AFRL-IF-RS-TR-2006-227
Final Technical Report
July 2006

ECONOMIC ANALYSIS OF CYBER SECURITY

Research Triangle Institute

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2006-227 has been reviewed and is approved for publication.

APPROVED: /s/

EUGENE D. TURNBAUGH, Capt., USAF
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Jr.,Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
JULY 2006

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
Sep 04 – Apr 06

4. TITLE AND SUBTITLE
ECONOMIC ANALYSIS OF CYBER SECURITY

5a. CONTRACT NUMBER
FA8750-05-C-0013

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Michael P. Gallaher, Brent R. Rowe, Alex V. Rogozhin, Albert N. Link

5d. PROJECT NUMBER
DHSB

5e. TASK NUMBER
RT

5f. WORK UNIT NUMBER
II

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Research Triangle Institute
2040 Cornwallis Road, PO Box 12194
Research Triangle Park North Carolina 27709-2194

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGA
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2006-227

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA#06-481

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Organizations typically use robust analysis techniques to determine how best to invest scarce resources that will lead to increased revenue and decreased costs. However, few organizations attempt such analysis for their cyber security mechanisms. Key performance and evaluation metrics are not available, so organizations rely on qualitative assessments; and even those with well-developed tracking systems do not have the tools to derive the cyber security data for use in quantitative budgeting processes. Using a case study approach, we interviewed organizations in a variety of sectors to understand their investment and implementation strategies, particularly focusing on the factors driving their level of security and the resources they rely on for planning and resource allocation. This report presents our findings and introduces an approach to consider the trade-offs between various investment and implementation strategies and public policy options. In general, we found that most organizations make decisions related to cyber security investments at the IT staff level, but there is a trend toward more management-level (e.g., risk management) decisions. Further, our analysis indicates that some organizations are more proactive (vice reactive) than others, and that the proactive organizations are also more reliant on external information resources when making investment decisions.

15. SUBJECT TERMS
cyber security mechanisms and investments, investment and implementation strategies, risk management

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
U	U	U	UL	110	Eugene D. Turnbaugh
					19b. TELEPONE NUMBER (*Include area code*)

Table of Contents

List of Figures

List of Tables

Executive Summary

The optimal level of cyber security investment depends on factors related to the efficiency of the investment, its marginal cost, and the security returns from the investment, 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 growing volume of evidence suggests that most organizations do not view their cyber security investment decisions in the same way that they view other investment decisions. Rarely does an organization undertake a comprehensive financial analysis (i.e., cost-benefit or rate-of-return analysis) prior to making the investment or deciding on the level of investment. In fact, in many instances organizations simply react to a breach or a 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 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.

This report summarizes our findings about cyber security investment strategies in the private sector based on a series of extensive interviews with U.S. organizations from several industry groups—financial services, health care, manufacturing, universities, Internet service providers (ISPs), electric utilities, and nonprofit research institutions, as well as 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 the level of resources they allocate to cyber security and the solutions they select.

ES.1 NEED FOR METRICS AND ANALYSIS METHODOLOGY: PAST RESEARCH

Conceptually in the literature, investment theory is discussed in terms of a net present value (NPV) or cost-benefit analysis. In terms of cyber security, 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 the 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.

Several metrics have been proposed in the literature to calculate and manage security costs in general; however, 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 and
- costs associated with past attacks.

Numerous organizations compile vulnerability databases and track the number of incidents reported by U.S. organizations. Many of these are private organizations, such as the security firm Counterpane, which provide 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. Still, current analyses indicate that this information cannot be used to accurately predict future attacks on a specific network.

Further, several groups have tried to estimate the approximate cost of cyber attacks. The Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey 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.

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, this report takes a step back and analyzes the organizational characteristics that affected cyber security investment decisions. What drives the level of due diligence within organizations? What information is available to support investment decisions? Who makes investment and implementation decisions? Are private incentives aligned with socially optimal investment?

ES.2 CYBER SECURITY INVESTMENT AND IMPLEMENTATION STRATEGIES: A CONCEPTUAL DESCRIPTION

From our interviews, we observed organizations' cyber security investment strategies as having two primary foci as indicated in Figure 1. 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 including qualitative assessments of which cyber security objectives/requirements are essential (and likely to be cost-effective) for the organization's operations.

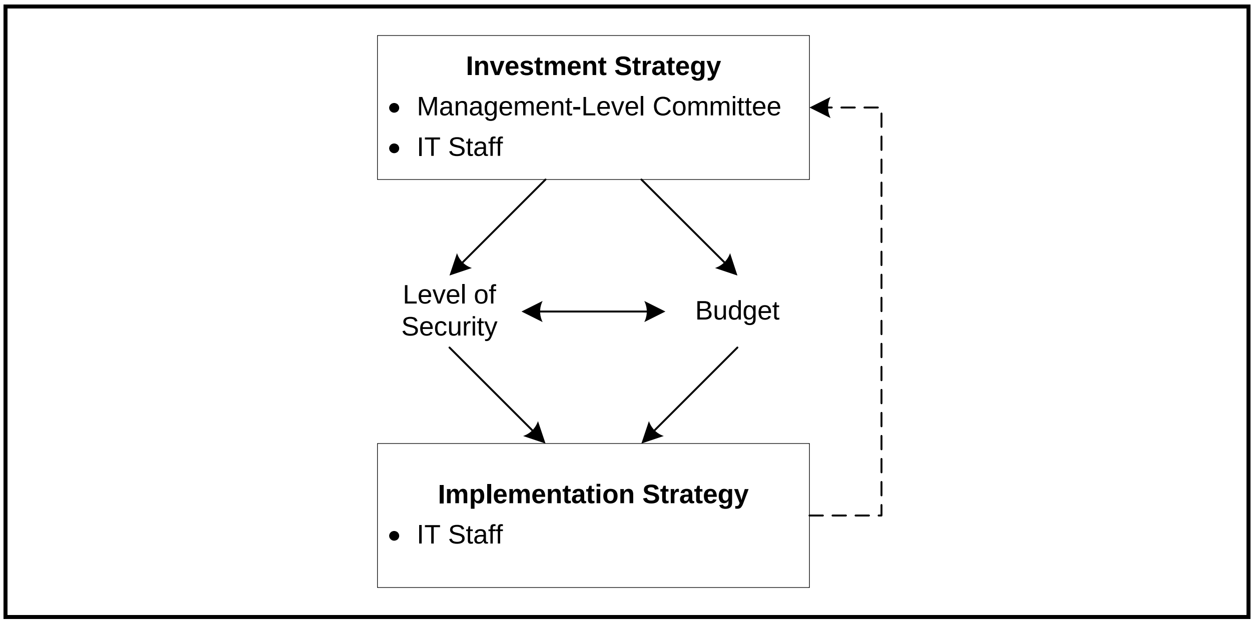

Figure 1: Cyber Security Investment and Implementation Strategy

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 an 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 devoted to testing and debugging.

The adoption of a proactive versus reactive strategy has an impact on IT expenditures and overall business operations. Table 1 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.

In some organizations, management staff 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 to determine the appropriate level of security or due diligence 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.

Table 1. Comparison between IT and Non-IT Costs and Benefits Based on Security Strategy

Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor)	• Cost: User inconvenience
	• Benefit: Decreased need for reactive labor	• Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation
	• Benefit: Decreased investments in proactive (risky) solutions	• Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

ES.3 CYBER SECURITY INVESTMENTS: EMPIRICAL EVIDENCE

To investigate the cyber security investment decision process, we conducted a series of in-depth interviews with manufacturing organizations, health care organizations, universities, Internet service providers (ISPs), electric utilities, nonprofit research institutions, and small businesses. We interviewed Chief Information Officers (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.

More than 75 percent of organizations in our study indicated that they have a structured budget process. However, the specific amount spent on cyber security varies across and within industry groups. On average, the organizations we spoke with spent 5.7 percent of their IT budget on cyber security. Table 2 provides a comparison of cyber security spending by industry group for the organizations with which we spoke.

We asked organizations about the involvement of different types of staff in their investment strategy phase. Generally, such decisions are made within one of two organizational areas: the IT department or a business strategy (“management”) department or committee (e.g., risk management). Table 3 shows, by industry group, where cyber security priorities and

Table 2. Average Cyber Security Budgets as a Percentage of IT Budgets, by Industry Grouping

Industry	Average Cyber Security Budget (as a percentage of IT budget)
Financial services	3.3%
Health care providers	6.2%
Manufacturing	4.2%
Small businesses	10.1%
Universities	3.3%
Other	8.5%
Total	5.7%

Table 3. Source of Cyber Security Investment Strategy

Industry Group	Within IT Department	Within Management Department
Financial services	33.3%	66.7%
Health care providers	33.3%	66.7%
Manufacturing	83.3%	16.7%
Universities	60.0%	40.0%
Other	85.7%	14.3%
Total	60.0%	40.0%

Note: Small businesses are not included because investment decisions are intermingled.

budgets are largely determined within the organizations. All parts of an organization are affected by IT-related decisions; however, most participants in our interviews indicated that IT staff were more responsible for cyber security investment decisions than were management-level staff or committees. Still, our interviews suggest that there is a trend toward cyber security being treated very holistically; management is beginning to realize that cyber security decisions should be viewed in terms of risk management.

Cyber security investment and implementation 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 *information resources* (e.g., NIST and International Standards Organization [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.

In most organizations with which 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.

None of the organizations 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.

However, we found that organizations rely on both internal and external information resources, which serve as drivers effectively determining the strategy used 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.

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 motivating investment strategy. For all organizations, IT staff knowledge and client demands were, on average, very important, ranking second and third respectively behind regulations. Table 4 provides average responses from interview participants concerning the relative importance of each factor in motivating their investment strategy.

Further, we asked participants about their relative use of information resources when determining implementation strategy and how to spend available resources (i.e., what hardware and software and policies and procedures are in place). Table 5 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.

Table 4. Drivers Affecting Organizations Cyber Security Investment Strategy

Categories	Average Percentage across Organizations
Client driven	16.2%
Regulation driven	30.1%
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%
Network history/IT staff knowledge	18.9%
Externally managed/determined	5.0%
Other	1.7%

Table 5. Organizations' Average Use of the Most Important Information Resources

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%

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 and American National Standards Institute (ANSI) regulations were important information resources.

In general, we found through our interviews that internal information resources were very important, both as drivers and as 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 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, but internally collected data is also a key input for decision makers. Internal resources include the collection and use of certain internal data, such as 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.

Based on our interviews, we found that implementation 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.

Respondents indicated that a significant cost of adopting more proactive strategies included 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 influenced 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. 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. We also looked for a correlation between an organization's proactive/reactive cyber security strategy and its reliance on external public information in its decision-making process; Table 6 generalizes the relationship we found.

Table 6. 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

This suggests that, from a policy perspective, public-sector effort to decrease cyber security breaches could focus on increasing the availability and usability of public domain information. That said, we also learned from the interviews that within an organization the optimal cyber security strategy is not totally proactive.

ES.4 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 investment by equating the marginal benefit 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 by using additional resources to enable more robust, quantitative investment analysis.

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, many investments 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 (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.

ES.5 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 decrease or remove any barriers 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. Although many groups attempt to provide information of various types (e.g., planning guidance, cost estimates), the organizations we spoke with (particularly small businesses) were interested in more information comparing types of products.

Furthermore, evaluating the effectiveness and efficiency of potential cyber security solutions is complex and costly. In many instances, 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.

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. 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.

ES.6 CONCLUSIONS

This report presents a conceptual approach to describing the components of a cyber security investment decision and the trade-offs between differing investment and implementation strategies; further, it provides 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.

1. Introduction

Little is known about how organizations evaluate their cyber security investments, where organizations obtain information relevant to such investments, and how they assess the benefits and costs of such investments. Economic theory suggests that an organization should evaluate cyber security investments using the same fundamental tools for evaluating any business investment. Private benefits would be weighed against investment costs, and the organization would then engage in increasingly stringent security activities until the marginal cost of an investment equals the marginal benefit from that investment.[1]

This optimal level of cyber security investment depends on factors related to the efficiency of the investment and its marginal cost, as well as the security returns from the investment and its marginal benefit. These factors are generally related to organizational and performance characteristics of the organization, such as its existing information technology (IT) characteristics, the compatibility of available cyber security technologies with current technologies, the security needs of the products and services the company 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, 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 decisions. Rarely does an organization undertake a sophisticated or even semisophisticated financial analysis (i.e., benefit-cost or rate-of-return analysis) prior to investing or deciding on the investment level needed. In fact, organizations simply react to a breach or compromise (hereafter referred to as a “breach”) and give the appearance of addressing the existing problem.

Such real-world practices lead 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 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 needed to make informed investment decisions. The second barrier is the externalities and public-goods nature of cyber security knowledge that

---

[1]This is a conceptual approach and represents a simplification of the necessary steps needed to determine the optimal course of action; however, most organizations implicitly use such a decision process every time they consider what investments (including those directed towards cyber security) they should make or request, even if they do not explicitly think about their actions and strategies in this way.

follows from cyber security investments. The first barrier could lead an organization to under- or overinvest in cyber security, and the second barrier leads to underinvestment.

Because of a lack of reliable, cost-effective information, most organizations do not have the historical information needed to make informed investment decisions based on the likelihood of future attacks.[2] Further, extreme cyber security events have a low probability of occurrence.[3] As a result, it is difficult, timely, and costly for an organization to assess the probability of a breach occurring, much less the related impacts (costs). These impacts include, but are certainly not limited to, potential downtime and remediation costs because of a breach and the overall reputational cost to the organization. Additionally, organizations lack the necessary information to assess cyber security technologies that are in-house or available from vendors and the implementation/maintenance costs of these technologies.

Relevant and applicable knowledge of the probability of being attacked and costs of a breach are scarce goods. Consortia and trade associations established by public and private organizations encourage information sharing; however, the lack of economic incentives to participate and share (i.e., free-rider problems) has limited their success.[4] As a result, private organizations with incomplete information may not be able to correctly calculate private benefits. 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.[5] 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.

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 (indirect) benefits in excess of private (direct) benefits. That is, an organization will not appropriate all of the benefits it receives from a cyber security investment; thus, from a social perspective, it is likely to underinvest in cyber security. From an economic perspective, it can be said that cyber security investments lead to cyber security–related information (data or simply experience and understanding) 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).

[2]Many organizations, particularly small businesses, may not have encountered a significant attack or a breach at all. Thus, such organizations (and all organizations to some degree) base decisions only on the attacks and breaches they have observed, and the appropriate responses based on this information. As such, decisions are based on incomplete information.

[3]After such events occur, they may actually have a higher probability of occurrence, especially when no easy remediation of the vulnerabilities and avoidance of the threats are possible.

[4]This relevant and applicable knowledge is, in part, codified but is 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.

[5]See Neumann (2004) for discussion of the need for more long-term planning for computer system and security development.

As an example, if an organization invests $1 in cyber security capital or labor, this will lead to several levels of benefits, only a small portion of which are directly realized by the organization. First, the organization will realize a reduced probability of a breach occurring, and this is a direct benefit to the organization.[6] The organization can roughly calculate the cost for it to repair any damage from a breach, such as recreating files or resetting passwords and then compare those benefits to the $1 cost (though the indirect costs are much harder to quantify; thus, there could be an underestimation of benefits). Second, society—other organizations and individuals—will realize a reduced probability of a breach occurring and thus avoid some costs associated with protecting themselves against breaches. These avoided costs, or social benefits, are not fully realized by the organization (they are realized to some degree in the sense that the organization's reputation could improve); thus, these secondary benefits do not fully enter into the organization's calculations for relating costs to benefits.

1.1 OUTLINE OF REPORT

This report summarizes our findings about cyber security investment strategies based on a series of extensive interviews with U.S. organizations from six composite industry groups, in addition to less-intrusive interviews with home users. Section 2 presents an overview of cyber security attacks and vulnerability estimates. Appendix A contains additional details on categories of attacks and cyber security technologies.

Section 3 provides an overview of cyber security investment and implementation strategies based on informal interviews and a review of the literature. The applicability of traditional corporate methodology (such as rate of return and benefit cost-analysis) is discussed as well as implementation strategies (such as proactive versus reactive).

Section 4 presents findings from RTI International's (RTI's) formal interviews and data collection. Descriptive statistics are presented by industry groups and indices were developed for implementation strategies and information sources.

Qualitative findings by industry are discussed in Section 5. Industry sectors include financial services, health care providers, manufacturing firms, universities, and small businesses. In addition, issues related to home users are discussed.

Finally, Section 6 presents conclusions and recommendations. The section summarizes the key drives and information sources influencing cyber security, discusses the public-goods nature of cyber security, and investigates government's potential role in enhancing cyber security.

---

[6] It must be noted that this result assumes that highly skilled labor is employed and that optimal decisions are made. Charette (1991) discusses assumed improvement based on cyber security investment that does not in fact result.

2. Review of Existing Statistics

The decision-making process for cyber security investments is based on the ongoing conflict between hackers and security administrators, involving a variety of motivations, goals, and security tools and procedures.[7] For organizations and individuals to determine the amount to spend on computer security, they need to be able to compute the vulnerability of their networks and the costs/losses associated with potential attacks; however, currently no methodology for such predictions has been widely accepted or implemented. 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). However, as Schechter notes, the necessary data for such analysis is not readily available and a standard methodology has not been identified.

Several metrics have been proposed in the literature to calculate and manage security costs in general. Annual loss expected, in which the expected rate of loss is multiplied by the value of the loss, is the most commonly used technique; however, Soo Hoo (2000) suggests 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. A further discussion of how available data, such as vulnerability reports (or the possibility that vulnerabilities exist that have not been reported), could be used in calculations of current risk or future loss projections is provided in Section 2.2.4; research in this area is extremely active and constantly expanding.

Although accurate data necessary for robust analyses are currently not available, two main sources 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:

- **Costs associated with past attacks.** Public and private organizations and collaborative groups administer surveys and/or use survey information from others to develop estimates of the likely costs of specific attacks or develop annual aggregates. Experts agree that none of these sources are comprehensive because of the changing nature of software that results in the development of new vulnerabilities, as well as the differences in metrics to measure the cost and the tendency of organizations to underreport or not report problems at all.
- **Attack and vulnerability statistics.** Public and private organizations exist that compile attack and vulnerability statistics and/or disseminate information about current and past vulnerabilities. These groups do not try to estimate the impacts of cyber attacks, rather, they aid researchers and organizations seeking to prevent

[7]See Appendix A for an overview of common types of cyber attacks and solutions.

problems and find solutions to future problems. Further, many attacks are not reported, and, as such, the available data should be viewed as an underestimate.

Section 2.1 describes some of the most well-known and widely used sources for these two categories.

2.1 CYBER VULNERABILITY AND ATTACK ESTIMATES

Numerous organizations compile vulnerability databases and patch information, and track the number of reported incidents. Many private organizations, such as the security firm Counterpane, provide 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. Table 7 lists publicly available data sources.

Table 7. Publicly Available Data Sources

Data Source	Type of Data Available	Limitations	Usefulness
SANS Institute/ NIST CSRC	Training, best practices, attack trends	No detailed information	Birds' eye, non-technical view of potential problems; good resources for activities
CERT/U.S. CERT/NIST ICAT vulnerability database/ security focus	Databases of vulnerabilities identifying the software versions that are susceptible, including information on the method of attack, ways of detecting the attack, and ways to prevent the attack	Incomplete information (based on voluntary reporting)	Potentially useful for calculations based on numbers of attacks; useful for seeing trends
Vendors	Databases of known attacks to their software, including the method of attack and how to patch their software and, in some cases, provide a solution to the impacts	Specific to one or a group of products	Very specific information on how to fix products

The National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC) maintains the ICAT Vulnerability Database,[8] a searchable index of vulnerabilities sorted using the common vulnerabilities and exposures list (CVE).[9] Through the ICAT system, users are linked to numerous publicly available vulnerability databases and sites describing patches (i.e., solutions to software problems).

Furthermore, 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

[8] See http://icat.nist.gov.

[9] The CVE database is maintained by MITRE Corporation and funded by the U.S. Department of Homeland Security. See http://cve.mitre.org.

Security Division (NCSD) at the Department of Homeland Security (DHS), both work, often together, toward this goal.[10]

The SANS Institute and the Center for Internet Security are membership-based organizations that charge fees for selected research, tools, and training services, but which also make available to the public general guides, white papers, and statistical counts and descriptions of recent attacks and current vulnerabilities. The SANS Institute maintains the Internet Storm Center, which promulgates information about urgent threats and maintains a list of the top 20 current vulnerabilities.

Many private companies, such as Symantec, issue reports, annually or biannually, on the state of Internet security and offer services for hire to organizations looking for more customized exercises. In its latest report dated March, 2005, Symantec reported an increase in the following types of vulnerabilities/threats:

- Web application vulnerabilities increased 82 percent over 18 months,
- malicious code threats to confidential information increased 50 percent over 18 months, and
- viruses and worms that affect Win32[11] applications increased by 64 percent over 6 months (Symantec, 2005).

Other organizations that distribute information on patches and general security include Internet Security Systems (ISS) X-Force, Security Focus, BugTrack.com, NT Bugtraq, and many more vendors and security organizations. Numerous private consortia, including industry Information Sharing and Analysis Centers (ISACs), track attacks and develop benchmarking tools and other resources for their members.

2.2 CYBER ATTACK COST ESTIMATES

Although experts agree that no accurate economic cost estimates are available on the impact of cyber security breaches, several sources are commonly cited in the media when approximate estimates are reported. The Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey, which is revised annually, has been conducted for the past 10 years by the CSI and FBI; the results, available to the public, describe the information provided by participants on the number of attacks on their networks, cost estimates by type of attack, and the security tools and policies in place. Computer Economics Inc. (CEI) and Mi2g are computer security consulting firms whose estimates on the impact of viruses, worms, and other attacks are routinely cited. Subscribers or clients only can usually access this data. Many other private consulting firms conduct surveys and estimate the costs of cyber security in the United States and/or to specific industries.

[10]Although CERT does collect extensive information, its disclosure policy has been the source of much debate. After being informed of or having identified a problem, it does not release the information publicly for approximately 45 days, during which CERT requests that the appropriate vendors fix the error (Jackson, 2001).

