner report points out, at the beginning stages of network growth, the majority of investment has to go into the basic infrastructure technologies such as firewalls and antivirus tools ("keeping bad guys out"), with reasonably stable costs (Wheatman et al, 2005). Once the network gets larger, the focus of investment shifts to "letting good guys in" technologies such as authentication and access management, that require much more effort in configuration and management. Since difficulty of providing additional security (in terms of the amount of resources required) increases at increasing rate, we assume that *R(N)* is an increasing convex function.

Resource requirement function reflects a peculiar nature of information security -- it is not a regular commodity good. As we argued before, it is a "near-public" good, and production of public goods is not straightforward. For instance, Varian (2004) considers three distinct alternative ways of providing system reliability – total effort (when individual efforts add up), weakest link (when reliability depends on the lowest effort level) and best shot (depending on the highest effort level). By introducing the resource requirement function, we can study multiple ways of security provisioning using the same analytical approach. Effort of provisioning security for a given network size balanced with additional benefits available to members define the value of the MSSP network. The net value of the network can then be written as:

$$W(N) = V(N) - R(N) \tag{4}$$

In order to ensure voluntary participation in the MSSP network, the firms must have some benefit as compared to handling their security on their own. If attack risk is the only consideration, then there are two potential metrics of such rationality. First, firms may want to make sure that potential damage that they face while being on the network is smaller than that of being alone. Second, firms may want to make sure that the fraction of security cost that they have to contribute to on the MSSP network is smaller than that of handling security alone, i.e.,

$$D(N)/N < D(1) \text{ (or, risk(N) < risk (1))} \quad ; \; R(N)/N < R(1) \tag{5, 6}$$

From the perspective of cost and damage only, when both of these conditions hold, firms have incentive to join the MSSP network; it is also not rational to join if both conditions are violated. The situation becomes ambiguous when only one of these conditions holds – e.g., when damage reduction requires too much resources, or when individually feasible contribution to the network does not reduce the damage to acceptable level. This ambiguity is resolved once the benefit of the network – V(N) – is considered. The ultimate individual rationality condition involves the fraction of net value of the MSSP network allocated to an individual firm: W(N)/N > W(1). Next, we explore the process of formation and growth of MSSP networks under different ownership structures. Since we assume that the firms in question are identical from the perspective of security needs, we assume that they will bear an equal fraction of risk after joining the MSSP network. Additionally, we assume that all MSSP network member firms are risk-neutral, individually rational and selfish (concerned with their payoffs only). Our model assumptions are described below:

- There is a single MSSP network, potential clients make decisions whether to join it or provide their own information security
- All clients are identical, risk-neutral, selfish, price-taking and individually rational
- Benefits and risks of being on the MSSP network are distributed equally among clients
- Once MSSP network is started, clients join one at a time.
- MSSP can deny entry to a new client, but will not expel an existing client

4. Making a Case for MSSP Networks

Before we tackle the issue of Formation and growth of MSSP networks, we first derive the conditions necessary for the existence of a MSSP network. A possible objective that provides positive benefits to MSSP network members is to maximize the total net benefits derived from the MSSP network:

$$\max W(N) \Leftrightarrow \max[V(N) - R(N)] \tag{7}$$

It is easy to verify that first order optimality condition for this optimization is

$$dR/dN = dV/dN \tag{8}$$

Let the solution to equation (7), i.e. the optimal social benefit maximizing MSSP size, be represented as N_s^*. We will discuss the properties and relative size of N_s^* a little later, first let us discuss the conditions under which MSSP networks are attractive options for firms depending on the damage function D(N). Recall from section 2 that $D(N) = P_a(N) \times P_s(N) \times N$, where $P_s(N)$ is decreasing in N, while product $P_a(N)$*N is increasing in N.

It is easy to verify that damage function may be either (a) monotonically increasing (local minimum at 1), (b) monotonically decreasing (local maximum at 1), or have a unique (c) local maximum or (d) local minimum in $(1, \infty)$. In case (a), MSSP network does not offer obvious benefits in terms of reduced risk and may not be attractive to firms. In cases (b) and (c), the most attractive MSSP network size is infinitely large and the problem is trivial (although in case (c) there may be an issue of critical mass in early stages of network formation). The most interesting case is when D(N) has an internal minimum point in $(1,\infty)$, which is associated with convexity of damage function. Therefore, this point forward, we assume that damage function is convex.

Assumption 1. Damage function D(N) is convex and has a unique minimum in $(1, \infty)$.

Now we are going to explore how this shape of damage function impacts the incentives of firms to join MSSP networks.

Proposition 1 (**Existence of"Hiding Effect"**). Suppose that damage function reaches its minimum at an internal point of $[1, \infty)$. Then it is individually rational for firms to join the MSSP network, as decision to join decreases the potential damage they are facing from attacks.

Proof. Convexity of D(N) implies $D(N)/N < D(1)$, i.e., in a larger network the individual risk to a firm is smaller. Q.E.D.

Proposition 1 provides an interesting and desirable characteristic that may be driving MSSP adoption. The "hiding effect" makes individual firms less attractive individual target since there may be several interesting targets. However, this does not alone explain the reason for MSSPs to be attractive. In fact, a more prominent effect is the effect of knowledge and security enhancement. Unless a higher level of security can be provided due to collective increase in the ability to provide security, the MSSP may not be attractive to the firms. Proposition 2 formally states the conditions for this phenomenon that we call "Collective Knowledge Effect" to exist.

Proposition 2. (Necessary condition of "Knowledge Effect"). Suppose probability of an attack taking place $P_a(N)$ is increasing in N, and probability of attack being successful $P_s(N)$ is decreasing in N. Then, joining a MSSP network reduces individual firms' risk if the marginal impact on a firm's risk due to increased exposure is less than the effect of lower marginal risk due to decrease in probability of success, i.e., $\left|P_a(N)P_s^{'}(N)\right| > \left|P_a^{'}(N)P_s(N)\right|$.

