MIS Quarterly

RESEARCH ARTICLE

GROWTH AND SUSTAINABILITY OF MANAGED SECURITY SERVICES NETWORKS: AN ECONOMIC PERSPECTIVE[1]

Alok Gupta
Department of Information and Decision Sciences, Carlson School of Management, University of Minnesota, Minneapolis, MN 55455 U.S.A. {alok@umn.edu}

Dmitry Zhdanov
Department of Operations & Information Management, School of Business, University of Connecticut, Storrs, CT 06269 U.S.A. {dmitry.zhdanov@business.uconn.edu}

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 the decision to outsource the security operations of an organization may seem counterintuitive, there are potential benefits from joining an MSSP network that include pooling of risk and access to more security-enabling resources and expertise. We examine structural results explaining the reasons firms join an MSSP network, and characterize the growth of MSSP network size under different forms of ownership (monopoly versus consortium). We find that the need for an initial investment in MSSP networks (which is necessary to overcome the stalling effect) only affects the optimal network size for a consortium but has no impact on the optimal network size for a profit-maximizing monopolist. Our results provide an explanation why the majority of the MSSPs are for-profit entities and consortium-based MSSPs are less common. Such a market structure can be attributed to the potential for larger size by the for-profit MSSP owner combined with beneficial pricing structure and a lack of growth uncertainty for the early clients.

Keywords: Information security, managed security services, outsourcing, network effects, network growth, network ownership structure

Introduction

With the use of new technologies such as cloud computing, storage area networks, and mobile business devices, firms increasingly find that they are unable to manage security of their own resources. This is leading to one of the most interesting emergent phenomena: outsourcing of information security. Outsourcing of security services is an interesting but perplexing phenomenon because firms are often ready to hand over the security of their valuable digital assets to outsiders. From $140 million in 2000, the market for managed security services had grown to the 2010 revenues of $2.3 billion in North America alone (Kavanagh and Pescatore 2010; Scholtz and Parveen 2007; Sturgeon 2004). The European managed security service provider (MSSP) market is estimated at $2.5 billion in 2011, with a compound annual growth rate of 14 percent from 2011 to 2015, while MSSP growth in Asia is recorded at 31 percent (Casper 2011; Walls 2010). Recent industry research shows that almost all of the companies getting the best results from their information security efforts use managed security services as a part of their IT security strategy (Baroudi 2008).

[1]T. S. Raghu was the accepting senior editor for this paper. Eric Walden served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

The cost/benefit tradeoffs for MSSP arrangements are a cause of concern for potential clients. The risks of working with an MSSP include issues of trust, dependence on an outside entity for support of critical functions, and ownership of systems. However, there are multiple benefits that individual firms can derive by using MSSPs, including cost savings, adequate staffing, focused skill set, objectivity, independence, liability protection, dedicated facilities, and round-the-clock service (Allen et al. 2003). As the market for managed security services continues to mature, Gartner Research recently classified it as an "early mainstream" environment. This implies that between 5 and 20 percent of the target audience is using MSSP services (van der Heiden 2010). Despite the fact that MSSPs have been around for more than a decade, there are still adoption concerns.

In this paper, we explore the structure of MSSP markets as well as their formation process and stability. We try to identify whether there are economic benefits for firms in hiring external entities to manage their security. We look at the economic incentives that lead to particular choices in security outsourcing. For example, it may be beneficial for firms to join larger groups (MSSP networks) to protect themselves from potential attacks by hiding among other targets (hiding effect), as well as obtaining information on a wider range of potential attacks and protection tools (knowledge effect). Two different types of ownership structures for MSSP networks are compared: (1) a consortium-based approach, where several companies pool their resources to collectively provide security for their computing resources, and (2) a for-profit provider managing security for a group of firms. The issue of the preferable form of ownership of a given MSSP network is one of the most perplexing since for-profit MSSPs dominate the marketspace. Our analytical results are the first of their kind to support the current market landscape and show that firms may have stronger incentives for joining a for-profit MSSP, especially initially, when network size is small. We also show that, as long as a for-profit MSSP network is viable, the size of a for-profit proprietary MSSP is no smaller than the size of a consortium-operated MSSP serving the same set of potential clients.

The dynamics of growth for these MSSP networks are examined, with the network starting with a small group of firms and growing over time. A key concern in such a network is that it is not economically viable until a certain size is achieved. In the network externality literature, this phenomenon is called *critical mass* (e.g., Economides 1996; Oren and Smith 1981). Surprisingly, the issues of growth and optimal size of a network are not nearly as extensively explored as are the issues of standards, coordination, and choice of network (Liebowitz and Margolis 1998). Weitzel et al. (2000) call for reconsideration and new work in the area of network effects for applications in modern IT markets, emphasizing evolutionary system dynamics as one potential direction of development. Walden and Kauffman (2001) call for research on whether network externalities exist in specific e-commerce settings and how they affect the behavior of the actors involved. In response to these calls for research, we define optimal growth rules with respect to the viability and size of MSSP networks.

The paper is organized as follows. In the next section, we review the relevant literature and reasons for analytical work in the MSSP network field. We then provide a conceptual basis for our analysis, including defining the constructs used to analyze the market structure for MSSPs. Structural results indicating why individual firms prefer to share resources for security purposes are presented, and the MSSP networks under the two ownership structures are analyzed. The implications of the theoretical results are also discussed. We conclude with a summary of contributions and directions for future research.

Background and Literature

We conceptualize an 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 form is where a set of core firms join their security efforts and create a consortium. In this case, efforts and benefits are likely to be similar among participants. Alternatively, an 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.

There are two reasons the problem of MSSP network formation is related to the general perspectives of alliance formation and incentive analysis for information security decisions. First, outsourcing of information security is a counterintuitive activity, and it is necessary to understand the incentives that firms have to pursue such activities. Second, in our work, we study the consortium, which relies on joint decision making, as a possible form of ownership for an MSSP network. Research into the theory of collective actions has looked at

the efficiency of defense alliances such as NATO and found that, due to the 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 either econometric analysis of the effect of disclosure on firms' market value (Campbell et al. 2003; Cavusoglu et al. 2004; Schechter 2005) or from the perspective of formal analysis of economic threats and markets for sharing security information (Kannan and Telang 2004; Ozment 2004; Schechter and Smith 2003). With the possible exception of Gal-Or and Ghose (2005), who show that sharing security information has greater benefits for larger firms, research in this area does not look at the issue of formation and growth of information sharing entities—the issue that we are trying to address. An example of an information sharing entity is an information sharing and analysis center (ISAC). ISACs were established by Presidential Decision Directive 63 in 1998. These entities are responsible for critical infrastructure protection in several key industries (communications, electricity, public transit, etc.). It is interesting to observe that government intervention was required to establish ISACs, although they serve private industries. It is also worth mentioning that the degree of participation in ISACs is different between industries. For example, in 2003, the overall reach of ISACs was 65 percent of private infrastructures in the United States. In that year, the Telecom ISAC reached 95 percent of all wireless communication providers, while the Healthcare ISAC was in its formative stages[2] (ISAC Council 2004).

In terms of network growth in the presence of network effects, different forms of obstacles to organic network growth are possible—for example, excess inertia or momentum, tipping, lock-in, insufficient waiting, etc. (Farrell and Klemperer 2007; Stango 2004). In addition, such dynamics lead to suboptimal network size and welfare distribution by market mechanisms (Church et al. 2008). To overcome such effects, a variety of tools, including pre-announcements, expectation management, and other forms of coordination, may be used (Farrell and Klemperer 2007; Shapiro and Varian 1999). In our setting, the obstacle to organic growth of the MSSP network we find is critical mass. We propose a way to overcome this problem by using the investment mechanism, which serves as a signal of confidence from network owners to customers and allows for further organic growth.

The 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 the ownership of ATM networks by banks, a consortium market structure may bring greater benefits to members, thus achieving greater size and social benefit than monopoly-owned networks. In the context of a two-tier industry where ATM network owners sell services to member banks, a consortium ownership structure takes advantage of positive network effects and may achieve a larger size than in the case of a single owner. However, in their formulation, the value of the larger network is strictly increasing. We compare the consortium and monopoly market structures for MSSP networks and find that, in information security settings, start-up is easier with a consortium-owned network, but the monopoly-owned network can reach larger size. Our setting differs in two significant aspects from that of McAndrews and Rob: first, there is no multi-tier competition between network owners; second, we consider not only the positive effects of being on an MSSP network (access to information, etc.), but also the associated negative effects (higher susceptibility of large networks to attacks and increasing costs of protection measures).

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

Finally, the direction of network effect is considered. The majority of the literature looks at network effects that are positive (i.e., larger network size leads to greater benefits for consumers) (Gandal 2002; Matutes and Regibeau 1995). 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 network effects, where the addition of new users deteriorates the value received by those already on the network. Examples of such negative effects are congestion and information overload (David and Steinmueller 1994; Gupta et al. 1997; MacKie-Mason and Varian 1995). 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.

[2]Healthcare ISAC became operational in 2010.

Compared to competition between standards, work on network size and the network formation process has received significantly less attention in the literature. One example is the work by 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 on the process in the context of MSSP networks.

Furthermore, Weitzel et al. (2000) propose reconsideration of 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 its destruction), and separation of consumers and producers. A similar set of issues is raised by DeLong and Froomkin (2000). We look at information security, which is a good that displays the properties of 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 them. We use pricing mechanisms to internalize security externalities resulting from increased network size.

As mentioned earlier, access to additional information about security incidents is one of the benefits of joining an MSSP network. Several studies have looked at the problems of sharing security information among different entities. Gordon et al. (2003) consider a case when two firms form a security information sharing alliance and show that sharing 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 the market share of competing companies; they also show that such benefits increase with firm size. Both of these models were developed in a game-theoretic setting involving two entities. 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 do not make 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.[3] In addition, the issue of free riding does not occur in our setting, as all effects are internalized using the pricing mechanism. Before presenting our formal models, in the next section, the properties of modeling constructs are described.

Model Preliminaries

Suppose there are multiple identical firms (from the perspective of security needs and benefits) that are considering joining a network of other similar firms. Let N denote the size of such a network. Without loss of generality, a single firm may be 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 attempt to estimate this damage and counter it with security efforts. We may quantify the damage that may be inflicted to the entire network by a given attack as

$$D(N) = P_a(N) \times P_s(N) \times N \quad (1)$$

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

Note that both the probability of an attack taking place and that attack 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. Note that these assumptions are realistic and reasonable. For example, larger networks are more likely to be attacked because they attract more attention. The likelihood of a random attack also increases with a larger network. Since firms are physically sharing the security technology, a failure in one infrastructure component (e.g., server-based antivirus) will affect all members, as opposed to the case when each firm maintains its own security infrastructure. Furthermore, even though the membership information of MSSP networks is not likely to be publicly available, attacks on different networks that are served by the same MSSP provider are more likely to occur due to topological proximity of these networks.[4] 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

[3]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.