[11]Win32 threats relate to any system running on Microsoft Windows platforms.

While these data are extremely suspect because of definitional issues and the difficulty involved in estimating both tangible costs (e.g., labor to fix the problem and downtime) and intangible costs (e.g., reputational problems) of cyber attacks, they nevertheless provide the government and other organizations with information by which to determine their optimal level of investment in cyber security. Below we introduce the types of information provided by several studies and briefly discuss the validity of each.

2.2.1 CSI/FBI Survey

The 2005 CSI/FBI Computer Crime and Security Survey, the ninth of its kind, represents the responses of 700 IT professionals in U.S. corporations, financial institutions, government agencies (federal, state, and local), medical institutions, and universities. Participants were surveyed to determine the spending of their organizations on cyber security, the number of breaches and the associated financial losses incurred during the previous year, and the preventative activities undertaken. For 2005, the survey results suggest total financial losses of approximately $130.1 million, primarily from viruses (approximately $43 million) (Gordon et al., 2005). Figure 2 provides estimates over the past 8 years.

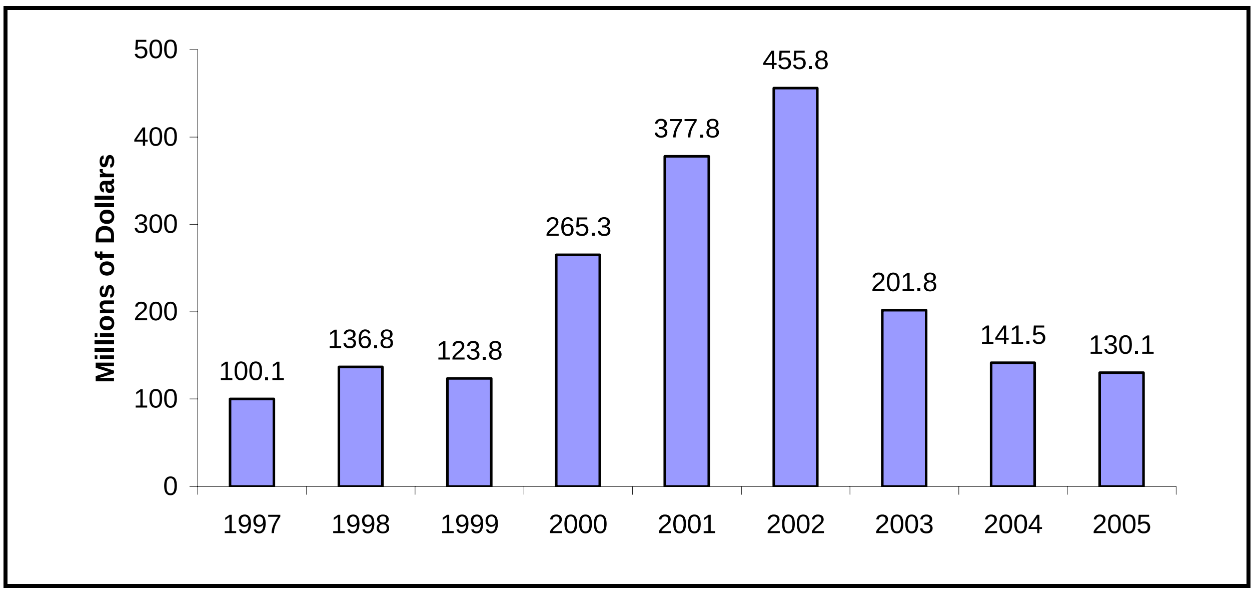

Figure 2: Cost of Computer Crime as Reported in the CSI/FBI Survey, 1997–2005

As the figure illustrates, the total cost of computer crime, including cyber security breaches, has decreased significantly since its peak in 2002. This decrease can be due to several factors. The total cost is based solely on the reporting of organizations that respond to the survey, a number that fluctuates each year. Further, information security has matured significantly over the past few years; therefore, organizations are better prepared for certain types of attacks, most importantly denial of service attacks and viruses.

The 2005 survey represents one of the best (but still unreliable) sources of information available; it is widely referenced by academics, government agencies, and companies providing security-related products or services. However, 20 percent of the responding organizations acknowledged that they do not report all computer intrusions to law enforcement because of the high cost of doing so.[12] Furthermore, cost-estimating procedures are not uniform; capturing labor resources allocated to security or employee productivity loss is not easy and is not always consistent.[13] Thus, the authors acknowledge that the information garnered by this survey, while accurate as reported by respondents, should not be considered a complete accounting of the costs of cyber security.

Still, the CSI/FBI survey results provide very informative qualitative information, in part because the survey represents the only longitudinal effort to study/gather such data. Specifically, the comparative difference between the losses perceived from types of breaches sheds light on the most important perceived attack threats. The following is a list of the eight breaches or attacks cited by CSI/FBI survey participants as the most costly to the United States:

1. Viruses: $42.8 million
2. Unauthorized access: $31.2 million
3. Theft of proprietary information: $30.9 million
4. Denial of service: $7.3 million
5. Insider net abuse: $6.9 million
6. Laptop theft: $4.1 million
7. Financial fraud: $2.6 million
8. Misuse of public Web application: $2.2 million

2.2.2 Computer Economics Inc.

For several years, CEI has published estimates on the financial costs of major virus attacks, both by attack and in the form of annual totals. The associated reports, as well as CEI's consulting service, are available for purchase. CEI's sources include data collected from its clients and other organizations around the world, a review of statistical reports and studies, surveys of security practices and spending, and the activity reports of security companies (Cisco Systems, 2002). According to the CRS, CEI has "developed benchmarks to measure the costs of recovery and cleanup after attacks, lost productivity, and lost revenue from downtime" (Cashell et al., 2004, p. 10). Table 8 provides CEI's worldwide estimates over a 7-year period, from 1997 to 2003.

---

[12] This perceived cost includes the cost of losing current customers or the lost potential revenue of future customers.

[13] According to the Congressional Research Service (CRS), the costs of public disclosure include financial market impacts, reputation effects, litigation and liability concerns, fear of job loss, and potentially more attacks (Cashell et al., 2004)

Table 8. CEI Worldwide Estimates of Virus Costs

Year	Economic Impact ($billion)
2003	13.5
2002	11.1
2001	13.2
2000	17.1
1999	12.1
1998	6.1
1997	3.3

CEI's estimates have been widely criticized because of the subjective nature of the calculations necessary to predict the impact of a worm or virus. According to experts, using available information, strict formulas cannot be used to predict the number of affected networks and hosts, the effects caused to each network or host (e.g., lost data, down time), or the work necessary to correct the problem. Furthermore, indirect costs such as company image and/or the release of confidential information are even more difficult to capture. In addition to the uncertainty in its methodology, CEI has a financial stake in cost estimates that attract media and customer attention; thus, an incentive exists for CEI to potentially inflate the figures.

CEI analyzed the annual cost to an e-business company of a malicious Internet attack, if the company did not have adequate security protection in place. Table 9 provides CEI's estimates of the annual economic impact of malicious attacks as presented in a 2002 white paper published by Cisco Systems.

Regardless, many organizations, including Cisco, CERT, and the *Wall Street Journal*, widely cite CEI's figures to describe the impact of worms and viruses, even though CEI representatives have acknowledged that their data are not scientifically calculated and require a good deal of guesswork (Lemos, 2002).

2.2.3 Mi2g

The British firm Mi2g has published numerous economic impact estimates for viruses and worms as well as the number of incidents reported monthly and annually by organizations around the world. In 2005, Mi2g estimated the total economic damage from all attacks around the world to be $506.8 million (Mi2g, 2005a). According to its Web site, the data Mi2g uses to calculate impact estimates originate from several main sources—relationships with executives in the banking, insurance, and re-insurance industries; monitoring of hacker bulletin boards and Web sites; relationships with "white hat" hackers; and relationships and anonymous communication with "black hat" hackers (Mi2g, 2005b).

Table 9. CEI Estimates of Annual Economic Impact of Malicious Attacks

Number of Nodes	Economic Impact on a Low-Intensity e-Business Company	Economic Impact on a Medium-Intensity e-Business Company	Economic Impact on a High-Intensity e-Business Company
25	$12,025	$31,085	$66,138
50	$25,200	$61,589	$131,040
100	$46,674	$109,684	$233,370
250	$108,375	$239,401	$509,363
500	$203,600	$430,614	$916,200
1,000	$402,225	$812,897	$1,729,568
2,000	$787,350	$1,554,229	$3,306,870
3,000	$1,244,970	$2,399,057	$5,104,377
5,000	$2,243,875	$4,113,023	$8,751,113
10,000	$4,065,416	$6,878,684	$14,635,498
20,000	$7,231,488	$11,555,918	$24,587,059
50,000	$16,789,500	$25,251,408	$53,726,400

Source: Cisco Systems, Inc. 2001. "The Return on Investment for Network Security." White paper. <http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.pdf>. San Jose: Cisco Systems.

Similar to CEI's estimates, Mi2g has come under significant criticism for greatly inflated estimates. The models used to calculate the estimates are proprietary; therefore, no one outside the company can evaluate the assumptions and methodologies. Furthermore, Mi2g has a financial stake in the cost estimates, just as CEI does.

The differences between CSI/FBI survey figures, CEI estimates, and Mi2g estimates are extremely great, causing concern about validity. Between 1997 and 2003, cyber-attack and crime estimates doubled according to CSI/FBI data, but CEI estimates show a quadrupling of costs, and Mi2g figures suggest a hundredfold increase during the same period. As such, many security professionals believe that these data are useless; alternately, others believe they provide valuable (albeit flawed) information that can aid decision making.

2.2.4 Other Cost Estimates

Several other well-known organizations have developed cost estimates of the impacts caused by security attacks. A report released by the United Kingdom's Department of Trade and Industry (DTI) and PricewaterhouseCoopers (PWC) in April 2004 provides the average costs of the largest security breach of the year, using data reported through a survey of companies. The results suggest that the total cost of the worst incident on average was £7,000 and £14,000 ($12,000 to $24,000) for all businesses, with large businesses experiencing damage between £65,000 and £190,000 ($112,000 to $328,000) (U.K. Department of Trade and Industry and PriceWaterhouseCoopers, 2004). DTI and PWC have completed a 2006 update to this survey, but at this time, the results have not yet been released.

Deloitte and Touche as well as Accenture have both conducted extensive surveys for the financial and business, technology, and security industries; Deloitte and Touche has made its reports publicly available, while Accenture charges a fee for access. Furthermore, other organizations such as TrendMicro, Jupiter Media Matrix, and Britain's IT Corporate Forum also have generated cost estimates used to describe the cost of inadequate cyber security.

2.2.5 Intangible Costs

In addition to tangible costs, such as additional labor and downtime (i.e., wasted labor), which are the basis of most of the estimates discussed above, intangible costs do and should factor into investment decisions. For example, if an organization has a widely known breach, it could lose current or future customers because of the effects on its reputation. It could also suffer legal repercussions and further reputation damage if confidential information is compromised, particularly now that various state privacy laws force organizations to release information on breaches when private information is lost.[14]

Several studies have looked at the impact of security breaches on stock market valuation in particular. Campbell et al. (2003) found limited evidence however of a long-run negative stock market reaction to public announcements of a security breach; when unauthorized access to confidential data occurred, they found the impact to be more significant. Hovav and D'Arcy (2003) found that over a 4 and a half year period, in general, the market did not react significantly when companies experienced a denial of service attack; however, they did conclude that attacks did have a more significant effect on "Internet specific" companies than other organizations. In the short run, Garg, Curtis, and Halper (2003) found that breaches resulted in an estimated 2.7 percent stock price drop in the first day and a 4.5 percent drop thereafter. Most recently, Smith and Smith (2006), using a set of 10 case studies from the literature, confirmed that short-run stock price changes do result from breaches. However, most research generally supports the conclusion that cyber security breaches have a negligible long-term impact.

[14]See the Privacy Rights Clearinghouse's catalog of all security breaches which have resulted in lost data since such state laws took effect, beginning with Choicepoint's breach in February 2005, at http://www.privacyrights.org/ar/ChronDataBreaches.htm. This site also maintains a list of current state privacy laws.

3. Cyber Security Investment and Implementation Strategies: A Conceptual Overview

This section presents an overview of the cyber security investment decision, with a particular focus on investment and implementation strategies used by organizations in various industries. This information is based on informal interviews with organizations and on the published literature. We make the distinction between analyses conducted as part of an *investment strategy* and analyses conducted as part of an *implementation strategy*. In this framework, management and/or IT staff work on the investment strategy largely through two main approaches—by setting a security budget (e.g., a certain percentage of the total IT budget) and/or by determining the level of security they want to achieve and maintain. IT staff typically are solely responsible for the implementation strategy, in which they determine the most efficient approach to meet the organization's security needs, whether through a more proactive or a more reactive approach. In smaller organizations, the distinction between the investment and implementation strategies 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.

Figure 3 presents an overview of an organization's cyber security decision process. It begins with determining an organizational cyber security investment strategy and prioritizing anticipated cyber security needs. These organizational-level decisions in turn guide the implementation strategy where specific security solutions are evaluated and compared.

Conceptually in the literature, the optimal cyber security *investment strategy* is discussed in terms of a net present value (NPV) or benefit-cost analysis. Using such techniques, 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. The NPV and benefit-cost analysis approaches are discussed further in Section 3.1.

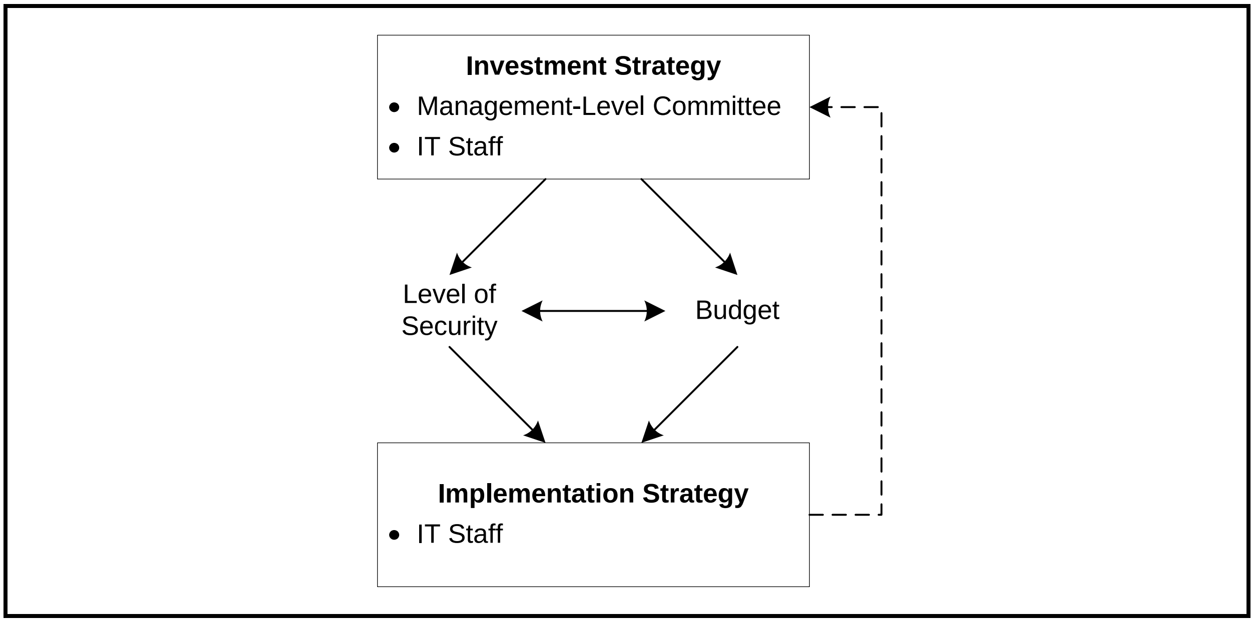

Figure 3: Cyber Security Investment and Implementation Strategy

However, organizations are quick to point out that the inputs to this type of quantitative analysis are difficult, costly, and, in many cases, impossible to obtain. As a result, when management staff are involved in cyber security decisions, they rely very heavily on qualitative assessments of their security needs, which are then compared to quantitative analyses of other (non-IT) needs and investment opportunities. Furthermore, during our informal interviews, organizations indicated that determining their cyber security strategy was driven by a range of internal and external factors, including regulations, client requirements, business requirements, and reputational concerns. These drivers are discussed in more detail in Section 4.

We have defined organizations' cyber security investment strategies in terms of two dimensions. One approach is to identify security *needs* and *priorities*, and referred to throughout this report as determining the "level of security." Essentially, this entails deciding on the optimal level of security and associated spending based on robust analysis. At this point in the strategic process, it may be difficult to explicitly quantify costs and benefits; thus, a qualitative assessment is made to determine which cyber security objectives/requirements are essential (and likely to be cost-effective) for the organization's operations.

A second approach is to determine the *level* or *share of resources* an organization should (or has available to) invest in cyber security. In this scenario, cyber security activities and purchases are determined by maximizing the use of a fixed amount of money from the organization's budget. This is a "second best" approach in that it may not explicitly identify cyber security needs and could result in either an underinvestment or an overinvestment in cyber security. However, these needs are implicitly weighed against competing needs and investment opportunities when the budget is determined.[15]

However, during our informal interviews, all participants indicated that they frequently incorporated a combination of targeted “level of security” and budget constraint requirements 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. Organizations cited that deciding the extent to which their cyber security strategies focused on preventive/proactive solutions versus reactive solutions was an important component of the implementation strategy.

Organizations with more proactive implementation strategies (e.g., more labor and software/hardware focused on preventing new types of breaches) indicated that this approach led to fewer breaches; however, organizations differed on the relative costs and benefits of more proactive versus more reactive strategies. In Section 3.2, we present a conceptual framework for considering the selection and implication of proactive versus reactive implementation strategies for either type of investment strategy introduced above.

3.1 CYBER SECURITY INVESTMENT STRATEGY

Determining the optimal level of cyber security investments or deciding how much to invest in cyber security is a complex decision that is made based on differing levels of information and on various business and regulatory requirements. In general, neither individuals nor organizations use quantitative methodologies to determine the optimal level of cyber security investments. Instead, organizations tend to use a more qualitative approach—identifying and prioritizing security needs based on regulations, customer needs, and specific network activities.

A business case including both preventive and recovery costs and changes could allow more accurate planning and accountability exercises; however, based on informal interviews with organizations and our review of the literature,[16] organizational network differences and the multitude of security products and services make the “business case” approach generally unsuitable in this situation. The preventive costs are a function of labor and capital spending, which can be easily calculated (once the proper metrics are defined), but the recovery costs are much more difficult to capture. Several major problems exist preventing such estimates from being readily available:

1. The future probability (prospective) of a cyber security breach is unknown. Differences in network topology and the dynamic nature of types of attacks and available solutions make any probability estimates inherently uncertain.

[15]Seventy-five percent of organizations have a structure budget process. While this does not imply that they are given a fixed budget, it does suggest that most decision makers must use some form of explicit or implicit metrics, either quantitative or qualitative, when receiving funding for cyber security.

[16]Many articles mention and evaluate the inadequacy of business case approaches to evaluating cyber security investments. CRS specifically discusses this dilemma in their report (Cashell et al., 2004).

2. The indirect and direct recovery costs (retrospective) of cyber security attacks is not known. No common metrics (and associated methodology) have been agreed upon to estimate or measure the cost of cyber security attacks; however, an estimate of the costs should be much more certain than for the prospective case (probabilities) above.

Organizations are reluctant to report cyber security breaches for, among other things, fear of public (customer) reactions. Instead of trying to perform a typical benefit-cost analysis, many organizations hire external auditors to determine their optimal level of security based on International Standards Organization (ISO) 17799 or NIST 800 series guidelines or customized recommendations. Other organizations use internal audit procedures. In some cases, metrics and methodologies used for physical security cost analysis are used for cyber security, but unlike a physical attack, "a cyber attack generally disables—rather than destroys—the target of attack" (Cashell et al., 2004, p. 30). Other commonly used methodologies include stock fluctuations, risk analysis techniques, and the following of competitors' policies and procedures.

Investments in cyber security are typically more difficult to evaluate than other decisions made by organizations because the costs and benefits cannot be easily observed or estimated. The costs of securing a network include

- hardware and software products, updates, and installations;
- effort spent by IT staff to test and implement security technologies, monitor the status of network security (including updating), and respond to any problems; and
- time involved in defining the policies and procedures to be used by IT staff as well as (more significantly and possibly importantly) those to which all staff must adhere.

The hardware and software purchases are the simplest to quantify, but the time spent by IT staff on security as opposed to other IT issues and the time spent by regular staff reading and following security policies cannot be captured easily. Cost can vary significantly by organization because of specifics of business operations and legacy systems.

The benefits are even more difficult to quantify. The desirable benefit is that the network and any data therein remain secure. Austin and Darby (2003) note that, particularly in an environment with high pressure to boost earnings, "when there is uncertainty about the level of uncertainty—that is, when it's unclear whether the loss-making event will happen with 0.01 percent probability or 0.001 percent probability—it becomes even harder to justify spending a lot of money to avoid the loss" (p. 123). A $1 million loss will only appear as a $100 loss in a financial calculation if it is predicted to have a 0.01 percent probability of occurrence; however, if that event does occur, the losses could be much larger than predicted because loss predictions could be similarly inaccurate.

IT managers are commonly asked to use some type of financial assessment techniques to justify their funding on security to company executives, even though they are known to be questionably accurate. In most instances, empirical analysis focuses on labor resources (as opposed to value of data or lost sales). For example, Gordon and Richardson (2004) conducted an interview with an Oracle representative who stated that when they were considering when to replace an intrusion prevention system (IPS), they analyzed how many alerts they were getting, how many people were needed to track down and resolve these alerts, and how many of the alerts were false positives. When compared with their tests of the new system, this helped them decide to immediately replace the system.

3.1.1 Corporate Investment Theory

Corporate finance theory has been researched extensively for the past 50 or 60 years; however, much of today's commonplace corporate investment strategy is based on ideas first proposed in the 1950s. Although cyber security investing introduces particular complexities that were not present 50 years ago, the theoretical framework is helpful to review as numerous other factors have caused finance models trouble in the past.