Proof: The total risk for a firm in a network of size N can be defined as

$$risk(N) = P_a(N) * P_s(N) \left(\equiv \frac{D(N)}{N}\right) \tag{9}$$

For an individual firm to join the network $risk(N) < risk(1)$ (10)

Differentiating (10) with respect to N, we get

$$P_a^{'}(N)P_s(N) + P_a(N)P_s^{'}(N) < 0 \tag{11}$$

Since $P_s(N)$ and $P_a(N)$ are non-negative and $P_a^{'}(N) > 0$ while $P_s^{'}(N) < 0$ from equations (2) and (3), the first term in (11) is positive and the second term negative. In order for the inequality to be satisfied, the magnitude of the second term must be greater than the magnitude of the first term. In other words

$\left|P_a(N)P_s^{'}(N)\right| > \left|P_a^{'}(N)P_s(N)\right|$. Q.E.D.

We have also verified existence of hiding effect as well as knowledge effect in the simulation described on pages 10-12. Figures 4 and 5 illustrated our findings, negative values of hiding effect indicate that a firm's expected damage from being on an MSSP network is smaller than that of being alone; similarly, negative values of knowledge effect indicate that additional information gained on larger network outweighs the danger of greater exposure.

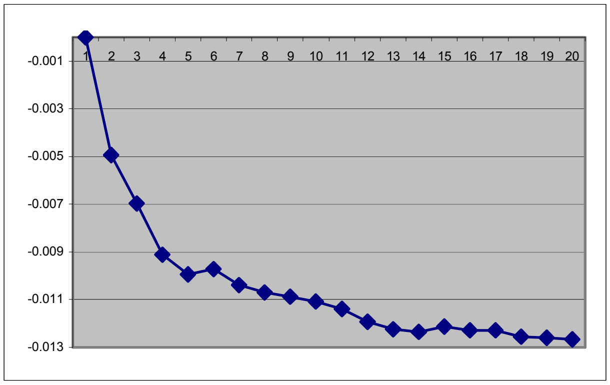

Figure 4.Hiding effect in MSSP simulation

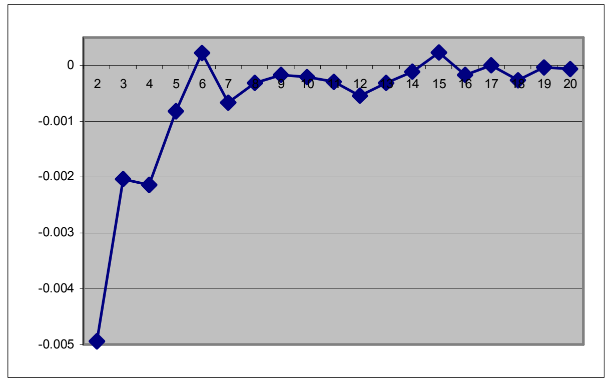

Figure 5. Knowledge effect in MSSP simulation

Proposition 2 indicates that while hiding effect may well be present, another important benefit that makes firm choose a MSSP network comes from the increased security potential due to increased knowledge and proficiency in security provision. "Knowledge effect" exists if the marginal amount of knowledge that firms gain in the larger networks outweighs the marginal increase in risk of attack on a larger network. However, the exact dynamics of MSSP network growth can be analyzed only by looking at R(N) and V(N) jointly. "Hiding effect" and "knowledge effect", described above, are important components of MSSP adoption decision, but are not the only relevant factors. As mentioned earlier, benefits that are received by the firms from joining the MSSP network are not defined solely by the reduced risk. The value of network assets and infrastructure, represented by value function V(N) is also important. Therefore, we need to balance both risk and rewards in analyzing firms' decisions. This requires the identification of the optimal total network size. One of the approaches to ensure positive benefits would be optimize the net benefits derived from the network, i.e., $\max W(N) \equiv \max[V(N) - R(N)]$. However, while maximizing the net benefit from the network may seen like a desirable goal for, at least, a consortium based MSSP, it is unlikely that a consortium with equal partnership can enforce the objective of maximizing net benefits. In the next section we consider two distinct market structures for MSSP networks and derive results regarding the optimal network size.

5. Analysis of Market Structure for MSSP Networks

As mentioned earlier we are interested in dynamics of MSSP network growth. Specifically, since it is unlikely that a network will have all the potential members joining at the same time, we are interested in finding out whether or not there are mechanisms that will provide incentives for firms to join an existing MSSP network. We are also interested in finding out, if the incentives to join a network exist, what the optimal network sizes would be under two different forms of market structures:

i. A consortium based MSSP network where several firms may join there efforts in providing security to their collective networks. Such networks may be started by, for example, a group of firms which conduct electronic transactions or information sharing with each other.

ii. A MSSP network facilitated by a for-profit firm that attracts various firms under one umbrella for the purpose of providing security solutions. This seems to be the most prevalent form of market structure for MSSP networks (Kavanagh, 2004).

Before we examine the specific market structure, let us outline the process that we consider for the formation and growth of a MSSP network. We assume that a set of firms initially join the MSSP network. In case of a consortium, these firms may be thought of as founding members and in case of a for-profit MSS provider, it may be the initial firms that the provider is able to attract to the network. Once the network is started, firms arrive one by one and the existing consortium members or the for-profit provider decide whether or not to accept a new member. We assume that each new incoming firm is a price taker, i.e., it agrees to pay whatever charges the consortium or the for-profit provider asks for as long as the expected benefits are greater than or equal to zero. We will first examine the structure of the MSSP network and issues that must be considered in the growth of such networks; then, we will look at the consortium-based market structure followed by the for-profit provider's network.

