Private Sector Cyber Security Investment Strategies: An Empirical Analysis*

Brent R. Rowe
Technology Economics and Policy
RTI International
browe@rti.org

Michael P. Gallaher
Technology Economics and Policy
RTI International
mpg@rti.org

March 2006

Abstract

Organizations typically use very robust analysis techniques to determine how best to spend resources in order to increase revenue and decrease costs or losses. However, few organizations attempt such analysis processes to determine the level and type of cyber security mechanisms in which they invest and which they maintain. Key performance and evaluation metrics are not available, so those organizations that use quantitative analysis techniques typically have well developed internal tracking systems and have spent considerable time analyzing their internal data. Using a case study approach, we conducted a series of interviews with large organizations in a variety of sectors in order to understand their investment and implementation strategies, particularly focusing on the factors which drive the level of security they maintain and the information resources they rely on for planning and resource allocation.

Here we present a qualitative discussion of some of our findings and introduce a conceptual approach to consider the trade-offs between various investment and implementation strategies and some public policy options.

*This paper is based on an ongoing study funded by the U.S. Department of Homeland Security.

1. Introduction

The optimal level of cyber security investment depends on factors related to the efficiency of the investment and hence its marginal cost and the security returns from the investment and hence its marginal benefit. These factors are generally related to organizational and performance characteristics such as an organization's existing information technology (IT) characteristics, the compatibility of available cyber security technologies with current technologies, the security needs of the products and services the organization provides, and the preferences/perceptions of its customers. In addition, expectations of future threats or compromises, vulnerabilities, and technical change influence the timing of investments and thus the costs incurred and the benefits received.

However, a volume of evidence suggests that most organizations do not view their cyber security investment decisions in the same way that they view other investment decision. Rarely does an organization undertake a sophisticated or even semi-sophisticated financial analysis (i.e., cost-benefit or rate-of-return analysis) prior to making the investment or deciding on the level of investment that is needed. In fact, in many instances organizations simply react to a breach or compromise (hereafter referred to simply as a "breach") and spend what it takes to solve the existing problem.

The result of such real-world practices leads to inadequate or uninformed evaluations or anticipations of security threats. In addition to the lack of quantitative analysis to assess the cyber security investment issue, at least two other so-called barriers limit an organization's ability to determine its optimal cyber security investment strategy. The first barrier is a limited availability of reliable, cost-effective information that would be needed to make informed investment decisions. The second barrier is the externalities and public-goods nature of cyber security knowledge (that follows from cyber security investments). The first barrier could lead an organization to under- or overinvest in cyber security, and the second barrier definitely leads to an underinvestment.

Relevant and applicable knowledge is a scarce good. Consortia and trade associations have been established by public and private organizations to encourage information sharing; however, the lack of economic incentives to participate and share (i.e., free-rider problems) has limited their success.[1] As a result, private organizations, because of information asymmetry, may not be able to calculate private benefits correctly. Or some sections within an organization may not understand the IT road map sufficiently to realize that reactionary investments are inefficient in the long run. In general, the lack of reliable information to inform the analysis may be one of the primary factors limiting the use of traditional economic methods for evaluating the efficiency by which cyber security investments are made.

[1] This relevant and applicable knowledge is, in part, codified but also, in part, tacit. Because of its tacit nature, the activities of consortia and trade associations are important. But also because of its tacit nature, the effectiveness of any information sharing depends on the experiential knowledge of those doing the sharing. Gordon, Loeb, and Lucyshyn (2003) provide additional discussion of information sharing and offer a model to help explain the impact of shared information on security.

Regarding the externalities and public-goods nature of cyber security, any investments in cyber security made by an organization, particularly of a proactive nature, will generate social benefits in excess of private benefits. That is, an organization will not appropriate all of the benefits it receives from a cyber security investment; thus, it will, from a social perspective, underinvest in cyber security. From a more economic perspective, it can be said that cyber security investments lead to cyber security-related information and that information has the characteristics of a public good. It is well known that public goods are typically underprovided by private markets as compared to their socially optimal levels of provision (Stigliz, 1988).

This paper summarizes our findings about cyber security investment strategies in the private sector based on an ongoing study for the U.S. Department of Homeland Security, which included a series of extensive interviews with U.S. organizations from several industry groups— six financial services firms, six health care providers, six manufacturing firms, seven universities, two electric utilities, two nonprofit research institutions, and one Internet service provider (ISP),, as well as six small businesses. The focus of our study was to investigate the decision-making process related to investments in cyber security. Investments, as we have defined them in this paper, include both hardware and software purchases and the determination and implementation of IT staff procedures and user policies. Essentially, we sought to analyze how organizations determine how much they should spend on cyber security and the solutions they select. For this paper, we summarize some general findings about investment strategy from our interviews and provide a new conceptual view of cyber security investments theory.

2. Need for Metrics and Analysis Methodology: Past Research

Conceptually in the literature, investment theory is discussed in terms of an NPV or cost-benefit analysis,[2] and in terms of cyber security investing, this framework should imply that the costs of cyber security investment opportunities should be compared to the expected benefits, where benefits are represented as avoided damages expressed in terms of the probability and expected cost of an event occurring. However, the inputs to this type of quantitative analysis are difficult, costly, and, in many cases, impossible to obtain. As a result, cyber security decision makers must usually rely on qualitative assessments of their security needs, which are then compared to quantitative analyses of other (non-IT) needs and investment opportunities.

[2] Corporate financing decisions, such as how much to invest in capital or R&D, prior to the late 1950s were largely based on anecdotal evidence and real experiences, but in 1958 Modigliani and Miller proposed using a more mathematical approach and laid the groundwork for modem neoclassical finance theory. In essence, it suggests that asset valuation models, which calculate organizations' value based on expected future net cash flows (including future investment decisions), should be used to determine how organizations should invest. Other researchers (Ross, 1978; Ryan, 1982) modified this basic idea and created the capital asset pricing model (CAPM), in which investments are made based on their comparability to returns available from government bonds or other relatively safe investments. Many organizations began to calculate a project's NPV, based on discounted cash flow analyses (DCF), and to compare this NPV with a certain "hurdle rate" to determine whether an investment should be made.

Schechter (2004) states that for businesses "security is an investment to be measured in dollars saved as a result of reduced losses from security breaches, or in profits from new ventures that would be too risky to undertake without investment in security" (p. 27). For organizations and individuals to determine the most appropriate level of spending on computer security, they need to be able to calculate the vulnerability of their networks and the costs/losses associated with potential attacks; however, no methodology for such predictions has been widely accepted or implemented.

Several metrics have been proposed in the literature to calculate and manage security costs in general. Annual loss expected (ALE), in which the expected rate of loss is multiplied by the value of the loss, is often discussed; however, Soo Hoo (2000) and others suggest that gathering accurate data for this formula is very difficult. Because of the irregularity of computer software development and the evolving nature of hackers, the future of security attacks is unpredictable.