Prior to the late 1950s, organizations made capital and R&D investment decisions largely based on anecdotal evidence and real experiences, but, in 1958, Modigliani and Miller proposed using a more mathematical approach. The theories they proposed were based on the assumption that markets operate efficiently, so economic models could be used to determine the viability of all investment decisions. In a working paper chronicling the historical development of corporate investment decision making, Dempsey (1996) looks critically at the positive and negative aspects of qualitative versus quantitative decision-making practices.

The theory proposed by Modigliani and Miller lays the groundwork for modem neoclassical finance theory; in essence, it suggests that asset valuation models, which calculate an organization's value based on expected future net cash flows (including future investment decisions), should be used to determine how an organization should invest. If a positive net present value (NPV) is generated, the investment should be made. 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.

However, these types of analyses, which according to Dempsey are still very pervasive in most corporate decision-making processes today, can lead organizations away from investments that cannot be easily quantified and/or ignore personal experiences and other more qualitative factors that need to be considered (Hayes and Abernathy, 1980). Hodder and Riggs (1985) and Hodder (1986) suggest that these issues do not reflect the deficiency of the NPV method, but rather an inappropriate application of NPV (e.g., by using incomplete data); they suggest that NPV provides an invaluable tool to evaluate potential investments (Hodder and Riggs, 1985).

Corporate investment decisions today largely rely on NPV or return on investment (ROI) calculations; however, according to Hayes and Abernathy (1980), many companies in the United States have suffered by putting too much stock in such quantitative models. Many factors, such as increased staff skills, new product developments, increased security, and changes in stock valuation cannot be accurately (or closely) captured in models. Therefore, these factors are often left out of investment decisions, causing some to say that organizations are generally too conservative.

As with these factors, cyber security introduces an additional cost that is very difficult to capture in a model. And as with other factors, such as staff experience, improvements in product quality, and physical security, organizations have largely relied on qualitative evaluations when comparing such investments with decisions that can be more easily quantified.

3.1.2 Cyber Security Risk Assessment and Investment Optimization Research

Over the past 10 years, academics, vendors, government organizations, and various consortia have conducted extensive research to determine the best methodology by which cyber security investments should be made. The Workshop on Economics and Information Security, held annually since 2002, has generated significant debate and publicity surrounding how economic methodology might be able to help refine investment decisions on security, [17] and numerous government bodies have produced metrics by which security can be measured and evaluated.

NIST published a document in July 2003 intended to assist organizations in measuring three key factors—the implementation of security policies, the effectiveness and efficiency of the security policies and mechanisms in place, and the impact of any security "events." The document, entitled "Security Metrics Guide for Information Technology Systems," provided instructions on how to determine what metrics would be most useful to an organization and the best ways in which to use them. Although it does not identify the specific metrics that should be used (the authors suggest that this should differ depending on organizational priorities and activities), it does provide a set of questionnaires that could be very useful in assessing the current infrastructure—hardware, software, administrative practices, user policies, and past occurrences, for example.

Other organizations such as ISO, the SANS Institute, and the numerous CERT centers have published similar materials. Although these are useful, they do not help organizations directly quantify their relative state of security and develop an investment plan based on costs (prevention, attack, and repair costs) and benefits (efficiency of the network and lack of costs).

Gordon and Loeb (2006) have written extensively on their effort to analyze investment decisions and the costs associated with cyber security intrusions using economic tools. In their recent book aimed at cyber security administrators and financial analysts, they provide an overview of a variety of qualitative and quantitative techniques available for assessing the relative value of cyber security investments. However, the more rigorous analyses they

[17] The Web site for the next Workshop on the Economics of Information Security, to be held in Cambridge in June 2006, is http://www.cl.cam.ac.uk/users/twm29/WEIS06/. Links to past workshops can be found via this Web site.

present require the estimation of the probability and the impact of specific types of breaches, values that differ significantly among organizations and are very difficult to calculate.

In an article in *Network Computing*, Gordon and Richardson (2004) state that one-third of respondents to a survey the authors administered indicated that they were using NPV as a major factor in determining the level of IT security investment. Although the authors praise organizations using an NPV instead of a simple ROI calculation, they point out that externalities may cause an NPV decision to be flawed because it does not consider the effects that inadequate security may have on other organizations. Varian (2000) further suggests that computer security in practice is “so poor” because the risk involved is widely shared. Anderson (2001) suggests similar problems, introducing economics ideas such as network externalities, asymmetric information, moral hazard, adverse selection, liability dumping, and the tragedy of the commons.

Soo Hoo and Schechter introduced novel ideas on how to best determine the appropriate level of security for an organization. In a working paper for the Consortium for Research on Information Security and Policy (CRISP), Soo Hoo (2000) discusses an econometric approach in which uncertainty and flexible modeling tools can be used with available data to determine appropriate security levels. In his doctoral dissertation, Schechter (2004) introduces the idea that a market could be created for vulnerabilities (in which they could be traded), and that the current price for a threat on a product could help consumers determine how secure it is.

Campbell et al. (2003) presented another analysis that looked at the effect of security scares on share prices. They suggest that a significant negative market reaction occurs following IT security breaches involving unauthorized access to confidential data. However, they did not find a significant change in the market if the breach did not involve confidential information.

Gartner, an IT consulting firm, has produced numerous reports on the use and value of quantitative and qualitative analysis of cyber security investment decisions. A November 2005 Gartner report, “Use a Cost-Benefit Approach to Justify Security Expenditures” (Scholtz et al., 2005, p. 1), recommends that “security teams should avoid basing information security expenditure requests primarily on undefendable financial ROI projections, and instead exploit clearly articulated, balanced value propositions.”

Finally, both Congress and the President have taken notice of the need for improved cyber security investing and the need for a better incentive structure to motivate optimal investing. The Subcommittee on Cyber Security, Science, and Research and Development of the U.S. House of Representatives released a report in December 2004 that noted that the Y2K problem and the electrical blackout in the Northeast could be used to help identify the cost of a cyber attack. Furthermore, the committee report suggested that the insurance and auditing industries would be best able to use past experience in developing cost methodologies for cyber security.

Further, back in 2002, the White House spent considerable effort working to encourage the insurance industry to offer cyber security insurance as a way to incentivize them to improve their cyber security measures. The idea goes that companies would be required by insurance companies to achieve a certain level of cyber security before they could get insurance, which they would need either to comply with regulations or to ascertain business deals or individual customer relationship (Krebs, 2002).

According to the 2005 CSI/FBI Survey, 25 percent of companies had reported that they acquired external cyber security insurance (Gordon et al., 2005). Although there is a wealth of information advocating the potential value of cyber insurance (Gordon, Loeb, and Sohail, 2003), many companies are not interested currently. The extensive audits required by security companies and the relatively expensive prices have been deterrents (D'Aqostino, 2003). Further, Ogut, Nirup, and Raghunathan (2005) point out that the interdependency of cyber risk results in an inefficient insurance market and that the imposition of legal penalties and increased information sharing were both needed in addition to any insurance to help achieve optimal investments.

Throughout the research conducted to date, many analysis techniques have been proposed however, no commonly held methodologies have been identified. However, all experts seem to agree that more information sharing could significantly improve security methodologies and consequently allow IT spending to be more in line with individual and organizational needs.[18]

3.2 CYBER SECURITY IMPLEMENTATION STRATEGY

Based on our interviews, RTI found that organizations tend to characterize their cyber security implementation strategies differently, but the broad concept of a proactive strategy versus a reactive strategy resonates well in discussions of strategic planning. That fact 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 benefit-cost analyses based on history, experience, and market pressures to determine the optimal level of effort that should be devoted to testing and debugging.

[18]Gordon, Loeb, and Lucyshyn (2003) discuss the problems underlying the current lack of adequate information sharing. They further introduce a model that empirically supports the assertion that more information sharing would lead to improved security. Additionally, Gal-Or and Ghose (2005) find that increased information sharing has a greater positive effect on security for larger firms and in more competitive industries.

Similarly, the optimal strategy mix of proactive versus reactive cyber security strategies for an organization depends on many factors. 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 cost. However, trying to anticipate and block all forms of rapidly evolving viruses can be expensive and perhaps only marginally effective. RTI 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 to be able to quickly implement patches when new viruses are identified.

However, 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. 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.

Further, it is not clear that proactive/reactive strategies are exclusive. While it is clear that those who are not proactive in their risk management will use purely reactive strategies, those who are completely proactive may also decide to adopt completely reactive strategies. The issue may not concern proactive and reactive strategies as much the reasoning that went into a decision. Further, being proactive could mean applying best practices or adding more security measures; the terms “proactive” and “reactive” are thus not prescriptive.

From our analysis it is obvious, however, that the adoption of a proactive versus reactive strategy has an impact on IT expenditures as well as on overall business operations. Table 10 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 reduce 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:

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

Table 10. Comparison between IT and Non-IT Costs and Benefits Based on Security Strategy

Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor)	• Cost: User inconvenience
	• Benefit: Decreased need for reactive labor	• Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation
	• Benefit: Decreased investments in proactive (risky) solutions	• Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

As shown in Figure 4, 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. The so-called iso-security curves that are farther from the origin represent higher levels of cyber security. In Figure 4, we also depict what is referred to as a budget line reflecting the monetary 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.

3.2.1 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

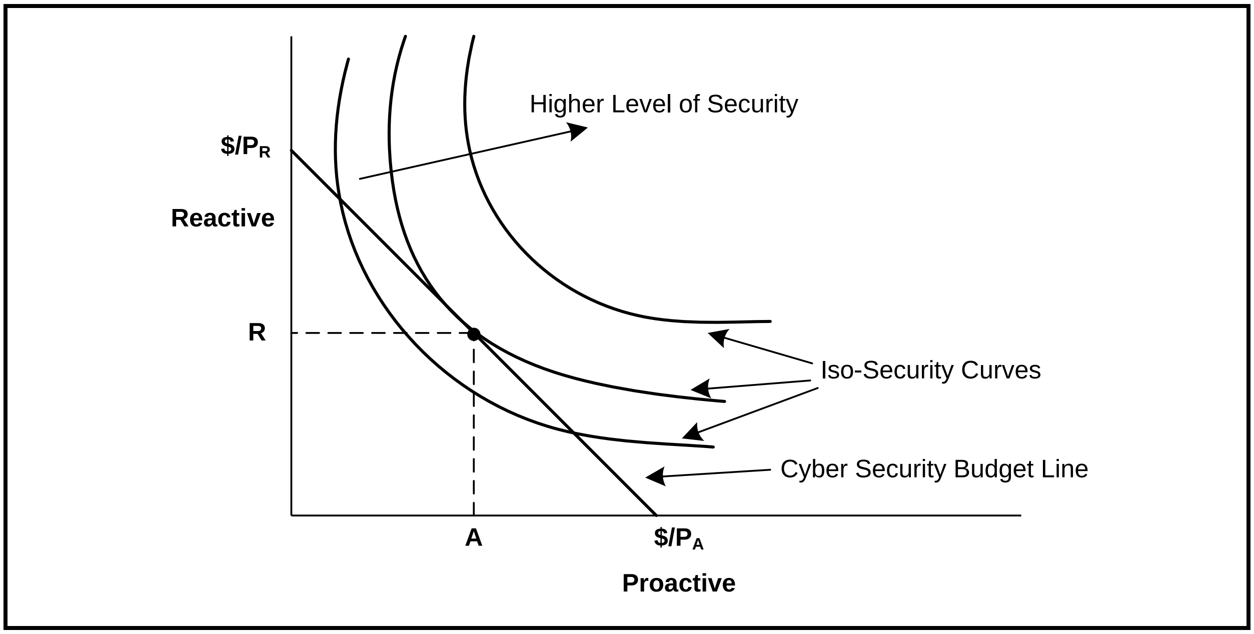

Figure 4: Firm Selection of Optimal Proactive / Reactive Mix to Maximize Security Subject to Budget Constraint

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 predetermined level of resources. This approach is similar to a production function economic model where output (security) is maximized subject to a budget constraint.

As illustrated in Figure 4, 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.

3.2.2 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 to determine the level of security or due diligence appropriate for the organization and then have the 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 4, the cost-minimizing approach is for an organization to identify the level of security that it determines is most appropriate for the organization, represented by the appropriate "iso-security curve."[19] 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 the 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 determined level of security 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.

3.2.3 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; society therefore 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 if not all of the costs are borne by the investing organization—if 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 reduces cost externalities. In addition, proactive investments are more information-intensive and are affected more by free-ridership issues, where the reduced sharing of information increases the cost of evaluating and adopting proactive strategies.

3.2.4 Cost Externalities

Figure 5 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 for a given budget constraint, when all cost externalities through the network are considered, a lower level of social cyber security is actually being achieved. As shown in Figure 5, the maximum level of security is now achieved by decreasing the mixture of reactive cyber security solutions.

[19] We use the term "iso-security curves" to describe different levels of security that organization set out to achieve. This terminology is based on economic production theory which describes "isoquants" in a similar way to show how two inputs can be combined in different ways to produce a given level of output.

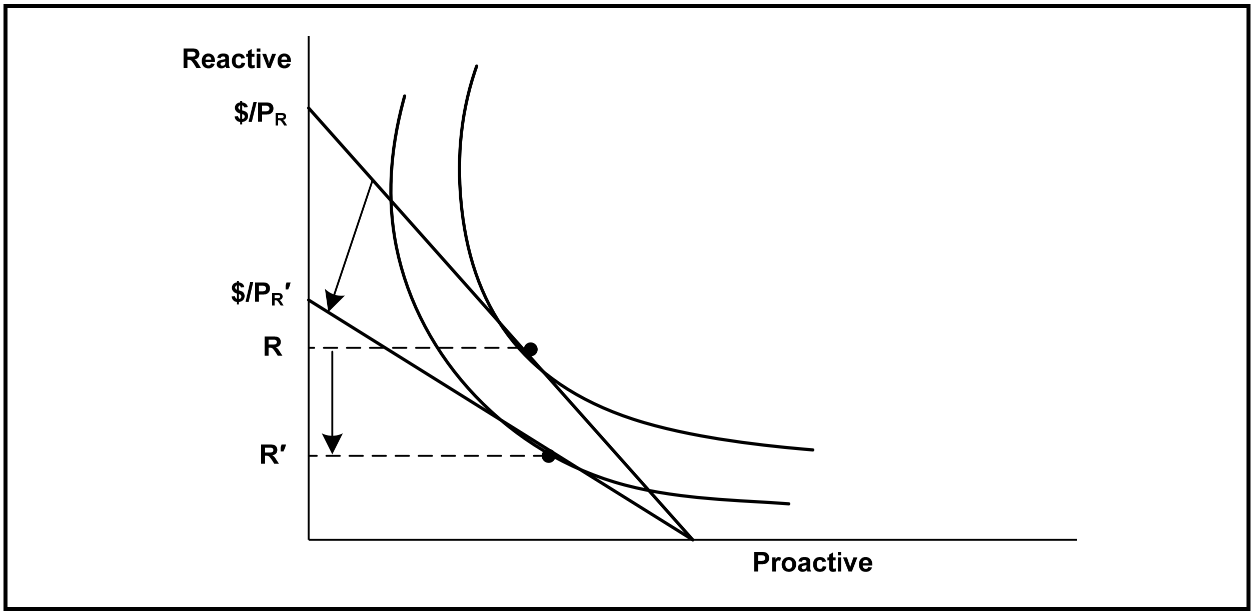

Figure 5: Internalizing Externalities Increases Price of Reactive Options ($P_R < P_R'$)

With regard to the cost-minimization strategy, incorporating cost externalities 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.

3.2.5 Information Sharing

Cost-minimizing and output-maximizing analyses can also be used to portray the impact of information sharing on the selection of proactive versus reactive strategies. As shown in Figure 6 in aggregate, information sharing decreases the price, P_A, of proactive solutions.[20] 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 the iso-security curve. The overall result is a higher level of cyber security achievable given the budget constraint.

[20]This statement implies that if more information sharing occurs by all organizations, on average, then the cost of being more proactive will likely decrease.

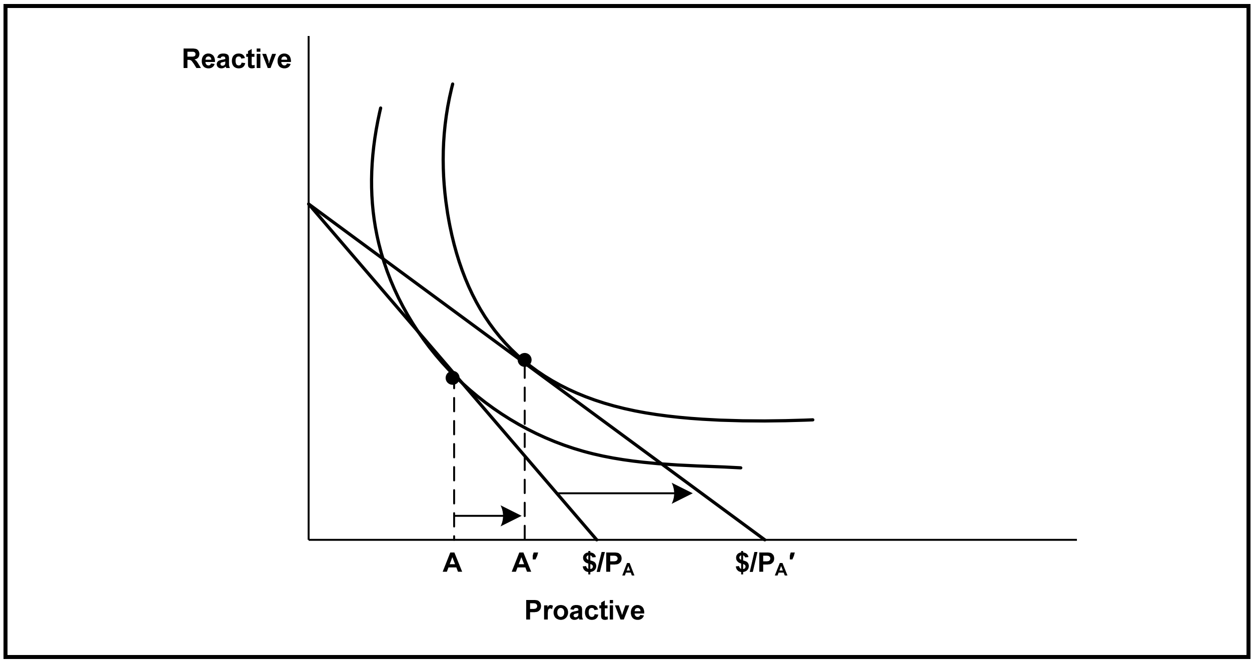

Figure 6: Information Sharing Decreases Cost of Proactive Options ($P_A > P_A'$)

The cost-minimization strategy is also affected by this shift. With the level of desired security held constant,[21] 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.

[21]Obviously, investing in a more proactive strategy versus a more reactive strategy imposes different risks on an organization. We assume that these risks are incorporated in the prices of the strategies.

4. The Cyber Security Investment Decision Process: Findings from Interviews

RTI undertook this study to investigate the decision-making process related to investments in cyber security. Investments, as we have defined them for this study, include both hardware and software purchases as well as decisions related to IT staff procedures and user policies. Essentially, RTI sought to analyze how organizations determine how much they should spend on cyber security and the solutions they select in terms of the models introduced in the previous section.

We conducted both informal discussions and formal interviews with cyber security experts and members of five main industry groups (as well as a few additional key representatives from other industries) to help us identify the links between organizational strategies and operating procedures and the relative importance of external and internal motivating factors and resources.

In this section, we first describe our informal and formal data collection activities. Subsequently, we describe the qualitative and quantitative information gathered from these interviews, as well as some of the barriers to the most efficient cyber security policies.

4.1 DATA COLLECTION

RTI interviewed organizations from five industry segments and categorized organizations by size within each industry group. All organizations with fewer than 50 employees were considered small businesses, and targeted interviews were conducted accordingly. Table 11 lists the five major industry groups and indicates the number of organizations in each industry group that participated in our interviews. RTI believes that this sample of 36 organizations is a representative sample of the major U.S. industries affected by cyber security breaches.

Having identified these representative groups, RTI developed separate interview guides for each industry group, with the overarching goal of investigating Internet stakeholders' investment decision-making processes. These interview guides, developed and pretested in March and April 2005, were intentionally designed to be very broad in scope. There were two reasons for this design strategy. First, as noted in Section 2, the extant literature is at best sparse in terms of quantitative information about IT investment decisions and

Table 11. RTI's Interview Participants by Industry

Industry	Participants
Financial services	6
Health care providers	6
Manufacturing	6
Small businesses	6
Universities	7
Other	5
Total	36

strategies. Thus, any systematic investigation of the investment decisions and strategies of organizations would be, by definition, exploratory in nature. Second, using multiple broad-based survey instruments would potentially identify critical issues that are specific to one industry but not to all.

Each interview guide included a common set of questions on budgeting, information tracking, and information utilization. However, changes were made in the interview guides to account for differences between industries. Also, additional industry-specific questions were asked related to regulatory effects; interaction with industry associations; and the impacts of customers, clients, and suppliers (as appropriate) on the organizations.

Between May and September 2005, organizations were contacted and interviewed. In some cases, organizations were only willing to talk at a very general level about cyber security and their organizations' strategy and use of internal and external information. We held eight such high-level (informal) discussions with organizations. In addition, 36 organizations participated in more formal interviews.

RTI believed that the most effective way to collect information that would be most useful in understanding the decision-making process of organizations was to go through a set a questions with each participant in real time as part of an extensive formal telephone interview. By collecting information in this manner, RTI could ensure not only that each respondent was interpreting our questions appropriately, but also that each respondent had the opportunity to elaborate on the responses and delve into important issues that were not explicitly discussed in the instrument.

We analyzed both the qualitative and quantitative information garnered from these interviews to identify themes among organizations within each industry group and across industry groups related to organizational strategies; the use of various internal and external information resources; and the effect of cyber security motivators.

4.2 EMPIRICAL RESULTS

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 are planning to begin restructuring 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 specific cyber security procedures and policies 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, and thus can potentially offer relevant views that could benefit the whole organization. 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 those administrative units are becoming more involved in decision making, most often related to user policies.