5.1. MSSP Network Structure and Growth- a Benchmark Case

One of the first ways to assess the potential size of an MSSP network is to define the condition for maximum network size by finding the largest N that solves the following problem:

$$W(N) = 0 \text{ or } V(N) = R(N) \tag{12}$$

This problem is similar to the case of perfect competition in economic analysis, when manufacturers sell their goods at cost. However, such a configuration is not likely to be sustainable by means of real market forces since the profits of the MSSP are equal to zero or, in case of a consortia, benefits to the member of consortia are zero. For the MSSP to have incentive of maintaining a network there must be positive profit from operation. Another approach to computing potential size of MSSP network is presented in the total benefit maximization problem discussed in previous section – Max W(N) (equations 7, 8). As discussed earlier the optimal solution occurs when the derivatives of the value and resource function are equal to each other. Figure 5 depicts this case: the slopes of the tangents are equal to each other and thus the difference between the value and resource function is maximized.

Figure 5 also depicts the range of possible network sizes for a MSSP network. As the figure indicates, the maximum size of MSSP network N_{max}, that can be formed without the loss of social efficiency, may be achieved when the value (*V(N)*) and resource requirements (*R(N)*) curves intersect. The optimal size of a MSSP network that maximizes social benefits, N_s^*, is achieved whenever the distance between the two curves is greatest (equation (8)). However, there is another interesting point – N_0, representing the minimum efficient MSSP network size. Up to this point, it is not individually rational for the firms to join the network, as the benefits are lower than cost. This is the well known start up or critical mass problem in network economics where growth of the network requires a minimal nonzero starting size (see, for example, Economides, 1996).

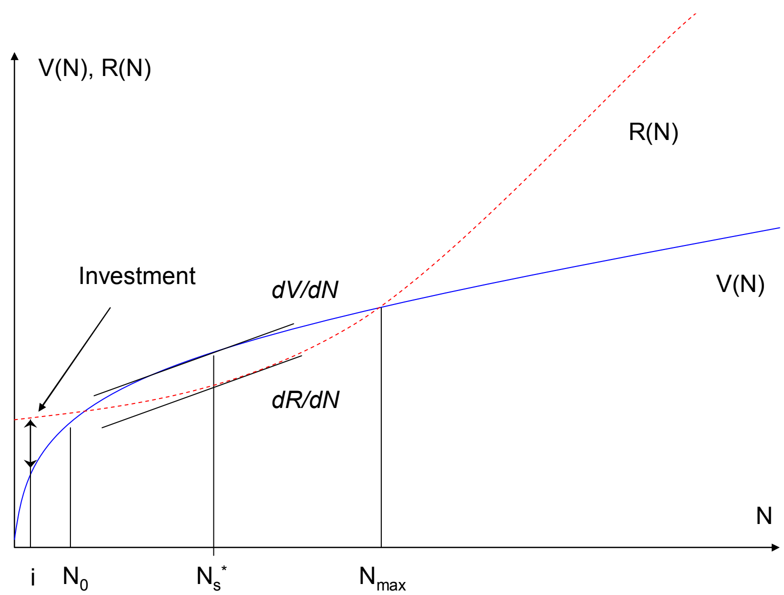

Figure 5: Number of Firms and MSSP Benefits

Since the attractiveness of a MSSP network is both a function of its value and the resource requirement which, in turn, depend on the network size, the expected size of the network plays a significant role in individual firm's decision to join the network (Katz and Shapiro, 1985, 1994; Bensen and Farrell, 1994; Economides, 1996). While the classical startup problem arises when consumers expect that no one would buy the good or that no complementary good would be available in the market, the problem arises in the MSSP network due to no instantaneous net benefit for a firm if there aren't enough members already. This phenomenon is related to the concept of critical mass (Rohlfs, 1974; Oren and Smith, 1981). The critical mass theory suggests that a sustainable growth of a network is attainable only if there is a minimal nonzero equilibrium size (Economides, 1996). In figure 1, N_0, represents this critical mass. If the initial size of the network, *i*, is less than N_0 then network cannot automatically (or "organically") grow. Economides and Himmelberg (1995) considers this as a "chicken and the egg" paradox since starting network size is too small to induce consumers into the network. We formally define the property of the critical mass problem in observation 1.

Observation 2 ("Critical Mass for MSSP"). If the initial size of the MSSP network is *i*, then, critical mass problem will be present if the smaller (or only) root of equation V(N)=R(N), N_0, is greater than *i*.

The intuition for this observation can be seen in figure 1; in the interval (0, N_0) the net benefits to firm joining the MSSP are negative since R(N) > V(N). When critical mass problem exists, there is a "deficit of value" in the amount of R(i) – V(i) for a small network, and investments have to be made to facilitate network growth. In case of the consortia this investment has to come from the foundational members, while in case of a for-profit provider this investment has to be made by the provider. Riggings et al. (1994) and Wang and Seidman (1995) also provide the results indicating the need to potentially subsidize the adoption of interorganizational networks. Both of these works show that adoption of systems like EDI may lead to creation of negative externalities for suppliers; when the corresponding positive externality for the buyer is large, she may choose to subsidize some suppliers to foster adoption. Riggins et al. (1994) show that, unless such subsidy is provided, the network adoption will stall after the initial takeoff. Our case is different, however, as "suppliers" and "buyers" of resources necessary to provide information security are the same entities; thus making even an initial "takeoff" problematic. We would explore the conditions under which the network grows "organically" to its efficient size by passing over the "hump" of critical mass. We, therefore, concentrate on defining rules under which firms may be willing to make initial investment to overcome startup problem and will study the effect of this investment on efficient maximum network size.