Although accurate data necessary for robust analyses are currently not available, two main types of data are available to organizations and individuals interested in a general understanding of the past costs of cyber security incidents and the current level of threat:

- attack and vulnerability statistics
- costs associated with past attacks

Numerous organizations compile vulnerability databases and patch information and track the number of incidents reported by U.S. organizations on an ongoing basis. Many of these are private organizations, such as the security firm Counterpane, that provide such information only to clients and/or use it to help provide the best security for their clients. However, many private and public organizations and consortia also collect information on types of attacks and their frequency and, in some cases, provide general or product-specific solutions.[3] Still, current analyses indicate that this information cannot be used to accurately predict future attacks on a specific network (Cashell et al 2004).

Further, several groups try to estimate the approximate cost of cyber attacks. The Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey[4] is largely considered the best available source. The results of the survey describe the number of attacks on participating organizations' networks and cost estimates by the type of attack. For the year 2004, the CSI/FBI survey estimates losses of

[3] For example, the National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC) maintains the ICAT Vulnerability Database, a searchable index of vulnerabilities sorted using the common vulnerabilities and exposures list (CVE). Through the ICAT system, users are linked to numerous publicly available vulnerability databases and sites describing patches (i.e., solutions to software problems). In addition, several government-funded organizations operate to collect vulnerability information and distribute it to the public. The CERT® Coordination Center at Carnegie Mellon University and U.S. CERT, the so-called operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS), both work, often together, towards this goal.

[4] The CSI/FBI survey has been conducted annually for 10 years and each year is revised to improve the accuracy of the data and enhance its usefulness. The aggregated responses are made publicly available.

approximately $130 million for the 700 organizations that participated in data collection efforts (Gordon *et al*, 2005).

Although extremely suspect because of definitional issues and the difficulty involved in estimating both the direct and indirect costs of cyber attacks, these data nevertheless provide the government and other organizations with some information to help in determining their optimal level of investment in cyber security. Varian (2000, 2002), Anderson (2001), Campbell et al (2003), and Schechter (2004), among others, provide discussion and analysis of the difficulties involved in accurately estimating the metrics necessary for robust analysis. A 2004 CRS report also provide an overview of many of the attempts at quantifying the cost and probabilities metrics organizations need (Cashell, 2004).

In most instances, empirical analysis focuses on labor resources (as opposed to value of data or lost sales). For example, Gordon and Richardson (2004) provide a case study analysis of upgrading to an intrusion prevention system (IPS), in which they found that the cost of the system was weighed against the labor savings.

Instead of investigating the optimal investment methodology or trying to estimate a model for determining either the costs of cyber security attacks or the probability of a future attack, we took a step back and analyzed the organizational characteristics that affect cyber security investment decisions. What drives the level of due diligence within organizations? What information is available to support investment decisions? [5] Who makes investment and implementation decisions? Are private incentives aligned with socially optimal investment? The remainder of this paper focuses on our interview findings and analysis.

3. Cyber Security Investments: Empirical Evidence

To investigate the cyber security investment decision process, we conducted a series of in-depth interviews with organizations in the manufacturing industry, health care organizations, universities, Internet service providers (ISPs), electric utilities, nonprofit research institutions, and small businesses. We interviewed CIOs, CSOs, and Directors of Information Security, depending on the structure of and the distribution of responsibilities within each organization; interviews on average lasted for an hour and a half.

A general theme that emerged during our interviews was that many organizations are undertaking an extensive review of how cyber security is viewed, and many have begun or plan to begin to restructure their processes. Specifically, there is a trend toward cyber security being treated very holistically; that is, organizations are beginning to realize that relevant information associated with cyber security issues includes much more than the views of the in-house IT staff. Decisions related to the amount of resources allocated each year on hardware and software and specifying cyber security procedures and policies

[5] Gordon, Loeb, and Lucyshyn (2003) provide a model-based approach to understanding the relationship between information sharing and both organizational decision making and the associated level of security maintained by an organization.

affecting users should be informed by a variety of sources within each organization, including but certainly not limited to, the IT staff's knowledge and expertise.

All parts of an organization are affected by IT-related decisions; thus, all parts of an organization can potentially offer relevant views that could benefit the whole. Therefore, management is beginning to realize that cyber security decisions should be viewed in terms of risk management. Every organization is vulnerable to the risk of a security breach, so protecting the privacy of the organization is a managerial issue of priority. Furthermore, many breaches can result in legal and human resources issues, so administrative units are becoming more involved in certain decision making, often related to the determination of user policies.

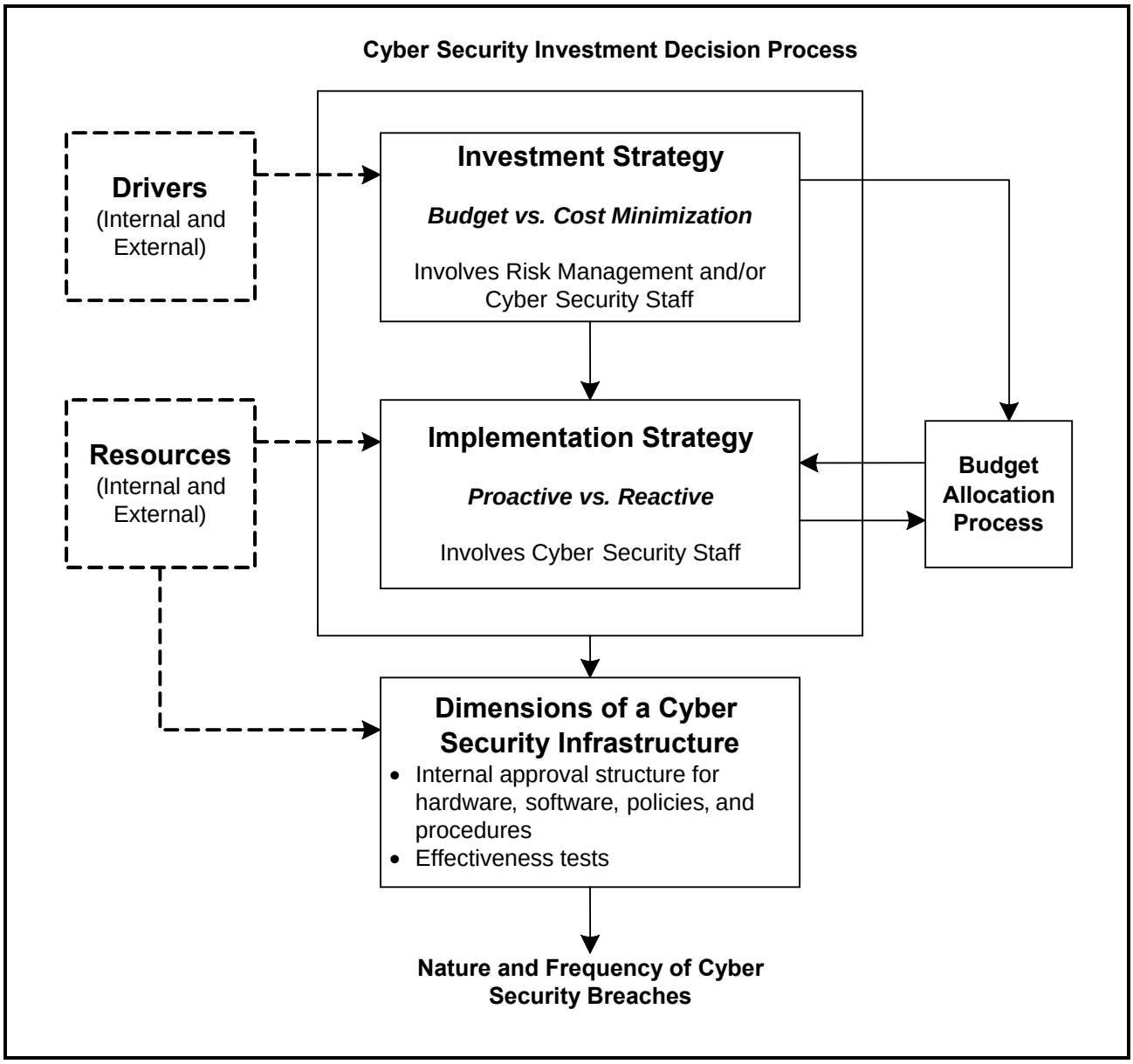
Schematically, Figure 1 is a diagram of the flow of decision making and the information sources that act as inputs to this process. To segment the decision-making process, we make a distinction between analyses conducted as part of an *investment strategy,* where management determines security priorities and investment resources in light of overall business operations, as opposed to analyses conducted as part of an *implementation strategy,* where IT staff determine the most efficient approach to meet the organization's security needs. In smaller organizations, the distinction between these two decision processes is blurred: the same staff are involved and analyses are intermingled. However, in larger organizations, organizational hierarchy leads to compartmentalizing different phases of the decision process that determine the overall level of cyber security.

