Will Outsourcing IT Security Lead to a Higher Social Level of Security?

Brent R. Rowe

RTI International
3040 Cornwallis Rd., Research Triangle Park, NC
browe@rti.org

ABSTRACT

More firms outsource information technology (IT) security activities each year, as they determine that they can achieve cost savings or a higher level of security at the same cost. However, despite the estimated benefits, many firms still fail to see a clear positive net benefit from their (private) perspective, given the risks and costs involved. This paper investigates the positive externalities associated with IT security outsourcing. My research suggests that, when one organization decides to outsource its security, both direct and indirect benefits can accrue to other organizations and Internet users. In this paper I analyze how a variety of decision characteristics affect whether and to what level such positive externalities will result. I also discuss implications for public policy and for firm-level decision making.

1.0 INTRODUCTION

More firms outsource IT security activities each year, as they determine that they can achieve cost savings or a higher level of security at the same cost. Although not all firms can outsource all or part of their IT security activities and see an increase in their level of security per dollar of investment, other firms are likely to benefit from one firm's decision to outsource. Outsourcing in general, and more specifically IT security outsourcing, has been shown to result in both a reduction in production costs and a freeing up of other resources.[1] However, as with other types

[1] To be clear, in this paper I use the word "outsourcing" to describe the relationship between a firm that pays another firm to conduct a certain activity on its behalf (e.g., accounting functions). We are not referring explicitly to offshore outsourcing, which brings with it additional costs and benefits.

of outsourcing, the private return on investment in outsourcing IT security could be reduced or become negative as a result of a variety of potential costs including both strategic risks (e.g., principal-agent problems) and operational risks (e.g., interoperability issues).

Firms considering whether to outsource their IT security activities make such a decision solely based on a perceived reduction in cost (or a higher level of security gained per dollar invested) at their organization. However, when organizations outsource some security activities, positive network externalities[2] may accrue to (1) other firms who outsource security activities to the same firm and (2) all other firms and individuals that use the Internet. The existence of these potential externalities has implications for decision makers at firms and for policy makers.

In this paper, I investigate several issues that influence whether one firm's decision to outsource IT security will result in a higher social level of security. First, I describe several types of IT outsourcing relationships. Using data from a study funded by DHS, I analysis of common outsourcing practices and causality between firm characteristics and types of outsourcing.[3] I look conceptually at an individual firm's decision to outsource IT security, including the benefits and costs. Next, I look at how one firm's decision to outsource affects other firms. In particular, I focus on how a firm's spending habits may change as part of the outsourcing decision, as well as the subsequent effect on the security of other firms. I also investigate how the structure of security providers' operations affect externalities. Finally, I discuss the implications of positive externalities resulting from IT security outsourcing.

2.0 DATA COLLECTION: RTI STUDY

Between 2004 and 2005, I worked on an RTI study funded by the Department of Homeland Security (DHS) that had as its goal to develop a robust understanding of the activities of firms surrounding their cyber security investment decisions. Our sample included 36 organizations that eventually provided data on all or almost all of our questions. An additional 21 would not provide data but were willing to discuss the issues in which we were interested in a broader sense. The organizations involved in this study represented a variety of sectors, chosen for their reliance on IT systems; they were financial services, health care providers, manufacturing, universities, small businesses, and several additional firms. Table 1 provides a breakdown by industry of the number of firms who provided data and those with which we had more qualitative discussions.

Along with several colleagues, I developed detailed survey instruments and interview guides. Our data collection strategy included providing each participating organization with a copy of their industry-specific survey and a statement of the purpose of the study. We followed the survey stage of data collection with either a

---

[2] Liebowitz and Margolis (1994) discuss the difference between network effects and network externalities. See Section 3 for a discussion of their paper. In this paper, I will leverage the distinction they draw between network effects that are common and network externalities that result because of a market failure.

[3] I use data from a study that I co-led for the U.S. Department of Homeland Security (DHS) on private sector investment decisions (Gallaher et al., 2006). Section 2 provides details on this study and the data collection efforts involved.

Table 1. RTI Study Data Collection Summary, By Industry

Industry	Provided Data	Participated in Qualitative Discussion
Financial services	6	5
Health care providers	6	2
Manufacturing	6	1
Universities	7	2
Small businesses	6	8
Other organizations	5	3
Total	36	21

site visit or an extensive telephone interview in all but two cases. I led all 36 interviews. The purpose of the post-survey discussions was to ensure consistency in the interpretation of each survey question across respondents and to allow each respondent an opportunity to elaborate on or clarify his/her responses. All collected data and descriptive information relates to 2005.

We asked questions related to the budgeting process, the primary people involved in the decision process, and the information utilized at various stages of investment; in total, we asked approximately 200 questions, including several large tables, and a small number of industry-specific questions. Mainly we focused on what information is being used at the "investment stage" and at the "implementation stage." By "investment stage", I mean the phase when firms decide how much to invest in cyber security and use one of two general approaches: (1) maximize security output subject to a budget constraint or (2) minimize cost to achieve their desired level of security.[4] By "implementation stage", I mean the time during which organizations actually implement a security plan: they begin to purchase hardware and software, and they implement security staff procedures and user policies.

Although our sample size was quite small, we gained invaluable insights into the cyber security investment decision processes of a variety of firm types and sizes. Specific to the focus of this paper, we asked five questions related to firms' outsourcing choices, and many firms were willing to discuss their reasons for deciding to outsource or not.

3.0 LITERATURE REVIEW

The costs and benefits of outsourcing have been studied extensively. Coase (1937) discussed costs associated with the market—for example, the cost of pricing goods, learning about available goods, learning about prices, negotiating contracts, and monitoring contractual performance—and he predicted that as these costs decreased more outsourcing would likely result.[5] Jensen and Meckling (1976)

[4] See more discussion of this in Gallaher et al (2006).

[5] Coase (1937) did not use the term "outsourcing" in his seminal paper. Rather he discusses the benefits of "exchange on the open market" and wrote that if the costs of the market decreased, more such exchange, or outsourcing, would result.

among others discuss the complexities of shifting control over operations of a firm away from the firm's owner(s). However, only recently have many studies looked empirically at the explicit benefits of outsourcing.