[4]We address model sensitivity to these assumptions later in the paper.

clients. Larger networks also have more resources to negate sophisticated attacks and benefit from 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.[5]

To further validate the assumptions of our model parameters, we used the network traffic data used in KDD Cup 1999[6] to construct innovative simulation experiments that can measure the parameters of our model using empirical measurements. The goal of our simulation is to model a learning process that takes place as the MSSP network grows. With each additional client that joins the network, there is an opportunity to observe some novel traffic patterns, which may lead to the discovery of new attacks as well as to refining the detection criteria for the known attacks. Our simulation design is described in Appendix A.

Figure 1 represents the experimental findings about the probability of an attack taking place and the probability of the attack succeeding, respectively. It approximates P_a as a ratio of attack types visible to a 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). P_s is represented as the classification error as described earlier. We see that $P_a(N)$ is increasing in N and $P_s(N)$ is decreasing in N, as we assumed before.

The value of the MSSP network comes from its ability to reduce potential damage to its members through superior technology and a larger amount of attack information. Figure 2 represents an approximation of such benefits by plotting unit expected risk of being on the network versus being alone. Based on these observations, we assume that the value of the MSSP network, $V(N)$, can be represented by an increasing, concave function. On one hand, the value derived by the members of the MSSP network has to increase with its size, otherwise all firms would prefer to provide their own security solutions. On the other hand, the growth of the MSSP value slows down with size, since larger networks attract more attacks, which are also more sophisticated. These tendencies are well understood by practitioners. For example, one major driver of joining an MSSP network is the ability to detect some attacks (namely, e-mail threats, botnets, and denial of service attacks) "in the cloud," that is, by aggregate events or traffic at the provider level (Baroudi 2008). The tendency of large networks to attract more attacks is illustrated by the U.S. Department of Veterans Affairs. It is the second-largest federal computing enterprise in the United States, and as stated by its cybersecurity chief, Bruce Brody, in 2002, "the magnitude of our enterprise alone makes it a target of malicious intent" (Hasson 2002).

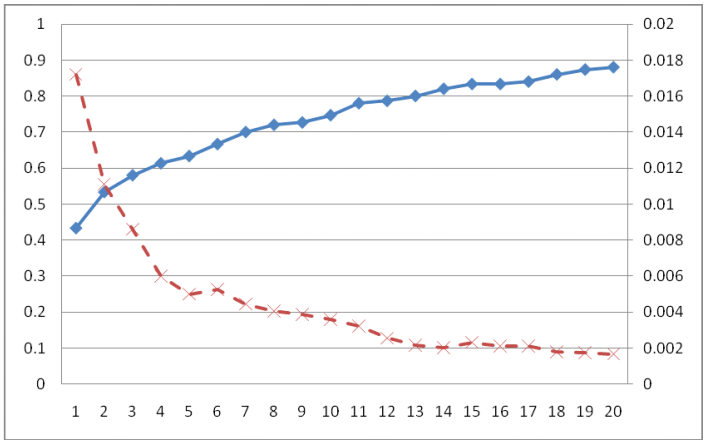
Once the potential value of the MSSP network has been estimated, it is necessary to understand the costs of maintaining such a network. Let $R(N)$ be an input requirement function that describes the amount of resources needed to provide the level of information security associated with the size of an MSSP network (i.e., the expense required to put in the countermeasures necessary to protect N clients). This assumption is a key differentiating point, different from the typical IT cost structure, and is based on reported experience in practice. For example, a recent Gartner report (Wheatman et al. 2005) points out that, at the beginning stages of MSSP network growth, the majority of the investment has to go into the basic infrastructure technologies such as firewalls and antivirus tools ("keeping bad guys out"), with reasonably stable costs. Once the network gets larger, the focus of investment shifts to "letting good guys in" technologies, such as authentication and access management, that require more effort in configuration and management. Since the difficulty of providing additional security (in terms of the amount of resources required) grows at an increasing rate, we assume that, mathematically, $R(N)$ is an increasing convex function.

The resource requirement function reflects a peculiar nature of information security: it is not a regular commodity good. 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. The effort of provisioning security for a given network size balanced with the additional benefits available to members defines the value of the MSSP network. The net value of the network can then be written as

$$W(N) = V(N) - R(N) \quad (2)$$

[5]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.

[6]The 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.



P_a = solid line, left axis; P_s = dashed line, right axis

Figure 1. Probability of Attack Occurrence and Attack Success in a Network of Given Size

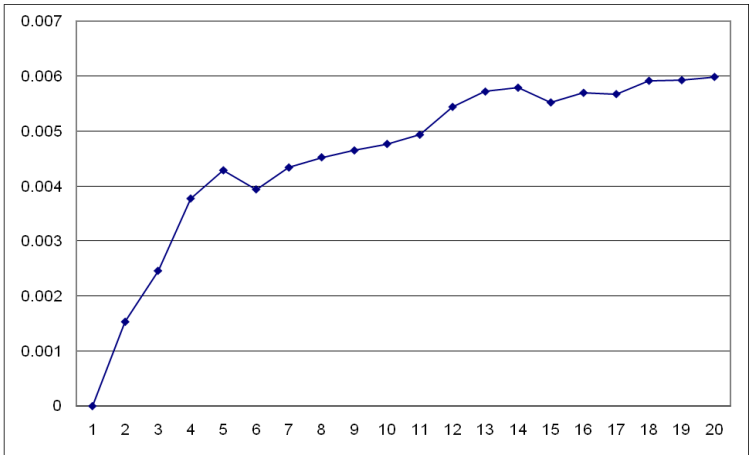


Figure 2. Approximation of Network Value from Simulation Data

In order to ensure voluntary participation in the MSSP network, the firms must have some benefit as compared to handling security on their own. If both benefits and costs of being a part of the MSSP network increase with the network size, it is not clear whether the firm should participate and hence the difference between the two should be considered an appropriate decision rule. However, if attack risk is the only consideration, then there are two potential metrics of such rationality. First, firms may want to make sure that any potential damage they face while on the network is smaller than what they face on their own. Second, firms may want to make sure that the fraction of the security cost they contribute to be on the MSSP network is less than the cost of handling security alone.

From the perspective of cost and damage only, when both of these conditions hold, firms have an incentive to join the MSSP network; it is not rational to join if both conditions are violated. The situation becomes ambiguous when only one of these conditions holds—for example, when damage reduction requires too many resources, or when the individually feasible contribution to the network does not reduce damage to an acceptable level. This ambiguity is resolved once the benefit of the network— $V(N)$— is considered.

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 concerned with their payoffs only. Our model assumptions follow:

- 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, self-interested, price-taking, and individually rational.
- The risks of being on the MSSP network are distributed equally among clients.
- Once the MSSP network is started, clients join one at a time.
- The MSSP can deny entry to a new client, but will not expel an existing client.
- Information about the current size and membership of the MSSP network is openly available.
- Both clients and the MSSP are able to anticipate the future size of the network.
- Clients are maximizing the value of their security effort (either stand-alone or as a member of the MSSP network).
- The MSSP has the objective function specific to its form of ownership: maximize member value for the consortium; maximize revenue for the sole for-profit provider.

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 an MSSP network. One possible objective that provides positive benefits to MSSP network members is to maximize the total net benefits derived from the MSSP network.

$$\max W(N) \Leftrightarrow \max[V(N) - R(N)] \quad (3)$$

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

$$dR / dN = dV / dN \quad (4)$$

Let the solution to equation (3)—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 the previous section that $D(N) = P_a(N) \times P_s(N) \times N$. We assume that the damage function is convex.[7]

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

We will now explore how this shape of damage function impacts the incentives of firms to join MSSP networks, starting with two intuitive observations of MSSP clients' behavior that we call a *hiding effect* and a *knowledge effect*. The hiding effect makes the individual firm less attractive as an individual target since there may be several interesting targets, while the knowledge effect exists if the marginal amount of knowledge that a firm gains in the larger network outweighs the marginal increase in risk of attack on a larger network. Both of these effects are emergent properties of the MSSP network and are not exogenous modeling constructs; they are characterizing firm behaviors in an MSSP environment. The hiding effect is a basic motivation for the firms to join the MSSP network, just to make an attack on a particular firm more complicated for the attackers. The knowledge effect, however, is the key to unlocking the power of the MSSPs and essentially their major selling point: to build up expertise on attacks and appropriate defenses by observing a large network of clients. Formally, the hiding effect captures the difference in exposure between being a part of an MSSP network and providing security alone for any particular firm, and can be measured as

$$H(N) = P_a(N) \times P_s(N) - P_a(1) \times P_s(1) \; (= D(N)/N - D(1)/1)$$

Similarly, the knowledge effect captures the improvement in security that is due to the addition of a new node to the network and can be measured as

$$K(N) = P_a(N) \times P_s(N) - P_a(N-1) \times P_s(N-1)$$

[7]It is easy to verify that the damage function may be either (1) monotonically increasing (local minimum at 1), (2) monotonically decreasing (local maximum at 1), or have a unique (3) local maximum or (4) local minimum in $(1, \infty)$. In case (1), the MSSP network does not offer obvious benefits in terms of reduced risk and may not be attractive to firms. In cases (2) and (3), the most attractive MSSP network size is infinitely large and the problem is trivial (although in case (3) there may be an issue of critical mass in the 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.

It should be noted that the desired values of both of these effects in an MSSP setting should be negative—this way they represent the *reduction* of exposure for an individual MSSP network. If these effects are positive in value, it is actually detrimental to the overall state of security in the network. Another observation is that, although both of these effects are emergent properties of the model, they have a mathematical relationship. Essentially, with the addition of each new member to the network, the knowledge effect represents an incremental change in individual exposure to attack as the result of access to new information. The hiding effect then becomes a cumulative change in the exposure level since the inception of the network. Formally, this result can be represented as

$$H(N+1) - K(N+1) = H(N)$$

The underlying structure and dynamics of these effects is presented in detail in Appendix B. We would like to note, however, that both hiding and knowledge effects provide intuition regarding the possible size and growth dynamics of the MSSP network. We will discuss these issues after the growth structure is presented. We have verified the existence of a hiding effect as well as a knowledge effect in the simulation described above; Figure 3 illustrates our findings. The negative values of the hiding effect indicate that a firm's expected damage from being on an MSSP network is smaller than that of being alone. Similarly, the negative values of the knowledge effect indicate that additional information gained on the larger network outweighs the danger of greater exposure.

The exact dynamics of MSSP network growth can be analyzed only by looking at $R(N)$ and $V(N)$ jointly. Therefore, we need to balance both risk and reward in analyzing firms' decisions. This requires identification of the optimal total network size. One of the approaches to ensure positive benefits would be to optimize the net benefits derived from the network (i.e., $W(N) \equiv \max[V(N) - R(N)]$). However, while maximizing the net benefit from the network may seem like a desirable goal for, at least, a consortium-based MSSP, it is unlikely that a consortium with equal partnership would be able to 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.