5.2. Consortium Based Market Structure

When security is provided jointly by the members of a consortium, each member contributes equally and receives equal benefit. We also assume that each member of consortium evaluates her own benefits before allowing a new entrant to join the consortium. We represent the total net benefits of the consortium as an aggregation of benefits of all the members of the consortium. Since all the members are identical, the benefits are identical for all the members; therefore, the benefit to each member can be computed by dividing total net benefits by the number of firms that are member of the consortium. We analyze this problem in two phases. First, we consider the case where the initial size of the consortium, *i*, is large enough so that the founding members don't need to make any additional investment, i.e, $i \geq N_0$. We will then consider the case where $i < N_0$ and the founding members have to invest a total of R(i) – V(i) to overcome the critical mass problem.

5.2.1 Consortium without need for initial investment

When there is no initial investment requirement, the problem of consortium is

$$\underset{j}{Max} \frac{V(j) - R(j)}{j} \forall j \geq N_0 \tag{13}$$

The first order optimality condition is given by

$$V'(j) - R'(j) = [V(j) - R(j)] / j \tag{14}$$

Let the optimal solution that satisfies equation (14) be represented by N_{cn}^* .The implication of the optimality condition is equation (14) is stated in proposition 3.

Proposition 3. (The Optimal Size of Consortium without Investment) Suppose that value function V(N) is concave and damage function R(N) is convex. Then, the optimal size of a consortium based MSSP with no initial investment, N_{cn}^*, will be less than or equal to the welfare maximizing MSSP network size N_s^*, i.e., $N_{cn}^* \leq N_s^*$.

Proof. The difference between the partial derivates of a concave, $V^{'}(j)$, and a convex function $R'(j)$, of a variable, j, is non-increasing as j increases. Therefore, since the R.H.S. in equation (14) is a positive number, j ≤ k where $V'(k) - R'(k) = 0$ -- the optimality condition for welfare maximizing solution. Q.E.D.

5.2.2.. Viability of a consortium

We now consider the case when the initial founders of a consortium need to make investment to facilitate the MSSP network, i.e., the initial network size $i < N_0$, the critical mass. In this case, firms will need to recover their initial investment from the benefits they receive from the MSSP. However, the question remains as to what should be the obligation of new firms that arrive to the MSSP network. Since we have assumed that the benefits of the MSSP consortium are equally shared by the members of the consortium it is reasonable to assume that the firms equally share the initial investment. Note that once the initial investment is made, no further investment is needed since the resource requirements, as compared to the benefits, are decreasing in the number of consortium participants. Start-up problem is resolved and network grows organically after the investment takes place.

Therefore, to negate stalling effect, we propose the following investment and investment-recovery approach. The initial investment amount $R(i) - V(i)$ is equally shared by the initial foundational members of MSSP with each member contributing an amount $L = [R(i) - V(i)]/i$.

Note that once the investment, L, is made any firm subsequently joining the network (as $i + k^{th}$ member) will not suffer any losses even if network size $(i + k) < N_0$ since enough investment has been made (and resource requirement $R(i + k) < R(i)$ and value $V(i+k) > V(i)$ – organic growth is possible). As discussed in the previous paragraph, to provide fair and sustainable investment incentives we assume that at any given state of the network size, the initial investment is equally borne by all the members of the consortium. Therefore, when $j+1^{th}$, member joins the consortium, they pay an initializing fee, $F = [R(i) - V(i)]/(j+1)$, which is equally divided among the j previous members, i.e., each of the previous j members receive an investment recovery of $L_r = [R(i) - V(i)]/j(j+1)$. It is easy to verify that this scheme results in all the j+1 firms equally sharing the cost of initial investment with individual contributions equaling $[R(i) - V(i)]/(j+1)$. To consider the property of this rule, let us first define the viability of a MSSP network with investment requirement to overcome critical mass problem.

Defn. (Viability of MSSP Network with Investment) Suppose the initial network size is *i,* optimal network size is N^* and minimum efficient network size is N_0. Then, MSSP network with investment requirement, to overcome critical mass problem, is viable if at the optimum network size, N^*, the benefits of the MSSP network are greater than the initial investment, i.e.,

$$V(N^*) - R(N^*) \geq R(i) - V(i); i < N_0 \tag{15}$$

Now, in terms of an investment sharing rule, an optimal rule will be such that it will allow the smallest possible starting network size *i*, thus ensuring viability at the smallest possible network size. As proposition 4 states, our rule that forces each consortium member to bear equal amount of initial investment, is optimal rule from the perspective of viability of a MSSP network.

Proposition 4. (Equal Sharing and MSSP Network Viability). Let there exist a network size *n* that allows investment recovery and network viability with equal sharing rule. Then, it is a minimum viable network size and equal sharing rule is optimal.

Proof. (By Contradiction) We will show that there is no other sharing rule that results in a smaller network size than equal sharing rule.

Let the investment is recovered at a minimum network size of *n* using the equal sharing rule

$\Rightarrow [V(n) - R(n)]/n \geq [R(i) - V(i)]/n \;\; \forall\, n$ members (16)

Now let there exists a rule such that the initial investment is not equally shared and the investment is recovered at size $m < n$.

$\Rightarrow [V(m) - R(m)]/m \geq L_j \; \forall\, j = 1, \ldots, m$ *where* L_j is the share of investment shared by member j. (17)

However, note that since m<n, and the investment is not equally shared

$L_j > [R(i) - V(i)]/m$ for at least some member j

$\Rightarrow [V(m) - R(m)]/m \geq [R(i) - V(i)]/m$ (18)

However, equation (18) implies that investment should have been recovered using equal sharing rule at size m < n – a contradiction since by assumption n was the minimum network size to recover the investment using equal sharing rule. Q.E.D.