During the investment strategy phase, decision making generally occurs within one of two organizational areas: the IT department or a business strategy ("management") department or committee (e.g., risk management).[22] Table 12 shows, by industry group, where cyber security priorities and budgets are determined within the organizations with which we spoke. Financial service and health care organizations are more likely to have investment strategies set by management-level groups, whereas manufacturing and universities are more likely to determine their investments strategies within IT departments.

Table 12. Source of Cyber Security Investment Strategy

Industry Group	Within IT Department	Within Management Department
Financial services	33.3%	66.7%
Health care providers	33.3%	66.7%
Manufacturing	83.3%	16.7%
Universities	60.0%	40.0%
Other	85.7%	14.3%
Total	60.0%	40.0%

Note: Small businesses are not included because investment decisions are intermingled.

[22]During interviews, all participants indicated that investments decisions involved IT staff and most had some upper-management involvement; however, all organizations were able to define their organization as making investment decisions in one framework more than the other.

As shown in Table 13, organizations with investment strategies determined within the IT department rely relatively more on internal information (tracking of compromise events in particular) than do organizations with investment strategies made within management groups. Though not statistically significant, this was a particularly surprising result. Both types of organizations also rely on external sources of information.

Table 13. Percentage of Organizations Internally Tracking Security Events, by Source of Cyber Security Investment Strategy

	Source of Cyber Security Investment Strategy	
Security Compromise	**Within IT Department**	**Within Management Department**
Denial of service	82.4%	66.7%
Unauthorized access to information	76.5%	83.3%
Viruses, worms, or spyware	88.2%	75.0%
Severe spam floods	88.2%	75.0%
Theft of proprietary information	88.2%	75.0%
Hardware theft	88.2%	83.3%
Abuse of the wireless network	64.7%	66.7%
Web site defacement	76.5%	66.7%
Misuse of public Web applications	76.5%	66.7%
Financial fraud	76.5%	75.0%
Eavesdropping on communications	64.7%	58.3%
Unauthorized modification of permissions	82.4%	66.7%

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

Further, organizations with investment strategies made within a management department or group are on average much more likely to track event/incident metrics, such as the number of IT staff hours needed to respond to an event and the number of user hours impacted by an event.

Schematically, Figure 7 provides a diagram of the flow of decision making and the information sources that act as inputs to this process. This figure is an expansion of Figure 3, which introduced the relationship between the formulation of an organization's investment strategy and its implementation strategy. Cyber security investment decisions are influenced by both internal and external sources of information, with a recent trend toward more diversity in the internal sources of information.

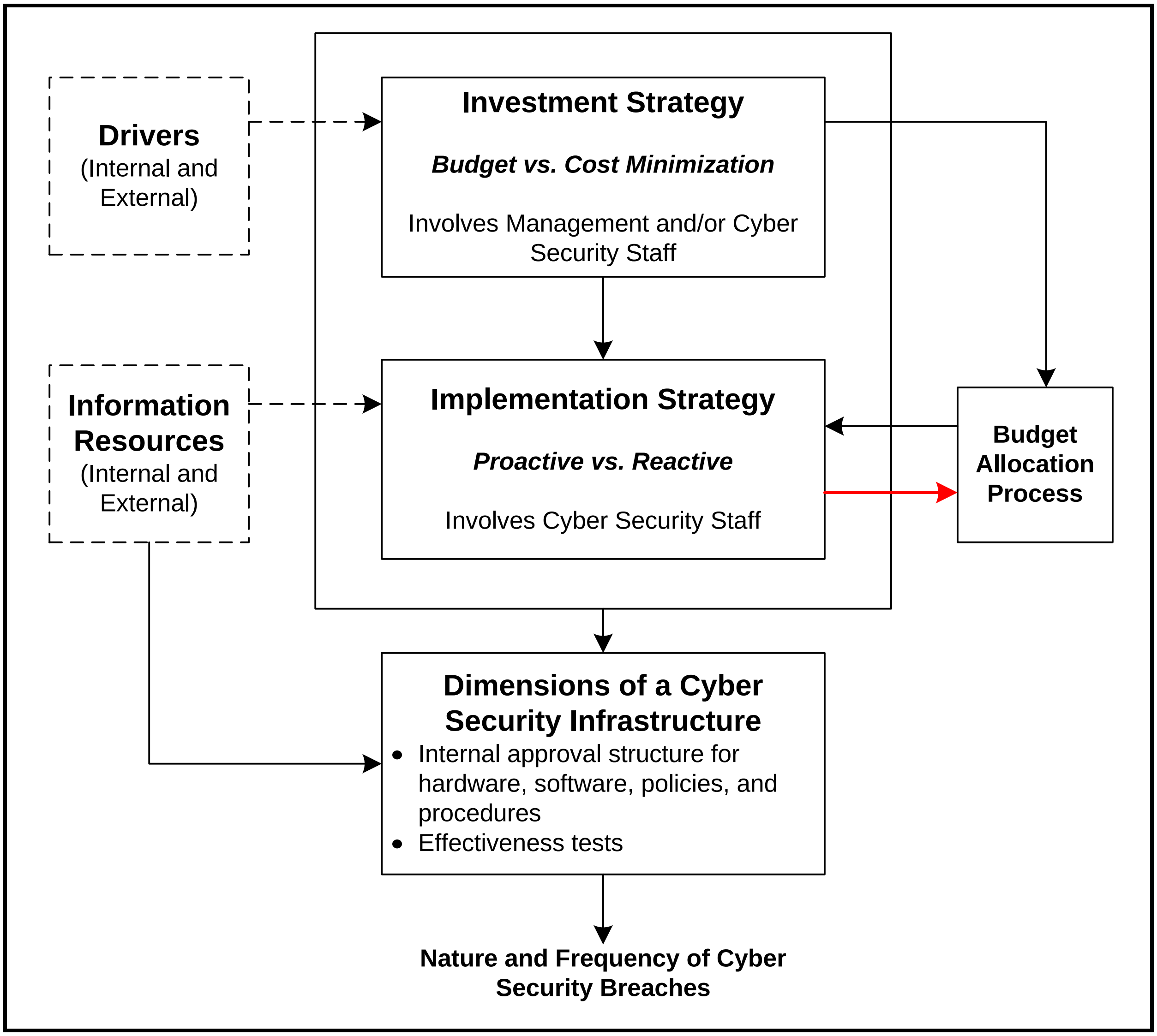

Figure 7: Diagram of Cyber Security Investment Decisions Inputs and Outputs

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, ISO, and American National Standards Institute [ANSI] publications and vendor recommendations) are used to inform specific capital investment decisions and how policies and procedures are made. Subsequently, organizations make 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.

Table 14 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.

Table 14. 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 ▪ 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

As noted in Section 3, in most organizations with which we spoke, the budgeting process was based significantly on the previous year's budget and, to a lesser extent, regulations or forecasts of anticipated needs. Only a few organizations determined the budget for cyber security through a cost-minimization strategy, including a rigorous benefit-cost analysis and/or a risk management framework. Thus, in Figure 7, the budgeting process is separate 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 red arrow between implementation strategy and budget allocation process.

The remainder of this report explains the importance of information resources in helping organizations find the most cost-effective implementation strategy. In this section, we follow the flow introduced in Figure 7. We discuss the investment strategy, the implementation strategy, and some of the specific intricacies of selecting and evaluating cyber security solutions.

4.2.1 The Investment Strategy

Using the information resources described above, organizations must develop a process for cyber security spending; this includes the budgeting process, capital labor resource allocation, and subsequently, evaluation of spending. An analysis has allowed us to better understand these processes and to identify several barriers to adoption of the most effective cyber security investment processes.

Cyber Security Budgets

More than 75 percent of organizations in our study indicated that they have a structured budget process. However, the specific amount spent on cyber security varies across and within industry groups. On average, the organizations with which we spoke spent 5.7 percent of their IT budget on cyber security; however, based on our limited sample, there are differences among industries. Table 15 provides a comparison of cyber security spending by industry group for the organizations with which we spoke.[23]

Table 15. Average Cyber Security Budgets as a Percentage of IT Budgets, by Industry Grouping

Industry	Average Cyber Security Budget (as a percentage of IT budget)
Financial services	3.3%
Health care providers	6.2%
Manufacturing	4.2%
Small businesses	10.1%
Universities	3.3%
Other	8.5%
Total	5.7%

Of the organizations with which we spoke, small businesses tend to spend a larger share of their IT budget on cyber security compared to other groups, while the financial services industry and universities tend to spend a smaller share. However, these differences across industries are likely to be reflective of economies of scale and the relative size of total IT budgets, as opposed to differences in the concerns with cyber security issues.

Whereas cyber security budgets are influenced by the factors discussed above, the cyber security officers we spoke with indicated that there was not always a direct link. Although our data indicated that slightly more than one-third of organizations view the previous year's budget as the primary determinant of their current cyber security budget, participants did imply that additional resources would be provided for perceived new threats. However, the main determinant of organizational budget change seemed to be the

[23]Several organizations with cyber security budgets that did not come from their IT budget had to estimate how the cyber security budget compared to the organizations' IT budget. Further, small businesses obviously have very different IT budgets than other organizations that participated in our interviews. If we weight the responses based on company revenue (as a very rough weighting factor), we get an average of ~5.0 percent, which, as we would expect, is a slightly lower percent than the total represented in Table 4-5.

effect of regulations. As a result, in many cases, IT departments were left to do the best they could to prepare for cyber security threats with essentially an exogenous security budget.

Cyber Security Expenditure Allocation

During our interviews, most organizations indicated that they perform ROI, IRR, NPV, or benefit-cost calculations as part of their cyber security investment decisions. However, when asked for specific examples of calculations conducted and how they generated the information, few were able to provide any details. One example cited was by a university that implemented an automated password reset system, allowing them to reduce their telephone calls to staff by 50 percent; for this they could compare the cost of the system to the labor savings. However, in no instance did any company provide us with an example in which they quantified the probability of an event or the associated expected damage. Two organizations indicated that such analysis was being conducted internally, but were unwilling to elaborate.

Cyber Security Drivers

In many instances, the target level of security and/or the resulting share of the IT budget directed toward cyber security were dictated by external factors. For example, organizations indicated that regulations were by far the most significant factor affecting their investment strategy; on average, organizations indicated that over 30 percent of their cyber security activities and investments were motivated by regulations. Similarly, the second greatest external influence was “client requirements”; many clients, VISA being the most often mentioned, require certain cyber security hardware, software, policies, and procedures and, in some cases, even insist on routine audits to engage in business relationships. Table 16 provides additional information on the relative importance of drivers motivating the level of security maintained by organizations that participated in RTI’s interviews.

4.2.2 The Implementation Strategy

Both internal and external information was found to be particularly important for IT staff involved in making implementation decisions. We offer for consideration that a regulation or a client requirement may influence an organization to take a more proactive approach to cyber security by forcing an organization to adopt more restrictive user policies and/or purchasing more state-of-the-art hardware and software technologies. Alternately, 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 16. Cyber Security Drivers: Interview Results

Categories	Average Percentage across Companies
Client driven	16.2%
Regulation driven	30.1%
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%
Network history/IT staff knowledge	18.9%
Externally managed/determined	5.0%
Other	1.7%

In this section, we focus on the use of information resources utilized by organizations when determining the appropriate proactive/reactive implementation strategy. This is a key to understanding the possible ways to influence how organizations make decisions. Furthermore, these same resources are used when organizations make decisions related to the specific dimensions of their cyber security infrastructure, including the hardware and software they will purchase, and the user policies and the IT staff procedures they will employ.

Table 17 shows the overall rankings of reliance on information resources for hardware/software decisions and IT security procedures and activities. These numbers represent the percentage of organizations ranking each resource either a 1, 2, or 3 based on their relative importance.

Internal Information

We found a heavy reliance on internal information resources for analysis. This includes the use of internal auditing; the relative involvement of the IT staff and in-house executives to determine the level of cyber security; and the tracking of internal IT information, such as the number of breaches, IT staff hours needed to resolve any problems, and user time required to reach a solution.

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 level of the staff.

Table 17. Information Resources: Interview Results

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%

Although our interviews did not attempt to discern the relative level of competence of the IT staff, it is important to note that we did hear numerous experts and industry members who indicated that the skill level of IT staff varies widely. Some staff failed to continue with self-education as technology changed, while others were 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' certification program, accredited by the American National Standards Institute 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 as well as to estimate costs and probabilities of attack.

Most organizations with which we spoke were tracking at least some internal information, but many were not using it as part of their investment decision process. Organized into five breach categories, Table 18 shows how industries compare in their tracking of information.

Financial organizations tend to track the most information on breaches. As a group, the manufacturing organizations with which we spoke tracked the least amount of information, with small businesses not far behind.

Additionally, we gathered information on whether organizations track the resource utilization of their cyber security staff. Table 19 summarizes this information. While most organizations (approximately 60 percent) are collecting data related to their response to cyber security problems, fewer than half are collecting data on total resource (labor) use related to cyber security. In our discussions, several organizations indicated that they did not see the need for tracking the hours of their cyber security staff time. In a couple of instances, the reason given was that the organization was so small that they did not think it made sense to collect such data, while others indicated that they trusted the judgment of their staff. Two other organizations commented that they could not get approval to collect such resource allocation data.

When we asked whether organizations were tracking the time spent by users on selecting passwords and receiving any cyber security training, executive-level involvement in security decisions, or business unit managers' participation, most organizations indicated that they do not track such information. Fewer than 20 percent collect information on users, while only 5 percent track executive-level or business unit managers' time.

Comparison of Information Resources

RTI also asked organizations about the external information resources they used. As presented in Table 20, external information includes both publicly and privately generated data and other information. Many organizations relied on vendor and customer suggestions to help them decide on the types of hardware and software to have in place. They similarly used NIST best practices[24] and relied on both external audits and outside consultants when making decisions on user policies and cyber security procedures.

[24]NIST has published more than 50 documents on a variety of security hardware, software, policies, and procedures. See http://csrc.nist.gov/publications/nistpubs/index.html.

Table 18. Percentage of Respondents That Track at Least One Type of Breach within Each Category

Type of Breach	Industries	Track Number of Incidents?	Track IT Staff Hours?	Track User Hours?
Denial of Service	Financial	83%	83%	33%
	Health Care	67%	17%	0%
	Manufacturing	50%	17%	0%
	University	100%	29%	14%
	Small Business	50%	17%	17%
	Other	100%	100%	100%
Viruses, Worms, Spyware, and Spam	Financial	100%	100%	67%
	Health Care	100%	83%	17%
	Manufacturing	67%	17%	17%
	University	100%	29%	14%
	Small Business	100%	50%	33%
	Other	100%	100%	100%
Unauthorized Access/ Network Abuse	Financial	100%	83%	50%
	Health Care	100%	33%	0%
	Manufacturing	67%	17%	0%
	University	100%	29%	14%
	Small Business	100%	50%	33%
	Other	100%	100%	100%
Web Abuse	Financial	100%	67%	33%
	Health Care	67%	33%	17%
	Manufacturing	50%	17%	17%
	University	100%	29%	14%
	Small Business	50%	17%	17%
	Other	100%	100%	100%
Theft/Fraud	Financial	100%	83%	50%
	Health Care	100%	50%	17%
	Manufacturing	50%	17%	17%
	University	100%	29%	14%
	Small Business	83%	17%	17%
	Other	100%	100%	100%

Table 19. Tracking of Cyber Security Resource Allocation

Resource	Percentage of Organizations
Responding to IT Security Problems	58.3%
IT Security Staff Education	44.4%
Monitoring IT Security Status	36.1%
Testing IT Security Measures	33.3%
Installing New IT Security Measures	33.3%
Gathering Information	25.0%
Other	11.1%

Despite significant variation, on average, organizations indicated that they depend more on internal than external resources. The relative importance of informational resources did vary across industry groupings and within industry groupings. Based on discussions, RTI coded the top three resources that each organization stated they used in determining their cyber security procedures and activities. The three most frequently mentioned resources were scored as a 1 and the rest were scored as a 0.[25] As such, a higher value implies that an organization valued a certain resource more highly than others.

In Table 20, we present a comparison of information resources used by industries to inform their implementation strategy. Although organizations relied on different internal and external resources, this grouping allows for comparison among industries and provides some interesting results.

Universities are the least reliant on external information sources, reflecting in-house expertise as well as the diversity of their needs. The health care industry is the most dependent on external public sources of information, and small businesses are the most reliant on external private (vendors) sources of information.

[25]Hypothetically, if a respondent told us that NIST best practices documents (public external), customer suggestions or requirements (private external), and internal audits (internal) were the three most important resources, then that respondent's organization would have three informational indices with the following values: external public resources = 1, external private resources = 1, and internal resources = 1. If instead the respondent told us that vulnerability estimates from U.S. CERT (public external), NIST best practices (public external), and ISO guidelines (public external) were the three most important resources, then that respondent's organization would have three information indices with the following values: external public resources = 3, external private resources = 0, and internal resources = 0.

Table 20. Types of Information Resources Used by Each Industry Group

Industries	Hardware and Software	Procedures	Policies
Financial			
Internal	1.50	1.17	1.17
External Public	0.33	1.33	1.17
External Private	1.17	0.50	0.67
Health Care			
Internal	0.83	0.83	0.50
External Public	1.08	1.83	2.00
External Private	1.08	0.33	0.50
Manufacturing			
Internal	0.80	0.83	1.00
External Public	0.60	1.50	1.17
External Private	1.60	0.67	0.83
University			
Internal	2.08	2.00	1.67
External Public	0.58	0.50	1.00
External Private	0.33	0.50	0.33
Small Business			
Internal	0.83	1.33	1.17
External Public	0.33	0.33	0.67
External Private	1.83	1.33	1.17
Other			
Internal	1.90	1.80	1.80
External Public	0.30	0.80	0.60
External Private	0.80	0.40	0.60
Total			
Internal	1.32	1.31	1.20
External Public	0.54	1.06	1.11
External Private	1.13	0.63	0.69

4.2.3 Dimensions of a Cyber Security Infrastructure: Summary Results

Although often not explicitly discussed, organizations determine what specific hardware and software they will purchase and what user policies and IT security procedures they will employ based on:

- The organizational investment strategy: is the Chief Information Security Officer (CISO) or Director of IT Security given a budget or does he work with a management committee to determine a target level of security and then spend the amount necessary to achieve that level? Most organizations have both factors at play.
- The organizational implementation strategy: does the organization take a more proactive versus reactive approach to security? Most organizations will have a blend of approaches.

Based on these factors, cyber security staff members are allocated resources (e.g., capital and labor) toward a variety of activities. While in most instances, organizations that we interviewed allowed cyber security staff to determine the best use of their time, responses varied on the type of security technologies purchased and on what vendors were selected. Interviews showed that:

- Approximately 75 percent the security products in use come from large, well-established companies (as opposed to smaller companies).
- Approximately 67 percent of these products are “well-tested” products (as opposed to being more innovative).[26]

Our interviews also included a discussion of what factors influenced organizations’ decisions to adopt a specific security technology or to invest in the adoption of a new user policy or procedural change. The following factors were most often cited:

- Likelihood to improve security: this factor was, not surprisingly, most often cited. The ability of the product or policy/procedure change to improve security, either to meet internal security objectives or to satisfy a government regulation, was very important to almost all respondents.
- Ability to improve productivity: the second most important factor, cited by more than one-half of the interview participants, was the ability of the procedure to improve the productivity of users and/or cyber security staff.
- Widespread industry use: approximately one-fourth of the organizations with which we spoke cited the use of the technology or policy/procedure by organizations in a similar market segment as a motivating factor.

At the bottom of the list of factors influencing organizations’ decisions on when to adopt a new technology, policy, or procedure was cost—including both the immediate and the projected total cost of ownership, or TCO. Small businesses were the exception and did consider TCO a relatively important factor.

[26]These figures are based strictly on participants in this study and should not be interpreted as statistically significant.

In addition to a discussion of the decision of *whether* to adopt a new technology, policy, or procedure, we asked interview participants how they decided from which company to purchase a new technology solution. Not surprisingly, most respondents noted that the effectiveness of the product was the most important consideration. However, most of the other factors cited received about equal weight. These factors included:

- cost (immediate and TCO),
- degree of homogeneity with the existing infrastructure,
- general interoperability of the product, and
- reputation of the vendor or service provider.

It is important to point out that cost was important when organizations were deciding from what company to purchase the security product.

When asked what usually caused organizations not to adopt technologies or make policy or procedural changes in the past, more than half of the respondents indicated each of the following factors (listed in order of the number of times each was mentioned, the first being the most frequent):

- disruption of user or cyber security staff productivity,
- expense of the product (immediate and TCO),
- too complicated/time consuming,
- lack of a perceived threat (difficulty convincing management), and
- anticipated staff resistance.

Of particular interest is that disruption of user and/or cyber security staff productivity was cited most often by organizations as a reason why a certain technology, policy, or procedure was not adopted. This indicates a major barrier to the adoption of adequate security processes. Although organizations did not cite cost as an important factor when deciding to adopt a new technology, policy, or procedure, it was mentioned as a reason why investments have not been made in the past.

Finally, organizations assess the effectiveness of their cyber security investments differently. Many rely on internal and external audits, and vulnerability tests to assess compliance with regulations and customer requirements, as well as whether the investments satisfy internal security goals.

4.3 IMPLICATIONS

In this section, we provide additional analysis of the relationships between organizations' strategies, information resource use, and cyber security investments. We build on the conceptual frameworks underlying the investment decisions introduced in Section 3.

Organizations and companies have different cyber security strategies. Based on our interviews, we found that strategies generally range 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 and a reactive strategy implies that an organization responds to known threats with typically established technologies so that security compromises can be addressed efficiently and effectively. RTI also gleaned from the interview process that fewer security compromises resulted when an organization or company adopted 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, RTI 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 with both proactive and reactive elements. Based on each respondent's characterization, RTI then asked about the extent to which the organization can adhere to its defined proactive strategy, where a response of 10 was "always" and a response of 1 was "never." RTI also asked, using the same response code, about the extent to which the organization always adhered to its defined reactive strategy. From these responses, a proactive index was constructed for each organization. It was constructed as the numerical difference between the extent to which the respondent stated that the organization always adhered to a proactive strategy minus the extent to which the respondent stated that the organization always adhered to a reactive strategy.[27]

Figure 8 shows the distribution of proactive indices for the 36 responding organizations. The industry for each is color coded.