Analysis of Market Structure for MSSP Networks

As mentioned earlier, we are interested in the dynamics of MSSP network growth. Specifically, since it is unlikely that a network will have all 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 structure:

1. A consortium-based MSSP network where several firms combine their efforts to provide security for their collective networks.

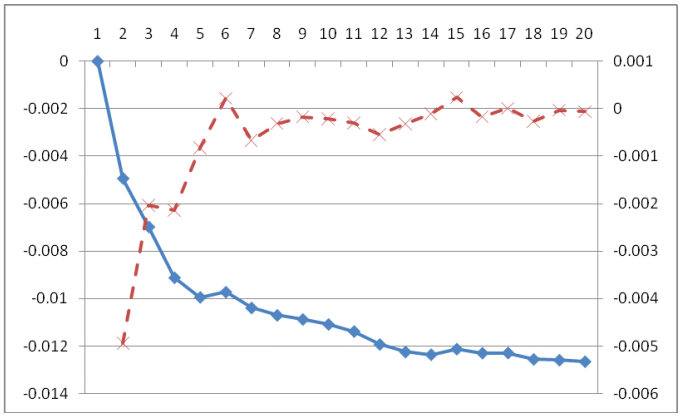
2. A MSSP network facilitated by a for-profit firm that attracts various firms under one umbrella for the purpose of providing security solutions. This seems to be the most prevalent form of market structure for MSSP networks.

While the market for managed security services is dominated by for-profit providers, a consortium of several firms jointly handling information security issues may be a viable form of MSSP. For example, a consortium of French firms known as CERT-IST was established in 1999 and outsourced to Alcatel to manage vulnerability and alert services (Martines et al. 2006). A government entity may also be the cause for the creation of the consortia. For example, the U.S. Department of Veterans Affairs established a consortium of five companies known as VA Security Team (VAST) in 2002. VAST handles incident analysis and response for the DVA (Hasson 2002). From the theoretical perspective, government mandated consortia may be helpful in preventing monopoly power in industries with sunk costs (Bailey 1981). Consortia are usually based on some sort of cost-sharing scheme that is fair to its members (Aloysius and Rosenthal 1999). Although it is hard to identify pure MSSP consortia, there are some meek attempts to get those going. A few examples include:

- ICSA Labs has recently announced its new Endpoint Security Consortium, which will develop ways to properly test anti-malware, and host intrusion prevention and detection and personal firewall technologies to certify integration between the products (Vahalia 2010)

- EnergySec, a private, nonprofit consortium of security professionals in the energy field was recently selected by Department of Energy to create a national cybersecurity organization for the energy sector (EnergySec 2010).

- Credit Union National Association selected Perimeter Internetworking as the "official" MSSP provider to its member credit unions. While not an in-house development, this is an acquisition of a unified integrated platform available to credit unions at a volume discount (Business Wire 2006).



Hiding effect = solid line, left axis; knowledge effect = dashed line, right axis

Figure 3. Hiding and Knowledge Effects in MSSP Simulation

Before we examine the specific market structure, let us outline the process that we consider necessary for the formation and growth of an MSSP network. We assume that a set of firms initially join the MSSP network. In the 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. Without loss of generality, we assume that the firms arrive sequentially in a single period. We assume that each new incoming firm is a price taker (i.e., it agrees to pay whatever charges are asked for by the consortium or the for-profit provider as long as the expected benefits are greater than or equal to zero). Note that since the payoffs are instantaneously computed and readjusted with each new client joining the MSSP network, if it is optimal to join now, from a firm's perspective, it will always be optimal to join in the future when the MSSP network is optimizing its size. Delaying, however, is not a beneficial strategy for any potential client in our setup because the MSSP network may reach its optimal size and not admit new participants. 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.

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:

$$W(N) = 0 \quad \text{or} \quad V(N) = R(N) \tag{5}$$

This problem represents the desired outcome in the case of a social planner concerned with providing adequate security for the largest number of entities, using all available resources. 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 consortium, benefits to all the members are zero. For the MSSP to have an incentive for maintaining a network, there must be positive profit from operation. Another approach to computing potential size of the MSSP network was presented in the total benefit maximization problem discussed in the previous section. The optimal solution occurs when the derivatives of the value and resource function are equal to each other. Figure 4 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 4 also depicts the range of possible network sizes for an MSSP network. As the figure indicates, the maximum size of an 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 an MSSP network that maximizes social benefits, N_s^*, is achieved whenever the distance between the two curves is greatest. 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 firms

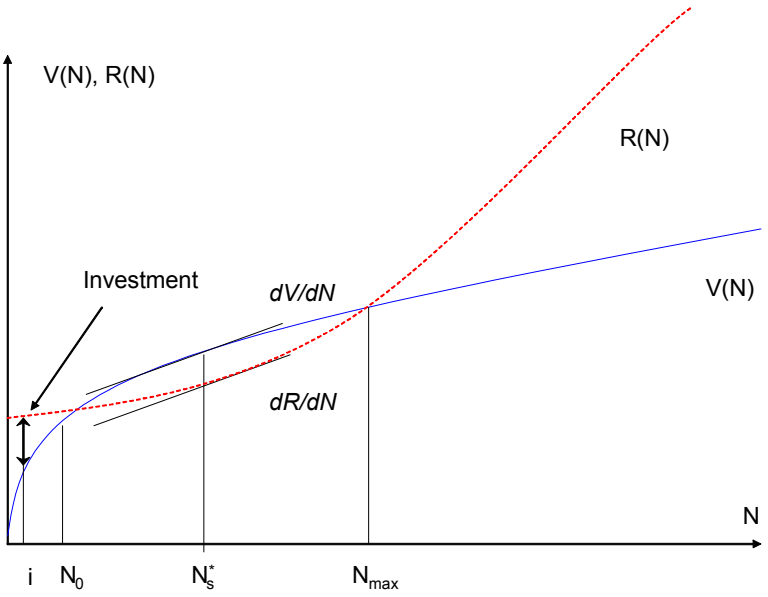


Figure 4. Number of Firms and MSSP Benefits

to join the network, as 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).

Since the attractiveness of an MSSP network is both a function of its value and the resource requirements which, in turn, depend on the network size, the expected size of the network plays a significant role in an individual firm's decision to join the network (Bensen and Farrell 1994; Economides 1996; Katz and Shapiro 1985, 1994). While the classical start-up 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 the lack of an instantaneous net benefit for a firm if there aren't enough members already. This phenomenon is related to the concept of critical mass (Oren and Smith 1981; Rohlfs 1974). The critical mass theory suggests that sustainable growth of a network is attainable only if there is a minimal nonzero equilibrium size (Economides 1996). In Figure 4, N_0 represents this critical mass. If the initial size of the network, i, is less than N_0, then the network cannot automatically (or "organically") grow. Economides and Himmelberg (1995) consider this a "chicken and egg" paradox since the 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 1 (Critical Mass for MSSP): If the initial size of the MSSP network is i, then the 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 4; in the interval $(0, N_0)$ the net benefits to the firm of joining the MSSP are negative since $R(N) > V(N)$. When the 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 the case of a consortium, this investment has to come from the founding members, while in case of a for-profit provider, this investment has to be made by the provider. Riggins et al. (1994) and Wang and Seidman (1995) provide similar results, indicating the need to potentially subsidize the adoption of interorganizational networks. Both of these works show that adoption of a system such as an 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. show that, unless such a subsidy is provided, network adoption will stall after the initial takeoff. Our case is different, however, as suppliers and buyers of the resources necessary to provide information security are the same entities, thus making even an initial takeoff problematic. We 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 an initial investment to overcome the start-up problem and will study the effect of this investment on efficient maximum network size.

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 the consortium evaluates its 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 to all members of the consortium. Since all members are identical, the benefits are identical for all members; therefore, the benefit to each member can be computed by dividing total net benefits by the number of firms that are members of the consortium.

Before proceeding to the analysis, we would like to make a brief comparison of our formulation with the common modeling approach in the cooperative game framework. While there are clear similarities, our method helps produce results similar to or more robust than those of a cooperative game. For example, the formulation of the MSSP dynamic growth process has all of the important properties of cooperative games, such as monotonicity (consortium payoff increases with size) and superadditivity (the combined benefits of two smaller consortia are smaller than those of a single large consortium). It also corresponds in properties to the common solution concepts such as the core and Shapley value. According to Shapley (1953, p. 316),

> The players…agree to play the game…in a grand coalition, formed in the following way: 1. Starting with a single member, the coalition adds one player at a time until everybody has been admitted. 2. The order in which the players are to join is determined by chance, with all arrangements equally probable. 3. Each player, on his admission, demands and is promised the amount which his adherence contributes to the value of the coalition….The grand coalition then plays the game "efficiently" so as to obtain …exactly enough to meet all the promises.

It is clear from this description that our formulation implements the Shapley value mechanism. In addition, we provide a description of the revenue sharing mechanism that implements the equal treatment property, and we prove the optimality of that mechanism. However, our approach makes fewer assumptions and provides additional results such as the implementation of an optimal, equal treatment-based consortium value distribution mechanism. More detailed comparison of our approach with the cooperative game setting can be found in Appendix C.

Next, we present the analysis of the dynamics and viability of an MSSP consortium. We study 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.

Consortium Without Need for Initial Investment

When there is no initial investment requirement, the problem of the consortium is to maximize the expected benefit for its members. Mathematically, it can be represented as

$$\underset{j}{Max} \frac{V(j) - R(j)}{j} \forall j \geq N_0 \tag{6}$$

This objective function for the consortium represents a fair allocation of resources and benefits among the consortium members; therefore, it is a preferred decision approach for the consortium-based MSSP. To solve the problem, we need to look at the first derivatives of decision functions. Thus, the first order optimality condition is given by

$$V'(j) - R'(j) = [V(j) - R(j)] / j \tag{7}$$

Let us define the optimal consortium size in this case as N^*_{cn} (where N^*_{cn} is a solution to equation (7)). It can be shown that, in this case, the size of consortium will never exceed the welfare maximizing size N^*_s (i.e., it is possible for the consortium to stop growing somewhat prematurely).[8] This implication is formally stated in Proposition 1.

> **Proposition 1 (The Optimal Size of Consortium Without the Need for Investment)**: The optimal size of a consortium-based MSSP with no need for initial investment (i.e., if the network is in post critical mass stage), N^*_{cn}, will be less than or equal to the welfare maximizing MSSP network size N^*_s (i.e., $N^*_{cn} \leq N^*_s$).

[8] All of the proofs are provided in Appendix D.

Viability of a Consortium

We now consider the case when the initial founders of a consortium need to make an investment to facilitate the MSSP network, that is, the initial network size $i < N_0$, the critical mass. Essentially, investment is the allocation of resources that a participating firm (or firms) has to make in order to make a consortium operationally feasible. 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 newly arriving firms 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 initial investment is shared equally among the firms. Note that once the initial investment is made, no further investment is needed since the resource requirements, as compared to the benefits, are decreasing with the number of consortium participants. Therefore, the start-up problem is resolved and the network will grow organically after the investment takes place.