5.2.3. Optimality of consortium with investment

Now, let us consider the problem of optimal consortium size with investment. The problem can be stated as:

$$\underset{j}{Max} \frac{V(j) - R(j) - C}{j} \; \forall j \geq N_0 \text{ where } C = R(i) - V(i) \text{, the initial investment} \quad (19)$$

The first order conditions for the optimum solution can be written as:

$$V'(j) - R'(j) = [V(j) - R(j) - C]/j \tag{20}$$

Let the optimal solution that satisfies equation (20) be represented by N_c^*. Proposition 5 below provides the surprising result regarding the optimal MSSP consortium size with initial investment as compared to optimal consortium size without initial investment.

Proposition 5. (Optimal Size of MSSP Consortium with Investment). Suppose that value function V(N) is concave and requirement resource function R(N) is convex. Then, optimal size of a MSSP consortium that requires initial investment to overcome critical mass problem, N_c^*, is equal to or greater than the optimal MSSP network size without investment, i.e., $N_c^* \geq N_{cn}^*$.

Proof.: Optimal consortium size without investment is a solution to equation (14):

N^*_{cn} = j: $V'(j) - R'(j) = [V(j) - R(j)]/j$

Further, optimal consortium size with investment is a solution to equation (20):

N^*_c = j: $V'(j) - R'(j) = [V(j) - R(j) - C]/j$

Since C is a positive number, the R.H.S. of equation (20) is smaller than the R.H.S. of equation (14).

Since the difference $V'(j) - R'(D(j))$ is decreasing in j, it follows that the solution to equation (14), N_{cn}^*, is smaller than solution to equation (20), i.e., $N_c^* \geq N_{cn}^*$ Q.E.D.

Another interesting question related to MSSP consortium is regarding the minimum initial size required for viability. Our analysis can answer this question as well. The answer comes from the realization that the maximum investment that can ever be recovered is $V(N^*_s) - R(N^*_s)$, i.e., the maximum net benefit. Therefore, the minimum starting size should be such that the required investment is less than or equal to maximum net benefit that the MSSP network can provide. Proposition 6 formalizes this result.

Proposition 6. (Minimum Viable Initial MSSP Consortium). Suppose that value function V(N) is concave and requirement resource function R(N) is convex. Then, the minimum starting network size is given by $I^* = \min\{i : V(N^*_s) - R(N^*_s) \geq R(i) - V(i)\}$

<u>Proof.</u>: Since $R(i) - V(i)$ is decreasing in $i < N_0$ and maximum recoverable investment is $V(N^*_s) - R(N^*_s)$, smallest viable initial network size is given by

$I^* = \min\{i : V(N^*_s) - R(N^*_s) \geq R(i) - V(i)\}$ Q.E.D.

Proposition 5 and proposition 6 provide some interesting and counterintuitive results with two important implications. First, the network size is greater when the firms are required to make an initial investment. Second, when firms make initial investment, it is feasible to achieve socially optimal network size N_s^*. Next we consider the problem of a monopolist, for-profit, MSSP.

5.3. Profit Maximizing MSSP:

Since we assume that firms are identical from the perspective of security needs, it is reasonable to assume that the monopolist is capable of exercising first-degree price discrimination with respect to network size and charge each customer an individual price equal to customer's valuation of the network. Since no customer has any positive valuation before the network reaches the minimum efficient size N_0, the provider attracts initial customers by providing free access to the network. Note that this pricing approach is consistent with Cabral et al. (1999), who find that a monopolist will find "introductory pricing" approach desirable in presence of network externalities. Similar to the consortium, if the initial number of the firms that the provider can attract is *i*, the total investment requirement is $L = [R(i) - V(i)]/i$. After N_0 customers have joined the network, the provider can then charge each subsequent customer a monopoly price $P^M_{N_0+j} = [V(N_0+j) - R(N_0+j)]/(N_0+j)$. However, for customers that arrive after the size N_s^*, the provider needs to potentially compensate some costumers who joined earlier since the overall shared benefits of the network go down. Recall that N_s^* is the size of network that maximizes average benefits to each client. Therefore, while marginal befefit for a new client added above N_s^* may be still positive and captured by the monopolist, existing clients may demand compensation for decreased benefits and even drop out of the network. Thus, compensation is necessary and its source has to be the price charged to the new client.

We now consider the drivers of growth of monopolist MSSP network. The revenue-maximization part[4] of profit maximizing provider's formal problem can be written as

$$\underset{j}{Max} \sum_{j=1}^{N} P_j^M \tag{21}$$

Subjected to: $$[V(j)] - R(j)]/j > P_N^M \forall j < N \tag{22}$$ [5]

Note that while this problem looks complex, it can be solved using a polynomial-time search algorithm.[6] The basic realization here is that when a firm k > N_s^* joins the MSSP network, the provider need to compensate all the customers who were initially charged an amount greater than

$$[V(k) - R(k)]/k.$$

It is clear from the discussion above that a monopolist, for-profit, MSSP may sustain a larger network than the net benefit maximizing size N_s^*. This implies that a monopolist may sustain a larger network than a consortium based MSSP (which will not grow beyond N_s^*). However, since the monopolist must recover its cost from the differential prices $[V(j) - R(j)]/j$ where j ≥

[4] Full problem of profit maximization also includes costs, they are considered on page 34. However, only revenues define the growth of network.

[5] If j<N_0, then $P^M_j = 0$, else $P^M_j = W(j)/j$ – monopolist gives free access to overcome initial stalling, then charges every client its true value

[6] A pseudo code for this polynomial time algorithm is provided in the online appendix.