Cyber security investment decisions are influenced by internal and external sources of information, with a recent trend toward more diversity in the internal sources of information. Initially, some external information (e.g., regulations, client requirements) and internal information (e.g., business process) can act as drivers, which, in addition to the budget determination process, largely determine an organization's implementation strategy.

Additional internal and external resources (e.g., NIST and ISO publications and vendor recommendations) are used to inform specific capital investment decisions and how policies and procedures are made. Subsequently, the organization makes specific investment and management decisions concerning cyber security hardware, software, IT staff procedures (labor), and user policies. The overall output of this process, in large part, determines the nature and frequency of breaches that occur.

In most organizations with whom we spoke, the budgeting process was based significantly on the previous year's budget and to a lesser extent on regulations or forecasts of anticipated needs. Only a few organizations determined the budget for cyber security through a rigorous cost-benefit analysis and/or a risk management framework. Thus, in Figure 1, the budgeting process has been separated from the investment decision process. In some cases, there is feedback between an organization's strategy for security and the budget it sets for cyber security; this is represented by the reverse arrow between implementation strategy and budget allocation process.

Figure 1. Diagram of Cyber Security Investment Decisions Inputs and Outputs



None of the organizations with whom we spoke felt that they had all the relevant expertise in-house to make effective cyber security investment decisions efficiently. Thus, external sources of security-related information are critically important. This reliance on external resources is a major focus of our findings and analysis.

3.1 Drivers and Resources

As discussed in Section 2, although the adaptation of the commonly used mechanism of cost-benefit analysis to support cyber security investment is conceptually straightforward, the expected damage or cost functions and threat probabilities needed to conduct this

analysis in practice are very difficult to calculate. As a result, most organizations rely largely on qualitative information to determine the optimal level of cyber security investment, relegating summary statistics analysis and empirical net present value (NPV) or cost-benefit analysis to a supporting or anecdotal role.

Organizations rely on both internal and external information resources, which serve as drivers effectively determining the strategy that each organization will use to approach cyber security investment decisions. For example, a regulation or client requirement may influence an organization to adopt a more proactive approach to cyber security by adopting more restrictive user policies and/or purchasing more state-of-the-art hardware and software technologies. Alternatively, not having enough information available in the public domain could cause an organization to adopt a more reactive strategy, addressing cyber security issues only when they affect business processes.

Table 1 provides a grouping of the major internal and external information sources that affect the cyber security investment decision process, either as *drivers* or as *resources* to cyber security practitioners or individuals responsible for approving cyber security purchases, policies, or procedures. Here, we present information related to the different types of information being used and discuss the use of these resources as gleaned from our interviews.

Regulations were the most often cited driver affecting organizations' investment strategy—on average, organizations indicated that approximately 30% of their motivation for security was accounted for by regulatory incentives. Only small businesses indicated that regulations were not their primary driver; they cited client demands as the most important factor

Table 1. Categorization of Relevant Drivers and Information Resources

Internal	External Public	External Private
	DRIVERS	
Business Process needs (i.e., strong business reliance on network) Major past breach	Regulations	Client demands Supplier demands
	INFORMATION RESOURCES	
Internal audits Staff experience/training Internally collected/calculated data (e.g., number of compromises, cost estimates) CEO/CTO/COO/etc. suggestions	NIST best practices ISO guidelines American National Standards Institute (ANSI) guidelines Security impact estimated (e.g., CSI/FBI survey) CERTS, SANS, etc.	Customer suggestions/ requirements Vendor suggestions/advice Conferences or trade publications Outside consultants Other organizations External audits

motivating their investment strategy. For all organizations, on average, IT staff knowledge and client demands were very important, ranking second and third respectively behind regulations. Table 2 provides average responses from interview participants with regard to the relative importance of each factor in motivating their investment strategy.

Table 2. Drivers Affecting Organizations Cyber Security Investment Strategy

Categories	Average Percentage across Organizations
Regulation driven	30.1%
Network history/IT staff knowledge	18.9%
Client driven	16.2%
Result of internal or external audit	12.4%
Response to current events (e.g., media attention)	8.2%
Response to internal security compromise	7.3%
Externally managed/determined	5.0%
Other	1.7%

Further, we asked participants about their relative use of information resources when determining their implementation strategy and determining how to spend available resources—what hardware and software they have in place and what policies and procedures they have determined. Table 3 provides a summary of organizations' responses during our interviews. In general, organizations indicated that staff knowledge and experience were the most important resources when determining what hardware and software to purchase and maintain, followed by internally collected data and vendor suggestions. Again, small businesses were the outlier—organizations in this category relied most often on vendor suggestions and outside consultants.

As for setting policies and procedures, most organizations suggested that staff knowledge and experience and regulations were the most important resources; however, internally collected data and internal audits were also ranked highly. Surprisingly, only health care organizations indicated significant use of NIST best practices, and almost no one indicated that International Standards Organization (ISO) and American National Standards Institute (ANSI) regulations were important information resources.