Figure 8 shows that the majority of organizations (29 of 36) in the RTI sample characterize themselves as relatively proactive (proactive index >0). Only 7 of 36 characterize themselves as relatively reactive (proactive index <0). The figure also shows that in most cases there is not a dominant pattern by industry; most of the organizations do not cluster by industry according to the value of their proactive index.

However, by averaging the proactive index by industry group, some trends do appear. Table 21 shows the mean proactive index for each of the six broad industry groups. Universities and small businesses are relatively much less proactive than health care organizations, financial services firms, or manufacturing businesses. Our "other" category includes organizations that adhere to a less divergent proactive versus reactive cyber security strategy.

[27]Theoretically, if an organization always adhered to a proactive strategy (score of 10) and never adhered to a reactive strategy (score of 1), RTI calculated a proactive index of 9 (10–1). Similarly, if an organization always adhered to a reactive strategy and never adhered to a proactive strategy, the proactive index was –9 (1–10). This proactive index is subjective in two ways. First, its construction is based on RTI's interpretation of the respondent's characterization of the organization's cyber security investment strategy. Second, assuming consistency in this characterization, the index still reflects only one respondent's opinion; certainly, it is possible for other knowledgeable individuals within the organization to have differing opinions depending on the scope of their expertise in the cyber security area. Given these caveats, and given the extant literature on cyber security investments and strategies, RTI believes that its effort in this regard is the first to attempt to quantify this important dimension.

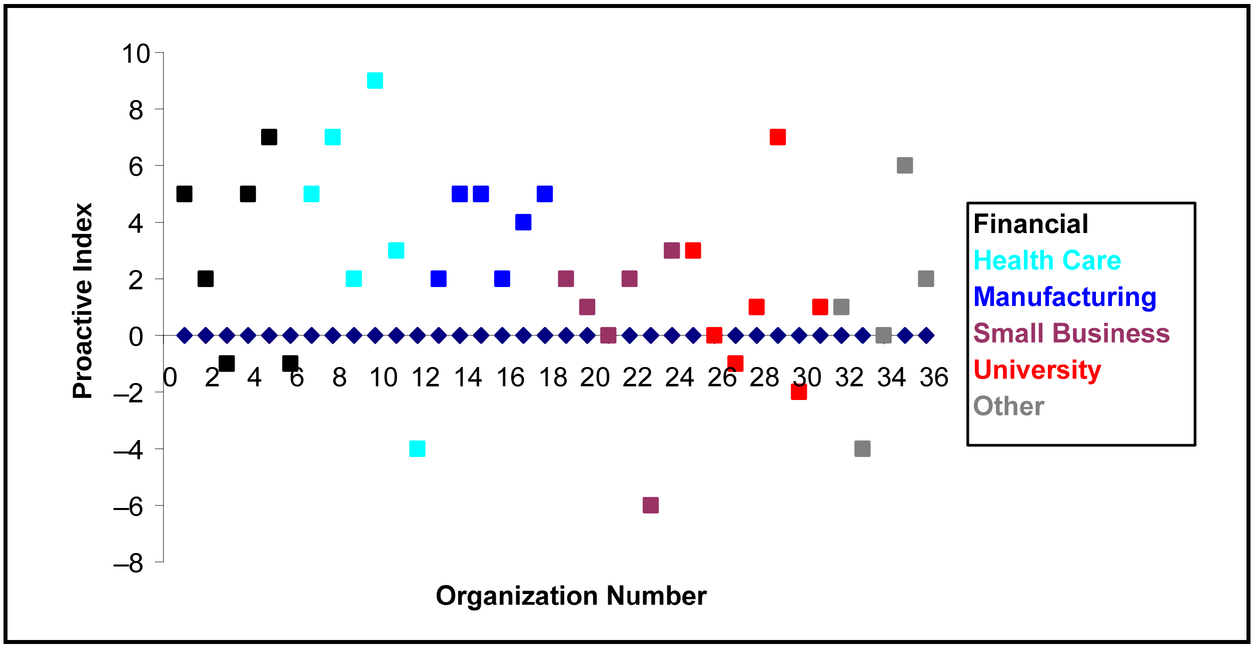

Figure 8: Distribution of Interview Responses Proactive vs. Reactive Strategy, by Industry Grouping

Table 21. Mean Proactive Index, by Industry Grouping

Industry Groups	Mean Proactive
Financial	2.833
Health Care	3.400
Manufacturing	3.833
Small Business	0.333
University	0.200
Other	0.750

4.3.1 Links between Information Sources and Proactive Strategies

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 cost-effectively obtain reliable information on the effectiveness of policies, procedures, or new technologies influences its overall cyber security strategy.

Based on this insight, it follows that industries that have more external public information available may pursue more proactive cyber security strategies. As a result, we looked for a correlation between an organization's proactive/reactive cyber security strategy and its reliance on external public information in its decision-making process.[28]

Table 22 shows the mean importance of external public resources for cyber security by industry group.[29] Health care organizations, financial service companies, and manufacturing companies rely relatively heavily on external public resources. In contrast, universities and small businesses rely relatively little on external public resources.

Table 22. Mean External Public Resources, by Industry Grouping

Industry Groups	Mean External Public
Financial	1.333
Health Care	1.600
Manufacturing	1.500
Small Business	0.333
University	0.600
Other	1.000

Focusing on the use of external public resources and anticipating some of the policy conclusions of this report, Figure 9 shows the relationship between the proactive index and the use of external public information for cyber security resources. Organizations in the health care industry, companies in the manufacturing industry, and small businesses are the most extreme examples that illustrate the trade-off between an organization's proactive cyber security strategy and its reliance on external public information resources.

In general, there is a discernable relationship between the use of public information resources and the more proactive the industry group. While causation cannot be determined from Figure 9, our interview-based information suggests that causation does flow from informational sources to strategy adoption.

[28]As introduced in Section 4.2, RTI complied information on three types of information resources—internal, private external, and public external—and created an informational index for each.

[29]A higher value implies that external public resources are utilized more by a certain industry group relative to other types of resources (external private and internal).

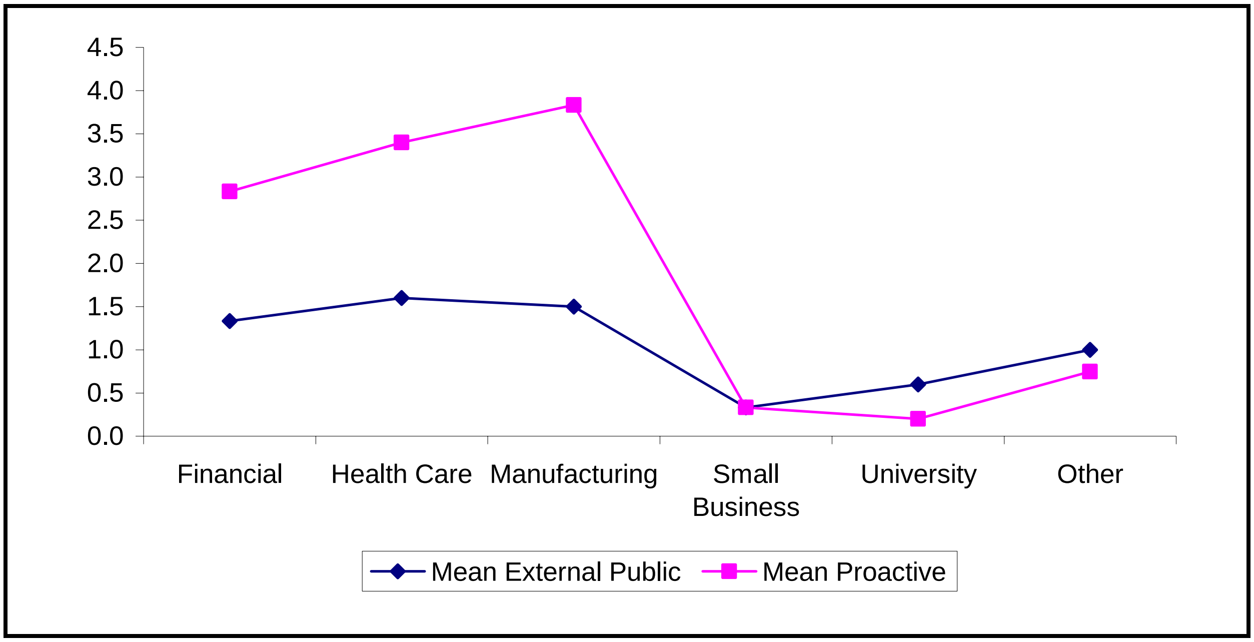

Figure 9: Mean Proactive Index vs. Mean External Public Resources by Industry Grouping (correlation coefficient = 0.93)

As the schematic in Figure 7 suggests, an organization's cyber security implementation strategy also influences dimensions of its investment decisions and the frequency of security breaches (about which no organization or company would discuss in any quantitative manner). Organizations were willing, however, as part of the interview process, to suggest the level of their cyber security investments as a percentage of their overall IT budget, as previously discussed. Some organizations were more precise about that percentage, while others were only willing to share that information in terms of a wide range of percentage values. RTI was able to obtain an estimate of the percentage of the IT budget spent on cyber security.[30]

Figure 10 shows that there is a relationship between an industry group's spending on cyber security as a percentage of its IT budget and its proactive nature. Figure 10 shows that there is not a one-to-one relationship across the industry groups, but, for example, small businesses, which are the least proactive, allocated the largest percentage of their budget to cyber security.

The following matrix in Table 23 generalizes from the above findings in terms of a conceptual relationship between an organization's or company's proactive versus reactive cyber security strategy and its use of resources for cyber security.

[30]When reported as a range, the midpoint of the range was used in the analysis.

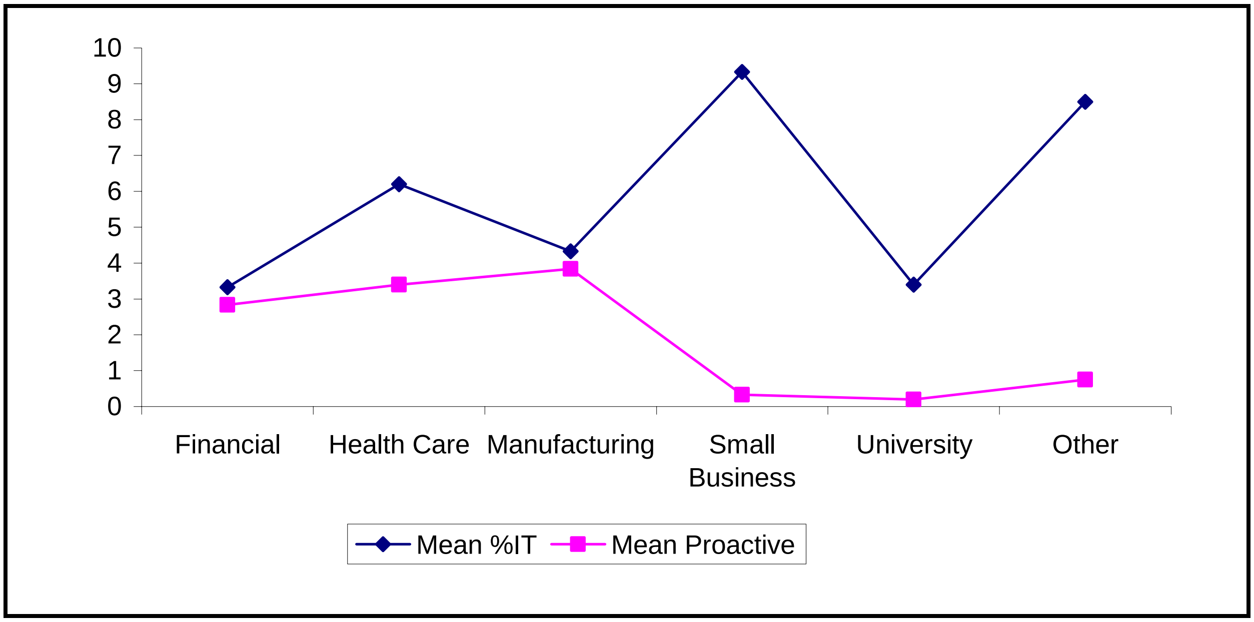

Figure 10: Mean Proactive Index vs. Mean Investment in Cyber Security, by Industry Grouping (correlation coefficient = –0.42)

Table 23. 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

This generalization, along with the interview information RTI assembled, suggested that fewer IT resources are needed to achieve a secure IT environment in a proactive organization.

This suggests that from a policy perspective, public-sector effort to decrease cyber security breaches could focus on increasing the availability and usability of public domain information.[31]

[31]However, RTI also learned from its interviews that within an organization, the optimal cyber security strategy is not totally proactive. Thus, in order to investigate a more statistically based conclusion, we used regression techniques to analyze our data.

4.3.2 Factors Influencing the Share of IT Security Expenditures

Based on interviewees' comments to the survey questions, discussions with numerous experts on cyber security trends and problems, and a review of the extant literature, we offer three hypotheses that we tested by regressional analysis:

- *Hypothesis 1: Organizations with structured cyber security budgeting processes will invest a larger share of their IT budget on cyber security.*
- *Hypothesis 2: Organizations that do not share security information will invest a larger share of their IT budget on cyber security.*
- *Hypothesis 3: Organizations that are more labor intensive in the creation of value will invest a larger share of their IT budget on cyber security.*

The first hypothesis reflects our understanding of what takes place during a structured or systematic annual cyber security budgeting process. Such activities, within the organizations that we interviewed, are more deliberate and incorporate reasoned forecasts of security needs. These organizations are also relatively more proactive and anticipatory in their strategy toward cyber security.

Our second hypothesis comes directly from the theoretical analysis of Gordon, Loeb, and Lucyshyn (2003), and postulates that companies that do not share information are less efficient and have spent a larger share of their IT budget on security. This follows logically from the theoretical and empirical literature related to efficiency gains in R&D from participation in research joint ventures (Hagedoorn, Link, and Vonortas, 2000; Hall, Link, and Scott, 2003).

Our final hypothesis reflects our understanding that many cyber security compromises originate internally from employees and that more labor-intensive industries (e.g., financial services, health care, and universities) may be impacted more heavily by cyber security problems. Thus, an organization with value being generated in a more labor-intensive way will require greater cyber security investments.

Thus, our statistical model is:

$$CSPct = f\,(Budget, ROIIRR, Emp, Coop, \mathbf{X})$$

where *CSPct* is the percent of an organization's IT budget spent on cyber security in 2005; *Budget* is a binary variable equaling 1 if the organization has a structured process for deciding its annual cyber security budget and 0 if otherwise; *ROIIRR* is a binary variable equaling 1 if the organization employs either a quantitative return on investment (ROI) or internal rate of return (IRR) analysis when deciding to adopt new cyber security technology and 0 if otherwise; *Emp* equals the ratio of employment to sales; *Coop* is a binary variable equaling 1 if the organizations shares tracked security compromise information with other organizations and 0 if otherwise; and **X** is a vector of other organizational characteristics.

Based on Hypothesis 1, our expectation is that the estimated coefficients on *Budget* and *ROIIRR* will be positive. Based on Hypothesis 2, our expectation is that the estimated coefficient on *Coop* will be negative. And based on Hypothesis 3, our expectation is that the estimated coefficient on *Emp* also will be positive. Fixed industry effects are accounted for in **X**.

The estimated results from the model in equation (1) are in Table 24. Each of our hypotheses is confirmed, to some degree, by the data. The results from the parsimonious specification in column (1) of the table confirm each of the three hypotheses. Organizations with structured cyber security budgeting processes allocate a greater percentage of their IT budget to cyber security; the estimate coefficients on *Budget* and *ROIIRR* are positive and significant. Organizations that are more labor intensive also allocate a greater percentage of their IT budget to cyber security; the estimated coefficient on *Emp* is positive and significant. Finally, organizations that cooperate and share security information allocated less of their IT budget to cyber security; the estimated coefficient on *Coop* is negative and significant. The overall fit of this specification is also significant.

Table 24. Estimated Regression Results (t-statistics in parentheses)

Variable	(1)	(2)	(3)
Budget	5.43 (2.69)*	5.83 (3.03)*	6.64 (3.01)*
ROIIRR	3.09 (1.82)***	3.08 (1.92)***	2.79 (1.40)
Emp	0.29 (3.02)*	0.295 (3.26)*	0.24 (1.60)****
Coop	–4.31 (–2.08)**	–2.75 (–1.30)	–2.79 (–1.25)
Service	—	–3.56 (–2.04)**	—
Financial	—	—	–3.26 (–0.98)
Health care	—	—	–4.84 (–1.30)
Manufacturing	—	—	–2.46 (–0.74)
Small businesses	—	—	1.39 (0.30)
Universities	—	—	–4.35 (–1.10)
Intercept	–1.84 (–0.85)	–0.73 (–0.35)	–0.24 (–0.07)
R^2	0.426	0.503	0.540
F-level	5.18*	5.45*	3.00*

Note: * denotes significance at the .01 level; ** at the .05 level; *** at the .10 level; and **** at the .15 level. "Other organizations" are captured in the intercept term in the specification in column (3).

The specification in column (2) includes a binary variable, *Service*, equal to 1 if the organization is a service organization (financial services, health care, and universities) and 0 if otherwise. Its estimated coefficient is significant; service organizations allocate a smaller percentage of their IT budget to cyber security than do organizations in other industry groups. However, *Service* is collinear with *Coop* and hence the significance of *Coop* declines although it remains negative as hypothesized.[32]

Finally, the specification in column (3) controls for the industry group of each organization. Little is gained from this more complete specification, and taken as a group, the industry variables are insignificant.

[32]When *Coop* is deleted from this specification, the level of significance of the coefficient on *Service* increases.

Although not hypothesized, we did include one additional binary variable in each of the three specifications that was equal to 1 if the organization's investment strategy is determined by the IT department, and 0 if determined by a management group. In no case was the estimated coefficient on this variable significant.

Implications of the Regression Findings

Caution should be exercised when generalizing from the results in Table 24 not only because of the small sample size but also because the statistical analysis is the first of its kind and there are no other studies for comparison purposes. That said, the findings do have organizational and public policy implications, which are explored in this section.

We assume that the actual level of investment in cyber security among the 36 organizations in this study is the optimal level given the information available to the organization; that is, these organizations are allocating resources rationally given their information set.[33] Our results therefore suggest, holding constant the level of compromises, that greater security information sharing among organizations, either individually or through consortia arrangements, increases internal security investment efficiency.[34]

We also consistently found a positive relationship between the structure of the investment decision-making process and the relative level of investment. This raises several issues, such as whether these investment decisions are made at the most appropriate organizational level (i.e., IT versus management), and if so, are traditional quantitative evaluation metrics the most appropriate metrics to use for cyber security? On the one hand, many organizations today estimate such metrics to enable rough cost-benefit analyses; on the other hand, benchmarking information and standard guidelines could make that process more efficient.

While organizations view many dimensions of their cyber security process as proprietary, and, as we found in this study, are reluctant to share investment information, even though companies that did not share information tended to allocate more of their IT budget to cyber security (possibly implying inefficiency). A broad-based confidential expenditure survey by a public-sector or nonprofit organization—perhaps patterned after the CSI/FBI Computer Crime and Security Survey—could serve the public good by allowing benchmarking and analyses aimed at investigating the socially optimal level of cyber security investments. There is precedence that this can be done appropriately as evidenced, for example, by the Census Bureau's handling of R&D information collected on behalf of the National Science Foundation through its RD-1 reporting form.

---

[33]Gordon and Loeb (2002) proffered a model for the optimal level of cyber security expenditures. Their model assumes a performance variable, such as potential loss from a compromise. Unfortunately, no performance information is in our dataset.

[34]Infrastructures to facilitate security information sharing are conspicuously absent from the Cyber Security Research and Development Act, P.L. 107-305. This is surprising since the White House (2003) acknowledged government's role in cyber security when transaction costs related to prevention are high. The transaction costs associated with intra-organization information sharing are indeed high because of the public good nature of information *per se*.

And finally, our finding that more employee-intensive organizations allocate a greater proportion of the IT budget to cyber security suggests that there may be some internal protection processes applicable to organizations across industries. If so, then standardized protocols embedded within network support would benefit all organizations. And, if relevant information about such security needs could be assembled from organizations by a public infrastructure such as NIST, such protocols could be updated on a timely basis.

5. Industry-Specific Cyber Security Investment Decisions

In this section, we provide qualitative discussions about our five major stakeholder groups—financial service providers, health care providers, manufacturing firms, small businesses, and universities. Financial service providers and manufacturing firms have generally the same outlook on cyber security, aside from regulation-specific impacts. However, health care providers, small businesses, and universities all have very unique challenges and perceive cyber security investment very differently.

We talked with several Internet service providers (ISPs), electric utilities, and nonprofit research institutions, but based on the small number of interviews we were able to conduct, we combined these into an “other” group for analysis and data presentation purposes. Section 5.6 provides a brief discussion on each of these groups. We also spoke with nine home users—a separate and very distinctly different group—and conducted extensive interviews to assess their cyber security investment strategies and the trade-offs they observe.

5.1 FINANCIAL SERVICES

Although the financial services industry receives the third most number of attacks, behind only the government and the manufacturing sector (International Business Machines, 2005), several expert and industry interviews suggest that the level of security is not as high as the public might believe. The financial services industry includes banking, investment, and insurance institutions, which have similar missions; however, small- and medium-sized banks and credit unions operate very differently from national and multinational corporations.

For our study, we conducted interviews with banking institutions, insurance companies, investment firms, and a Federal Reserve branch. We contacted 34 organizations, had informal discussions with 12 people, and conducted 6 formal interviews. Generally, the organizations with which we spoke had a similar focus and strategy related to cyber security; differences we observed seemed to be related to staff rather than to business differences. Compared to the other industries with which we spoke, financial firms viewed security as less important than either the performance of the network and the convenience to users (internal staff). As one representative of a medium-size local investment firm commented, “security always takes a backseat to business.”

One U.S. regional bank executive was very open about his past experience as an industry consultant. He indicated that his experience caused him to characterize much of the industry as having very inadequate cyber security investments. During his first 6 months in his current position, he has doubled the cyber security budget for his organization.