Görg and Hanley (2004) studied outsourcing in the electronics industry in Ireland and found that outsourcing increases profitability at larger firms. However, Kimura (2002) was unable to tie outsourcing to higher profits, which would imply a cost-savings effect, at manufacturing firms in Japan, and Görzig and Stephan (2002) found differing results looking at production verses service industries in Germany.[6]

The nature of network effects and network externalities have been the source of many studies. Liebowitz and Margolis (1994) provided a distinction between the two terms. They suggested that network effects are changes in product or service value based on the number of "users" and are common. However, they reserved the term "network externality" to describe situations in which the price of a good or service may not fully be inclusive of all network effects.

The potential existence and size of network externalities is usually part of any discussion of the appropriate role of government; if private incentives are significantly misaligned with social incentives, then government often becomes involved. Externalities can be either positive or negative; both cases motivate the consideration of government involvement to increase the overall social good resulting from individual and organizational actions. Katz and Shapiro (1985) famously wrote about the positive externalities, or network effects, using Liebowitz and Margolis' terminology, associated with technology adoption. They suggested that the utility derived by a consumer from a product could depend on the number of users of that product. The potential of an analogous relationship is the focus of our analysis of the social benefits of outsourcing IT security.

The economics of cyber security has become a relatively robust field[7]; however, relatively few studies have focused on the economic aspects of outsourcing IT security. Three researchers at the National Center for Supercomputing Applications (NCSA) at the University of Illinois—William Yurcik, Win Ding, and Xiaoxin Yin—have conducted extensive research on the decision of firms to outsource, specifically addressing the costs and benefits to both managed security service providers[8] (MSSPs) and the deciding firms. Gupta and Zhdanov (2006) provide the first analysis which discusses the network effects associated with outsourcing; they also provide an excellent analysis of how MSSPs may develop and associated service pricing schemes.

---

[6] The authors found that when German manufacturing firms outsourced material production there was a positive correlation with profits, while outsourcing services was negatively correlated with profits.

[7] Anderson and Moore (2006) recently published an article in Science summarizing the extensive literature in this research area, including research on investments in security, privacy issues, software development, insurance, and vulnerability discovery.

[8] MSSPs are firms that provide a wide range of security services. In this paper, we will use the term MSSP to refer to anyone providing security services, including both firms that only provide security services and firms that have other business products/services and also offer security services (e.g., Internet service providers [ISPs]).

4.0 TYPES OF IT SECURITY OUTSOURCING

IT security outsourcing relationships can take many forms, and as such, we provide here an overview of common types of IT security outsourcing relationships and types of MSSPs. Organizations can outsource six main technical tasks: (1) penetration or vulnerability testing, (2) security auditing, (3) system monitoring, (4) consulting, (5) forensics, and (6) general system management. Firms also outsource legal assistance and insurance to protect against potential liability issues or major losses associated with cyber events. Table 2 provides data on the main types of activities currently being outsourced. The 2006 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey found that 61% of firms outsource no IT security services (Gordon et al., 2006). While technical definitions differ slightly, our study for DHS found that approximately 72% of firms do not outsource monitoring activities, the term most aligned with the CSI/FBI definition of IT security services.[9]

The least intrusive outsourcing is vulnerability testing; under such an agreement, an external firm is hired to attempt to break into a company's network and identify areas of vulnerability. Our data collection for DHS found that approximately 58% of organizations outsourced vulnerability testing. The CSI/FBI survey found approximately 66% conducted penetration testing, though they do not indicate the percentage of such activities that are outsourced. It would seem that hiring someone external to attempt to break into a network would be much more effective than having someone who works on the network, and has detailed knowledge of the system configurations, conduct such an exercise. However, outsourcing this service can cost between $12,000 and $15,000 (Pappalardo, 2005).

Security auditing entails a comprehensive assessment of security hardware, software, policies, and procedures. In the CSI/FBI survey, 62% of firms reported that they hired external security auditors the previous year. Usually this type of service is conducted once or twice per year. It allows an organization to get a "report card" from an external firm based on an extensive assessment of the security measures in place. Using an external firm ensures that firms benefit from knowledge of both successful and unsuccessful solutions being employed at other firm; this information would be acquired by MSSPs from previous clients, but may not be as accessible to internal auditors.

System management is when a firm is hired to fully manage the firewall, virtual private network (VPN), and intrusion detection hardware and software protecting a company's network activities. This is the most intrusive form of security outsourcing. In a 2002 article in IEEE Computer Magazine, Schneier asserted that management of a company firewall, VPN, and intrusion detection infrastructure is "too central" to a company's operation for it to be efficiently and effectively

[9] While not explicitly stated, the CSI/FBI survey questions that support this data seem to refer to outsourcing technical security services such as monitoring and system management. In RTI's study, we did not collect information on the outsourcing of system management; however, we did additionally collect information on the outsourcing of installation, implementation, and maintenance and found that 47.3% of firms do not outsource any of these activities.

Table 2. Percentage of Companies That Outsource

Type of Outsourcing	Percent
Purchase third-party insurance	22.2%
Monitoring of IT security issues	27.8%
Installation, implementation, and/or maintenance	52.8%
Vulnerable assessment/planned compromise	58.3%
Security auditing	62.0%[a]
Purchase legal consultation (internal or external)	63.9%

* The majority of the data in this table is from RTI's study for DHS (Gallaher et al., 2006); [a] Data on security auditing is from the CSI/FBI Computer Crime and Security Survey (Gordon et al., 2006).

outsourced.[10] According to Schneier, there is no profitable business in managing firewalls or, more broadly, managing network security for other companies, and he points to past relationships in which companies outsourcing such activities have demanded too much individual attention for the money they were paying. Alternately, Ortiz (2007) suggests that companies should outsource firewall management, as well as several other functions that generally support the management of network security—intrusion detection and prevention, patch management, antivirus, and vulnerability assessment.

System monitoring, consulting, and forensics are all less intrusive than system management. A firm can be hired to perform 24/7 monitoring and interpretation of system events throughout the network, including unauthorized behavior, malicious hacks, denial of service (DOS) attacks, anomalies, and trend analysis. We found that only 28% of companies outsource security monitoring (Gallaher et al, 2006). In talking with several of the firms that do not outsource security monitoring, we heard anecdotal evidence of very costly (and unsuccessful) attempts at outsourcing monitoring in which it became apparent to the firms that the upfront transactions costs were going to be too high (in dollar terms and time) to achieve the short- or medium-term savings that were desired.