In order to negate the start-up problem, we propose the following investment and investment-recovery approach: The initial investment amount $R(i) - V(i)$ is equally shared by the initial founding members of the MSSP network 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 (organic growth is possible since $V(i + k) + L > R(i + k)$). 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 the $j+1^{th}$ member joins the consortium, it pays an initializing fee[9] in the amount of $F = [R(i) - V(i)] / [j(j + 1)]$, which is equally divided among the j previous members; that is, 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 of the $j+1$ firms equally sharing the cost of the initial investment with individual contributions equaling $[R(i) - V(i)] / [j(j + 1)]$ for each firm. To see whether this rule is appropriate, let us first define the viability of an MSSP network with an investment requirement to overcome the critical mass problem. This definition specifies that a network that cannot recoup its initial investment is not viable.

> **Definition (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. Also suppose that the MSSP network requires an investment to overcome the start-up problem (i.e., $i < N_0$). Then, this network is viable if at the optimum network size, the benefits of the MSSP network are greater than the initial investment; that is,

$$V(N^*) - R(N^*) \geq R(i) - V(i);\ i < N_0 \tag{8}$$

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 2 states, our rule that forces each consortium member to bear an equal amount of the initial investment is the optimal rule from the perspective of viability of an MSSP network.

> **Proposition 2 (Equal Sharing and MSSP Network Viability)**: Let the investment i be recovered by using the equal sharing rule at a given size n. If n is viable, then n is the minimal viable network size and the equal sharing rule is optimal.

Optimality of Consortium with Investment

Now let us consider the problem of optimal consortium size with investment. The problem of the consortium, as before, is to maximize the benefits for its members; however, we also need to account for the start-up costs. Mathematically, this problem can be stated as

$$\underset{j}{Max} \frac{V(i) - R(j) - C}{j} \forall j \geq N_0 \tag{9}$$

where $C = R(i) - V(i)$, the initial investment

As before, we need to identify the first order conditions for the optimum solution, which is

$$V'(j) - R'(j) = [V(j) - R(j) - C] / j \tag{10}$$

Let N_c^* denote the optimal consortium size in the presence of the initial investment (N_c^* is a solution of equation (10)).

[9]For example, Denver's Greater Metro Telecommunications Consortium (GMTC) has the following statement on its website: "Reimbursement by the new Members of the Consortium for the expenses of the Consortium resulting from addition of the new Member, including, but not limited to, reasonable attorneys' fees, consultants' fees, accountants' fees, engineering fees and all other such reasonable out-of-pocket expenses as may be incurred" (http://www.gmtc.org/membership/how_to_join_agreement.asp).

Then, Proposition 3 provides a surprising result regarding the optimal MSSP consortium size with initial investment as compared to optimal consortium size without initial investment.

> **Proposition 3 (Optimal Size of MSSP Consortium with Investment)**: The optimal size of an MSSP consortium that requires the initial investment to overcome the critical mass problem, N_c^*, is equal to or greater than the optimal MSSP network size without investment (i.e., $N_c^* \geq N_{cn}^*$).

Another interesting question related to an MSSP consortium is with regard to 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 equal to $V(N_s^*) - R(N_s^*)$,that is, the maximum net benefit of the consortium. Therefore, the minimum starting size should be such that the required investment is less than or equal to the maximum net benefit that the MSSP network can provide. Lemma 4 formalizes this result.

> **Lemma 4 (Minimum Viable Initial MSSP Consortium)**: The minimum starting network size is given by $I^* = min\{i: V(N_s^*) - R(N_s^*) \geq R(i) - V(i)\}$.

Proposition 3 and Lemma 4 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 an initial investment, it is feasible to achieve the socially optimal network size N_s^*. We illustrate the relative size of an MSSP consortium under different conditions in example 1.

Example 1: Suppose that the value and resource requirement functions have the following functional forms

$$V(N) = 10\,N^{1/2};\;\; R(N) = 0.1\,N^2 + 17$$

where N is an integer number no smaller than 1.

Both of these functions conform to the assumptions presented earlier. It is easy to verify that the net benefit maximizing consortium size, N_s^* is 9.

Suppose that the consortium was started by two firms that jointly assume the start-up cost of 3.256 (since $V(2) - R(2) = -3.256$). In this case, the optimal size of the consortium, N_c^*, is 8, as the maximum benefit that each firm can achieve with an initial investment of 3.256 is $[V(8) - R(8) - 3.256] / 8 = 0.203$. However, if the consortium was started by four firms, then, since there was no initial investment required, the optimal consortium size with no investment would become $N_{cn}^* = 7$ since $[V(7) - R(7)] / 7 = 0.651$ while $[V(8) - R(8)] / 8 = 0.611$.

Figure 5 illustrates the relative ordering of possible consortia sizes. Note that the minimum viable size is two firms, since a network started by one firm can't recoup the initial investment (best benefit in this case is achieved at size $N = 9$ and is equal to $[V(9) - R(9) - 7.1] / 9 = -0.244$, since the initial investment required from a single founding firm is $V(1) - R(1) = -7.1$)

In this example, all three possible consortia sizes (without investment, with investment, and net benefit maximizing) are distinct, representing a general case of ordering described in Propositions 1 and 3. Occasionally they may coincide, but the general ordering is the same.

Next we consider the problem of a monopolist, for-profit, MSSP.

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 charging each customer an individual price equal to the 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 an "introductory pricing" approach desirable in the presence of network externalities. Similar to the consortium, investment is the allocation of resources that the monopolistic provider has to make in order to make a for-profit MSSP operationally feasible. 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 and the necessary critical mass is achieved, the provider can then charge each subsequent customer a monopoly price $P_{N_0+j}^M = [V(N_0 + j) - R(N_0 + j)] / (N_0 + j)$. However, for customers that arrive after the size N_s^*, the provider needs to potentially compensate some customers who joined earlier since the overall shared benefits of the network decrease. Recall that N_s^* is the size of network that maximizes average benefits to each client. Therefore, while marginal benefit 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 only source can be the price charged to the new client.

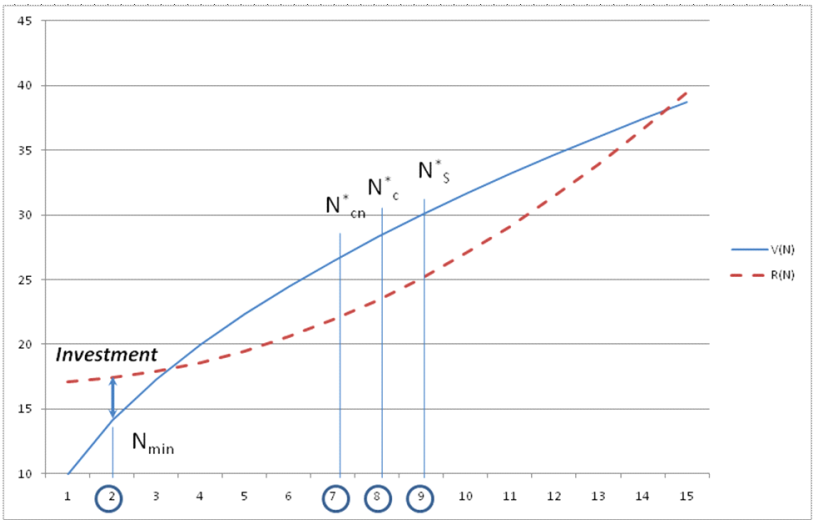


Figure 5. Ordering of Possible Consortia Sizes

We now consider the drivers of growth of a monopolist MSSP network. In order to maximize the revenues,[10] the monopolist establishes a differential pricing scheme, while making sure that there are still incentives for customers to join the network. This problem can be written as

$$\underset{j}{Max} \sum_{j=1}^{N} P_j^M \tag{11}$$

Subject to

$$[V(j) - R(j)]/j > P_N^M \forall j < N \tag{12}^{11}$$

Note that while this problem looks complex, it can be solved using a polynomial-time search algorithm.[12] The basic realization here is that when a firm $k > N_s^*$ joins the MSSP network, the provider needs to compensate all customers who were initially charged an amount greater than $[V(i) - R(k)]/k$.

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, as was shown earlier, will not grow beyond N_s^*). Since the monopolist must recover its cost from the differential prices where $[V(j) - R(j)]/j$ where $j \geq N_0$, the viability size for the for-profit MSSP is higher than the consortium. The viability condition for the monopolist can simply be stated as

$$\sum_{j=N_0}^{N_m^*} P_j^m \geq R(i) = V(i) \tag{13}$$

where N_m^* is the optimal network size as a solution to equations (11) and (12)
P_j^m are the adjusted prices charged under the provider's pricing scheme
$R(i) - V(i)$ is the initial investment made by the provider

Note that the optimal network size for a for-profit provider, unlike a consortium, does not depend upon the initial investment. However, the viability of the MSSP network does depend on the initial size i. Therefore, a for-profit monopolist will not start an MSSP network unless the condition in equation (13) is satisfied. Therefore, as a strategy, the provider will offer network access for free to all firms that initially sign up for the MSSP network. Proposition 5 formally provides the condition for the monopolist MSSP network to be greater than the net benefit maximizing network size.

Proposition 5 (Monopolist MSSP Versus Social Net Benefit Size): The monopolist MSSP may have

[10]The full problem of profit maximization also includes costs, and they are considered next. However, only revenues define the growth of the network.

[11]If $j < N_0$, then $P_j^M = 0$, else $P_j^M = W(j)/j$ —the monopolist gives free access to overcome initial stalling, then charges every client its true value.

[12]A pseudocode for this polynomial time algorithm is provided in Appendix F.

a larger network size than the social net benefit maximizing size if it can provide sufficient compensation for all current members of the consortia who lose value due to the addition of another member beyond the social benefit optimal. The price charged to the extra member is the source of this compensation.

Corollary 5.1 **(Monopolist MSSP Versus Consortium MSSP)**: The monopolist MSSP, if viable, will have a network that is at least as large as a consortium MSSP for the same set of firms.

Corollary 5.2 **(Monopolist MSSP versus Consortium MSSP Viability)**: Under certain conditions, while the consortium is viable, the monopolist is not.

Example 2 provides further intuition by considering the specific case when the $(N_s^* + 1)^{st}$ customer only affects the previous customer (i.e., customer N_s^*).

Example 2: Suppose the only firm affected by the addition of $(N_s^* + 1)^{st}$ firm is the $N_s^{*\text{th}}$ firm (which joined the network last). Then the provider can at least have a size of $N_s^* + 1$ if $P_{N_s^*}^M < 2\,P_{N_{s+1}^*}^M$. In other words, if the price charged to a new customer is greater than the price charged to $N_s^{*\text{th}}$ customer, then the monopolist MSSP provider can sustain a network size larger than the 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[13] for the dominance of for-profit MSSP networks over the consortium-based approaches. A summary of our results is presented in Table 1.