5.1.1 Drivers: Motivational Factors

All financial institutions with which we spoke indicated that regulations, specifically the Gramm-Leach-Bliley Act (GLB) and the Sarbanes-Oxley Act (SOX), had caused their cyber security budgets to increase, and in many cases, had forced company executives to give cyber security issues more attention. For example, according to the Federal Trade Commission (FTC), which monitors compliance with GLB, in August 2004, Nationwide Mortgage Group and Sunbelt Lending Services, Inc., were charged with failing to comply with GLB security requirements (FTC, 2004).

Furthermore, as of March 2006, 23 state laws have been passed that require organizations to inform consumers when their personal information might have been compromised (Consumers Union, 2006). Quite a few financial institutions have had breaches that require such disclosure; as a result, many financial institutions have begun to spend more money on IT security, and many have created separate IT security departments.

5.1.2 Information Resources

Most financial institutions rely on qualitative information to make their investment decisions; however, most do track information on breaches and use of IT staff time. Several even try to track the value of attacks by a combination of IT staff hours, users' time, and impacts on current or prospective client relationships. All financial institutions with which we spoke track the effect of the network or an application going down because of a cyber security breach, whereas only two-thirds of other organizations track this information.

Although most members of the financial industry indicated that they do not provide any data to consortia, they were among the most active organization in providing information to a small peer group and/or participating in best practices sharing groups, such as the Financial Services Information Sharing and Analysis Center (FS ISAC). However, one large insurance provider indicated that they are not members of the FS ISAC because of the $75,000 annual membership fee.

Additionally, Gartner seemed to be a particularly important resource for people in this industry. Several organizations mentioned Gartner as one of their most important resources for informing and shaping cyber security investment decisions. The Chief Information Security Officer (CISO) of a southeast U.S. banking institution indicated that if Gartner recommends a certain technology solution, management always approves the solution.

5.1.3 Impact/Opinion of Regulations/Standards

As mentioned above, GLB and SOX have a significant impact on the relative level of security in the financial services industry. In most cases, people seem to believe that the impact of these regulations has been positive, though several mentioned a very high compliance cost. One respondent noted that regulations need to be more prescriptive, while another noted that the regulations should only be viewed as a baseline that should have been in place anyway.

5.2 HEALTH CARE PROVIDERS

The health care industry is an extremely diverse industry, including small urgent care facilities, family medicine practices, large hospitals, and other managed health care organizations. Based on these functional differences, these organizations manage cyber security in a variety of ways—some operate from one central office, while others have separate cyber security divisions within each business unit or regional facility—and their routine procedures can differ greatly. For instance, a small clinic and a large research hospital do not view cyber security similarly. Therefore, we decided to focus on larger organizations and not small offices, including medical, dentistry, and optometry practices that share more in common with other small businesses.

We conducted extensive interviews with large health care providers, many with multiple branch offices/hospitals, and with the North Carolina Healthcare Information and Communications Alliance, Inc., (NCHICA) a health care industry group in North Carolina.[35] We contacted 29 organizations, held informal discussions with 7 organizations, and conducted 6 formal interviews. The health care facilities with which we spoke described their environments as very heterogeneous, with users involved in research, clinical, and administration activities and a wide variety of hardware and software components in use on part of their IT networks, creating significant complexity.

Each hospital system with which we spoke coordinated its cyber security effort and investments both at the central level and at regional/branch offices. At the central level, the Information Security Officer told everyone on the network what applications they could have and what user polices should be in place, although doctors often have a particularly strong influence over the cyber security of the organizations. Although overall budgeting and maintenance of the network backbone and associated cyber security problems was centralized in all organizations, some gave more or less control over cyber security spending and administration to regional and branch offices.

In one instance, the branch offices each had security officers who made decisions about cyber security staffing, certain user policies, and tracking and spending activities. Although a central budget helped to pay for some access to and maintenance of the overall network, each office had its own cyber security staff and maintained its own hardware and software, including tracking of any problems. Alternately, other organizations kept control of all staff at a central office and interacted with branch offices when necessary.

[35]NCHICA coordinates a health care industry working group and had placed significant importance on several groups addressing security and privacy issues. One particularly important result of this work was a document that providers could give to vendors to easily convey their security requirements. See NCHICA's Web site at http://www.nchica.org.

In certain circumstances, we were told that security restrictions had been reduced in clinics and hospitals to enable a certain piece of software or hardware needed for a medical procedure. One hospital system with which we spoke was owned solely by the physicians; its cyber security administrators said that, although security is not reduced because of complaints, cyber security staff must spend a significant amount of time explaining policies and procedures that might slow productivity.

5.2.1 Drivers: Motivational Factors

Unlike another type of company that might lose some business if its cyber security was too lax or if its user policies were too restrictive, each health care organization we spoke with noted that a hospital could lose a life if a certain IT system were to fail or if cyber security impeded a certain procedure. Both of these concerns have an observable impact on the relative importance placed on cyber security at these facilities. For example, several organizations stated that they have different security requirements for administrative offices, clinical settings, and operating rooms related to password protection of systems; operating rooms have little security because it could restrict emergency needs.

Regulations seem to be the main factor accounting for approximately 45 percent of the motivation for the level of cyber security at each health care provider. Most participants felt as though regulations, Health Insurance Portability and Accountability Act (HIPAA) in particular, gave them much more flexibility in their investments, policies, and procedures—several organizations noted that if they cite “HIPAA compliance” as the reason for a new product/service or policy or procedure change, it will be approved. One organization offered the idea that HIPAA is based largely on NIST and ISO requirements, so if an organization is in compliance with these, then HIPAA would be easy.

One provider indicated that the standards they decide on as an organization play a large role in dictating the level of cyber security; thus, staff knowledge and experience is very important to cyber security.

5.2.2 Information Resources

The health care organizations we spoke with tried to conduct some data tracking and analysis, but only about half tracked the hours spent by staff members. They all claimed to be conducting ROI, IRR, and/or benefit-cost calculations, but rarely performed any quantitative analysis of their cyber security. Only a small percentage of projects were justified by looking at staff hour savings.

5.2.3 Impact/Opinion of Regulations/Standards

As mentioned above, HIPAA has had a significant impact on the security of health care organizations. In most cases, organizations believed that the impact had been positive, though excessive monetary resources had been used. Several organizations noted that they had been regulated by state laws directing their treatment of personally identifiable health information for more than 5 years, and in all cases we heard that these organizations had to have much stronger policies and procedures in place compared to HIPAA. If a state has stronger laws than HIPAA, the organizations within the state must comply with the more stringent standard.

5.2.4 Barriers to Adoption / Potential Solutions

Doctors are worried about the effect of cyber security on patient care, and this has affected the level of cyber security in some instances. However, hospitals did not mention a large number of barriers to adoption, and they seemed to receive the most support of any industry for their investment needs.

5.3 MANUFACTURING FIRMS

Manufacturing companies are actively cutting costs through supply chain integration and just-in-time supply delivery; however, according to organizations with which we spoke, increased reliance on electronic business communications and reduced inventories have increased the cost of cyber security events. The organizations included semiconductor manufacturers, conglomerates with electronics and health care products, and pharmaceutical firms.

For our study we had informal discussions with eight organizations, and conducted formal interviews with an additional eight organizations. Generally, the organizations had a similar focus and strategy related to cyber security; differences we observed seemed to be related to general organizational changes (e.g., mergers and acquisitions). As compared to the other industries we interviewed, manufacturing firms viewed security as necessary for business.

5.3.1 Drivers: Motivational Factors

All manufacturing firms indicated that regulations, specifically SOX, had caused their cyber security budgets to increase and, in many cases, had forced company executives to give cyber security issues more attention. Specifically, pharmaceutical firms face a large variety of additional regulations from the U.S. Department of Agriculture (USDA) and U.S. Food and Drug Administration (FDA).

As indicated above, customer and supplier relationships are a major driver, affecting the level of cyber security maintained by many manufacturers. In several cases, companies told us that they were forced to improve security measures to conduct business with suppliers and customers.

5.3.2 Information Resources

Aside from small businesses, manufacturers seemed to listen to vendors more than any other industry when deciding on the hardware and software they should invest in. Furthermore, when deciding on their cyber security staff procedures and, to a lesser extent, their user policies, manufacturers relied heavily on external public resources. Several organizations mentioned participating in various consortia, including the FBI’s InfraGuard program and Forrester’s Security Risk Management Council, and one organization noted significant information and data sharing with key clients and partners.

The manufacturing industry also collected less information about breaches than any other group. Although a majority of the organizations tracked the number of breaches, almost one-third did not, and only one organization tracked information on the effect specific breaches had on users and the cyber security staff. Organizations indicated that they did not see the need for tracking such information.

5.3.3 Impact/Opinion of Regulations/Standards

As mentioned above, SOX has had a significant impact on the relative level of security in the manufacturing industry. In most cases, people seem to believe that the impact of these regulations has been positive, although several people mentioned that there is a very high compliance cost. Others indicated, however, that SOX did not require very robust security measures and, aside from the necessary paperwork, has almost no associated compliance costs.

For some organizations, many other regulations, including FDA and USDA regulations and sections of the Patriot Act, impact cyber security investment and implementation strategies. As in other industries, organizations dealing with multiple regulatory requirements found compliance to be very difficult.

5.4 UNIVERSITIES

Universities and colleges, referred to as “universities” in this report, have the least stringent cyber security user policies and overall investment strategies of any group we spoke with. University networks are used by several client groups—university staff members, faculty performing research, and students—and each group has unique challenges. Universities need open networks for researchers and students to develop new ideas and to freely communicate. State and federal regulations (e.g., the Federal Information Rights and Privacy Act, or FIRPA) also restrict their ability to monitor student online activity. One university has identified 20 different security zones on its campus, with each zone having its own set of unique security policies and procedures.

To further complicate network security administration, the clients, particularly the student population, are a very dynamic group. Each year, approximately one-fourth of the student population leaves the network and a new group of students enter; these new students usually have a much lower level of knowledge of security than those leaving, so frequent training must occur. One university indicated that it spends a substantial amount of money on training students and faculty on security policies.

We contacted 15 universities, including a mixture of private and public institutions; had informal discussions with 9 universities; and conducted 7 formal interviews. All of the cyber security administrators with whom we spoke worked within their university’s IT department, so they received a share of the IT budget. Although each organization invested in cyber security mechanisms that had relatively little effect on network performance and user convenience, the organizations had very different investment strategies.

Technically, some universities with which we spoke did not have a firewall; however, most believed the networks were still very safe. Several universities were working under an end-to-end security framework—applications had security built in and did not rely on network-level security. However, many vendors' products do not have built-in security, so organizations that followed this strategy developed more applications internally or negotiated with vendors to develop more robust internal security for their products.

5.4.1 Drivers: Motivational Factors

Depending on the makeup of the university, many regulations may have an impact on the level of security. Most have felt some effect from HIPAA and FIRPA, as well as requirements from VISA for e-commerce activities and GLB for accounting activities. Additionally, some universities had medical schools and veterinary schools that caused them to face more stringent HIPAA requirements, as well as USDA and FDA regulations. Furthermore, if any faculty were conducting research for the Department of Homeland Security, universities faced additional regulations. The result was many different regulations affecting the way cyber security technology, policies, and procedures were maintained, and additional reporting was required in some cases to prove compliance. In some states, additional regulations and/or state government budgeting affected the level of security maintained by public universities.

Universities also considered current events (i.e., reported breaches) to be a significant motivation for cyber security investments. More than any other group, universities indicated that security breaches in the media or reported through various government and nonprofit data collection organizations caused them to react by changing their investment strategy by creating different technology solutions, polices, or procedures.

5.4.2 Information Resources

Universities are more reliant on internal private resources than any other group. In particular, they used their staff experience and internally collected data to inform their implementation strategies. In our interviews, half of the organizations commented that they believed they hired the best cyber security staff in the industry, many educated by their institutions, and that their staff were very proud of the experience and skills they maintained. Universities seemed very hesitant to talk about any need for additional information.

Furthermore, this group, on average, conducted more quantitative data analysis than the other groups. Universities attempted to assign relative importance to attack types and security solutions and to plan their spending accordingly. However, very few tracked cyber security staff time and user time spent resolving breaches or on any proactive security activities.

5.4.3 Barriers to Adoption / Potential Solutions

Universities face more explicit barriers than most other groups, although on average they were more confident in the effectiveness of their cyber security activities. As discussed before, in many cases, universities are restricted by a large number of state and federal regulations and they must deal with a very diverse user community. Furthermore, because they are motivated by the idea of "academic freedom," they are pushed from all groups to allow maximum network performance and minimize user inconvenience; both of these restrict their ability to impose many cyber security solutions and policies.

5.5 SMALL BUSINESSES

For the purposes of this study, we generally focused on small businesses that had a particular interest in the integrity of their data, either because of potential reputation (i.e., potential loss of business) or legal (e.g., regulatory) effects. Thus, we talked with law firms, optometry offices, pharmacies, dentist offices, small software companies, and accounting firms. We had informal discussions with eight organizations, and conducted six formal interviews. Each organization shared a focus on the bottom line as the main driver for any internal investment decisions, particularly preventative spending, such as the costs associated with proactive cyber security activities. However, each organization approached cyber security a little differently and had a unique set of issues to address.

Investment decisions are generally made by the owner(s) or senior managers within the organization. In some cases, one staff member with some interest in IT issues was designated to oversee the IT network, but the investment decisions still needed approval from senior management. Usually cyber security recommendations were made by an outside contractor who had been hired to install and maintain the IT network (including the cyber security) for the business.

The contractors were usually able to justify a basic level of cyber security measures (e.g., antivirus software and firewalls); however, it seemed to be a common concern of these consultants that it was difficult to justify more powerful (and costly) cyber security software and hardware. Although consultants were obviously interested in encouraging organizations to spend more money to improve their profits, the organizational approval structures seemed to have some flaws.

In one law firm, for example, the decision was either to buy more computers or to improve the network cyber security. Furthermore, money that was not spent became part of the partners' annual bonuses, so they had a personal incentive not to spend too much. Without quantitative measures available to justify additional spending, cyber security spending often became a lower priority in most of the small businesses with which we spoke.

One small business, a dentistry firm, had a different perspective on cyber security. The dentists owned two offices and had a network between the offices. They viewed investing in IT and the associated security as essential for the success of their business. These dentists structured patient interaction so that IT was critical to service (i.e., each patient area had a computer system and monitor that displayed records, including X-rays); when the network was down, they essentially could not work. Thus, they were willing to spend extra money on cyber security to ensure network performance and data integrity.

5.5.1 Drivers: Motivational Factors

Of the factors affecting small businesses' level of cyber security, our interviews suggested that external management (e.g., hiring a firm to install and maintain cyber security components) accounted for the majority of the basis for the cyber security measures maintained by these businesses. Despite the hierarchical restrictions that seemed to inhibit spending on cyber security, when asked to rank a list of factors that influenced the decision of whether to adopt a new security measure or implement a new user policy or cyber security administrator procedure, surprisingly, only the law firm ranked immediate cost and total cost of ownership first and second out of six possible choices.

In contrast, the two dentists' offices responded that the potential to improve cyber security staff productivity and the ability to improve security were the most important factors in deciding whether to adopt a new security measure or to implement a new user policy or cyber security administrator procedure. Generally, however, cost was much more of a concern for small businesses than any other industry group we studied.

5.5.2 Information Resources

In general, small businesses paid particular attention to vendors and consultants because these were the most accessible resources. In most cases, small businesses do not hire full-time IT staff, so they must rely on contractors, other consultants, and vendors' suggestions to decide what cyber security measures would be the most helpful and what vendor(s) to select.

Contractors were the main influence on small businesses' decisions on what cyber security procedures and user policies should be in place. Contractors also used NIST best practice documents and regulatory guidelines (e.g., HIPAA). In a few cases, contractors collected data about a network, including the number of past compromises and associated cost(s) to assess the best policies and procedures to employ. Rarely do small businesses track their resource allocation (e.g., staff hours spent on specific proactive and reactive activities).

We generally heard that small businesses were not using any quantitative techniques to justify cyber security investments. Although some were collecting data on the number of security events and incidents, the cyber security staff time needed to resolve the breaches, and the user time needed to resolve them, this information was most often used qualitatively. To justify spending, they assessed their needs based on past spending, current threats, and amount of money available, the latter being the most important.

Although the U.S. Small Business Administration, NIST, and the FBI work together in an effort to provide small businesses with resources to help them set up and maintain cyber security, it seems that few small businesses know about this information, and even fewer are able to use more than online documentation. Most of the workshops are only offered in larger cities to which many small businesses cannot travel easily, and online information is very general.

Some small businesses do use resources provided by industry associations. However, these seem to largely be in the health care industry. For example, the American Dental Association (ADA), in which four out of five dentists in the United States are members, provides cyber security information in the form of how-to CDs and booklets. Both dentists with whom we spoke indicated that they had consulted these resources.

5.5.3 Impact/Opinion of Regulations/Standards

Many of the small businesses with which we spoke, including an optometry office, a pharmacy, and a dentist, were affected by HIPAA because they worked with individual health care data. In general, they had to spend some money on compliance (in several cases, outsourcing the development of necessary changes), but they did not find HIPAA to be overly burdensome. One dentists' office indicated that it would not have had any more security without HIPAA than it did with HIPAA, though it would have had less paperwork. Another dentists' office agreed that HIPAA had a positive impact on the cyber security of health information.

Most small businesses, including the law firm and software firms, are not currently affected by government regulations dictating restrictions or requirements on cyber security. Except for HIPAA, no other regulation has reached into the small business arena.

5.5.4 Other Industry Factors

Customer and supplier relationships have an effect on the cyber security of small businesses. One dentists' office noted that vendors supplying electronic claims services required it to increase cyber security by implementing specialized equipment. Presumably, this increased the level of cyber security. Furthermore, the pharmacy with which we spoke is strengthening its cyber security in anticipation of an increase in online prescription requests and renewal services over the next several years.

As with other industries, the level of cyber security in small businesses is very dependent on the knowledge and expertise of the IT staff, or in many cases, the consultants controlling the cyber security. Unfortunately, businesses often do not have the resources to identify or pay highly skilled contract workers or an experienced in-house IT person. Although we did not attempt to assess the level of cyber security of each organization, it is likely that small businesses have a reduced level of expertise in cyber security when compared to larger organizations.

5.5.5 Barriers to Adoption/Potential Solutions

Small businesses in general do not feel as though they are in great danger from cyber security breaches; however, they also do not have the information necessary to make good investment decisions. They are budget-constrained more than any other group, and subsequently (or additionally), they do not believe they have the resources necessary to efficiently invest their resources.

5.6 OTHER ORGANIZATIONS

In addition to the five industries focused on in this study, we investigated cyber security investments within several additional industry groups that help to support the digital infrastructure of our country, namely, electric utilities and Internet Service Providers (ISPs). These two groups are faced with significant challenges for a variety of reasons, and currently are both under extreme pressure to increase their level of cyber security. In this section, we briefly introduce some of the problems specific to each of these two industry groups.

5.6.1 Electric Utilities

During the past 20 years, growth in the U.S. transmission and distribution (T&D) system has not kept pace with growth in electricity demand. As a result, system monitoring and real-time control have become increasingly important as reserve margins have been lowered to increase capacity utilization. Network security is essential for the electric utility system because of the cascading nature and extremely high cost of power outages. Outage costs to utility customers can be severe, and utilities have been criticized for not making the appropriate investments to offset these costs.

Based on our interviews, electric utilities have been under an extreme amount of pressure to improve their cyber security infrastructure, including the threat of government regulations. In the past, electric utilities have been able to impose their own restrictions and requirements through a self-regulatory body, the North American Electric Reliability Council (NERC). Since the passage several years ago of NERC's standard 1200 on cyber security, electric utilities have been "regulated" to maintain a certain level of cyber security activities; however, this standard has provided a high level and relatively nonrestrictive approach to cyber security activities.

In the past 2 years, following the major blackout in the northeastern United States and possibly as a response to potential government regulation, NERC crafted a much more restrictive set of regulations, NERC Standard CIP–002–1. According to the two electric utilities we interviewed, although still in the draft stage, this new set of regulations will impose a substantial cost on the industry. There seemed to be significant concern about whether some electric utilities would need to request government assistance or to increase billing rates to implement the new infrastructure and procedures.

Furthermore, our interviews indicated that these new regulations are causing widespread organizational restructuring; thus, cyber security investment and implementation strategies will probably look very different in the next year or two.

5.6.2 Internet Service Providers

ISPs include telecommunications companies that provide telephone service and connectivity to the Internet directly to customers. The maintenance, and hence the security, of the connections that these companies monitor and service is vital for each company to remain competitive. However, as a critical piece of the U.S. infrastructure, this maintenance is an important issue for society as a whole. Specifically, the security of an ISP's networks can directly influence the security of its customers' networks. These companies should have significant private motivations to maintain security networks; however, they may not bear the full costs of cyber security events that also affect their customers.

We were only able to interview two ISPs, and only one participated in a formal interview; however, we also spoke with individuals at the IT ISAC, and other experts provided information on the security investments made by ISPs. One key issue that arose was that, in addition to specific government pressure to provide more security, ISPs currently must maintain very secure networks and provide substantial security measures to comply with the regulations imposed on their customers, who are in every industry.

More recently, there has been a push for ISPs to take a more active role in providing security to their customers. By serving the pipeline for all Internet traffic, large ISPs have the ability to detect many types of traffic that could be security attacks and to stop the more obvious traffic rather than allowing it to continue; however, this line is blurry. In a recent article in *CIO* magazine, the CIO of the Federal Trade Commission indicated that regulations might be imposed if ISPs did not themselves decide to start monitoring and filtering Internet traffic (Villano, 2005).

5.7 HOME USERS

In addition to investigating the cyber security investment decisions made by a variety of private and nonprofit organizations, we conducted interviews with nine home users who subscribe to either cable modem or DSL Internet service. In general, what we found was that the level of security maintained by users primarily depends on what the PC maker provides to people who purchase their computers (approximately 85 percent cited this as their top driver). Furthermore, we found that, in response to a security problem, most home users (approximately 70 percent) have either purchased additional security products, downloaded free shareware security programs, or hired a consultant.