N_0, the viability size for the for-profit MSSP is higher than the consortium. The viability condition for the monopolist can simply be stated as

$$\sum_{j=N_0}^{N_m^*} P_j^m \geq R(i) - V(i) \tag{23}$$

where N_m^* -- is the optimal network size as a solution to problem (21-22);

P_j^m -- are the adjusted prices charged under the providers pricing scheme; and

R(i) – V(i) – is the initial investment that provider made

Note that the optimal network size for a for-profit provider, unlike consortium, does not depend upon the initial investment. However, the viability of the MSSP network does depend upon the initial size *i*. Therefore, a for-profit, monopolist, will not start a MSSP network unless the condition in equation (23) is satisfied. Therefore, as a strategy the provider will offer the network access for free to all the firms that initially sign up for the MSSP network. Proposition 7 formally provides the condition for the monopolist MSSP network to be greater than the net benefit maximizing network size.

Proposition 7. (Monopolist MSSP versus Social Net Benefit size). Suppose that net benefit maximizing network size is N_s^* and monopolist MSSP is viable. Then, monopolist MSSP may have larger network size than social net benefit maximizing size, if $P_{N_s^*+1}^m > \sum_{j \in \Omega} P_j^m \big/ (x+1)$, where *x* is the number of firms whose benefits are reduced below the price charged to them due to the introduction of the new customer and Ω is the set of individual firms so affected.

Proof.

i) Note that, a monopolist MSSP profits cannot be maximized on a network size that is smaller than social net benefit maximizing size, i.e., N_m^* can not be less than N_s^*.

Assume contrary, profits are maximized at $N_m < N_s^*$. Then, there are one or more potential customers in interval (N_m ; N_s^*], who will get positive benefit from joining the network, since N_s^* is the socially optimal size. Charging these customers any positive price up to their willingness to pay and letting them join the network will increase monopolist's profit. But, N_m was a profit-maximizing point for the monopolist – a contradiction. Thus, N_m^* is at least equal to N_s^*.

ii) We now just need to prove that under certain circumstances $N_m^* > N_s^*$. Consider a case when a monopolist provider attracts one more customer than at the optimal net benefit maximizing network size N_s^*, then by definition

$$V(N_s^*) - R(N_s^*) > V(N_s^* + 1) - R(N_s^* + 1) \tag{24}$$

However, there may be other firms k $\leq N_s^*$ such that

$$V(k) - R(k) > V(N_s^* + 1) - R(N_s^* + 1) \tag{25}$$

Let the set of these customers be defined as $\Omega = \{k : V(k) - R(k) > V(N_s^* + 1) - R(N_s^* + 1)\}$

Each of these customers will require compensation defined by

$$Comp_k = [V(k) - R(k)]/k - [V(N_s^* + 1) - R(N_s^* + 1)]/(N_s^* + 1) \tag{26}$$

Since $[V(k) - R(D(k))]/k = P_k^m$ and $[V(N_s^* + 1) - R(N_s^* + 1)]/(N_s^* + 1) = P_{N_s^*+1}^m$, we can rewrite (26) as

$$Comp_k = P_k^m - P_{N_s^*+1}^m \tag{27}$$

The total compensation then is

$$\sum_{k \in \Omega} Comp_k = \sum_{k \in \Omega} P_k^m - xP_{N_s^*+1}^m \text{ where } x = |\Omega| \text{, i.e., cardinality of set } \Omega \tag{28}$$

Since the price charged to this $(N_s^* + 1)^{st}$ customer should be enough to cover the total compensation, we have

$$P^m_{N_s^*+1} \geq \sum_{k\in\Omega} P_k^m - xP^m_{N_s^*+1} \Rightarrow P^m_{N_s^*+1} \geq \sum_{k\in\Omega} P_k^m \Big/ (x+1) \qquad \text{Q.E.D.} \qquad (29)$$

***Corollary*: (Monopolist MSSP vs Consortium MSSP).** Monopolist MSSP, if viable, will have a network not smaller than a Consortium MSSP.

Proof. From Proposition 7, Monopolist MSSP size is greater than social benefit, $N_m^* \geq N_s^*$.

However, Consortium provider will not grow its network beyond N_s^*, as it decreases total and average benefit to its members: $\forall$ N > N_s^*, W(N) < W(N_s^*) $\Rightarrow$ W(N)/N < W(N_s^*)/ N_s^*).

Thus, $N_m^* \geq N_s^* \geq N_c$ Q.E.D.

Example below provides further intuition by considering the specific case when the $(N_s^*+1)^{st}$ customer only affects previous customer, i.e., customer N_s^*.

<u>Example</u>

Suppose, the only firm affected by the addition of $(N_s^*+1)^{st}$ firm is $N_s^{*\,\text{th}}$ firm. Then the provider can at least have a size of N_s^*+1 if $P^M_{N_s^*} < 2P^M_{N_s^*+1}$. In other words, if the twice the price charged to new customer is greater than the price charged to $N_s^{*\,\text{th}}$ customer, then the monopolist MSSP provider can sustain network size larger than social benefit-maximizing size.

The size and viability results for the networks under the two market structures and different starting conditions provide some interesting insights. These results also shed light on why the for-profit MSSP networks may be more preferable by firms, at least at the beginning. Since the firms that join a monopolist's network early are guaranteed positive benefits as long as the network survives there is higher incentive to join a for-profit network. On the other hand, a consortium based network may require firms to share investment costs at the beginning creating risk, which a risk neutral firm may not want to bear. Therefore, our results provide economic rationale[7] for the dominance of for-profit MSSP networks over the consortium based approaches. Summary of our results are presented in Table 1:

MSSP Type\effects	Consortium MSSP	Monopoly MSSP
Effect of initial investment on network size	Initial investment may induce larger size	No effect
Maximum size	Not larger than net benefit maximizing	May be larger than net benefit maximizing
Viability	Minimum start-up size may be smaller than monopolist	Due to zero prices at start-up may require larger initial size