Effect of Assumptions on Model Performance

As with all economic models, it is necessary to discuss the robustness of the model results to the changes in the original assumptions. Specifically, we need to discuss the role of the probability of an attack, $P_a(N)$, the shape of the resource requirement function, $R(N)$, and the impact of the probability assumptions on the dynamics of the hiding and knowledge effects and implications for MSSP growth. We will also explore the impact of the client firm heterogeneity on the dynamics of MSSP network growth.

In our formulation, we assume that the probability of an attack taking place increases with the size of the network, since larger networks attract more attention—for example, the Department of Veterans Affairs. However, one might argue that this probability should stay fixed (since attacks are random) or even decrease (since larger networks may intimidate potential attackers). We need to make two observations here. First, if attack probability is in fact constant or decreasing, then our results become stronger, since the knowledge effect becomes more prominent. By assuming the increasing probability of an attack, we are actually studying the most problematic situation for an MSSP. Second, we can argue that, realistically, the probability of an attack should increase with the size of the MSSP network. The addition of each new client provides extra possible attack vectors for the existing clients. Thus, addition of the N^{th} client introduces $N - 1$ new connections that need to be monitored. This situation is depicted in Figure 6.

As for the shape of the resource requirement function $R(N)$, we need to note that, again, we are considering the most general form of the cost function—that is, increasing at the increasing rate (convex). A similar assumption was also made by DiPalantino et al. (2010) in their analysis of competition and contracting of service industries with congestion. The convex resource requirement function $R(N)$ allows for multiple sets of functional forms that are more restrictive in nature including linear, power, and exponential functions, as illustrated in Figure 7. However, our general results still hold.

Structure of Attack Probabilities: Its Effect on Hiding and Knowledge

There could be interesting dynamics of hiding and knowledge effects based on the different functional forms of the underlying probabilities P_a and P_s. We decided to explore numerically how different magnitudes and trends in P_a and P_s affect the knowledge and hiding effects. The biggest issue is which one of these probabilities dominates, and that is determined by the functional forms. Given a large number of possible functional forms, a computational analysis is more appropriate than a formal model.

[13] In addition to the expertise-based arguments.

Table 1. Comparison of Consortium-Based and Monopoly MSSP Networks

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

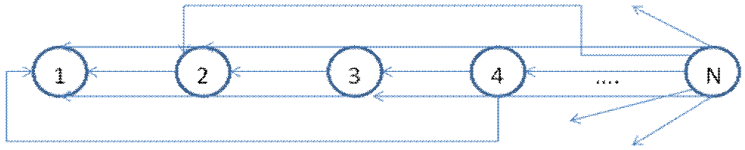


Figure 6. Nth Client Introduces N – 1 Possible Attack Vectors on Existing Systems

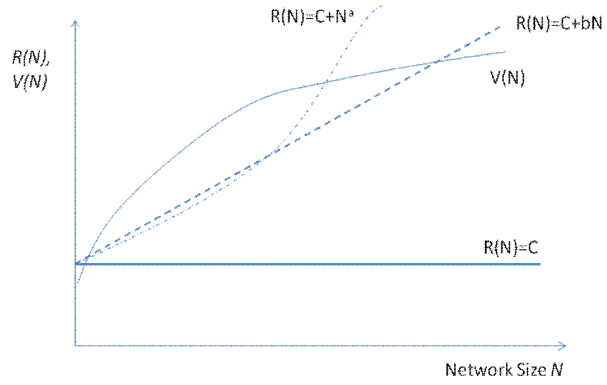


Figure 7. Convexity of $R(N)$ Allows for a Variety of Formulations

We picked the form of $P_a = N / (N + 1)$. It asymptotically approaches 1 as N grows, reflecting the fact that larger networks are more likely to be attacked. In the limit, it also behaves in a similar way to the first-degree polynomial. Basic intuition suggests that the state of the system would be then impacted by the limit degree associated with P_s, which may be higher or lower than 1. A possible functional form for it is $P_s = a + (1 – a) / (N^k)$, where $0 < a < 1$, $k > 0$. In this case, a is the residual probability of attack success (this is how close we can get to perfect attack detection as the network grows) and k is the speed of learning (if it is high, we converge to the asymptote very fast; if it is low, larger network is needed to gain the same knowledge).

We have explored the dynamics of hiding and knowledge effects for several combinations of a and k. The intuition suggests that asymptotic behavior (cases when N is large) should be more or less the same, with knowledge effect eventually converging to zero and hiding effect converging to some related stable value. However, there are more interesting dynamics in the earlier stages of network growth, which are really the region of interest to MSSP members: we know that MSSP growth will stop at some size. These early-stage dynamics may influence the resulting size of the network. Figure 8 presents the dynamics of hiding and knowledge effects as the model parameters change.

The area with mesh shading represents system behavior, which is the focus of our work. Low values of a indicate that there is a substantial amount of knowledge to be gained, while moderate values of k indicate that learning takes place at a moderate rate. In this region, we see essentially the same pat-

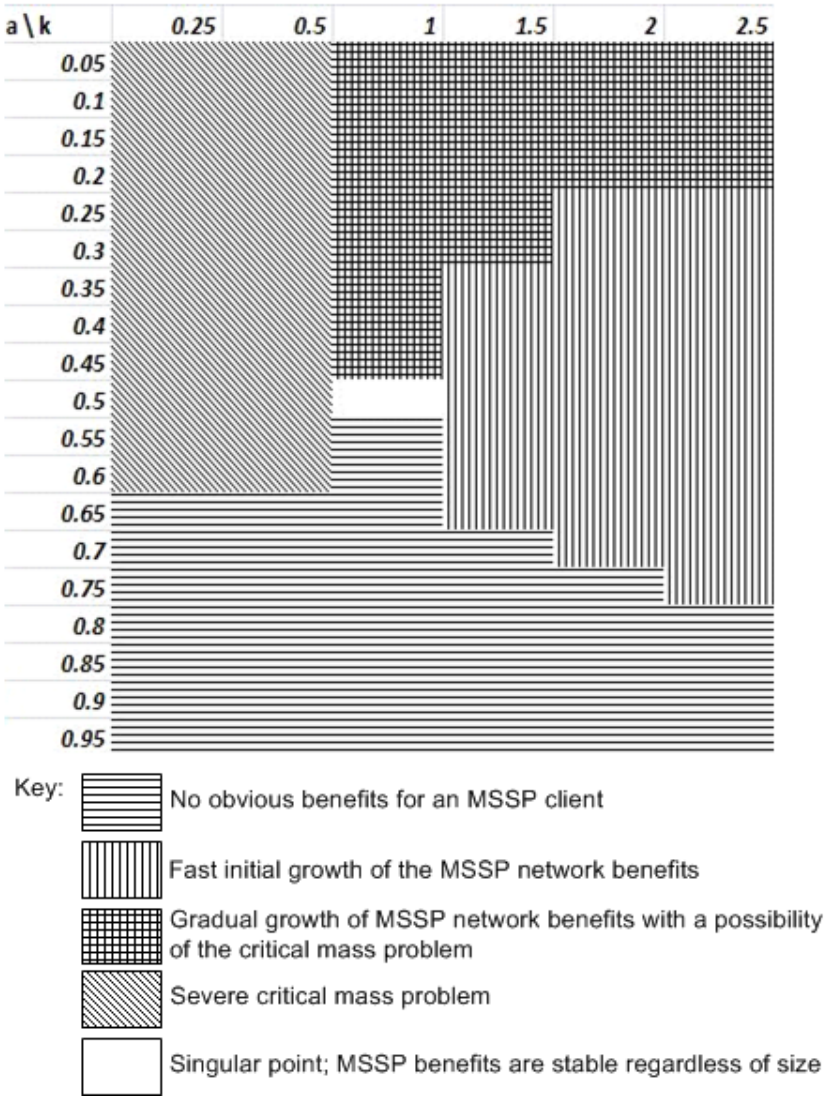


Figure 8. A Contour Plot of Sensitivity of Hiding and Knowledge Effects

tern that we observed in our simulations. First, both effects are negative in value, which is good for the MSSP—it means that new members joining reduce the potential negative impacts. Second, we observe the forecasted asymptotic behaviors.

The area with diagonal shading corresponds to situations where the critical mass problem is more severe. In this region, the potential amount of knowledge to be gained is smaller than in the previous case (higher values of a), and the learning rate is slower (smaller values of k). Because of that, at the start of network evolution, knowledge effect is positive in value, which is detrimental to the overall state of security. This exacerbates the critical mass problem: at the early stages of MSSP, in addition to the start-up cost, there is little if any value to join. However, as the network grows, knowledge effect reaches the desirable region and hiding effect tends to follow. Unfortunately, the network may have to be too large (and, therefore, prohibitively costly) to tap into the expected benefits.

The area with horizontal shading corresponds to the cases where there are no obvious benefits for the firms to join an MSSP network, or a situation where the potential for learning is limited (high values of a). Not surprisingly, both hiding and knowledge effects stay in the positive (detrimental)

region, indicating that when there is no valuable information in a larger network, firms should not join an MSSP and should provide their own security.

In contrast, the area with vertical shading addresses cases where learning in the network is very quick and most of the value is realized in the early stages of network growth (high values of k). Here, essential knowledge is gained quickly due to a faster learning rate. This may represent another limiting condition to the growth of the MSSP network: very quick capture of potential value.

Finally, the unshaded area represents a singular case ($k = 1$, $a = 0.5$). Here, all of the reduction in the probability of attack success (P_s) is immediately and equally offset by the increase of the probability of an attack taking place (P_a). Both knowledge and hiding effects are identically equal to zero, and firms are indifferent between being an MSSP member or a stand-alone entity. Given the overhead costs of running an MSSP, it is unlikely to be started.

In summary, we identify how the intensity of learning and learning potential may affect the MSSP size and growth dynamics. Slow learning may reinforce the start-up problem, while fast learning may lead to a smaller MSSP network. When the learning potential is not very high and there are substantial barriers to information acquisition, an MSSP is probably infeasible. Not surprisingly, an increase in the speed of learning (k) values promotes faster network growth, while an increase in residual attack probability value (a) makes an MSSP unattractive across all values of k.

Impact of Client Firm Heterogeneity on the Network Growth Dynamics

The assumption of identical clients for an MSSP makes modeling and analysis more convenient, yet takes away from the realism of the situation where no two clients are exactly the same. Therefore, we had to explore the impact of possible heterogeneity in client attributes on the analytical results and predictions of our model. We find that our predictions are robust to the heterogeneity of the client firms, and all the structural results hold even in this situation. Specifically, the ordering of MSSP sizes in monopoly versus consortium scenarios still hold, as well as the viability predictions for the consortium and the monopolist. We performed this exploration by means of a simulation.