In general, through our interviews, we found that internal information resources were very important, both as drivers and information resources. Internal audits, the involvement of IT staff and in-house executives in determining the level of cyber security, and the tracking of internal IT information (e.g., the number of breaches, IT staff hours needed to resolve any

Table 3. Organizations Average Use of the Most Important Resources[a]

Resource Type	Hardware and Software	IT Security Procedures/ Activities
Government regulations	18.1%	44.4%
Customer suggestions/ requirements	16.7%	12.5%
Vendor suggestions/advice	30.6%	8.3%
NIST best practices	12.5%	26.4%
ISO guidelines	5.6%	9.7%
ANSI guidelines	5.6%	5.6%
Security impact estimates (e.g., CSI/FBI survey)	2.8%	6.9%
CERTs, SANS, etc.	6.9%	12.5%
Conferences or trade publications	22.2%	12.5%
Outside consultants	15.3%	13.9%
Other organizations	13.9%	4.2%
External audits	11.1%	12.5%
Internal audits	11.1%	33.3%
Staff experience/training	66.7%	51.4%
Internally collected/ calculated data (e.g., number of compromises, cost estimates, etc.)	36.1%	31.9%
CEO/CTO/COO/etc. suggestion	11.1%	5.6%
Other	2.8%	2.8%

[a] Organizations were asked to rank the resources based on their importance. The figures in this table indicate the percentage of organizations that ranked each factor either a 1, 2, or 3.

problems, and user time required to reach a solution) were all important for analysis purposes.

Most internal information is built on previous knowledge and experience from IT staff members. Thus, the validity and completeness of this information depended on the relative skill levels of the staff.

Although our interviews did not attempt to discern the relative level of competence of the IT staff, it is important to note that numerous experts and industry members indicated that the skill level of IT staff varies widely. Some staff failed to continue with self-education as technology changes, while others are not aware of the business repercussions of certain actions. Both inadequacies can cause significant security problems (although both inadequacies can be ameliorated through internal human resource expenditures).

Many different private and nonprofit organizations, including Cisco and Information Systems Audit and Control Association (ISACA), provide a variety of certification courses. There are certification programs for specific technologies, as well as more general programs. The certified information systems security professionals (CISSP) certification program, accredited by ANSI and ISO, seemed to be the most respected.

In addition to IT staff knowledge and ability, internal resources include the collection and use of certain internal data. Such information includes data on breaches—the number of breaches incurred by an organization of various types, the number of cyber security staff hours needed to resolve the attacks, the eventual solution, and the number of user hours required for resolution—as well as resource utilization information (i.e., how IT staff spend their time). Internally collected information can be analyzed to determine specific vulnerabilities and resource utilization and to estimate costs and probabilities of attack.

4. Cyber Security Investment Strategies: Findings

Organizations often have very different broad cyber security strategies. However, based on our interviews, we found that strategies can generally be characterized along a spectrum ranging from proactive to reactive, where a proactive strategy implies that security compromises are anticipated and safeguards are built into the IT system to prevent them; a reactive strategy implies that an organization is responding to known threats with typically established technologies so that security compromises can be addressed efficiently and effectively. We also gleaned from the interview process that fewer security compromises result when an organization adopts a proactive strategy as opposed to a reactive strategy, but the frequency and extent of such compromises—realized or averted—were not disclosed.

During the interview process, we asked respondents to characterize their cyber security activities and strategies in terms of proactive or reactive. In most cases, an organization employed a cyber security strategy that had both proactive and reactive elements. We also asked about the extent to which they always adhered to their defined reactive strategy using the same response code. From these responses, a proactive index was constructed for each organization.[6] Manufacturing firms indicated that they were the most proactive, followed closely by health care and financial organizations; small businesses and universities were both much less proactive, though they were still more proactive than reactive.

Respondents indicated that a significant cost of adopting more proactive strategies was evaluating and testing new cyber security procedures and technologies. An organization's ability to obtain reliable information in a cost-effective manner on the effectiveness of policies, procedures, or new technologies influences their overall cyber security strategy.

Based on this insight, it follows that industries having greater availability of public information may pursue more proactive cyber security strategies. As a result, we looked for

[6] See Gallaher, Rowe, and Link (2006) for a more expanded description of how our proactive indices were calculated and analyzed.

a correlation between an organization's proactive/reactive cyber security strategy and its reliance on external public information in their decision-making process.[7] The matrix in Table 4 generalizes these findings in terms of a conceptual relationship between an organization's proactive versus reactive cyber security strategy and its use of resources for cyber security.

Table 4. Relative Proactive / Reactive Strategy by Use of Public and Private External Resources

	Reactive Cyber Security Strategy	Proactive Cyber Security Strategy
Use of external public resources for cyber security	Low	High
Use of external private resources for cyber security	High	Low

Further, preliminary regression analysis has shown that organizations which are more proactive tend to share information more often and tend to consistently track the impact of breaches on users (internal staff), where as organizations that are more reactive tend to focus on simply tracking the number and type of events so that they can respond to breaches when they occur.

5. Cyber Security Investment and Implementation Strategies: A Conceptual Description

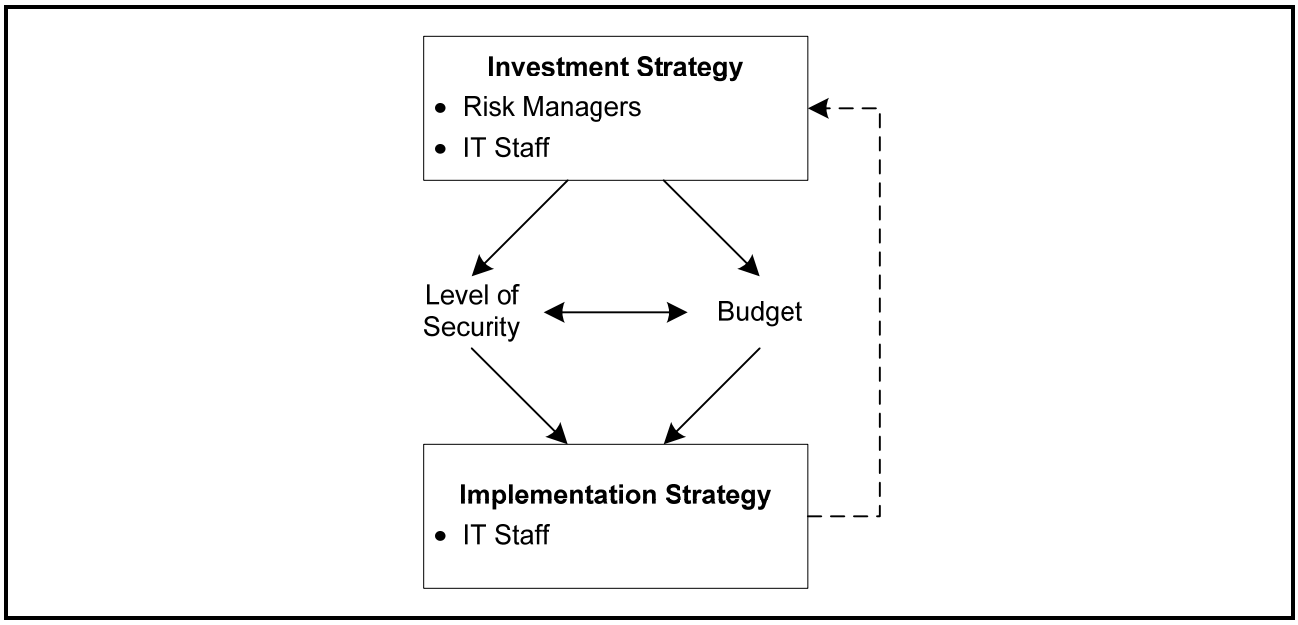
Based on our qualitative and quantitative findings, we have developed a new approach to thinking about alternate investment strategies and the trade-off between proactive and reactive implementation strategies.