To determine the implementation strategy for cyber security, home users relied on a variety of resources, but eight out of nine respondents indicated that they did not feel comfortable with their level of understanding of security problems or potential solutions. So many simply relied on what was provided when they purchased their computer(s). However, over half of the people we spoke with also relied on a friend or colleague to help them decide on any additional security hardware or software to install on their computers and/or to learn about security procedures (i.e., how to configure a router to be more secure) they should use.

We also asked home users to describe the amount of time and money they spend each year on cyber security products or services, excluding any products that include security components (e.g., routers or operating systems). When we asked about spending habits, we found that more than 50 percent spend less than $20 per year, while the remainder spend from $21 to $80 per year. As for time spent on security issues (e.g., installing patches, running debugging programs), one-third spent 2 hours or less per year, one-third spent between 2 and 10 hours per year, and a full one-third spent more than 10 hours per year (some up to 30 hours per year).

During our interviews, we asked whether people viewed themselves as being secure on a scale from 1 to 10, and the average response was 7.1. This indicates that home users generally feel that they are secure. However, when we discussed what information they might lose in a breach, many indicated that they do not keep personal information on their computer.

To gauge their relative willingness to pay for security, we asked participants whether they would pay their ISP to provide increased security options—more than half indicated that they would be willing to pay 10 percent more than their normal ISP monthly service rate for additional security, although only 15 percent would pay 25 percent more.

6. Conclusions and Recommendations

As we have emphasized throughout this report, little is known about how organizations evaluate their cyber security investments, where organizations obtain relevant information, and how organizations assess the benefits and costs of such investments. Our interview-based findings and analysis represent a first step toward understanding these issues. Still, more information is needed before definitive public policies can be evaluated and selected.

One clear fact is that different industries are motivated by different cyber security drivers/concerns and that industries rely on different sources of information in support of their cyber security investment and implementation decisions. However, our interviews point to some common issues related to the public-goods nature of cyber security that could help inform government's role in enhancing security.

6.1 SUMMARY OF INDUSTRY FINDINGS

The following summarizes key findings, by industry.

6.1.1 Financial Services

- Regulations, specifically the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act (SOX), have caused the financial service sector's cyber security budgets to increase and, in many cases, have forced company executives to give more attention to cyber security issues.
- Recently passed state laws, which require organizations to inform consumers when their personal information may have been compromised, are beginning to lead to an increase in cyber security spending and have increased the trend of creating separate cyber security departments.
- Although most members of the financial industry indicated that they do not provide any data to consortia, financial organizations were among the most active in providing information to a small peer group and/or participating in best practices sharing groups, such as Financial Services Information Sharing and Analysis Center.

6.1.2 Health Care Providers

- Based on functional differences within the health care system, organizations manage cyber security in a variety of ways: some operate from centralized offices, while others have separate cyber security divisions within each business unit or regional facility.
- Existing regulations, such as HIPAA, provide sufficient flexibility in their investments, policies, and procedures, and the healthcare providers with which we spoke indicated that HIPAA has had a major impact on the level of cyber security maintained by the industry.

- While some doctors are worried about the effect of cyber security on patient care, in general, providers did not mention a large number of barriers to adoption of adequate cyber security technologies, polices, and procedures. Of the industries we interviewed, the health care industry seemed to receive the most internal support (e.g., from executive-level staff) for cyber security investment needs.

6.1.3 Manufacturing

- Manufacturing companies are actively cutting costs through supply chain integration and just-in-time delivery of supplies; however, according to the organizations we spoke with, increased reliance on electronic business communications and reduced inventories have increased the cost of cyber security events.
- Manufacturing firms can be affected by numerous regulations, ranging from SOX to regulations from the U.S. Department of Agriculture and the Food and Drug Administration, leading to complicated cyber security requirement issues.
- Most of the manufacturing companies indicated that the impact of regulations has been positive, although several companies mentioned very high compliance costs and confusion about requirements.

6.1.4 Universities

- Universities and colleges have the least stringent cyber security user policies and overall investment strategies of any group interviewed, reflecting the unique challenges of maintaining an open network for researchers and students to develop new ideas and to communicate freely. However, on average, universities are confident in the effectiveness of their cyber security activities.
- Universities face more explicit barriers than most other groups because (1) they must deal with a very diverse user community, including students, staff, faculty, and researchers; and (2) they are restricted by privacy regulations, as well as by regulations affecting many research activities, often limiting the available cyber security options.
- Universities are more reliant on internal private resources than any other group. In particular, universities depend on staff experience and internally collected data to inform implementation strategies.

6.1.5 Small Businesses

- Cyber security investment decisions are generally made by the owner(s) or senior managers of the organization, with supporting recommendations from outside contractors hired to install and maintain the IT network. Generally, costs are a greater concern for small businesses than for any other industry group we studied.
- Most of the small businesses with which we spoke indicated they are not affected by government regulations dictating restrictions or requirements (with the exception of HIPAA requirements) related to cyber security.
- The information and support resources available to small businesses are viewed to be minimal, but varied by business type. Few small businesses know about small business information services provided by organizations, such as NIST or the Small Business Administration, and most small businesses feel they do not have the information necessary to make good investment decisions.

6.2 IMPLICATIONS OF 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 with the use of additional resources to enable more robust, quantitative investment analysis.[36]

We learned from our interviews, and from the extant academic and professional literature, that there are at least two barriers limiting an organization’s ability to determine a socially optimal cyber security investment strategy. The first barrier is the limited availability of reliable, cost-effective information on which the organization can make an informed investment decision. The second barrier is 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 (or mis-invest) in cyber security from a social perspective, and the second barrier would definitely result in underinvestment from a social perspective.[37]

It is difficult, timely, and costly for an organization to assess the probability of a security breach, much less to assess the possible related impacts. These impacts include, but are certainly not limited to, assessing the effectiveness of available cyber security technologies that are in-house or available from vendors, the implementation/maintenance costs of these technologies once identified, and the overall reputational cost to the organization from experiencing a breach.

Relevant and applicable knowledge is a scarce good. Consortia and trade associations 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.

[36]Typically, public goods are thought of as things that are used by everyone, but that no one entity is sufficiently incented to optimally provide. The interesting thing about the information infrastructure is that every single piece is owned by a for-profit entity, which is incented to assure that its part of the information infrastructure is functioning. That said, there are very likely parts where underincentment occurs, ISPs that handle traffic for an e-tailer, for example.)

[37]Note that it was not the objective of this study 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 into future policy analysis.

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 (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.

6.3 GOVERNMENT'S ROLE IN ENHANCING CYBER SECURITY

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 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. Although many groups attempt to provide such services, the organizations we spoke with (particularly small businesses) were interested in more information comparing types of products. Also, 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. All the organizations with which we spoke were 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.

Another possibility is that 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).[38] Related to security breach costs that spill over throughout the network, a potential role for the government is to design mechanisms that redistribute the costs (i.e., reduce spillovers and externalities) to better provide

[38]The real question is how closely can the social and private optimums be aligned? Companies are not in the business of providing socially optimal anything, but will certainly do so if they see it as being in their (private) best interests. Rational risk management processes can serve to bring the two much closer into alignment.

incentives for individual organizations to enhance their cyber security. Examples of this include regulations that define activities or security thresholds that must be met. The associated threat of litigation from being out of compliance is another way 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. Putting the responsibility with those who have the control is important; the private sector could be at least as good as the government if they evaluated the risks they were facing.

However, based on our interviews, organizations have mixed opinions regarding whether regulations or business mandates were an efficient means of enhancing cyber security. 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.

There was also 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.

6.4 FUTURE RESEARCH

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. As such, the following is a sequential list of suggested future policy-related research on cyber security investment activity.

1. Conduct an expanded interview- and survey-based study with the goal of more explicitly understanding how organizations, from their private perspectives, reach what they consider to be an optimal mix of proactive versus reactive cyber security investment decision strategies.
2. Investigate organizations' specific barriers that inhibit their use of external resources. We expect that there will be differences among identifiable barriers that apply to the use of hardware, software, and cyber security procedures.
3. Investigate the flows and magnitudes of cost externalities to determine who actually bears the costs of cyber security breaches. For example, are the costs pushed upstream to suppliers (rather than manufacturers), or are costs pushed downstream to final consumers?
4. Develop public policy recommendations to remove these identified barriers and enhance the efficiency with which public sector organizations minimize internal breaches. We expect, based on our preliminary knowledge, that our set of recommendations will include both the promulgation and dissemination of

technical knowledge as it relates to hardware and software and of procedural knowledge as it relates to the establishment of internal protocols/activities.

References

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

Answers.com. 2005. “Definition for VPN.” <http://www.answers.com>.

Austin, Robert, and Christopher Darby. 2003. “The Myth of Secure Computing.” *Harvard Business Review* June:120-136.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market.” *Journal of Computer Security* 11:431-448.

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.

Charette, Robert N. July 1991. “The Risks with Risk Analysis.” Inside Risks column. *Communications of the ACM* 6:106.

Cisco Systems, Inc. 2001. “The Return on Investment for Network Security.” White paper. San Jose: Cisco Systems. <http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.pdf>. Accessed March 2005.

Cisco Systems, Inc. 2002. “Economic Impact of Network Security Threats.” White Paper. San Jose: Cisco Systems.

Common Vulnerabilities and Exposures (CVE). 2005. *MITRE CVE*. <http://www.cve.mitre.org/compatible>. Accessed December 2005.

Consumers Union. “Notice of Security Breach State Laws.” Last updated March 27, 2006. <http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf. Accessed April 2006.

D’Aqostino, D. August 8, 2003. “Insuring Security.” *CIO Insight* <http://www.cioinsight.com/article2/0,1397,1216110,00.asp.> Accessed April 2006.

Dempsey, Mike. 1996. “The Development of a Theory of Corporate Investment Decision Marking: An Historical Perspective with Implications for Future Development and Teaching.” Leeds, UK: School of Business and Economics Studies, University of Leeds.

Federal Trade Commission (FTC). November 16, 2004. “FTC Enforces Gramm-Leach-Bliley Act’s Safeguards Rule Against Mortgage Companies.” <http://www.ftc.gov/opa/2004/11/ns.htm>. Accessed November 2005.

Gal-Or, Esther and Anividya Ghose. June 2005. “The Economic Incentives for Sharing Security Information.” *Information Systems Research* 16(2):186-208.

Garg, Ashish, Jeffery Curtis, and Hilary Halper. March/April 2003. “The Financial Impact of IT Security Breaches: What Do Investors Think?” *Information Systems Security*.

Gordon, L.A., M.P. Loeb, and T. Sohail. 2003. “A Framework for Using Insurance for Cyber-Risk Management.” *Communications of the ACM* 44(9):70-75.

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.

Gordon, L.A., and R. Richardson. 2004. “Infosec Economics: New Approaches to Improve Your Data Defenses.” *Network Computing* April:67-70.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and R. Richardson. 2005. *2005 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Gordon, L.A., and M.P. Loeb. 2006. “Managing Cyber Security Resources: A Cost-Benefit Analysis.” New York: McGraw Hill.

Hagedoorn, J., A.N. Link, and N.S. Vonortas. 2000. “Research Partnerships.” *Research Policy* 29:567-586.

Hall, B.H., A.N. Link, and J.T. Scott. 2003. “Universities as Research Partners.” *Review of Economics and Statistics* 85:485-491.

Hayes, R.H., and W.J. Abernathy. 1980. “Managing Our Way to Economic Decline.” *Harvard Business Review* July-August:67-78.

Hodder, J. 1986. “Evaluation of Manufacturing Investments: A Comparison of U.S. and Japanese Practices.” *Financial Management* Spring:17-24.

Hodder, J., and H. Riggs. 1985. “Pitfalls in Evaluating Risky Projects.” *Harvard Business Review* January-February:128-135.

Hovav, Anat, and John D’Arcy. 2003. “The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms.” *Risk Management and Insurance Review* 6(2):97-121.

ICSA Labs. 2005. “The Security Device Event Exchange (SDEE).” <http://www.icsalabs.com/icsa/topic.php?tid+b2b4$52d6a7ef-1ea5803f$4c69-ff36f9b5>. Accessed April 17, 2006.

InformationWeek. “Study: Spammers, Virus Writers Getting Chummy.” <http://www.informationweek.com/story/showArticle.jhtml?articleID=29101653&tid=6007>. Accessed February 2005.

International Business Machines (IBM). August 2, 2005. "IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005." http://www-03.ibm.com/industries/financialservices/doc/content/news/pressrelease/1368585103.html. Accessed December 10, 2005.

Internet Engineering Task Force. 2005. "The Intrusion Detective Message Exchange Format." <http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt>. Accessed December 2005.

Jackson, William. January 2001. "CERT's Full-Disclosure Is Responsible, but Mistrust Remains." *Government Computing News*.

Krebs, Brian. June 27, 2002. "White House Pushing Cybersecurity Insurance." *Washington Post*.

Lemos, Robert. January 21, 2002. "Data on Internet Threats Still Out Cold." Available at <http://news.com.com/Data+on+Internet+threats+still+out+cold/2100-1001_3-819521.html>. Accessed October 2005.

Mi2g. 2005a. "SIPS Report (January)." <http://www.mi2g.com/cgi/mi2g/press/ged2004.pdf>.

Mi2g. 2005b. "Frequently Asked Questions—SIPS & EVEDA—v1.00." <http://www.mi2g.com/cgi/mi2g/press/faq.pdf>. Accessed February 2005.

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.

Neumann, Peter. June 2004. "Optimistic Optimization." *Communications of the ACM* 47:6.

O'Brien, Timothy L. December 4, 2005. "Online Scammers Go Spear-Phishin'." *New York Times*.

Ogut, Hulisi, Menon Nirup, and Srinivasan Raghunathan. June 2005. "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk." Presented at the 2005 Workshop on the Economics of Information Security and Harvard University.

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* 9(4):443-458.

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

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

Smith, L. Murphy, and Jacob Smith. March 2006. "Cyber Crimes Aimed at Publicly Traded Companies: Is Stock Price Affected?" Presented at the American Accounting Association Southeast Region Conference.

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

Sophos. “Sophos Virus Analyses.” <http://www.sophos.com/virusinfo/analyses/w32blastera.html>. Accessed February 2005.

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

Symantec. March 2005. “Symantec Internet Security Threat Report: Trends for July 04-December 04.” Volume 7.

U.K. Department of Trade and Industry and PriceWaterhouseCoopers. April 2004. “Information Security Breaches Survey 2004.” <http://www.dti.gov.uk/industry_files/pdf/isbs_2004v.3.pdf>.

Varian, Hal. June 1, 2000. “Managing Online Security Risk.” *New York Times*.

Villano, Matt. November 1, 2005. “Seeing No Evil.” *CIO Magazine*.

Appendix A
Vulnerabilities and Cyber Security Technologies

The decision-making process for IT security is based on the ongoing conflict between hackers and security administrators, involving a variety of motivations, goals, and security tools and procedures. In this appendix, we describe the goals and motivations for hackers and then define the tools and activities they use to achieve their goals. Then we discuss general tools, processes, and activities that IT security administrators and users use to prevent attacks from hackers. Finally, we discuss technical performance issues of cyber security technologies and emerging threats. Hackers is one category of unauthorized users. Criminals, terrorists, and hostile nation-states are three other categories of attackers. The distinction is important in terms of motivation, resources available to finance the attack, and potential targets. In this report our focus is on cyber attacks from hackers and, to a lesser extent, criminals.

A.1 VULNERABILITIES

The cyber infrastructure used by public and private organizations and individuals can be viewed as consisting of three categories of resources: *computing resources,* such as CPUs and memory, used to run applications; *storage resources*, such as disk drives and storage area networks (SANs), used to store data; and *network resources,* including routers, wireless access points, and hubs, which connect multiple storage and computing resources together. Unless physical security breaches are considered, some network resources must be compromised for an attacker to access any other resources or any user or administrator applications. Thus, network resources are the most common target because they could allow the attacker to threaten applications, operating systems, or storage or computing resources once inside. The following discussion provides insight into the potential goals of attackers and the tools and methods they use to attack specific resources.

A.1.1 Goals of Attackers

In general, attacks on the cyber infrastructure can be identified as pursuing one or more of the following goals, all of which can inflict economic damage on the target.

Goal 1: Damaging or diminishing the effectiveness of vital cyber infrastructure components. These attacks generally cause one or more vital pieces of a network's infrastructure to become either inoperable or cause them to operate at a diminished capacity. Examples include denial of service (DoS) and distributed DOS (DDoS) attacks or attacks that may cause a vital router or server to reboot or go off-line. These attacks could be directed at a specific organization or individual or intended to disrupt service for a large number of "hosts" (i.e., end users) or networks.

The attacker could disrupt service for a large number of hosts or networks either through worms or viruses that can infect a host and propagate to other connected hosts (important data on the infected hosts may be destroyed in the process as a by-product or direct consequence of the virus activity).

Another widespread application of this goal is spam, or Unsolicited Commercial E-mail (UCE). A large number of spam messages originating from or sent to a single e-mail server can crash it or, at the very least, degrade its performance, which causes delays in the delivery of important e-mail messages.

Goal 2: Gaining unauthorized access to the target's sensitive information. Most businesses are vitally dependent on their proprietary information, including new products information, personnel data, or client records. An attacker may derive direct economic benefits from gaining access to and/or selling such information. For example, attacks may be preceded by worms and viruses that create back doors in the target's infrastructure (e.g., Blaster worm) for an attacker to enter and collect the information. Other ways of gaining confidential information include

- sniffing vital information from the network traffic originating or intended for the target;
- guessing or cracking passwords on the systems of interest to gain access to the system; or
- causing a "privilege escalation," in which an *insider* working in the organization uses security holes to increase his/her access level.

A special example of such attacks is *phishing*, in which the attacker attempts to extract private confidential information from targets by crafting forged e-mails or Web sites that pretend to originate from or belong to an entity the target may trust (e.g., a bank, a health provider). Such e-mails generally attempt to solicit credit card numbers, social security numbers, bank account numbers, or other private information from their targets for further resale or misuse.

Furthermore, once access has been attained, attackers cannot only extract and use or sell private information, but they can also modify or delete sensitive information, resulting in significant consequences for their target(s).

Goal 3: Gaining unauthorized access to cyber resources for illegal use. Anyone, from an individual owning a computer attached to the Internet via a broadband connection to an employee of a large enterprise with multiple sites networked together, may possess resources that an attacker may wish to take advantage of. The most likely types of resources to become the targets of an attack are storage and network resources. Disk space resources might be used for storing illegal images of DVDs, MP3s, and videogames, or attackers might use specific compromised hosts to originate spam and DoS attacks directed at other sites.

Furthermore, hackers may break into systems to get free services, such as free access to the Internet using a corporate or personal wireless access point. Another example is attacks on the billing infrastructure of cellular providers with the purpose of receiving free or reduced-fee access to the cellular networks. Cellular providers tend to be more vulnerable to these attacks compared to fixed-infrastructure carriers because of the novelty of cellular technology; the convergence of digital and voice services on a single network, allowing attackers to introduce attack packets into the network more easily; and the fact that newer cellular networks usually have a direct connection to the Internet, making them vulnerable to attacks from the Internet.

As mentioned above, hackers typically attempt to take advantage of their victims' storage and network resources. Attacks in which the attacker gains access to computing power have been theorized in the literature; however, they remain relatively rare.

A.1.2 Combining Goals

An attacker pursuing one of the goals described above may in fact go through several steps, which include one or more of the other goals, before the final goal is achieved. An example of such behavior may be an attacker who first scans a portion of a network to find any vulnerable hosts, uses an exploit to gain access to a number of personal computers with broadband connections (Goal 3) to perform a DoS attack on part of a target's infrastructure (Goal 1), such that the attack disables the protective infrastructure of the target and the attacker may gain access to the target's confidential information (Goal 2).

Such scenarios are not uncommon in today's Internet. The Blaster worm that targeted hosts running MS SQL server applications took control of the vulnerable hosts (Sophos, 2005). Its goal was a DoS attack on the Microsoft Web site that was scheduled to start on a specific day, when all of the infected hosts would begin generating bogus traffic intended to disrupt Microsoft's infrastructure. It appears to have been the final goal of this particular attack; however, as stated above, more sophisticated multistage attacks are possible.

Recent information indicates that spammers and virus writers are finding benefits in cooperation: up to 86 percent of spam contains viruses that may take control of an infected host and use it as a relay to distribute more spam (InformationWeek, 2005). This new and troubling development elevates spam from the level of a nuisance to a serious cyber security threat.

A.1.3 Information Gathering by Attackers

Most cyber attacks are preceded by a phase during which attackers gather as much information about the "target" (e.g., an organization, individual, or network component) as possible. When a specific organization or individual is targeted, the methods involved in gathering information include network scans to determine the topology of the target network; information about the target from open sources (e.g., the Internet, print, or other types of media); and social engineering, which involves holding conversations with employees, usually under an assumed identity (e.g., a subcontractor or an employee from a remote company site). A common type of attack today that pursues this goal is *wardriving*, where vulnerable wireless access points are identified and mapped using wireless laptops equipped with a global positioning system (GPS).[39]

Furthermore, information gathering can be directed at specific network components, hardware, or software. For example, an attacker may work to find a bug or hole in an operating system or application that is widely used so that an attack can easily be made on many individuals and/or organizations at the same time. In all cases, the information-gathering phase helps identify weaknesses in the target infrastructure that can later become a target of direct attacks.

A.1.4 Types and Methods of Attacks

As indicated in the previous section, cyber attacks can be broadly classified as pursuing one of three goals. The means by which these goals may be pursued differ depending on the scale of the attack, the type of resource involved, and the final goal (in the case of a multistage attack). Table A-1 presents a tabulated breakdown of the major types and methods of attacks observed in today's Internet along with the possible intended goals of the attack.

A.2 COMMON SECURITY TOOLS AND PROCEDURES

Currently available security tools vary widely in the kinds and number of attacks they address, effectiveness, cost, and complexity. Some are created for a specific, very narrow purpose, such as virus scanners, network traffic, or file encryptors, while others are capable of monitoring the health of an entire corporate network with multiple agents distributed throughout and tasked with preventing attacks of multiple kinds (e.g., intrusion detection/prevention systems). Additionally, several activities can be used to restrict or minimize the number of successful attacks.