In the simulation, we explore the network growth of an MSSP with a random sequence of client arrivals. The clients vary in their ability to learn from attacks and implement security solutions, thus bringing different incremental contribution to the overall value of the MSSP network. From the formal perspective, this different level of inherent capability may be represented as a different "size" of the client firms. In the formal analysis presented earlier, clients are identical and of size 1; for the simulation, we are drawing the size of each potential client from a uniform distribution over the interval (0.5; 1.5). The clients still join the network one by one; therefore, at any step N, overall size of the network is the sum of the sizes of all previous entrants. We denote it N_adj.

We generate a random sequence of potential clients. Then, this sequence is presented to both the consortium and the monopolist MSSP, who make the decisions regarding the viability of the MSSP and the size at which the network will stop growing (optimal size). To preserve the logic of the analysis, we assume that the MSSP provider knows the sequence of arriving clients beforehand.[14]

The decisions made by the MSSP depend on the network value and resource requirement functions: $V(N)$ and $R(N)$. For the resource requirement function, we assume the same conceptual approach as for the theoretical analysis: arrival of a new client requires an investment of a certain amount of resources, regardless of client size. We chose the functional form of $R(N) = 0.1\ N^2 + 14.5$. For the network value function, however, we reflect the heterogeneity of the clients and formally model it as $V(N) = 10\ N\_adj^{1/2}$.

While the functional forms are conforming with the theoretical formulation, the choice of these specific coefficient values ensures that it is individually rational for all clients to join the MSSP network (i.e., no rational client will want to provide its security in a stand-alone mode). It also makes the problem configuration such that there is a critical mass problem in the early stages of the network growth such that it is necessary to have two to five client firms in the network to overcome the critical mass problem. In terms of the initial investment, we assume that the monopolist has to make the investment at size $N = 1$: $L = R(1) - V(1)$, that is, it needs to provide the services even to one client. For the consortia, we consider the case of more than one founding member, for example for two founding members, $L = R(2) - V(2)$, etc. We also implement the consortium and monopolist pricing strategies as described in the paper.

[14]If this assumption is not true and the MSSP makes the decision whether to admit or reject the new client at the moment of client arrival (and without knowledge of subsequent clients), then optimization is not possible and the actions of the provider can be, at best, based on some sort of heuristic. Analysis of a stochastic client arrival problem is beyond the scope of this work.

Table 2. Summary of the Simulation Environment by the Severity of the Critical Mass Problem

Number of Firms Needed to Overcome Critical Mass Problem	Number of Outcomes
2	3,026
3	5,849
4	1,064
5	59
6	2
TOTAL	10,000

Table 3. Summary of the Simulation Results for User Heterogeneity (10,000 Repetitions)

MSSP Type	Number of Times Started	Average Size
Monopolist	4,940	8.483
Consortium with two founding members	9,965	5.897
Consortium with three founding members	9,999	5.483
Consortium with no initial investment requirement (5+ founding members)	10,000	5.455

Given this setup, we generated 10,000 random sequences of clients and subjected them to the consortium and monopolist decision making, tracking the following information:

- Whether, given the current sequence of clients, it is viable to start a MSSP network in case of monopolist, consortium with investment requirement (based on two or three founding firms), and consortium without investment requirements (based on at least 5 founding firms)

- Relative ordering of the sizes for the monopolist and consortia described above.

Tables 2 and 3 represent the summary of the simulation analysis. Table 2 describes the general simulation environment as represented by the severity of the critical mass problem. In most cases, two or three member (client) firms are enough to overcome the critical mass problem in the network, more severe cases of four or more members needed to overcome the critical mass are not as common.

Table 3 represents the decision to start the MSSP network of a particular type. As can be seen, the monopolist MSSP is started in 49.4 percent of the cases, while a consortia of some form is started in over 99 percent of the cases. This confirms one of our main results: that a monopolist MSSP may be facing more difficulties in staying viable due to the nature of its pricing structure (introductory and/or compensatory pricing).

Table 3 also represents the average MSSP network size for the monopolist and different type of the consortia. The monopolist has the largest network, followed by the consortia of two founding members, three founding members, and, finally, no requirement for initial investment. We note that in all simulation results the MSSP sizes conform exactly to the theoretically predicted results.

Therefore, as demonstrated by our simulation model, our theoretical predictions remain robust and practically usable even if one of the limiting assumptions—user homogeneity—is relaxed.

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 an MSSP network to pool risk may be outweighed by the substantial start-up costs required under a consortium-based approach; this is evident from the analysis that simultaneously considers positive and negative network effects via the shapes of value and resource requirement functions. We also examine the growth and structural charac-

teristics 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 the 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 the 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 a profit-maximizing approach. Since joining a profit-maximizing provider has less risk during start-up as compared to a consortium where an initial investment may be required, our results provide economic rationale for the observed phenomena of existence of more for-profit MSSP networks as compared to MSSP consortia. We also show that a for-profit provider may achieve larger network size than a consortium. Another issue is the transparency of the MSSP network formation mechanism: in the case of a consortium, all members are aware of the composition of the consortium, while the monopolist does not have to disclose its client list.[15]

From a managerial perspective, two issues are important. First, both the hiding effect and the knowledge effect are valid practical concerns. The hiding effect essentially has been the driver behind offerings of ISPs that provide frequent reallocation of discontinuous blocks of IP addresses to their clients. With such IP schemes (we refer to them as "lattice IPs"), it is becoming harder for attackers to figure out the topology of a 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 the Code Red II worm, which was programmed to frequently attack machines in the same subrange of IP addresses.[16] The knowledge effect also becomes important for discovery of novel attacks. Since most patches as well as antivirus 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 with greater ease by a number of connected parties.

The second issue is important for those who decide to start an MSSP network. The consortium model may be a harder sell in the beginning, as all starting members are required to invest up front. On the other hand, a monopoly-type MSSP can provide incentives (discounts) to early adopters, but may be faced with the 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 to join and when to do so.

The limitations of this work include the fact that we only consider the case when MSSP customers are identical and the order in which they join the network is not relevant. In future work, we will extend our model to try and identify the effects of different types of customers on the system as well as the effects of the sequence of their decisions. Additionally, as Sundararajan (2004) points out, network effects may depend on the type of customers, thus giving rise to nonlinear pricing schemes. We will develop specific incentive mechanisms and pricing schemes for MSSPs to attract customers that differ in size, expertise, and need.

Acknowledgments

The authors would like to thank the participants of the Sixth Workshop on the Economics of Information Security (WEIS-2007) and the IDS Research Workshop at the University of Minnesota for their helpful comments and suggestions.

References

Allen, J., Gabbard, D., and May C. 2003. "Outsourcing Managed Security Services," Report CMU/SEI-SIM-012, Software Engineering Institute, Carnegie Mellon University, Philadelphia, PA (http://www.cert.org/archive/pdf/omss.pdf).

Aloysius, J. A., and Rosenthal, E. C. 1999. "The Selection of Joint Projects by a Consortium: Cost Sharing Mechanisms," *The Journal of the Operational Research Society* (50:12), pp. 1244-1251.

Bailey, E. 1981. "Contestability and the Design of Regulatory and Antitrust Policy," *The American Economic Review* (71:2), pp. 178-183.

Baroudi, C. 2008. "Best Practices in Choosing and Consuming Managed Security Services," Aberdeen Group, Boston, MA, January 31 (http://www.aberdeen.com/summary/report/benchmark/4581-RA-managed-security-services.asp).

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

Business Wire. 2006. "The Credit Union National Association (CUNA) Selects Perimeter Internetworking(TM) as Their Exclusively, Endorsed Managed Security Provider; Fully Integrated Security Services for CUs Available Through CUNA, Perimeter Alliance," AllBusiness.com, March 1 (http://www.allbusiness.

[15]We thank an anonymous reviewer for suggesting this scenario.

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

com/company-activities-management/operations/5455653-1.html; retrieved February 5, 2011)

Cabral, L. M., Salant, D. J., and Woroch, G. A. 1999. "Monopoly Pricing with Network Externalities," *International Journal of Industrial Organization* (17), pp. 199-214.

Camp, L. J., and Wolfram, C. 2000. "Pricing Security," in Position *Papers for the Third Information Survivability Workshop*, Boston, MA, October 24-26, pp. 31-39.

Campbell, K., Gordon, L, Loeb, M., and Zhou L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (11:3), pp. 431-448.

Casper, C. 2011. "MarketScope for Managed Security Services in Europe," Gartner Research, Stamford, CT, October 24 (http://www.gartner.com/it/products/research/ research_services.jsp).

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

Church, J., Gandal, N., and Krause, D. 2008. "Indirect Network Effects and Adoption Externalities," *Review of Network Economics* (7:3:1) (http://www.bepress.com/rne/vol7/iss3/1/).

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

DeLong, J. M., and Froomkin, A. M. 2000. "Speculative Microeconomics for Tomorrow's Economy," in *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, D. Hurley, B. Kahin, and H. Varian (eds.), Cambridge, MA: MIT Press, pp. 6-44.

DiPalantino, D., Johari, R., and Weintraub, G. 2010. "Competition and Contracting in Service Industries," Working Paper, Stanford University (http://www.stanford.edu/~rjohari/uploads/slg.pdf).

Economides, N. 1996. "The Economics of Networks," *International Journal of Industrial Organization* (16:4), pp. 675-699.

Economides, N., and Flyer, F. 1997. "Compatibility and Market Structure for Network Goods," Discussion Paper No. 98-02, Stern School of Business, New York University.

Economides, N., and Himmelberg, C. 1995. "Critical Mass and Network Evolution in Telecommunications," in *Toward a Competitive Telecommunications Industry: Selected Papers from the 1994 Telecommunications Policy Research Conference*, G. Brock (ed.), Mahwah, NJ: Lawrence Erlbaum Associates, pp. 47-63.

EnergySec. 2010. "DOE Selects EnergySec to Create the National Electric Sector Cybersecurity Organization," press release, October 14 (http://tdworld.com/the_smarter_grid/highlights/doe-energysec-cyber-security-1010/).

Farrell, J., and Klemperer, P. 2007. "Coordination and Lock-In: Competition with Switching Costs and Network Effects," *Handbook of Industrial Organization*, Volume 3, M. Armstrong and R. Porter (eds.), Amsterdam: North-Holland, pp. 1976-2072.

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

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

Germain, J. 2004. "Managed Security Services: A Hedge Against E-Mail Attacks," TechNewsWorld, May 25 (http://www.technewsworld.com/story/33989.html).

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

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

Gupta, A., Stahl, D. O., and Whinston, A. B. 1997. "A Stochastic Equilibrium Model of Internet Pricing," *Journal of Economic Dynamics and Control* (21), pp. 697-722.

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

Hasson, J. 2002. "VA Bolsters IT Security," *Federal Computer Week*, August 12 (http://fcw.com/articles/2002/08/12/va-bolsters-it-security.aspx).

ISAC Council. 2004. "Reach of the Major ISACs," white paper, ISAC Council.org (http://www.isaccouncil.org/index.php?option=com_docman&task=doc_view&gid=14&Itemid=208).