Figure 2 presents a simplified view of an organization's cyber security decision process based on the flow chart originally presented in Figure 1. It begins with determining an organizational cyber security investment strategy—either prioritizing anticipated cyber security needs or setting a budget. These organizational-level decisions, in turn, guide the implementation strategy where specific security solutions are evaluated and compared.

From our interviews, we observed organizations' cyber security investment strategies as having two primary foci as indicated in Figure 2. One approach is to identify security *needs* and *priorities* and set investment levels accordingly; we refer to this approach as determining the "level of security." Essentially, this approach entails determining the optimal level of security and associated spending based on robust analysis. The "optimal level" represents the best determination that can be made with available information, often

[7] We compiled information on three types of information resources—internal, private external, and public external—and created an informational index for each.

Figure 2. Cyber Security Investment and Implementation Strategy



A second approach is to determine the *level or share of resources* (budget) that an organization should (or has available to) invest in cyber security. In this scenario, a certain amount of money comes out of the organization's budget, and cyber security activities and purchases are determined by maximizing the use of available resources. This is a "second best" approach in that it may not explicitly identify cyber security needs and thus could result in either an underinvestment or overinvestment in cyber security. However, implicitly these needs are weighed against competing needs and investment opportunities when the budget is determined. Often, organizations simply continue to fund the cyber security budget at the level of the previous year.

During our informal interviews, Chief Security Officers (CSOs) indicated that they frequently were motivated by a combination of targeted "level of security" requirements and budget constraints when formulating their cyber security *implementation strategy*. In contrast to the investment strategy, the implementation strategy is conducted almost solely by IT staff and involves collecting and evaluating information on specific cyber security solutions obtained from both internal and external sources. As discussed previously, an important component of the implementation strategy cited by organizations that were interviewed was to what extent cyber security strategies should focus on preventive/proactive solutions versus reactive solutions. This logically raises the question—what is the optimal strategic mix of proactive versus reactive cyber security activities for an organization?

Whereas a proactive strategy, in general, leads to fewer cyber security breaches, in some instances a reactive strategy may be more cost-effective. An analogy can be made as to how extensively a software programmer should test a new software product prior to installation. Any programmer will tell you that it is impossible (or prohibitively expensive) to

develop error-free software code. Thus, programmers select a level of (proactive) testing and debugging activities, knowing that in the future some errors will be identified that require (reactive) fixes, patches, and work-arounds. Experienced programmers implicitly conduct cost-benefit analyses based on history, experience, and market pressures to determine the optimal level of effort that should be devoted to testing and debugging.

Similarly, the optimal strategy mix of proactive versus reactive cyber security strategies for an organization depends on many factors,[8] and the line between proactive and reactive investment strategies is not always clear, nor is the line necessarily based on technology. The definition of a proactive versus reactive technology changes over time as the technology becomes established and eventually obsolete.[9]

The adoption of a proactive versus reactive strategy has an impact on IT expenditures and overall business operations. Table 5 provides an overview of both types of costs as they relate to being proactive or reactive. Proactive strategies have regulatory and reputational benefits, and because they are likely to lead to fewer events, can decrease business interruptions. However, respondents in our interviews said that proactive strategies can be restrictive. Close to one-third of the organizations we spoke with said that user convenience was equally, if not more, important than security, which led them to use reactive strategies in some instances.

Below we discuss two conceptual approaches from microeconomics that can be used to evaluate the optimal level of proactive versus reactive cyber security activities:

- output (i.e., level of security) maximization subject to a fixed budget constraint
- cost minimization subject to a fixed level of output (i.e., level of security)

As shown in Figure 3, organizations indicated to us that they strive to identify an appropriate balance/combination between proactive (A) and reactive (R) cyber security strategies. Drawing from economic theory, we illustrate this trade-off between implementing a reactive strategy (vertical axis) and a proactive strategy (horizontal axis) in terms of a family of curves that are concave to the origin. These so-called iso-security curves that are farther from the origin represent higher levels of cyber security. Also in

[8] For example, some dimensions of a proactive strategy, such as staff training and adoption of innovative strategies in a timely fashion, can yield significant benefits at reasonable costs. However, trying to anticipate and block all forms of rapidly evolving viruses can be expensive and perhaps only marginally effective. We learned of a number of instances where the most appropriate (i.e., cost-efficient) strategy was a reactive one. Specifically, it is most efficient to rely on existing, proven security technologies and then be able to quickly implement patches when new viruses are identified. Gordon and Loeb (2006) note that many organizations investments in cyber security increase after a breach.

[9] For example, periodically requiring users to change their password, once viewed as a proactive policy, has fallen out of favor. Users who are forced to periodically change their password are more likely to write it down or reuse a password used elsewhere, risking a security breach. Similarly, employing a person to monitor an intrusion detection system might be proactive, but if the person is looking for trends with which they are already familiar, this technique may be reactive. In addition, hiring someone to break into a network might be proactive, but if the person is using a vulnerability scanner that uses only known vulnerabilities, the strategy is reactive.

Table 5. Comparison between IT Costs and Non-IT Benefits Based on Security Strategy

Security Strategy	IT Costs	Benefits to the Organization (non-IT)
Proactive	Investments are cutting-edge hardware and software and the associated information gathering, installation, debugging, and maintenance costs	Fewer events—regulatory and reputation benefits, fewer business interruptions
Reactive	Infrastructure (mostly labor) resources needed to respond quickly and effectively Resources needed to repair damaged systems and data Potential damage to reputation	User convenience, flexibility to accommodate diverse business environments

Figure 3, we depict what is referred to as a budget line reflecting the resources ($) available to the organization to support/invest in cyber security. For example, if the organization allocated all of its cyber security resources toward a proactive strategy it would find itself at the point labeled $\$/P_A$; alternatively, if it allocated all of its cyber security resources to a reactive strategy it would find itself at the point labeled $\$/P_R$, where P_A and P_R are conceptually the unit price of a proactive and a reactive activity, respectively.

5.1 Maximizing Security Subject to a Budget Constraint

Although most organizations do not use solely a cost-minimizing or budget constrained approach, our interviews indicate that more organizations tend to rely on their budgets to drive the level of security they have in place (rather than the inverse relationship). Cyber security staff frequently indicated that their budgets are basically fixed (or change modestly from year to year); as a result, they view their role as essentially maximizing the level of security that can be provided subject to a fixed or predetermined level of resources.[10] This approach is similar to a production function economic model where output (security) is maximized subject to a budget constraint.