Consulting and forensics services are also offered by many MSSPs. Consulting relationships involve hiring an outside firm to help provide general or specific advice on security purchases or practices. Forensics services are usually employed to help find a specific problem or track how and why someone was able to breach a network.

Based on the type of outsourcing relationship, costs and benefits will differ significantly. Although Schneier (2002) suggests that organizations should not outsource management, he advocates for the outsourcing of vulnerability testing,

[10] Of note, Bruce Schneier, a former NSA cryptographer, is the founder and CTO of BT Counterpane, an MSSP focused mainly on outsourced security monitoring, in addition to other security services. A newer version of his write-up on what security services to outsource is available at Counterpane's website at http://www.counterpane.com/why-outsource.pdf. In this more recent article (2006), Schneier does not mention that security management services should not be outsourced, however, he does point to the MSSP's lack of knowledge of the impact of a security problem on a specific customer's business as the main drawback to outsourcing. Schneier has been very active since the beginning of the study of the economics of information security.

monitoring, consulting, and forensics. Others (e.g., Ortiz [2007]) advocate the outsourcing of as many security functions as possible.[11]

4.1 Industry Breakout

Tables 3 and 4 provide additional information from our survey data collection on whether organizations in certain industries outsource various IT security functions and if they outsource multiple functions. Universities generally do not tend to outsource technical services; only legal assistance is purchased by more than 20% of the universities we interviewed (Gallaher et al, 2006). Small businesses, in contrast, outsource many functions; two-thirds of the small businesses with which we spoke outsource installation, implementation, and maintenance of hardware and software; monitoring; and vulnerability testing.

We found that more than 80% of organizations outsource one of the five functions listed in Table 3— installation, implementation, and maintenance of hardware and software; monitoring of IT security issues; vulnerability testing; third-party insurance; or legal consultation. However, only 63% outsource one of the explicit security functions—installation, implementation, and maintenance of hardware and software; monitoring of IT security issues; or vulnerability testing. Table 4 provides a breakdown of firm outsourcing of multiple activities. More than 50% of organizations with which we spoke outsource two of the explicit technical security functions, and more than one-third outsource all three on which we focused (Gallaher et al, 2006).

4.2 Types of MSSPs

Aside from the matter of what type of outsourcing to undertake, firms also have to determine to whom they will outsource. Essentially, there are three main types of MSSPs: pure-play MSSPs—firms only offering IT security services—that frequently target small and medium businesses; IT outsourcer MSSPs—firms offering both IT and IT security outsourcing—that focus on Global 500 companies; and carrier MSSPs—Internet service providers (ISPs) offering IT security services—that deliver a broad range of business network services. However, MSSPs continue to merge; in particular, large IT services companies such as IBM and BT have been acquiring pure play MSSPs such as ISS and Counterpane. In this paper, I will not address the pros and cons of different types of MSSP models.

5.0 IT OUTSOURCING: BENEFITS AND COSTS

Specialization in providing IT security services and the resulting benefits from economies of scale generally should result in efficiency gains to the economy. The proven theory of specialization of labor says that firms are most productive when they spend their resources on one or a handful of specific activities. This is

[11] Most firms with which we spoke indicated that they wanted some control of their IT security functions, though several small businesses seemed willing to completely outsource all of their IT security activities.

Table 3. Percentage of Companies That Outsource, by Industry

Company Type	Installation, Implementation, and Maintenance	Monitoring of IT Security Issues	Vulnerable Assessment/ Planned Compromise	Purchase Third-Party Insurance	Purchase Legal Consultation (Internal or External)
Financial	50.0%	50.0%	100%	50.0%	83.3%
Health care	66.7%	0%	33.3%	33.3%	66.7%
Manufacturing	83.3%	33.3%	66.7%	0%	50.0%
Other	40.0%	20.0%	80.0%	40.0%	60.0%
Small business	66.7%	66.7%	66.7%	16.7%	66.7%
University	14.3%	0.0%	14.3%	0%	57.1%
Average	52.8%	27.8%	58.3%	22.2%	63.9%

* Source: Gallaher et al (2006).

Table 4. Percentage of Companies That Outsource One, Two, or Three Functions

Company Type	Outsource Something (1 of 5)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (1)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (2)	Outsource Installation, Implementation, and Maintenance, or Vulnerable Assets (All 3)
Financial	100%	100%	50.0%	50.0%
Health care	83.3%	66.7%	33.3%	0%
Manufacturing	100%	100%	50.0%	33.3%
Other	100%	100%	20.0%	20.0%
Small business	100%	83.3%	66.7%	50.0%
University	50.0%	14.3%	14.3%	0%
Average	83.3%	62.5%	58.3%	37.5%

* Source: Gallaher et al (2006).

particularly true for small businesses. For example, a biotechnology research firm is likely to spend its resources most efficiently by hiring labor to conduct research, while they may consider outsourcing functions such as accounting, legal services, and IT operations, including IT security.

An organization considering outsourcing IT security goes through the classic "make versus buy" decision making process. In the simplest scenario, the costs of conducting IT security in-house as opposed to outsourcing should be the same, but several economic concepts help to explain confounding factors on each side of the decision. If a company "makes" a product (or service) themselves, they will not incur any transactions costs associated with outsourcing to another firm. In contrast, the

company can decide to outsource and their costs will be reduced as a result of several factors: (1) specialized knowledge/skills of the MSSP, (2) ordinary scale economies that exist because the MSSP's technical skills represent a non-rival input[12], and (3) network effects. However, they will incur transaction costs and other risks described below.

The focus of this paper is on the network externalities associated with outsourcing security. Network effects imply that each additional firm engaging in the same activity has a positive effect on the benefits of all other firms; for example, the more people use Microsoft Excel, the more utility current users gain because they can share their work with more people. The argument in the case of IT security is that if one firm outsources security, the cost for them to attain a certain level of security is lower because the MSSP uses information from other firms that outsource security services to them to provide better service to all their customers. The more customers they have, the lower the cost (or higher security provided per dollar) that results.

IT security outsourcing should have the same basic cost and benefits as other types of outsourcing relationships, though IT security outsourcing does present unique challenges. For an individual firm and for IT security staff members, outsourcing IT security has substantial costs and benefits that vary based on many firm-specific factors. These costs and benefits have not been well defined, due to the both the relatively new nature of IT security activities and the dynamic nature of attack types. Further, outsourcing of IT security is likely to occur in bundles causing the costs and benefits to be non-linear in nature. As such, the decision to outsource IT security is less than straightforward for many firms.