Kannan, K., and Telang, R. 2004. "An Economic Analysis of Market for Software Vulnerabilities," in *Proceedings of 2004 Workshop on Economics of Information Security,* Minneapolis MN, May 13-14 (http://www.dtc.umn.edu/weis2004/kannan-telang.pdf).

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

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

Kavanagh, K., and Pescatore, J. 2010. "Magic Quadrant for MSSPs, North America", Gartner Research, Stamford, CT, November 29 (http://www.gartner.com/it/products/research/research_services.jsp).

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

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

MacKie-Mason, J., and Varian, H. 1995. "Pricing Congestible Network Resources," *IEEE Journal on Selected Areas in Communications* (13:7), pp. 1141-1149.

Martines , F., Oualid, G., Tapia, S., and Gras, D. 2006. "Managed Security Services: From Monitoring to Response," *Alcatel-Lucent Telecom Review* (http://www.key4biz.it/files/000039/00003965.pdf).

Matutes, C., and Regibeau, P. 1996. "A Selective Review of the Economics of Standardization: Entry Deterrence, Technological Progress and International Competition," *European Journal of Political Economy* (12), pp. 183-209.

McAndrews, J., and Rob, R. 1996. "Shared Ownership and Pricing in a Network Switch," *International Journal of Industrial Organization* (14), pp. 727-745.

Olson, M., and Zeckhauser, R. 1996. "An Economic Theory of Alliances," *The Review of Economics and Statistics* (48:3), pp. 266-279.

Oneal, J. 1990. "The Theory of Collective Action and Burden Sharing in NATO," *International Organization* (44:3), pp. 379-402.

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

Ozment, A. 2004. "Bug Auctions: Vulnerability Markets Reconsidered—An Economic Analysis of Market for Software Vulnerabilities," in *Proceedings of 2004 Workshop on Economics of Information Security,* Minneapolis, MN, May 13-14 (http://www.dtc.umn.edu/weis2004/ozment.pdf).

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

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

Sandler, T. 1993. "The Economic Theory of Alliances: A Survey," *The Journal of Conflict Resolution* (37:3), pp. 446-483.

Sandler, T. 1999. "Alliance Formation, Alliance Expansion, and the Core," *Journal of Conflict Resolution* (43:6), pp. 727-747.

Schechter, S. 2005. "Toward Econometric Models of the Security Risk from Remote Attacks," *IEEE Security and Privacy* (3:1), pp. 40-44.

Schechter, S., and Smith, M. 2003. "How Much Security Is Enough to Stop a Thief?," in *Financial Cryptography: Lecture Notes in Computer Science* (2742), Berlin: Springer, pp. 122-137.

Scholtz, T., and Parveen, K. 2007. "MarketScope for Managed Security Services in Europe, 2007," Gartner Research, Stamford, CT (http://www.gartner.com/it/products/research/research_services.jsp).

Shapely, L. S. 1953. "A Value for n-Person Games," in *Contributions to the Theory of Games* (Volume 2), H. Kuhn and A. W. Tucker (eds.), Princeton, NJ: Princeton University Press, pp. 307-317.

Shapiro, C., and Varian, H. 1999. "The Art of Standard Wars," *California Management Review* (41:2), pp. 8-32.

Stango, V. 2004. "The Economics of Standard Wars," *Review of Network Economics* (3:1), pp. 1-19.

Sturgeon, W. 2004. "What Is the Future of Your Security?," Silicon.com, September 22 (http://software.silicon.com/security/0,39024655,39124203,00.htm).

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

Vahalia, K. 2010. "Endpoint Security Consortium to Improve Critical Class of Security Products," *InfoTech Feature,* December 13 (http://it.tmcnet.com/topics/it/articles/126112-endpoint-security-consortium-improve-critical-class-security-products.htm).

van der Heiden, G. 2010. "Hype Cycle for IT Outsourcing, 2010," Gartner Research, Stamford, CT July 30 (http://www.gartner.com/it/products/research/research_services.jsp).

Varian, H. 2004. "System Reliability and Free Riding," working paper, University of California, Berkeley, School of Information Management and Systems (http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability)

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

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

Weitzel, T., Wendt, O., and Westrap, F. 2000. "Reconsidering Network Effect Theory," in *Proceedings of the Eighth European Conference on Information Systems*, Vienna, Austria, July 3-5, pp. 484-491.

Wells, A. 2010. "MarketScope for Managed Security Services in Asia/Pasific," Gartner Research, Stamford, CT, September 17 (http://www.gartner.com/it/products/research/research_services.jsp).

Wheatman, V., Smith, B., Shroder, N., Pescatore, J., Nicollet, M., Allan, A., and Mogull, R. 2005. "What Your Organization Should Be Spending for Information Security," Gartner Research, Stamford, CT (http://www.gartner.com/it/products/research/research_services.jsp).

About the Authors

Alok Gupta is the department chair and Curtis L. Carlson Schoolwide Chair of Information Management at the Department of Information and Decision Sciences, Carlson School of Management, University of Minnesota. He received his Ph.D. from the University of Texas, Austin, in 1996. His research has been published in top quality interdisciplinary journals such as *Management Science*, *Information Systems Research*, *MIS Quarterly*, *INFORMS Journal on Computing*, *Communications of the ACM*, *Journal of MIS*, *Decision Sciences*, *Journal of Economic Dynamics and Control*, *Computational Economics*, *Decision Support Systems*, *International Journal of Electronic Commerce*, and *IEEE Internet Computing*. He serves on the editorial boards of *Management Science*, *Information Systems Research*, *Journal of MIS*, and *Decision Support Systems*.

Dmitry Zhdanov is an assistant professor in the Operations and Information Management Department at the School of Business, University of Connecticut. He received his Ph.D. from the University of Minnesota in 2007. His research has been published in journals such as *Information Systems Research* and *INFORMS Journal on Computing.* He serves on the editorial board of *Electronic Commerce Research and Applications* and is also a Certified Information Systems Security Professional (CISSP).

MIS Quarterly

RESEARCH ARTICLE

GROWTH AND SUSTAINABILITY OF MANAGED SECURITY SERVICES NETWORKS: AN ECONOMIC PERSPECTIVE

Alok Gupta
Department of Information and Decision Sciences, Carlson School of Management, University of Minnesota, Minneapolis, MN 55455 U.S.A. {alok@umn.edu}

Dmitry Zhdanov
Department of Operations & Information Management, School of Business, University of Connecticut, Storrs, CT 06269 U.S.A. {dmitry.zhdanov@business.uconn.edu}

Appendix A

MSSP Simulation Design Based on KDD Cup Data Set

The original dataset consists of data on over four million connections each described by 42 attributes (e.g., duration, protocol, etc.) and identified either as normal traffic or one of 24 attack types. Our simulation is designed as follows:

1. A total of 20,000 connections were randomly selected from the original dataset to form the simulation training set; 16 attack types were represented in the simulation set.
2. The simulation training set was duplicated to represent the simulation test set with the same distribution of attacks as in the training set.
3. The 20,000 connections in the 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. The 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 the C4.5 algorithm (Quinlan 1993).
7. The output of C4.5 algorithm was tested against a random subset of attacks from the testing set. The testing subset is half the size of the training subset. The proportion of misclassified attacks in the testing subset was computed and provided the probability of attack success, P_s (on the assumption that if the attack was not identified correctly, then no appropriate defense would be activated).
8. Network size was incremented by 1 (until it reached 20; for example, after first iteration, network size = 2, pool of connections = 2,000). Return to step 5.

The data was averaged over 10 simulation runs.

Reference

Quinlan, J. R. 1993. *C4.5: Programs for Machine Learning*, San Mateo, CA: Morgan Kauffman.

Appendix B

Comparative Dynamics of Hiding and Knowledge Effects

Let us define the hiding effect in the network of size N as $H(N)$ and the knowledge effect as $K(N)$.

Recall from equation (1) that damage on the network of size N is defined as

$$D(N) = P_a(N) \times P_s(N) \times N$$

where N is network size, and P_a and P_s are probability of attack taking place and attack success, respectively.

By definition, the hiding effect captures the difference in exposure between being a part of an MSSP network and providing security alone for any particular firm.

$$H(N) = D(N) / N - D(1) / 1$$

Similarly, the knowledge effect captures the improvement in security state due to the addition of a new node to the network.

$$K(N) = P_a(N) \times P_s(N) - P_a(N-1) \times P_s(N-1)$$

To explore the relative magnitude of these two effects, consider a network of size $N + 1$.

$$\begin{aligned} &H(N+1) - K(N+1) = \\ &[P_a(N+1) \times P_s(N+1) - P_a(1) \times P_s(1)] - [P_a(N+1) \times P_s(N+1) - (P_a(N) \times P_s(N)] = \\ &P_a(N) \times P_s(N) - P_a(1) \times P_s(1) = H(N) \end{aligned}$$

We see that for a network of any size, addition of a new node produces an incremental change in the magnitude of hiding effect that is equal to the magnitude of the current knowledge effect. This result may be formulated as a lemma.

Lemma 1. Given the definitions of the hiding and knowledge effects, for any network size N, the following relationship holds:

$$H(N+1) - K(N+1) = H(N)$$

The implications of this result are twofold. First, it means that, in general, the hiding effect dominates the knowledge effect. Second, the extent of this dominance grows with the size of the network, if both effects are present and monotonic (these conditions hold in our formulation).

Appendix C

Correspondence of MSSP Growth Model with the Constructs of the Cooperative Game Theory

1. General properties of cooperative games

   1.1 In general, cooperative game theory models assume that there is a finite number of players (N). The MSSP model allows for an unlimited number of potential clients. However, the solution area for the MSSP problem includes a finite number of clients N_{max}. Growing the network beyond this size is going to lead to the loss of efficiency since the gross costs of this approach outweigh gross benefits. Thus, we can consider a game which has N_{max} players.

   1.2 A coalition game with transferrable utility is a pair $G = (N, v)$ where N is a coalition and v is a function that associates a real number $v(S)$ with each subset S of N. In our case, the set of players is N_{max}, and the coalition function $v(S)$ is defined based on the consortium rules.

   1.3 A game (N, v) is superadditive if $(S, T \subseteq N \text{ and } S \cap T = \varnothing) \Rightarrow v(S \cup T) \geq v(S) + v(T)$. Clearly, this condition holds in our case, since any two subsets of firms cannot achieve a better outcome than a larger consortium.

   1.4 A game is weakly superadditive if $v(S \cup \{i\} \geq v(S) + v(\{i\})$ for all $S \subseteq N$ and $i \notin S$. This condition holds in our formulation, since addition of each new member for a consortium increases total consortium benefits by the amount which exceeds an individual value of being alone.

   1.5 A game is monotonic if $S \subseteq T \subseteq N \Rightarrow v(S) \leq v(T)$. In our setting, smaller consortia have a smaller amount of total benefit, thus the monotonicity property holds.