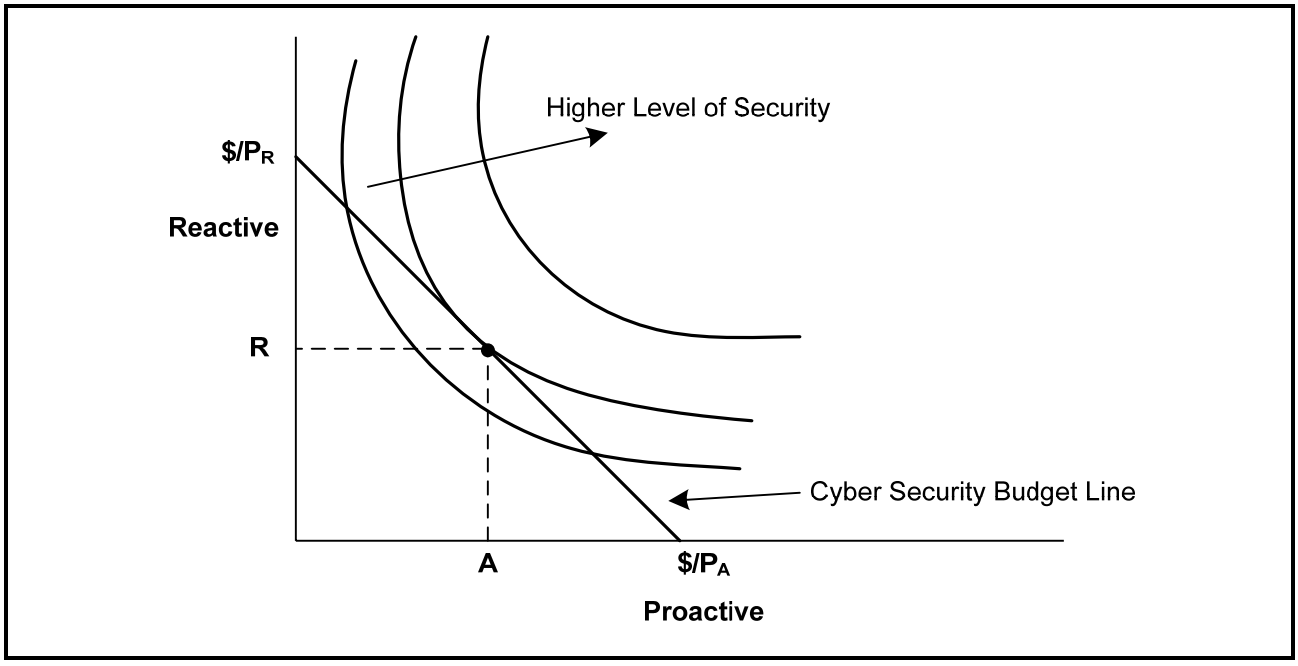
As illustrated in Figure 3, if we take the organization's IT budget as given (fixed), the optimal strategy mix is at the point of tangency between its budget line (the slope of which is determined by the perceived relative cost of proactive and reactive activities) and the highest iso-security curve that can be attained. This optimal point represents the optimal mix of reactive, R, and proactive, A, strategies.

5.2 Cost Minimizing Approach to Cyber Security

Organizations' risk management staffs look to leverage a wide range of information and expertise when assessing cyber security threats and developing a cyber security investment strategy. Such capabilities enable organizations with a more holistic view of cyber security

[10] Gordon and Loeb (2006) similarly address this reality of cyber security—that suboptimal investments are often necessary because of budget constraints.

Figure 3. Firm Selection of Optimal Proactive / Reactive Mix to Maximize Security Subject to Budget Constraint ($)



to determine the level of security or due diligence appropriate for their organization and then have their IT staff develop the most cost-effective implementation strategy. In this way, organizations seek to minimize costs while achieving a desired level of security. This strategy will include a combination of proactive and reactive measures. Investments in cyber security are costly as are repairs from breaches. Thus, an organization will select a cyber security strategy that minimizes what it views as net costs. This can involve investing in both cyber security hardware and software and staff training, as well as modifying organizational operations that could increase day-to-day operating costs by restricting how IT systems can be deployed or how users can access/interact with IT systems.

As shown in Figure 3, in the cost-minimizing approach is for an organization to identify the level of security that they determine is most appropriate for their organization, represented by the appropriate iso-security curve. This level is then taken as fixed and the budget line is adjusted in or out based on the total level of spending necessary to achieve the desired security and their perceptions of the cost of being more proactive or more reactive. The appropriate balance or combination of using a proactive and reactive strategy is then based on the level of security they determine and the budget line that creates a point of tangency. This enables the firm to spend the optimal level of investment dollars on proactive and reactive strategies based on a specific desired level of security.

5.3 Conceptual "Levers" Affecting the Relative Use of Proactive Versus Reactive Strategies

The above models focus on the private costs and benefits as they relate to private organizations. However, the private benefits implicit in these models may not represent the total social costs and benefits if externalities are considered; hence, society may benefit from a different mix of proactive versus reactive strategies. As introduced earlier, the public-goods nature of cyber security may distort private investments from what is socially optimal for society as a whole. Market failures may lead to underinvestments in cyber security because not all of the costs are borne by the investing organization because cost externalities of security breaches are incurred by other organizations in the network. In addition, the public-goods nature of information sharing and dissemination may lead to limited sharing of information about threats and solutions, commonly referred to as free-rider tendencies.

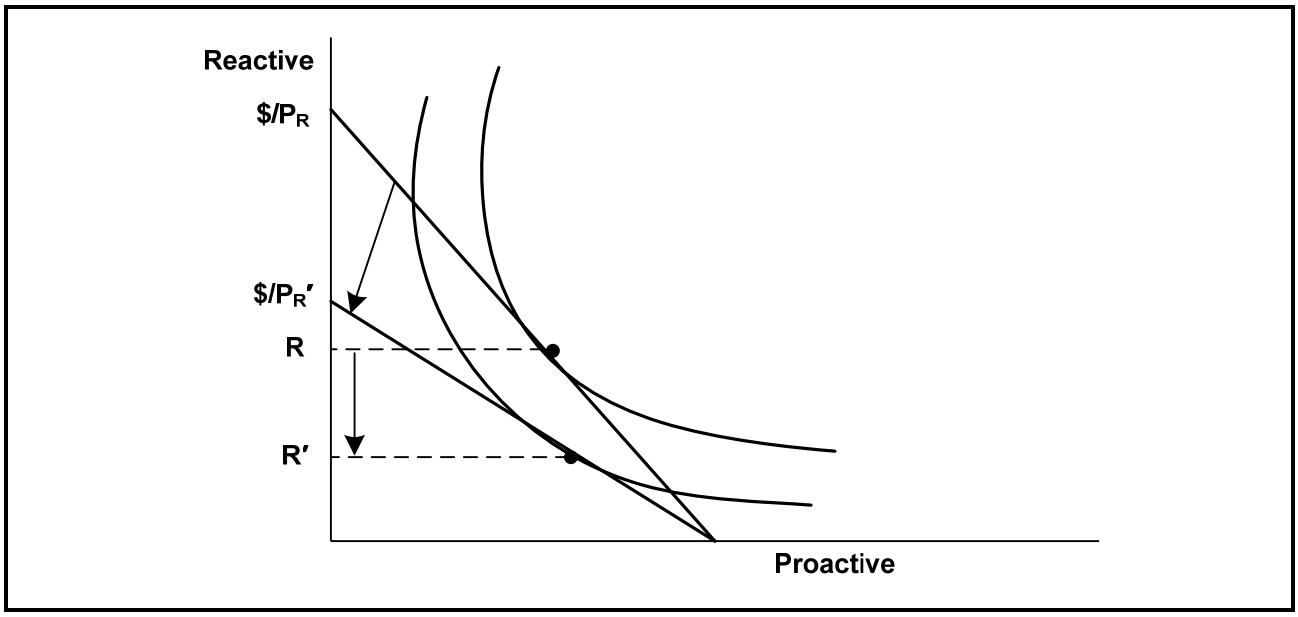
Issues of cost externalities and information free-ridership also have implications for selecting a more proactive versus a reactive cyber security strategy. In general, a reactive strategy is more likely to lead to cost externalities on organizations throughout the network because of the nature of the network. In contrast, a proactive strategy minimizes breaches and hence reduces cost externalities. In addition, proactive investments are more information intensive and hence are affected more by free-ridership issues where the reduced sharing of information increases the cost of evaluating and adopting proactive strategies.