5.1 Benefits

The practice of outsourcing generally allows organizations to focus on activities in which they can most efficiently use their labor resources, while paying other firms to perform functions in which they are less efficient. As discussed in Section 3, outsourcing of certain functions is commonly believed to result in productivity gains (cost savings). Outsourcing IT security to an MSSP has many of the same cost savings or quality improvement benefits as outsourcing other functions; essentially, hiring the same amount of IT security labor at an MSSP should result in higher security per dollar invested or, stated another way, lower cost per unit of security improvement. An MSSP develops an experienced staff that spends all of their time monitoring networks and keeping abreast of new vulnerabilities, new hacker tools, and new security and software products and patches.

However, certain factors make the benefits of IT security outsourcing likely to be larger than typical outsourcing benefits. Economies of scale and a more experienced staff are typical outsourcing benefits, but in the case of IT security,

[12] Economic theory uses the term nonrival inputs to describe inputs that may be expensive to acquire or develop but have a very low cost to reproduce or reuse. The skills and knowledge developed by an MSSP represent an input that is essentially nonrival; producing each additional unit of "security service" is cheaper because more skills and knowledge already exist and can be reused at little additional cost.

companies also benefit from information sharing and, in some cases, liability reduction or reduced costs to comply with regulations.

Much literature has investigated the benefits of sharing data on cyber security breaches and potential solutions and generally found that sharing leads to decreased spending and increased levels of security (Gordon et al., 2003; Gal-Or and Ghose, 2005; Landwehr, 2002). Sharing data and information on breaches allows firms to benefit from the lessons learned of other firms. In typical sharing structures (e.g., government-created Information Sharing and Analysis Centers [ISACs]), however, there is a strong incentive for firms to free ride—that is, make use of other firms shared data without sharing data themselves. As such, very few firms share information; our study found that approximately 25% of firms share information, and many of these indicated that they did not share detailed information about their security environment (i.e., equipment, software, policies, and procedures) or breaches.

Outsourcing IT security can help to solve this problem. When a firm outsources security monitoring services, for example, the MSSP analyzes their security infrastructure and collects data on incoming and outgoing network traffic. This information is then combined with the same types of information and data from other firms that outsource to the same MSSP. As the number of firms that outsource to one MSSP increases, the MSSP is able to analyze a larger set of data and network configurations with which to predict and identify problems and more quickly determine and implement (or recommend) the best solutions.[13]

Organizations are wary of providing data to public or private sharing consortia (e.g., ISACs) because (1) they cannot be guaranteed that other firms will share the same amount (and detail) or data and (2) they do not trust other organizations to maintain the integrity of the data they share.[14] While not without risk, outsourcing to an MSSP virtually eliminates any concern over free riding[15], and in the case of data integrity concern, the outsourcing firm is very likely to have strong liability measures in place to ensure that the MSSP to which they outsource will be held strictly liable for any and all negative effects if they share any customer data. As such, by outsourcing, organizations essentially are participating in a low-risk information-sharing relationship in which free riding is not possible.

Firms also might be able to benefit from assistance with regulations and liability issues. If the firm is regulated, its MSSP might be able to help the firm prove that it is compliant; MSSPs are likely to have their policies and procedures formally

---

[13] Note that because of the information sharing benefit, firms that outsource are likely to select MSSPs that have a large number of clients (a proxy for their reputation) so that this benefit is amplified. Ding et al (2005) discuss how the motivation for MSSPs to grow their customer base and the improvement to customer service quality that results is an excellent example of incentives alignment. This also implies that larger MSSPs will tend to dominate the market for more than simple economies of scale reasons.

[14] Hulme (2002) describes results from a survey in which less than 10% of respondents indicated that they contacted an ISAC after a security incident.

[15] Firms decide to outsource different types of activities (and some outsource more activities than others), so a firm that only outsources monitoring activities to one particular MSSP may benefit from the fact that another firm outsources monitoring, system management, vulnerability testing, etc. to the same MSSP. However, there is much less risk involved in providing information to an MSSP. Full anonymity is guaranteed and the data shared is likely to be more secure.

documented for use in both sales activities and contractual negotiations with customers. Thus, MSSPs could provide such materials to customers whose IT security infrastructure and practices are affected by regulations to help them show that they have conducted due diligence in assessing and mitigating system vulnerabilities to meet the appropriate standard of care. Furthermore, if a firm is sued, the MSSP could again help the firm confirm its compliance with a certain level of due diligence or detail the events of a certain event (e.g., security breach) in question.

5.2 Costs

Despite the many benefits, all types of outsourcing can be quite risky and can involve many costs. The most often discussed risk related to outsourcing is usually the effect of the principal-agent problem; first described by Jensen and Meckling (1976), the principal-agent problem exists when the incentives of an individual in a management role at a firm are not aligned with the interests of the owner or shareholders of the organization. For example, a CEO who does not receive stock in his company might not be as concerned with how his actions affect the share price. Similarly, a manager at a small business who does not get some share of the profits may not try to reduce costs or boost sales through extra effort or more efficient work.

In the area of IT security, the principal-agent problem is even more difficult because it is very hard to tell how much effort the MSSP is exerting. Security problems likely will result at most firms even if their MSSP has aggressive security measures in place,[16] and as such, the outsourcing firm might not realize if the MSSP is shirking or not performing their service at the level claimed. As a result, the incentive for MSSPs to shirk is quite high. However, outsourcing still occurs, so presumably MSSPs must not shirk much or else their shirking cannot adequately be observed and firms that outsource are not aware of the true extent of shirking.[17]

Shirking can be mitigated by several factors. An open flow of information about service quality and appropriate assignment or distribution of liability can both help. As mentioned above, the first solution is very difficult to employ with respect to IT security outsourcing activities. The IT security environment changes frequently (i.e., new types of attacks emerge), and the time to monitor the service being provided could at least partially negate the benefits (cost savings) being sought by a firm. However, an MSSP's reputation, though not likely based on explicit knowledge of the firm's actual activities, can provide at least some measure of motivation for firms not to shirk. If a firm is thought to be shirking, the effect on their business could be extreme, and as such, it may not be worth the risk for them to shirk to any significant degree.