2. Solution concepts of cooperative games

   2.1 For a game (N, v), a feasible payoff vector is defined as $X^*(N, v) = \{x \in \mathbf{R}^N \mid x(N) \leq v(N)\}$. Basically, feasible payoff should not exceed the total worth of the game. Let Γ be a set of games. Then, a solution on Γ is defined as a function σ that associates with each game $(N, v) \in \Gamma$ a subset $\sigma(N, v)$ of $X^*(N, v)$. Intuitively, a solution is a system of reasonable restrictions on X^*.

   2.2 One possible solution for a cooperative game is known as the core. The core $C(N,v)$ is defined as $C(N,v) = \{x \in X^*(N, v) \mid x(S) \geq v(S) \forall S \subseteq N\}$. In the case of the MSSP game, the winning coalition (members of the consortium) get a payoff equal to the worth of the consortium, so the concept of the core is valid in our case.

   2.3 The core as a solution to the cooperative game is anonymous (independent of the names of players) and Pareto optimal. Clearly, in our case, any firm can be a member of an MSSP and their particular identities are not relevant. Our solution is also Pareto optimal, since in the formed consortium, no member may be made better off without making another member worse off.

   2.4 A solution must be reasonable from above and below. Let b_i represent the i^{th} member incremental contribution to the coalition. Then, the solution is reasonable from above if $((N, v) \in \Gamma, x \in \sigma(N, v)) \Rightarrow x^i \leq b^i_{max}(N, v) \forall i \in N_i$.

   It is reasonable from below if $((N, v) \in \Gamma, x \in \sigma(N, v)) \Rightarrow x^i \geq b^i_{max}(N, v) \forall i \in N_i$.

   This means that each member of the coalition must be paid an amount that does not exceed the maximum individual contribution to the coalition, while also providing individual incentives to join the coalition. The core is reasonable from above and below. In the MSSP case, there is individual rationality for each member to join (reasonable from below), and none of the members are paid more than the maximum possible individual contribution (reasonable from above). Thus, our solution achieves the same results as the core with respect to the reasonableness requirement.

   2.5 Another solution concept is known as the Shapley value. It is based on the *a priori* evaluation of the coalition game by each of its players. Besides Pareto optimality, it also satisfies the null player property and the equal treatment property. The null player property

states that each player without an impact on the solution should get a payoff of zero. The equal treatment property states that players with equal contributions to the coalition should get the same payoffs. In our case, the players are identical and they get equal payoffs. There are no dummy players in our formulation.

The Shapley value is defined as $\left\{ \phi^i(v) = \sum_{S \subseteq N} \frac{|S|!(n-|S|-1)!}{n!} \left(v(S \cup \{i\} - v(S)) \right) \right\}$

According to Shapley (1953, p. 316),

> The players in N agree to play the game v in a grand coalition, formed in the following way: 1. Starting with a single member, the coalition adds one player at a time until everybody has been admitted. 2. The order in which the players are to join is determined by chance, with all arrangements equally probable. 3. Each player, on his admission, demands and is promised the amount which his adherence contributes to the value of the coalition (as determined by the function v). The grand coalition then plays the game "efficiently" so as to obtain $v(N)$—exactly enough to meet all the promises.

It is clear from this description that our formulation implements the Shapley value mechanism. In addition, we provide a description of the revenue sharing mechanism that implements the equal treatment property, and we prove the optimality of that mechanism.

Therefore, the formulation of the MSSP dynamic growth process has all of the important properties of cooperative games, such as monotonicity and superadditivity. It also corresponds in properties to the common solution concepts such as the core and Shapley value. However, our approach makes fewer assumptions and provides additional results such as the implementation of an optimal, equal treatment-based consortium value distribution mechanism.

References

Peleg, B., and, Sudhölter, P. 2003. *Introduction to the Theory of Cooperative Games*, Boston: Springer.

Shapley, L. S. 1953. "A Value for n-Person Games," in *Contributions to the Theory of Games* (Volume 2), H. Kuhn and A. W. Tucker (eds.), Princeton, NJ: Princeton University Press, pp. 307-317.

Appendix D

Proofs of Propositions

Proposition 1 (The Optimal Size of Consortium without Investment). 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: Suppose that value function $V(N)$ is concave and the damage function $R(N)$ is convex. Then, 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 $V'(j) - R'(j) = [V(j) - R(j)] / j$ is a positive number, $j \leq k$ where $V'(k) - R'(k) = 0$—the optimality condition for a welfare maximizing solution. Q.E.D.

Proposition 2 (Equal Sharing and MSSP Network Viability). Let there exist a network size n that allows investment recovery and network viability with the equal sharing rule. Then, it is a minimum viable network size and the 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 the equal sharing rule.

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

$$\Rightarrow [V(n) - R(n)] / n \geq [R(i) - V(i)] / n \; \forall \; n \text{ members} \tag{D4}$$

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

$$\Rightarrow [V(m) - R(M)] / m \geq L_j \; \forall \; j = 1, \ldots, m \tag{D5}$$

where L_j is the share of investment shared by member j.

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.

$$\Rightarrow [V(m) - R(m)] / m \geq [R(i)] / m \tag{D6}$$

However, equation (D6) implies that investment should have been recovered using the equal sharing rule at size $m < n$—a contradiction since by assumption n was the minimum network size to recover the investment using the equal sharing rule. Q.E.D.

Proposition 3 (Optimal Size of MSSP Consortium with Investment). The optimal size of an MSSP consortium that requires the initial investment to the 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: Suppose that value function $V(N)$ is concave and the requirement resource function $R(N)$ is convex. Then, the optimal consortium size without investment is a solution to equation (D7):

$$N_{cn}^* = j: \; V'(j) - R'(j) = [V(j) - R(j)] / j \tag{D7}$$

Further, optimal consortium size with investment is a solution to equation (D8):

$$N_c^* = j: \; V'(j) - R'(j) = [V(j) - R(j) - C] / j \tag{D8}$$

Since C is a positive number, the R.H.S. of equation (D8) is smaller than the R.H.S. of equation (D7).

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 the solution to equation (20) (i.e., $N_c^* \geq N_{cn}^*$). Q.E.D.

Lemma 4 (Minimum Viable Initial MSSP Consortium). The minimum starting network size is given by $I^* = \min\{i: V(N_s^*) - R(N_s^*) \geq R(i) - V(i)\}$.

Proof: Since $R(i) - V(i)$ is decreasing in $i < N_0$ and maximum recoverable investment is $V(N_s^*) - R(N_s^*)$, the 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 (Monopolist MSSP Versus Social Net Benefit Size): The monopolist MSSP may have a larger network size than the social net benefit maximizing size if it can provide sufficient compensation for all current members of the consortia who lose value due to the addition of another member beyond the social benefit optimal (i.e., $P_{N_s^*}^m > \sum_{j \in \Omega} P_j^m \big/ (x+1)$, 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: Suppose that the net benefit maximizing network size is N_s^* and the monopolist MSSP is viable.

(1) Note that the profits of a monopolist MSSP cannot be maximized on a network size that is smaller than the social net benefit maximizing size; that is, N_m^* cannot be less than N_s^*.

Assume the contrary, that 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 the 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^*.

(2) 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,

$$V(N_s^*) - R(N_s^*) > V(N_s^* + 1) - R(N_s^* + 1) \quad \text{(D9)}$$

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

$$V(k) - R(k) > V(N_s^* + 1) - R(N_s^* + 1) \quad \text{(D10)}$$

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

$$Comp_k = [V(k) - R(k)] / k - [V(N_s^* + 1) - R(N_s^* + 1)] / (N_s^* + 1) \quad \text{(D11)}$$

Since $[V(k) - R(D(k))] / k = P_k^m$ and $[V(N_s^* + 1) - R(N_s^* + 1)] / (N_s^* + 1) = P_{N_s^*+1}^m$ and , we can rewrite (D11) as

$$Comp_k = P_k^m - P_{N_s^*+1} \quad \text{(D12)}$$

The total compensation then is

$$\sum_{k \in \Omega} Comp_k = \sum_{k \in \Omega} P_k^m - xP_{N_s^*+1}^m \text{ where } x = |\Omega|, \text{ cardinality set of } \Omega \quad \text{(D13)}$$

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

$$P_{N_s^*+1}^m \geq \sum_{k \in \Omega} P_k^m - xP_{N_s^*+1}^m \Rightarrow P_{N_s^*+1}^m \geq \sum_{k \in \Omega} P_k^m \Big/ (x+1) \qquad \text{Q.E.D.} \quad \text{(D14)}$$

Corollary 5.1 **(Monopolist MSSP Versus Consortium MSSP Size)**: The monopolist MSSP, if viable, will have a network not smaller than a consortium MSSP.

Proof: From Proposition 5, the monopolist MSSP size is greater than the social benefit, $N_m^* \geq N_s^*$. However, the consortium provider will not grow its network beyond N_s^*, as it decreases total and average benefits 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.

Corollary 5.2 **(Monopolist MSSP Versus Consortium MSSP Viability)**: There may be instances when a consortium MSSP is viable, while a monopolist MSSP is not viable.

Proof: Recall that the viability condition for a MSSP network is given by the need to recover the initial investment: $I^* = \min\{i : V(N_s^*) - R(N_s^*) \geq R(i) - V(i)\}$.

In the worst case scenario, the monopolist will start with a network of size 1, while a consortium may have more founding members. Since $R(i) - V(i)$ is decreasing in $i < N_0$, there is a chance that the monopolist will have to make a larger investment. Even if this investment is equal to that of the consortium, the monopolist is following zero-price strategy for the initial few clients, while the consortium begins the cost recovery immediately via its pricing and reallocation scheme. Finally, in some cases the monopolist needs to collect the compensatory payments (if any) in the amount of $\sum_{k \in \Omega} Comp_k = \sum_{k \in \Omega} P_k^m - xP_{N_s^*+1}^m$.

Since the consortium is not facing any of these costs, it may survive on a network with a smaller total potential value than the monopolist. Therefore, there may be cases when, all things being equal, the consortium is profitable and will start, while the monopolist is not profitable and will not start. The reverse is not the case. Q.E.D.

Appendix E

Pseudocode for Profit Maximizing Provider's Pricing and Allocation

If ($k < N_0$)
    Set $P_k = 0$
End If
Else If ($k >= N_0$ and $k <= N_s^*$)
    Set $P_k = [V(k) - R(k)] / k$
End Else If
Else If ($k >= N_s^*$)
    Set $P_k = [V(k) - R(k)] / k$
    For ($n = N_0$ to N_s^*) do
        If ($P_n > [V(k) - R(k)] / k$)
            Total refund = 0
            For ($m = n$ to $k - 1$) do
                Refund firm m amount (R_m) = $P_m - [V(k) - R(k)] / k$
                Total refund = total refund + $P_m - [V(k) - R(k)] / k$
            End For
            If (Total refund > $[V(k) - R(k)] / k$)
                Reject entry to firm k
            Else
                For ($m = n$ to $k - 1$) do
                    Commit R_m
                    $P_m = [V(k) - R(k)] / k$
                End For
            End Else
        End If
    End For
End Else If