5.3.1 Cost Externalities

Figure 4 shows how internalizing cost externalities affects the optimal proactive versus reactive cyber security strategy mix. Incorporating cost externalities increases the price, P_R, of reactive cyber security solutions, which rotates the budget curve inward. In terms of the output maximization strategy, this reflects that, when all cost externalities through the network are considered, for a given budget constraint, a lower level of (social) cyber security is actually being achieved. As shown in Figure 4, the maximum level of security is now achieved by decreasing the mixture of reactive cyber security solutions.

With regard to the cost-minimization strategy, incorporating cost externalities that are incurred throughout the network increases the cost of reactive activities, which, in turn, affects the necessary budget to maintain the level of security desired. Because reactive activities have become relatively more expensive, the result is that when cost externalities of reactive measures are incorporated in the investment decision, the cost-minimizing solution is to shift toward a more proactive cyber security strategy to reduce the cost necessary to achieve the desired level of security.

Figure 4. Internalizing Externalities Increases Price of Reactive Options ($P_R < P_R'$)



5.3.2 Information Sharing

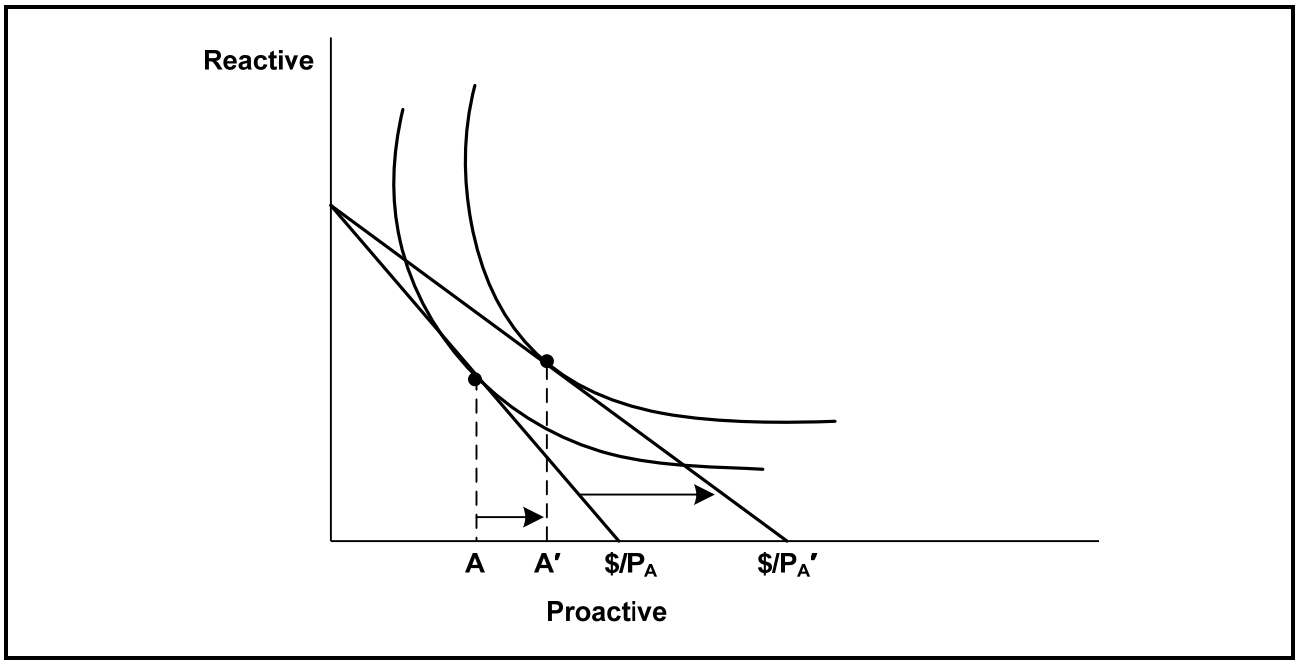
Cost-minimizing and output-maximizing analyses can also be used to visualize the impact of information sharing on the selection of proactive versus reactive strategies. As shown in Figure 5, information sharing decreases the price, P_A, of proactive solutions. This rotates the cyber security budget line outward. In the security-maximizing approach, this increases the amount of proactive solutions that can be implemented with the given budget constraint, thus, leading to an increased proportion of proactive solutions at the tangent point of the budget curve and iso-security curve. The overall result is a higher level of cyber security achievable given the budget constraint.

The cost-minimization strategy is also affected by this shift. With the level of desired security held constant, the necessary budget line could be shifted inward and more focus put on proactive strategies, while the same level of security is maintained at a lower overall cost.

6. The Public-Goods Nature of Cyber Security

The public-goods nature of information networks provides insight into the barriers affecting the development and adoption of cyber security solutions. Economic theory holds that an organization should evaluate its optimal-level cyber security investments by equating the marginal benefit that it receives from an additional "unit" of security with the marginal cost of achieving that "unit." However, because of the public-goods nature of cyber security, it is likely that the optimal level of investment from its private perspective will be less than the optimal level of investment from a social perspective. Furthermore, the optimal investment from the private perspective could be improved on by using additional resources to help enable more robust, quantitative investment analysis.

Figure 5. Information Sharing Decreases Cost of Proactive Options ($P_A > P_A'$)



As discussed previously, at least two barriers limit an organization's ability to determine a socially optimal cyber security investment strategy—the limited availability of reliable, cost-effective information that could be used for the organization to make an informed investment decision and the cost externalities that spill over to organizations throughout the network as a result of security breaches. The first barrier could lead an organization to under- or overinvest in cyber security from a social perspective, and the second barrier would definitely lead the organization to underinvest from a social perspective.[11]

Relevant and applicable knowledge is a scarce good. Consortia and trade associations have been established to encourage information sharing; however, the lack of economic incentives to participate and share information, particularly data, has limited their success. As a result, private organizations would be unable to correctly calculate private benefits. In general, the lack of reliable information to inform analysis may be one of the primary factors limiting the use of traditional economic methods for evaluating the efficiency by which cyber security investments are made.