Liability alignment, however, could help. The establishment of strict liability in outsourcing relationships would mean that the MSSP would be fully liable for any successful attacks on one of their customers. This paradigm is not likely to exist

---

[16] Security mechanisms are not available that can totally prevent malicious traffic and allow only desired traffic onto a network.

[17] Ding and Yurcik (2006) provide support for the theory that uncertainty in service quality (i.e., the possibility of shirking) does not significantly offset the advantages of outsourcing.

because of the constantly evolving nature of security attacks means that some successful attacks will almost certainly occur. Negligence is when a firm is held responsible if they do not provide "adequate" security—standard of care—as determined by a contract and a court of law.

In the past, MSSPs have not borne much if any liability for security breaches. According to several sources (e.g., Hamblen [2004) Weiler [2002]), MSSPs generally state in their contracts that they cannot identify all incidents, and as such, when an incident does occur, they are not liable for the damages. A still open question for debate is whether the legal system could help realign liability issues concerning IT security events. With change in the legal system and if there is a significant lack of information about the quality of service being provided by MSSPs, the percentage of firms outsourcing IT security may not increase significantly in the short-run.

A multitude of additional risks are involved in IT outsourcing, many of which are shared with other types of outsourcing relationships. A working paper by Clemons and Aron (2004) discusses two additional types of outsourcing risks: potential theft of propriety information and postcontractual renegotiation. In the case of IT security, the MSSP could steal proprietary information (referred to as "poaching") from its customers and sell this information to competitors. The MSSP could renegotiate the price of its contracts with customers after the outsourcing firms feel locked in; this is often called postcontractual renegotiation, or opportunistic repricing, and it occurs when a firm decides to raise its price after its customers have invested in setting up the relationship and are unlikely to enter into a new relationship. Finally, the MSSP could go bankrupt, as was the case with Salinas and Pilot Network Services between 2000 and 2001 (Schneier, 2002). Ding and Yurcik (2006) provide evidence that bankruptcy risk may indeed offset the advantages of outsourcing in some cases.

Outsourcing also involves explicit costs that appear in some form or another regardless of the riskiness of the relationship. Most significantly, transactions costs and interoperability costs with an MSSP can be quite high. MSSPs often establish a slate of security packages that address different company characteristics and needs, but firms differ in many ways that cannot always be considered prior to the initiation of a relationship. Firms differ in the ways in which they use the Internet, the sensitivity of their data, the regulations with which they must comply, and the management oversight of their security. Additionally, when information (e.g., data on access and breaches) needs to be transferred, interoperability problems are likely to result. As such, at the beginning of and at periodic times throughout every outsourcing relationship, there will be an upfront investment required to minimize transactions and interoperability costs throughout the term of the relationship.[18]

The main "losers" in IT security outsourcing will be IT security staff who work onsite at companies who decide to outsource their security activities. Although outsourcing doesn't necessarily mean a net societal loss of security jobs, it does imply a shift from one position, for example at a manufacturing firm, to another position at

[18] Ding et al. (2005) suggest that transactions costs may be higher for outsourcing IT security than other outsourcing relationships because the outsourcing structure/process is not standardized in this area, and there is uncertainty about the frequency and effect of cyber attacks that could cause significant variation in coordination costs.

an MSSP. For the security director or manager at the manufacturing firm, cost per unit of security is the motivating factor in making the decision to outsource or not. However, using the same example, security staff at the manufacturing firm have an incentive to explicitly suggest or imply that the costs to outsource will be higher and benefits will be lower than will actually be the case during and after the transition to outsourced security services, assuming outsourcing will result in some layoffs at the manufacturing firm.

6.0 FACTORS INFLUENCING THE POSITIVE EXTERNALITIES-NATURE OF OUTSOURCING IT SECURITY

If we assume that outsourcing leads to better security at firms that outsource, a simple analysis would suggest that the resulting change would be a Pareto improvement, meaning that no other firm would be made less secure by this decision. Further, as described in Section 5.1, it's possible that most or even all other firms and individuals could benefit, if only slightly from one firm's decision to outsource IT security. However, the indirect effects may not be so straightforward. There are several key factors that influence whether one organization's decision to outsource will benefit (or even possibly impose a cost on) other individuals and firms, and if so, to what extent. Relevant issues include the following questions:

1. How does one firm's decision to outsource affect that firm's level of spending on security?
2. What type and/or level of outsourcing is necessary for benefits to other firms or individuals to result?
3. How does one firm's decision to outsource affect other firms' decision to outsource?
4. How do MSSP structural issues or policies/activities affect the nature of any externalities that may result?

If one firm increases its level of security, the firm will not be used to spread attacks through the network, and thus all firms should be slightly more secure (Camp and Wolfram, 2000; Gallaher et al., 2006; Varian, 2002). However, increased security at one or a group of firms can also have a negative externality because this change causes attackers to look for less-secure firms to attack. In a similar scenario, Ayres and Levitt (1998) describe the effect of increases in home security by one home owner on a neighbors' likelihood of being attacked; they suggest that when one firm decides to install a home security system, neighboring homes' probability of being attacked increases. The implication of this relationship is that improvements in IT security at one or a group of firms could result in a negative externality being imposed on other firms—the probably that they would be attacked could increase if attackers viewed them as less secure, and hence better targets.

Further, Thompson (1972) suggested in the American Economic Review that when a new individual or firm (with more valuable data) joins a group, the group is more at risk of being attacked because it is a more valuable target to attackers. In the case of IT security activities, when a new firm joins an MSSP, this would imply

that the entire group of firms that outsource to the same MSSP may become more at risk of being attacked. Technically speaking, it is possible that an attack on an MSSP's firewall could result in the acquisition of data from all customers. Although it is very likely that each customer's data will have different encryption, breaking encryption today is much easier than in the past. Through the use of botnets—networks of hijacked or "zombie" computers—hackers are able to effortlessly assign hundreds of computers to work together to test combinations of characters to crack a code. As such, MSSPs could become large "honeypots"; that is, hackers might see them as very profitable targets and thus worth extra time and effort to attack. The effect first described by Thompson could negate some of the positive private and social benefits of outsourcing; however, it might also alleviate concerns of other firms over the "home alarm system" effect of improved security described above.