Table 1. Comparison of consortium-based and monopoly MSSP networks

6. Conclusions and Directions of Future Research

In this paper we examine the economic rationale for MSSP networks, i.e., to provide an economic rationale for why firms may choose to outsource security. Our results demonstrate that there are multiple interplaying factors that define attractiveness of MSSP networks to potential customers. The desire of firms to join a MSSP network to pool risk may be outweighed by the substantial start-up costs required under a consortium based approach. We also examine the growth and structural characteristics of optimal networks under a consortium based market structure and under a for-profit MSS provider, representing a monopolist setting. We identify the existence of "critical mass" problem in the formation of viable MSSP networks and suggest approaches that help overcome the critical mass problem. We show that our approach to overcome "critical mass" problem is optimal since it supports the minimum feasible initial network size for a feasible consortium based MSSP network. We define optimal growth strategies and economic rationale for viable MSSP networks under a consortium based approach and profit maximizing approach. Since joining a profit maximizing provider has less risk during the start-up as compared to consortium where an initial investment may be required, our results

[7] Besides the expertise based arguments.

provide economic rationale for the observed phenomena of existence of more for-profit seeking MSSP networks as compared to MSSP consortia.   We also show that a for-profit provider may achieve larger network size than a consortium.

From managerial perspective, two issues are important. First, both hiding effect and knowledge effect are valid practical concerns. Hiding effect has been essentially the driver behind offerings of ISPs which provide frequent re-allocation of discontinuous blocks of IP addresses to their clients. With such IP schemes (we would like to call them "lattice IPs"), it is becoming harder for attackers to figure out the topology of target company's network, as they no longer can assume that subsequent IP numbers are logically connected. It also may help to reduce the damage from automated attacks such as Code Red II worm, which was programmed to frequently attack machines in the same sub-range of IP addresses[8]. Knowledge effect also becomes important for discovery of novel attacks. Since most patches as well as anti-virus database updates are distributed using a "pull" from the client, many systems remain unprotected even when the remedies are available. Monitoring of all patches and threats is a daunting individual task, but it may be handled easier by a number of connected parties.

Second issue is important for those who decide to start a MSSP network. Consortium model may be a harder sell in the beginning, as all starting members are required to invest upfront. On another hand, a monopoly-type MSSP can provide incentives (discounts) to early adopters, but may be faced with a task of attracting more customers to have a viable network. Knowledge of these implications may also influence an individual firm's decision on which type of network and when to join.

The limitations of this work include the fact that we only consider the case when MSSP

---

[8] ½ of all probes from an infected machine will start with the same /8 network and 3/8 of all probes will start with the same /16 network. (if infected machine's IP address is 192.168.6.4, then probes will start with 192 or 192.168)

customers are identical and the order of them joining the network is not relevant. In future work we will extend our model to try and identify effects of different types of customers on the system as well as the sequence of their decisions. Additionally, Sundararajan (2004) points out that network effects may depend on the type of customers, thus giving rise to non-linear pricing schemes. We will develop specific incentives mechanisms and pricing schemes for MSSPs to attract customers that differ is size, expertise, and need.

References

Allen, J., D. Gabbard, C. May, “Outsourcing Managed Security Services”, *CERT,* 01/21/2003

Bensen, S.M. and J. Farrell, "Choosing How to Compete: Strategies and Tactics in Standardization", *Journal of Economic Perspectives,* 1996 (8:2), 117-131.

Camp, L.J., and C. Wolfram, “Pricing Security”, *CERT Information Survivability Workshop*, Boston, MA Oct. 24-26, 2000, 31-39.

Campbell, K., L. Gordon, M. Loeb, L. Zhou “The economic cost of publicly announced information security breaches: empirical evidence from the stock market”, *Journal of Computer Security*, 11(3), 2003, 431-448

Carbal, L. M., D. J. Salant, G. A. Woroch, “Monopoly Pricing with Network Externalities,” International Journal of Industrial Organization, 1999 (17), 199-214.

Cavusoglu, H., B. Mishra, S. Raghunathan “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers”, *Int. Journal of Electronic Commerce*, 9(1), 2004, 70-104

Computerwire, news reports (online database), 2002.

Cowen, Tyler, "Public Goods and Externalities". *The Concise Encyclopedia of Economics.* Library of Economics and Liberty. Retrieved October 13, 2005 from the World Wide Web: http://www.econlib.org/library/Enc/PublicGoodsandExternalities.html

Church, J., N. Gandal, D. Krause « Indirect Network effects and Adoption Externalities », http://spirit.tau.ac.il/public/gandal/ine.pdf; 2002

Dang Van Mien, A., K. Praveen. "European MSSPs Value Trusted Relationships Not Just Technology", *Gartner Research,* 03/18/2003

David, P., W. Steinmueller, "Economics of Compatibility Standards and Competition in Telecommunication Networks", *Information Economics and Policy,* 6 (1994), 217-241

Economides, N., "The Economics of Networks," *Int. J. of Industrial Org.*, 1996 (*16:4)*, 675-699.

Economides, N. and F. Flyer, "Compatibility and Market Structure for Network Goods" (November 1997). NYU Stern School of Business Discussion Paper No. 98-02.

Economides, N. and C. Himmelberg, "Critical Mass and Network Evolution in Telecommunications," in Gerard Brock (ed.), *Toward a competitive Telecommunications Industry: Selected Papers from the 1994 Telecommunications Policy Research Conference*, University of Maryland, College Park, MD, 1995, 31- 42.

Farrell, J., P. Klemperer, "Coordination and Lock-in: Competition with Switching Costs and Network Effects", *http://paulklemperer.org*, 2006

Farrell, J. and G. Saloner, "Installed Base and Compatibility:Innovation, Product Preannouncements, and Predation", *The American Economic Review*, 1986 (76:5), 940-955

Gal-Or, E., A. Ghose, "The Economic Incentives for Sharing Security Information", *Information Systems Research,* 2005, 16(2), 186-208

Gandal, N., "Compatibility, Standardization, and network Effects: Some Policy Implications", *Oxford Review of Economic Policy,* 18(1), 80-91, 2002

Germain, J. "Managed Security Services: A Hedge Against E-Mail Attacks", *TechNewsWorld,* 5/25/2004.