Regarding the externalities and public-goods nature of cyber security, any investment an organization makes in cyber security, particularly of a proactive nature, will likely generate social benefits in excess of private benefits. That is, an organization will not appropriate all of the benefits it receives from a cyber security investment, because some of these benefits

[11] Note that we did not attempt to assess whether organizations are currently behaving optimally or whether there is a potential underinvestment by organizations in cyber security. However, an assessment of barriers to adoption of cyber security solutions is an important input necessary for more complete future policy analyses.

(also referred to as positive network externalities) spill over to organizations throughout the information system. Thus, from a social perspective, this can lead to an underinvestment in proactive cyber security solutions. Similarly, if the private costs do not reflect the true social costs of security breaches (negative externalities) it logically follows that organizations may underinvest in cyber security because of its public-goods nature.

7. Public Policy Implications

The theoretical basis for government's role in any market activity, cyber security related or otherwise, is based on the concept of market failure. Market failure is typically attributed to market power, imperfect information, externalities, and public goods. Government's role, then, is to lessen or remove any barriers that are associated with market failure and the like: in our case, the proper role for government might be to avoid underinvestment in a proactive strategy toward cyber security.

Government's tools to accomplish this goal are limited, but the quantitative and qualitative information we collected during our interviews suggests several areas of potential focus.

One possibility is that the government could help fund the collection, analysis, and dissemination of both reliable and cost-effective information related to cyber security. For example, everyone with whom we spoke was interested in continued research focused on estimating the cost of breaches and the probability of future attacks, both of which are extremely difficult to determine. Although many groups exist that attempt to provide information of various types, the organizations with which we spoke (particularly small businesses) were interested in more information comparing types of products. Also, several experts and organizations identified certification of skilled professionals as a key area that would enable more effective and efficient cyber security investing.

Furthermore, evaluating the effectiveness and efficiency of potential cyber security solutions is a complex and costly activity. In many instances, the taxonomy and metrics do not exist to facilitate comparisons of competing technologies. The government could underwrite the research and implementation costs for organizations that are pilot testing new innovations. This might increase investments in innovative cyber security strategies, shifting investments toward the socially optimal proactive level (as was the case when the government enacted the 1981 Research and Experimentation tax credit).

Another potential role for the government would be to design mechanisms that redistribute the costs (i.e., reduce spillovers and externalities) to better provide incentives for individual organizations to enhance their cyber security. Examples of this include regulations that define activities or security thresholds that must be met and the threat of litigation from being out of compliance. Both of these offer ways to make private organizations bear the social costs of security breaches. The private sector also engages in similar activities by requiring suppliers and partners to meet cyber security requirements and conduct regular security audits. In both cases, the intent is to internalize cost externalities so that organizations have the proper incentives when evaluating cyber security investments.

Based on our interviews, organizations have mixed opinions regarding whether regulations or business mandates were an efficient means of enhancing cyber security.[12] Because industries and business operations are unique, "one-size-fits-all" solutions may not lead to efficient solutions. In most cases, organizations believe that the impact of these regulations has been positive by increasing the overall level of security, although several organizations mentioned a very high compliance cost. Still, there was no consensus about how regulations could be improved. Several respondents noted that regulations need to be more prescriptive, while others noted that the regulations should only be viewed as a baseline, providing organizations with the flexibility to select the lowest cost solution.

8. Conclusions

In this paper, we offer a conceptual approach to describing the components of a cyber security investment decision and the trade-offs between differing investment and implementation strategies; further, we provide empirical evidence that a connection may exist between an organization's use of external public information and its relative mix of proactive and reactive strategies. Clearly, more information is needed about factors that influence an organization's investment and implementation strategies before any determination of specific government actions or other tools is made.

In particular, policy makers and organizations would benefit from a robust analysis of the difference between the social and the private costs of cyber security. Such an analysis could investigate the flows and magnitudes of cost externalities to determine who actually bears the costs of cyber security breaches. These are essential questions for policy makers interested in determining the most appropriate government involvement.

[12] Zhang (2005) estimates that the net private cost of the Sarbanes-Oxley Act, which imposes many requirements on the network security of public companies, will be approximately $1 trillion (2005).

References

Anderson, Ross. 2001. "Why Information Security is Hard—An Economic Perspective." Presented at the Annual Computer Security Applications Conference, New Orleans, LA.

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

Cashell, Bryan, William D. Jackson, Mark Jickling, and Baird Webel. April 2004. "The Economic Impact of Cyber-Attacks." Congressional Research Service (CRS). CRS Report for Congress.

Gallaher, M.P., Rowe, B.R., Link, A.N., January 2006. Economic Analysis of Cyber-Security and Private-Sector Investment Decisions. Draft report to DHS, RTI International, Research Triangle Park, NC.

Gordon, Lawrence, and Robert Richardson. 2004. "Infosec Economics: New Approaches to Improve Your Data Defenses." *Network Computing* April:67-70.

Gordon, Lawrence, Martin Loeb, William Lucyshyn, and Robert Richardson. 2005. *2005 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Gordon, Lawrence, Martin Loeb, and William Lucyshyn. 2003. "Sharing Information on Computer Systems Security: An Economic Analysis." *Journal of Accounting and Public Policy*. Vol. 22, pp. 461-485.

Gordon, Lawrence and Martin Loeb. 2006. "Managing Cyber Security Resources: A Cost-Benefit Analysis." New York: McGraw Hill.

Modigliani, F., and M.H. Miller. 1958. "The Cost of Capital, Corporation, Finance, and the Theory of Investment." *American Economic Review* 48(3):261-297.

Moitra, S.D., and S.L. Konda. December 2000. "A Simulation Model for Managing Survivability of Networked Information Systems." Carnegie Mellon Software Engineering Institute. <http://www.sei.cmu.edu/publications/documents/00.reports/00tr020.html>.

Ross, S.A. 1978. "The Current Status of the Capital Asset Pricing Model." *Journal of Finance* 33:885-901.

Ryan, R.J. 1982. "Capital Market Theory—A Case Study of Methodological Conflict." *Journal of Business Finance and Accounting*:443-458.

Schechter, Stuart. May 2004. "Computer Security Strength & Risk: A Quantitative Approach." PhD thesis, Harvard University.

Scholtz, T., J. Heiser, J. Pescatore, and R. Mogull. November 30, 2005. Gartner Report entitled "Use a Cost-Benefit Approach to Justify Security Spending."

Soo Hoo, Kevin J. June 2000. "How Much is Enough? A Risk-Management Approach to Computer Security." PhD thesis, Stanford University.

Stigliz, Joseph. 1988. *Economics of the Public Sector.* New York: W.W. Norton and Company.

Varian, Hal. June 2000. “Managing Online Security Risk.” *New York Times*.

Varian, Hal. May 2002. “System Reliability and Free Riding.” In: Proceedings of the First Workshop on Economics and Information Security. May 16-17. University of California, Berkeley.

Zhang, Ivy Xiying. 2005. “Economic Consequences of the Sarbanes-Oxley Act of 2002”. AEI-Brookings Joint Center for Regulatory Studies. <http://www.aei-brookings.org/admin/authorpdfs/page.php?id=1154> June 2005.