6.1 How Much Do Firms That Outsource Spend on Security?

According to our data collection, firms spend approximately 5.7% of their IT budgets on IT security. This figure is a little higher than found by other data sources such as the 2006 CSI/FBI Computer Crime and Security Survey results, which was completed by approximately 610 respondents and found IT security spending to be approximately 5.0% of IT spending (Gordon et al., 2006). Although our sample was small, when looking at firms that outsource versus those that do not, our data show that firms that outsource one or more services[19] spend approximately 5.5% while those that outsource nothing spend 6.2%. Firms that outsource at least two services spend approximately 3.6% as compared to firms that do not outsource two services that spend 6.8%. These numbers show some possible cost-savings benefit resulting from outsourcing; however, no study has attempted to discern a difference between individual firms spending before and after they decide to outsource one or more security activities.

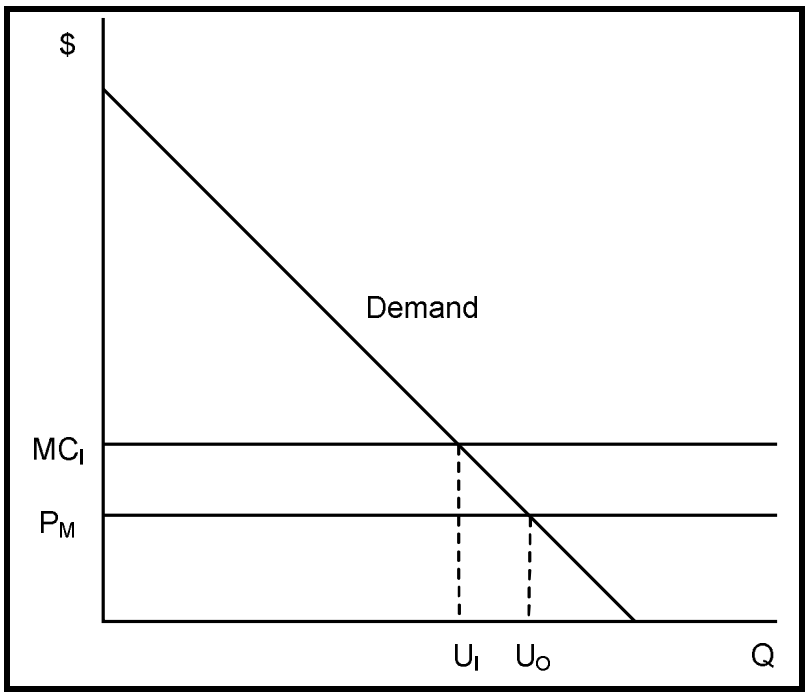
The elasticity of demand for security is important to consider. If security has an elastic demand function, then if outsourcing can reduce the price of one unit of security, firms should decide to consume more or increase their security. More specifically, if a firm decides that it can outsource part of its security and pay less per unit of security, we should assume that the firm would consume more security. Figure 1 shows the likely result if we assume that outsourcing is less costly than companies conducting IT security activities internally.[20] More security in total will be consumed when firms transition from spending money on security internally, where the marginal cost of each unit of security is MC_I, to spending P_M, the market price of outsourced security, per unit. However, this does not necessarily suggest that an individual firm will increase or decrease their level of spending.

---

[19] This includes the following three services: installation, implementation, and maintenance of security equipment and/or software; monitoring of security issues; and evaluation of security holes through a planned compromise.

[20] Discussion of changes of one "unit of security" does not accurately represent actual changes in IT security by an individual firm. Security is generally improved by purchasing a new piece of security hardware or software or adding a new staff member. These changes would more appropriately appear graphically as a "lumpy" demand curve, similar to a step function.

Figure 1. Change in Total Market IT Security Consumption, Outsourcing versus Internal



Security has many characteristics that are very different from normal goods. When a firm increases its spending on security, it may or may not be guaranteed to see improvements (e.g., better network performance, reduced downtime, or fewer breaches) because of the frequency with which new types of attacks develop. Further, it is difficult to determine how much an individual firm will decide to spend on security, based on a variety of subjective factors, such as their perceived likelihood of being breached and their level of trust in the services provided by the MSSP to which they outsource some or all security services.

For purposes of explanation, if we assume that a firm (let us call it Firm A) will only decide to outsource some IT security activities to an MSSP (Firm X) if it perceives a higher security per dollar invested, we still do not know how much Firm A will spend on IT security. If Firm A spends the same amount (or more) than it spent before it decided to outsource, I assume that Firm A will attain a higher level of security. Alternately, Firm A could assess how much it needs to spend (we will assume less than before) to achieve the same level of security before it decided to outsource its security. Or, Firm A could decide to spend less than this amount, possibly because of a changing budget or a strategic change[21], and thus end up with a lower level of security than before their outsourcing began.

[21] A firm may decide to spend less than enough to equal the security their had before because the firm is cutting all costs; for example, the firm sales may be down or they might decide to become the "low cost" or discount provider of a certain product or service. Alternately, a firm may decide that given the new security per dollar

To expand the scope of this scenario, suppose several other firms (B, C, and D) also outsource to Firm X. They similarly went through a cost-benefit analysis and determined that outsourcing to Firm X would result in costs savings. Of course many other firms (small and large) and individuals either decide to outsource to another firm or do not outsource their security at all.[22]

If one firm or individual's security is improved, there can be a multiplicative effect. Varian (2004) describes IT security in three ways—total effort, weakest link, and best shot.[23] In reality, there is likely to be a mixture of these conceptual frameworks affecting all users' security. If a firm is at a critical point (e.g., feeds traffic to other firms), the best shot model would be particularly fitting, and similarly, if one firm's lacking security allows an attacker into a group of shared networks, the weakest link scenario would make the most sense. However, in general, the total effort case is the most applicable. Anderson and Moore (2006) suggest that security changes by a firm generally fall into the total effort, or sum of efforts, case, in which any firm that increases its individual level of security will increase the security of all.

As a result of how much Firm A decides to spend on security after making the decision to outsource, several types of positive externalities could result. First, if one firm decides to outsource security activities, the MSSP can use their data and lessons learned from analyzing their network to benefit all other customers of the same MSSP. Second, if the deciding firm becomes more secure, all of society (firms and individuals) become more secure because there is a lower probability that the deciding firm will be used by attackers as a "staging point" to attack others. And finally, there will be a larger benefit to society because of the improved security of all customers of the MSSP.