Gordon, L., M. Loeb, W. Lucyshyn, “Sharing Information on Computer Systems Security: An Economic Analysis”, *Journal of Accounting and Public Policy,* 2003, 22, 461-485

Grajek, M. “Network Effects, Compatibility and Adoption of Standards: Essays in Empirical Industrial Economics”, unpublished Doctoral Dissertation*, Humboldt-Universitat zu Berlin,* 2004

“Insecurity Alert*”, Total Telecom Magazine*, January 2005

Hausken, K., “Income, Interdependence and Substitution Effects Affecting Incentives for Security Investment”, *Journal of Accounting and Public Policy,* 2006, 25(6) 629-665

Kannan, K., R. Telang, “An Economic Analysis of Market for Software Vulnerabilities”, *Proceedings of WEIS-2004*

Katz, M. L. and C. Shapiro, "Network Externalities, Competition, and Compatibility," *American Economic Review*, 1985 (75), 424-440.

Katz, M. L. and C. Shapiro, "Systems Competition and Network Effects," *Journal of Economic Perspectives*, 1994 (8), 93-115.

Kavanagh, K. “North America Security Services Market Forecast: 2001-2006”, *Gartner Research,* 10/9/2002

Liebowitz, S., S. Margolis, S. “Path Dependence, Lock-In, and History”, *Journal of Law, Economics and Organization*, April 1995 (11), 205-226.

Liebovitz S., and S. Margolis, "Network Externalities (Effects)". *The New Palgrave Dictionary of Economics and the Law.* London, Macmillan Reference, 1998 (2), 671-674.

MacKie-Mason, J., H. Varian “Pricing Congestible Network Resources”, http://www.ischool.berkeley.edu/~hal/Papers/pricing-congestible.pdf, 1994

Matutes, C., P. Regibeau, “A selective review of the economics of standardization: Entry deterrence, technological progress and international competition", *European Journal of Political Economy,* 12 (1996), 183-209

McAndrews, J., R. Rob, "Shared ownership and pricing in a network switch", *International Journal of Industrial Organization,* 14(1996), 727-745

McKenzie, M., "Information Security: An Ounce of Prevention," *CISCO BIS*, April 25, 2003.

Olson, M., R. Zeckhauser, "An Economic Theory of Alliances", *The Review of Economics and Statistics*, Vol. 48, No. 3. (Aug.,1966), pp. 266-279.

Oneal, J., "The Theory of Collective Action and Burden Sharing in NATO", *International Organization*, Vol. 44, No. 3. (Summer, 1990), pp. 379-402.

Oren, S. S. and S. A. Smith, "Critical Mass and Tariff Structure in Electronic Communications Markets," *Bell Journal of Economics*, 1981 (12:2), 467-487.

Ozment, A. "Bug Auctions: Vulnerability Markets Reconsidered", *Proceedings of WEIS-2004*

Phifer, L. "Managed Security Service Provider Survey", *ISP Planet,* 12/21/2004.

Riggins, F., C. Kriebel, T. Mukhopadhyay, "The Growth of Interorganizational Systems in the Presence of Network Externalities", *Management Science,* 1994 (40:8), 984-998

Rohlfs, J., "A Theory of Interdependent Demand for a Communications Service," *Bell Journal of Economics*, 1974 (5:1), 16-37.

Sandler, T., "The Economic Theory of Alliances: A Survey", *The Journal of Conflict Resolution*, Vol. 37, No. 3. (Sep., 1993), pp. 446-483.

Sandler, T. "Alliance Formation, Alliance Expansion, and the Core", *Journal of Conflict Resolution*, Vol. 43, No. 6, 727-747 (1999)

Schechter, S. "Toward econometric models of the security risk from remote attacks", *IEEE Security and Privacy,* 3(1), 2005, 40-44.

Schechter, S., M. Smith “How Much Security Is Enough to Stop a Thief?”, *Lecture Notes in Computer Science,* v 2742 (2003), 122-137

Shapiro, C., H. Varian, “The Art of Standard Wars”, *California Management Review;* 41(2), Winter 1999, pp. 8-32

Stango, V. “The Economics of Standard Wars”, *Review of Network Economics,* 3(1), 1-19, 2004

Starner, T., “Teleworking takes off”, *IQ Magazine,* November-December 2003.

Sturgeon, W. “What Is The Future Of Your Security?”, *silicon.com Software,* 9/22/2004

Sturgeon, W. “Cheat Sheet: Managed Security Services”, *silicon.com Software,* 9/24/2004

Sundararajan, A. “Nonlinear Pricing and Type-Dependent Network Effects”, *Economic Letters,* 2004 (83), 107-113

Varian, H. “System Reliability and Free Riding”, *UC-Berkeley,* working paper, 2004.

Walden, E. and R. Kauffman, “ Economics and Electronic Commerce: Survey and Research Directions”, *International Journal of Electronic Commerce, 2001 (54), 94-115*

Wang, E. and A. Seidmann, “Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies”, *Management Science,* , 1995 (41:3), 401-418

Weitzel, T., O. Wendt, F. Westrap, “Reconsidering Network Effect Theory”, *ECIS 2000*

Welsh, T., “Divide and Conquer?” *CBR Research,* 2003, 29-32.

Wheatman, V., B. Smith, N. Shroder, J. Pescatore, M. Nicollet, A. Allan, R. Mogull, “What Your Organization Should Be Spending for Information Security”, *Gartner Research,* report ID G00126733, 9 March 2005.

Yasin, R. “Enterprises Size Up Managed Security”, *Internet Week,* 6/19/2001