In order to determine the specific benefits and level of such that will result from one firm's decision to outsource, several investment scenarios must be considered as follows:

1. Firm A spends same as before: Several parties should see improvements in security.

    - Firm A – Potentially large benefit because of increased security.
    - Firms B, C, and D – Substantive benefits because Firm X can use information from Firm A's configuration and security problems to help improve security at B, C, and D.

---

ratio, they want to cut back on security costs by 30%, while only lowering their level of security by 5 or 10%. This could be a perfectly rational decision under certain business circumstances.

22 When talking about small businesses and home users, the term "outsource" could mean relatively simple relationships with ISPs; for example, an ISP may offer monitoring services.

23 Total effort means that all of the efforts of all organizations and individuals impact the overall security of a particular network (or the Internet). Weakest link means that if one organization or individual has particularly bad security, the security of all others is based on the one bad organization. Best shot means that if one organization has very good security, their security means will help to protect others and thus others do not need to exert much effort.

- All other firms/individuals – Very small benefits will also accrue to all other firms and individuals because Firm A, as well as Firms B, C, and D, have a lower probability of propagating security problems.

2. Firms A spends enough to equal the same level of security as before: Firm A will not see an improvement in security, but other groups and individuals should.

    - Firm A – Benefits from cost savings without compromising security.
    - Firms B, C, and D – Substantive benefits because Firm X can use information from Firm A's configuration and security problems to help improve security at B, C, and D. Smaller relative to their benefits in Scenario 1.
    - All other firms/individuals – Very, very small benefits will also accrue to all other firms and individuals because Firms B, C, and D have a lower probability of propagating security problems. Smaller relative to Scenario 1.

3. Firm A spends less than enough to equal the same level of security as before: Other groups and individuals could still see improvements in security.

    - Firm A – Benefits from cost savings, but with lower security. Assuming the firm is a rational actor, the firm will be no worse off because the outsourcing alternative represented a new profit-maximizing point at a lower level of security.
    - Firms B, C, and D – Some benefit because Firm X can use information from Firm A's configuration and security problems to help improve security at B, C, and D.
    - All other firms/individuals – Extremely small benefits will also accrue to all other firms and individuals as Firms B, C, and D see additional benefits.

As described above, if we assume that firms will consume more security if the price per unit of security decreases, then Scenario 3 is not likely to occur. However, many firm characteristics that have not been discussed in this paper may exist that determine the level of spending a firm sets after it decides to outsource certain activities. This issue merits further study.

6.2 What Type or Level of Outsourcing Benefits Others?

The type of security outsourcing and the number of activities outsourced by firms affects the resulting benefits that other firms observe. Monitoring and system management will result in the most benefit to other firms. Firms will directly benefit from the knowledge that the MSSP adds by seeing additional network traffic and

information on both network characteristics and breach attempts. This will substantively improve the security of other firms that hire the same MSSP, but also will improve the security level of all other firms and individuals slightly.

Vulnerability testing, security audits, and installation outsourcing by one firm may benefit other firms and individuals as well, though not as directly. If the outsourcing firm increases their security, then the general level of social IT security should increase. Further, as with monitoring and systems management outsourcing, the MSSP that conducts periodic services (e.g., vulnerability testing, security audits, installation services) will gain knowledge that may help it provide better service to other firms that hire the same MSSP to conduct such activities. As such, other customers of the same MSSP should benefit.

If a firm outsources more than one activity, the potential benefit to other firms, both customers of the same MSSP(s) and all other firms/individuals, should increase.

6.3 How Does One Firm's Decision to Outsource Affect Other Firms' Outsourcing?

One firm's decision to outsource is not usually known by other companies, unless the hiring firms make this public knowledge. However, MSSPs do use the number of customers they have as a marketing tool (i.e., representative of the MSSP's reputation) to get additional customers. And as such, one firm's decision to outsource will likely have an effect, as more firms decide to outsource to the same firm because of both the marketing effect of additional customers and, possibly, the firm's estimated cost savings.

A more thorough analysis of the impact of one firm's decision to outsource on other firms' outsourcing might include a game theory analysis.

6.4 What MSSP Structural Issues or Activities/Policies May Affect the Existence or Nature of Any Externalities?

As we consider the potential social effects of MSSP relationships, we also should analyze the development of the MSSP market and any actions MSSPs may take that could affect the realization of social benefits. Previously, we discussed some of the costs and benefits of outsourcing IT security. The general tradeoff for an individual firm is that, on one hand, an MSSP can provide benefits to customers because of the firms' specialization (i.e., expertise) and ability to utilize knowledge gained from working with multiple customer networks; however, on the other hand, as discussed previously, the MSSP could decide to shirk and not perform its security functions as promised, possibly without the customer's awareness. This basic scenario of how the MSSP should act and how they will act becomes even more complex when we consider how the MSSP market is structured and at what level an individual MSSP may decide to invest.

The industry structure is of particular importance. If an MSSP continues to benefit from an increasing number of customers (i.e., the MSSP observes diminishing marginal costs for each additional customer added), then the market

should lead toward a monopoly structure. During the past several years, MSSP providers have merged as described above. The MSSP market seems to be a classic case of knowledge-based economy theory—knowledge can be reused infinite times with no deterioration of value and network effects result.

However, a monopoly structure is not likely to result at least in the short-term because, currently, MSSPs serve different markets. Two main markets exist: (1) firms that serve small and medium businesses and (2) firms that provide more customized services and tend to serve larger organizations. These firm types have very different needs and hence the MSSPs who target them require very different structures.

Also affecting the existence of externalities is the pricing scheme of MSSPs. Gupta and Zhdanov (2006) describe potential pricing schemes for hypothetical private and non-profit MSSPs. They discuss the difficulty in securing initial investments in MSSP networks to reach a point of profit, in the case of private firms, or just to cover all start-up costs, in the case of non-profit consortia. They also discuss the optimal size of an MSSP network, which they suggest exists for non-profit consortia, but not for private, for-profit firms.

Leveraging Gupta and Zhdanov's research and Margolis and Liebowitz (1994) work on network externalities,[24] it seems that MSSP may change prices based on number of users and as such, capture some of the network effects nature of outsourcing within the price being charged. Using Margolis and Liebowitz' logic, if the price decreases as the number of customers increases, this could be the result of simple cost reduction (or reuse of the same inputs) or it could imply a positive externality. If confirmed by further investigation, this would suggest that the only true externality from one firm's decision to outsource IT security activities is the impact on organizations other than the MSSP's other customers. However, it is also important to note that, as discussed previously, IT security is not commoditized and there is not evidence that MSSPs' commonly change their prices. As such, the idea that differentiated pricing for the first and subsequent customers of an MSSP will occur may be relatively unlikely.

7.0 IMPLICATIONS AND COMPLICATIONS

There are conflicting data on the trends in the growth of security outsourcing. Market research has shown that the outsourced security market continues to grow each year, and as such, the benefits to outsourcing should result in a socially higher level of security for all. However, survey research, such as the CSI/FBI survey, has not shown an increase in the number of firms outsourcing security. If the security market is growing, this would imply that either more companies are outsourcing or those that do outsource are outsourcing more functions. Survey research would seem to support the later. Furthermore, outsourcing habits have changed, as firms seem to be becoming more selective about what processes and activities provide the most net benefits.

Private firms do not consider spillover effects when they consider whether to outsource their security or how much to spend on security. However, many firms are

[24] Margolis and Liebowitz (1994) suggest that

deciding to outsource security operations because they are able to see private net benefits in the form of cost savings or security improvement per dollar of investment.[25] Still, even if a firm does decide to outsource, it may not invest at the socially optimal level since the resulting benefits will be shared with other firms and individuals.

Government may have a role to play to ensure that organizations consider the social benefits of outsourcing security when making their decision. As opposed to other types of outsourcing (e.g., home alarms), IT security is different in the following ways: (1) the probability of an attack is very uncertain; (2) research suggests very large social costs associated with bad security by one firm; (3) the problem of IT security is very new compared to other security issues (e.g., home break-ins); and (4) IT security problems are very complex and evolving. Large social costs are being imposed by organizations that have ineffective IT security, and this cost is not included in the price of IT security products and services. The resulting negative externality implies a potential need for government intervention.

The government could subsidize outsourcing. For example, organizations could get a tax benefit for certain types of IT security outsourcing, if they spend at least the same amount of money as before the outsourcing. Alternately, government could work with industry to help market the benefits of outsourcing. However, additional research is needed on the effects of outsourcing – spending (costs) and changes in security (benefits) – on firms that decide to outsource and externalities that may affect other firms and individuals.

REFERENCES

Anderson, R. and T. Moore (2006). "The Economics of Information Security." Science 314(5799): 610-613.

Ayres, I. and S. Levitt (1998). "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack." The Quarterly Journal of Economics 113 (1): 43-77.

Camp, L.J. and C. Wolfram (2000). "Pricing Security." In Proceedings of the CERT Information Survivability Workshop, Boston, MA, pp. 31-39.

Clemons, E. and R. Aron (2004). "Maximize Your Outsourcing Benefits Through Complexity Arbitrage." Wharton School of Business Working Paper.

Coase, R.H. (1937). "The Nature of the Firm." Econometrica 4 (16): 386-405.

[25] MSSPs sell their services based on showing firms a return on their investment. As this industry matures, the management security services market and the firms that comprise it may be in a prime position to provide very useful information on the return on security investments.

Ding, W. and W. Yurcik (2005). "Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers." Presented at the International Conference on Telecommunication Systems—Modeling and Analysis, Dallas, TX, November 17-20.

Ding, W. and W. Yurcik (2006). "Economics of Internet Security Outsourcing: Simulation Results Based on the Schneier Model." Presented at the Workshop on the Economics of Securing the Information Infrastructure (WESII), Washington D.C., October 23-24.

Ding, W., W. Yurcik, and X. Yin (2005). "Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers." Presented at the Workshop on Internet and Network Economics (WINE), Hong Kong, China, December 15-17.

Gallaher, M., B. Rowe, A. Rogozhin, and A. Link (2006). "Economic Analysis of Cyber Security and Private Sector Investment Decisions." Report prepared for the U.S. Department of Homeland Security.

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

Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson (2006). 2006 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, pp. 1-25.

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

Görg, H. and A. Hanley (2004), "Does outsourcing increase profitability?" Economic and Social Review 35: 267-288.

Görzig, B. and A. Stephan (2002). "Outsourcing and firm-level performance." Discussion Paper No. 309, German Institute for Economic Research.

Gupta, A. and D. Zhdanov (2006). "Growth and Sustainability of Managed Security Services Networks: An Economic Perspective." Working paper.

Hamblen, M. (2004). "Farming Out Security: How to Choose a Security Provider." ComputerWorld. January 19, 2004.

Hulme, G. (2002). "With friends like this." Information Week, July 8, 2002. Available at http://www.informationweek.com/story/showArticle.jhtml?articleID=6502813 .

Jensen, M.C. and W.H. Meckling (1976). "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure." Journal of Financial Econometrics 3 (4): 305-360.

Katz, M. and C. Shapiro (1985). "Network Externalities, Competition, and Compatibility." The American Economic Review 7(3): 424-440.

Kimura, F. (2002). "Subcontracting and the performance of small and medium firms in Japan." Small Business Economics 18: 163-175.

Landwehr, C. (2002). "Improving Information Flow in the Information Security Market." Presented at the Workshop on the Economics of Information Security, University of California, Berkeley, May 16-17.

Leibowitz, S.J., S.E. Margolis (1994). "Network externality: an uncommon tragedy." Journal of Economic Perspectives 8 (2): 133-150.

Ortiz, S. (2007). "Five Security Functions to Outsource, and Why." CIO Digest, January/February 2007.

Pappalardo, D. (2005). "Users bank on managed security services." NetworkWorld, July 11, 2005. Available at http://www.networkworld.com/news/2005/071105-managed-security.html.

Schneier, B. (2002). "The Case for Outsourcing Security." Supplement to IEEE Computer Magazine 35(4): 20-21, 26.

Schneier, B. (2006). "Why Outsource?" Counterpane Internet Security White Paper. Last updated April 2006. Available at http://www.counterpane.com/why-outsource.pdf.

Thompson, E.A. (1972). "The Taxation of Wealth and the Wealthy." The American Economic Review 62 (1/2): 329-330.

Varian, H. (2004). "System Reliability and Free Riding." White paper. Last updated in November 30, 2004.

Weiler, R. (2002). "Decision Support: You Can't Outsource Liability for Security." InformationWeek, August 26, 2002.