Table A-2 provides an overview of the common types of security tools and activities described above. This table describes each tool type, gives examples of the type of tool, and describes the type(s) of attack(s) the tool is capable of addressing by either detecting or preventing it. Finally, some disadvantages and performance metrics for each tool type are indicated.

[39] The following is an example scenario of wardriving: a hacker equipped with a wireless laptop and a GPS unit can walk or drive around "listening" for available wireless access points and map their locations based on the GPS data and the direction of the signal. This information can be used later to gain access to companies' or individuals' infrastructure, depending on the security mechanisms in place.

Table A-1. Types of Cyber Attacks and Associated Goals

Attack Type	Description	Goal(s)	Method(s)	Notes
Network probing/ scanning	Primary goal is to glean as much information as possible about the target infrastructure—network topology, operating systems, and applications in use—any other types of information that allows identification of weaknesses for further exploitation. Usually causes no direct damage.	[a]	Network-mapping tools like *nmap* can be used to determine how many hosts are attached to a network within a specific address range, what operating system (OS) version and patchlevel they are running, and what network applications are available.	
Distributed DoS	Large number of hosts with broadband connections begin generating bogus traffic targeted at a single site in a coordinated manner, disrupting the service provided by the site.	1	Packet or connection generator capable of producing large amounts of legitimate-looking Internet traffic.	The attacking hosts must be compromised prior to the attack through other means, like worms or trojans.
Other DoS	Any other direct attack on the infrastructure that causes degradation or failure in performance.	1	Sending malformed packets that cause a router to reboot. Misconfiguring pieces of infrastructure like routers and firewalls to which the attacker may have gained access through other means.	
Spam	Although usually not intended to directly harm the recipients, can nonetheless cause damage to the vital infrastructure by overloading e-mail relays and security tools associated with them.	1	Software capable of sending out e-mail at the same time to a very large number of recipients. Recipient lists are gleaned from Web sites, newsgroups, Internet Relay Chart (IRC) channels; probed from poorly configured mail servers and resold to spammers.	
Traffic analysis/ sniffing	Packet sniffing is performed using special software capable of intercepting copies of packets. It may pursue probing to find out more about the target as well as attempting to sniff (e.g., clear-text login passwords or other types of sensitive information for further misuse).	2	A packet sniffer installed on a compromised host on a network to which the target directly attacks, or the network that the target's traffic traverses. The job of a hacker becomes significantly easier if wireless infrastructure is being attacked, because it makes it simpler for the hacker to listen in on the traffic.	

(continued)

Table A-1. Types of Cyber Attacks and Associated Goals (continued)

Attack Type	Description	Goal(s)	Method(s)	Notes
Application/ host compromise	Host or application compromise can be achieved in a number of ways: exploiting bugs in applications running on the host remotely or locally and gaining unauthorized access by using information gained from probing or through a back door installed by a worm or a virus.	2, 3	Worms, viruses, and trojans can be used to compromise a host or an application running on a host. Also, illegal privilege escalation (e.g., to administrative privileges) can be achieved locally if the attacker has a nonprivileged login to a host running a vulnerable application.	
Account/ identity/ information theft	The pursued goals could be both gaining access to more private information and gaining access to resources for further misuse.	2, 3	Methods vary from phishing and social engineering to recovering sensitive information from stolen or discarded equipment. Cross-site scripting is another example in which malicious code is injected into Internet bulletin boards or Web sites that may steal identities of people logging in later.	This type of attack overlaps with traffic sniffing, because information gleaned from the passing traffic can be used to forge identities.
Zero-day attacks	Attacks of unknown nature and goals.	1, 2, 3	An example is when first victims of a new virus are identified. The nature of a virus, its mode of propagation, and the extent of the damage it causes may be unknown until it is analyzed by security tool vendors or the Computer Emergency Readiness Team (CERT).	Some network security tools are capable of detecting that something out of the ordinary is happening without being able to pinpoint exactly what is happening. This requires a high degree of human involvement.

[a]This is a precursor to most types of cyber attacks and associated goals.

Some of the tools can be used by both an attacker and a security administrator for different purposes. For example, a careful administrator uses a penetration testing tool to check for any loopholes into the network. An attacker uses the same tool to identify the same loopholes before attacking the network. The tools/security methodologies listed below are not all independent of each other; they represent a common set of tools, without any attempt to create a seamless organization.

Most of the tools work as a combination of hardware, firmware, and software components. Generally, higher-performing enterprise-level tools tend to have a higher proportion of hardware components as compared to small business or personal tools, which are mainly designed to run on the individual personal computers inside the network.

Table A-2. Common Security Tools and Methodologies

Type of Tool / Security Methodology	Types of Attacks Addressed	Disadvantages	Performance Metrics
Firewalls	Capable of addressing a wide range of attacks by stopping the malicious traffic from penetrating the protected network. May address DoS, probing/scanning, host compromise, zero-day attacks.	Create obstacles to network traffic. May make it difficult or impossible to run certain types of applications (e.g., video-conferencing or other peer-to-peer applications). May limit network performance by becoming the bottleneck.	Measures of network throughput. Many vendors advertise 1Gbps interfaces on their firewalls, but they are not capable of sustaining traffic at those speeds.
Content filters	Viruses, worms, trojans, spam. Some types of network-based intrusions that include sending malicious code or data directly into vulnerable applications can also be filtered out if integrated into the firewall solution.	May impose performance limitations on the servers running the content filters (e.g., mail servers equipped with spam and virus scanners).	False-positive rate, frequency and availability of updates.
Intrusion detection/ prevention systems (IDS/IPS)	Cover the broad range of known and unknown attacks. Capable of responding in real time to specific threats by, for example, partitioning affected networks, real-time filtering of traffic, raising alarms, and identifying affected hosts and networks. Response is governed by enterprise-wide sets of policies.	Inherit the disadvantages of firewalls. Require a knowledgeable staff to maintain. Costly at the enterprise level.	False-positive rate, measures of network throughput.
Access control	Makes unauthorized privilege escalation more difficult. Allows creation of more flexible access control schemes that provide for a minimally necessary level of access to users at a fine-grained resolution (e.g., per-application, database). This is known as the least-privilege principle. It also provides for separation of duties such that multiple personnel are required to authenticate sensitive transactions to reduce the internal opportunities for abuse.	Must be carefully administered. May require a centralized policy repository and a knowledgeable staff.	Ease of administration.
Strong user authentication	Makes identity theft more difficult either by making it more difficult to steal the necessary credentials (passwords) or by making the credentials harder to forge (biometric solutions, magnetic swipe cards, PKI certificates).	Additional expenses required to enable and administer. Requires a knowledgeable staff.	Cryptographic strength in PKI certificates, cost, ease of administration (in biometrics and card-based access) and maintenance.

(continued)

Table A-2. Common Security Tools and Methodologies (continued)

Type of Tool / Security Methodology	Types of Attacks Addressed	Disadvantages	Performance Metrics
Cryptography	Provides mathematical methods for protecting the confidentiality of communication channels and establishing and assuring identities of communicating parties. Thus, makes it difficult to forge identities and eavesdrop on communications channels.	Cryptographic techniques usually carry performance and/or economic costs. Performance and economic costs have a trade-off in that higher performing (hardware based) cryptographic solutions carry a higher cost of introduction. Since cryptography	Cryptographic strength, cost, ease of administration and maintenance.
Cryptography (continued)		is based on complex mathematical transformations of data, more complex transformations gain better security but require more computing power to implement. This power comes either from dedicating more of the general computing resources to cryptographic transformations or introducing dedicated hardware-based solutions to offload the transformations.	
Hardening	Addresses all types of attacks by making the cyber infrastructure inherently more difficult to attack by reducing the number of vulnerabilities.	Requires knowledgeable staff and investment of time. Conflicts between OS patches and applications are not uncommon (e.g., a specific application may run only with specific sets of patches and adding a new patch may break an application). Hardware hardening carries a higher economic cost because it may require replicating resources or keeping critical infrastructure lightly loaded to allow for bursty load spikes.	Availability of patches, measure of application problems related to frequent patching, percentage of critical patch coverage, monitoring how well the system has weathered spikes in load (natural or attack related)
Auditing	Addresses all types of attacks by uncovering known vulnerabilities and detecting intrusions based on anomalies in audited logs. Auditing may also look for anomalous accesses to data or resources from both inside and outside the organization based on log and access control information, thus addressing hacker attacks as well as insider attacks.	Time consuming if done manually (it can be automated), requires knowledgeable staff.	Time invested vs. number and seriousness of uncovered problems.

(continued)

Table A-2. Common Security Tools and Methodologies (continued)

Type of Tool / Security Methodology	Types of Attacks Addressed	Disadvantages	Performance Metrics
End user and administrator training	All types of attacks.	May be costly and time consuming. Data on vulnerabilities and ways of dealing with them are constantly updated, requiring continuous education, which requires training to be a continuous ongoing process.	Time invested vs. number of security incidents, speed with which the incidents are handled.
Insurance	All types of attacks.	May be costly. It may be difficult to estimate correctly short- and long-term effects of a cyber attack on a large enterprise.	Payoff vs. cost of insurance and cost of recovery from an attack or security incident.

Although performance metrics for each tool are available, in general assessing the effectiveness of any specific system containing multiple components is difficult, because the proof of its effectiveness lies partly in the absence of security incidents. Some comparative analysis can be performed based on the number of incidents discovered/prevented before and after the introduction of a new system or component. Better inferences can be made if information about numbers and types of security incidents is available within a particular business sector and size, so that organizations can compare their results to other organizations engaged in a similar line of business. This presumes better reporting of incidents by everyone involved than is observed today. Improvements in security tool interoperability may in part help solve this problem by providing a common base for reporting security incidents.

The following sections introduce common categories of tools and activities and give examples of each for enterprise, small business, and personal network environments, as appropriate.

A.2.1 Security Tools and Methods

This section provides a more detailed description of the major categories of tools and methods that are used to provide security through a combination of hardware and software products and administrator (and possibly user) involvement.

Firewalls. A firewall is a combination of hardware and software mechanisms that allow for the isolation of a segment of a network from the rest of the Internet. Typical firewall functions include traffic filtering[40] and network address translation (NAT). Firewalls can be

[40] Traffic filtering refers to the ability of a network device to inspect incoming packets in real time and reject or accept them based on a set of rules or policies. Typical reasons to reject packets would be packets coming from the Internet and attempting to create a connection with a host inside the protected network to which connections are not allowed.

stateless (e.g., traffic filtering) or stateful;[41] stateful firewalls create more flexible and fewer restructure access policies. The sets of rules and policies governing the firewall behavior can be static or dynamic, capable of responding to threats in real time.

Regardless of the scope of deployment (enterprise, small business, or personal network), firewalls perform similar functions. Differences lie in performance, ability to respond to detected attacks, and the proportion of hardware elements. Enterprise firewalls typically are dedicated pieces of hardware capable of isolating a network consisting of thousands of computers. Firewall performance is scaled down for small business environments in which weaker, less complex firewalls are more commonly used. In personal network environments, a firewall can be an embedded hardware device or a piece of software installed directly on a home computer.

Furthermore, some firewalls are dedicated to filtering a specific type of traffic, such as isolating cellular GPRS networks from the Internet.

Content Filtering. Content filtering comprises a number of approaches and mechanisms. The commonality lies in their ability to scan network traffic in real time and either alert the recipients to the possible malicious nature of the traffic or block the traffic from getting to its destination completely. This function is similar to traffic filtering, commonly performed by firewalls, but in content filtering the content of the traffic is inspected.

In the enterprise environment, examples of content filtering include mail gateways equipped with virus and spam filters that either place questionable e-mail messages in quarantine or mark them as containing questionable content. In small business and personal network environments, similar tools can be deployed as part of the e-mail client solution.

Firewalls may also be capable of content filtering. This is an advanced firewall function typically available in enterprise-level systems. These devices are capable of scanning network packets passing through them for signatures of known intrusion methods, such as viruses or worms.

Intrusion Detection/Prevention Systems (IDS/IPSs). An intrusion detection/prevention system is a combination of hardware and software mechanisms capable of alerting system administrators to an intrusion (in real time or after the fact) and, in some cases, capable of responding by preventing the spread of intrusion.

In the enterprise environment, IDS/IPSs are complex systems, consisting of multiple components and management stations. IDS/IPSs are capable of monitoring the state of the hosts connected to the network and real-time monitoring and filtering of network traffic.

---

[41] Stateful firewalls, or connection-tracking firewalls, go a step further than stateless firewalls by attempting to associate each packet with an existing connection and making decisions about accepting or rejecting packets based on this information as well. For example, if a Web session has been allowed to be established between a Web browser inside the firewall-protected network with an outside server, a connection-tracking firewall will accept follow-up packets going back and forth between the browser and the server based on the existing connection state.

They usually absorb the functionalities of firewalls, content filters, and virtual private networks (VPNs)[42] into a single solution.

In small business environments and personal networks, an IDS may be as simple as a file system integrity checker, capable of detecting alterations of vital executables (e.g., system-level files that are part of essential applications or the operating system) made by an intruder and alerting the system administrators to that fact. Another type of a host-based IDS may monitor the traffic entering and leaving the host and alerting the user to anomalous behaviors (e.g., ZoneAlarm)

Access Control. Access control refers to a methodology that allows system administrators to assign access rights to users (i.e., login/read/write/modify/view/execute/etc) in a flexible fashion. It allows the designation of a minimal set of rights needed by users to perform their functions. Such assignments create environments that are intrinsically more secure as compared to those in which users find themselves in possession of rights that are not necessary for their day-to-day activities and thus open possibilities for abuse.

Implementations of flexible access control are OS and application specific. Examples include access control lists (ACLs),[43] controlling access to files or databases, boot passwords, and application-level passwords.

Strong User Authentication.[44] Strong user authentication implies establishing the identity of a user through multiple methods that are difficult to circumvent. This may mean that a user identity is established through a password,[45] using his/her biological attributes (e.g., palm/fingerprints or retinal images), or a system in which a user possesses a secret that is impossible to guess or calculate (e.g., Public Key Infrastructure [PKI][46] certificates).

---

[42]According to Answers.com (2005), a VPN is defined as "a private network that is configured within a public network (a carrier's network or the Internet) to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks (WANs) that span large geographic areas to provide site-to-site connections to branch offices and to allow mobile users to dial up their company LANs."

[43]ACLs are a matrix-like approach to assigning privileges to users. The rows include users, and the columns include permissions at very fine levels of granularity (e.g., read/write/execute/access settings for files or folders). These lists can create management challenges because of the amount of information in such a matrix.

[44]Strong authentication is also referred to as a two-factor authentication and is defined as containing two of the three following components: something a person knows, has, or is. PKI certificates make user electronic credentials harder to forge by introducing strong cryptographic methods in credential verification. Biometrics verifies identity by analyzing unique physiological attributes (retinal pattern, finger- or palmprint) that are difficult to replicate. Magnetic (or other type) ID cards require possession of the card to validate the identity.

[45]In most enterprises, plain-text passwords (e.g., johnSmith9!) are used at the host level; however, after a user enters his or her password at a computer, the operating system encrypts the password before checking with the necessary server for a user's permission.

[46]According to Answers.com (2005), PKI is defined as "a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages (see code signing), which ensures that messages have not been tampered with. For more on how certificates and public keys are used, see digital certificate."

At all levels of deployment, strong user authentication can take the forms of encrypted passwords, smart cards, biometric access devices, PKI, Kerberos,[47] and other secure access methods/tools.

Cryptography. Cryptography provides for a set of techniques that allow people to conceal data and establish its integrity (i.e., lack of unauthorized modification) and/or authenticity of communications channels through mathematical transformations. The complexity of transformations usually directly relates to cryptographic "strength"; thus, stronger cryptographic techniques require more complex transformations as opposed to weaker ones. Cryptography can provide the following:

- Data confidentiality, intended to conceal the data from eavesdroppers. Data confidentiality is achieved through a process of encryption—a transformation of what is referred to as "clear text" data into a form that cannot be understood without reversing the transformation. The transformation is performed using one or more keys. Such a key can be a secret shared between the sender and receiver (symmetric) or use of a combination of public (known to everyone) and private (known only to the owner) keys (asymmetric). Examples of symmetric key encryption algorithms are DES and AES. An example of asymmetric encryption algorithm is RSA.
- Data integrity, intended to prevent unauthorized modification. Data integrity assurance is achieved by computing a short (compared to the data) message digest of the data and transmitting the digest along with the data. The recipient can then recompute the digest and compare it to the received one to verify that the data have not been verified in transit. Depending on the desired level of security this function can be achieved by applying a one-way hash function to the data, which does not require possession of any keys to be computed and thus does not provide good security, since an attacker can alter an intercepted message and then replace the digest in the message with the new recomputed value. Another way to guarantee data integrity is to pass the data through either an HMAC (Hashed Message Authentication Code) or a CBC-MAC (Cipher Block Chaining Message Authentication Code). Both require existence of a preagreed upon secret key between the sender and the receiver. The sender uses his copy of the key to compute the message digest and transmit it along with the message; the receiver uses his copy of the key to verify that the computed digest matches the received one.
- Data authenticity, intended to ensure the identity of the originator of the data. Data authenticity can be guaranteed by computing a signature of the message and transmitting it along with the message, similar to the digest in the data integrity function. The crucial difference is that this time the signature is computed using a secret key known only to the sender (private key), while the receiver uses a different key (public key), usually known to everyone and associated with the identity of the sender, to compute the signature and compare the results.

[47] According to Answers.com (2005), Kerberos is defined as "an access control system that was developed at MIT in the 1980s. Turned over to the IETF for standardization in 2003, it was designed to operate in both small companies and large enterprises with multiple domains and authentication servers. The Kerberos concept uses a 'master ticket' obtained at logon, which is used to obtain additional 'service tickets' when a particular resource is required."

- Nonrepudiation, making it impossible to deny that a party has sent or received specific data. The nonrepudiation function is generally related to the authenticity function in that the presence of a message signature that was computed from a private key known only to the owner guarantees that only the owner of that key could have originated the message.

Some or all of these can be applied to communications channels or data in general (e.g., files) depending on the requirements and policies of the organization. Many security tools include cryptographic functions as part of their processes. VPNs are a common example: they frequently provide all four of the functions described above to create a private network within a public network, so that access to it is tightly controlled and communications are confidential. It is becoming more and more common to see VPNs built on top of suite of protocols standardized by IETF IPSEC as opposed to earlier solutions that tended to use weaker semiproprietary protocols. Cryptographic functions are also commonly built into Web browsers in the form of implementations of the protocols standardized by IETF TLS/SSL. They help secure the communications that occur between Web browsers and Web servers in a course of a, for example, session between a bank and its client.

A.2.2 Security Practices/Activities

The tools described above require a certain amount of maintenance and updating, and all staff (including both IT staff and users) have important roles in implementing a secure network. This section briefly describes several specific activities that help improve the relative security level of an organization.

Hardening. Hardening means taking reasonable measures to ensure the security of the cyber infrastructure. This activity usually includes keeping the applications and operating system up to date with available updates offered by vendors and restricting access to vital infrastructure elements both through the network through cryptographic means and by fine-tuning access controls as well as by protecting physical access to critical pieces of infrastructure.

An example of hardening that is common at all deployment levels is patching or promptly applying security updates issued by the operating system or application manufacturers. This process results in the reduction/mitigation of vulnerabilities in the infrastructure, thus making the infrastructure as a whole more secure and reliable. Patching may be manual or performed using automated tools.

At the enterprise and small business levels, hardening may also mean physically restricting access to critical pieces of equipment, such as routers and servers.

Hardening firmware may mean keeping up with the latest firmware updates from equipment manufacturers. Hardware hardening may take the shape of using well-established vendors for critical pieces of equipment, maintaining hardware homogeneity for the purposes of quick replacement, and replicating important functions in multiple instances of hardware to cope with spikes in load occurring either naturally or caused by malicious activity.

Auditing. Auditing implies automated or manual scanning of logs and verification of system compliance to company security policies by, for instance, checking access lists against the policy and checking system configuration settings for example.

An organization should possess a security policy to which all of the elements of its cyber infrastructure must adhere. The process of verification of this adherence may be manual or automated depending on the scale of the organization and the comprehensiveness of the security policy. This verification may include “penetration testing,” in which internal staff or contractors try to break into or find holes in the infrastructure to identify and expose weaknesses in the policy or its implementation.

Auditing also refers to periodic checking of available logs of users’ activities and incoming and outgoing network traffic to search for anomalies that may indicate intrusions. Large enterprises may employ keystroke monitoring tools and packet sniffers to monitor their employees’ activities.

End-User Training and Policies. End-user training may include certification training for the IT staff to ensure their proficiency with available security tools and proper understanding of incident-reporting procedures; user training in common security precautions; and familiarization of CIOs, CEOs, and board members with best practices, advantages of incident reporting, and membership in information-sharing organizations such as the ISAC for the purpose of improving the security environment in their organization.

Furthermore, users and IT staff should be directed by specific guidelines dictating their IT activities. For example, users should have specific policies to follow when accessing their network remotely, taking data “off campus,” making changes to their computer’s applications or operating system, or engaging in other activities identified as potential security threats.

A.3 TECHNICAL PERFORMANCE ISSUES

Each type of security tool comes with its own performance limitations. However, performance metrics vary greatly across tools and methods, making comparisons difficult. The performance of firewalls is typically measured by the amount of traffic that the NIDS and the VPNs are capable of handling. For content filters, such as virus scanners, performance is measured in terms of time elapsed between the discovery of a new worm, virus, or trojan and the availability of the mail server and the additional load they place on the mail server (this may be measured in the number of e-mail messages processed on a hypothetical but common server configuration). Manufacturers generally advertise performance characteristics of their products and, if the results are favorable, those of a few close competitors. Publications like *InfoWorld* and *CNET* sometimes also perform independent comparisons of similar security products and make the results available to the public.

A.3.1 Interoperability

As the threats faced by corporate IT departments grow in their complexity and scale, so do the tools they employ to address those threats. Integrated systems combining individual components such as packet sniffers, firewalls, and virus scanners are beginning to appear. These systems consolidate multiple functions into a single solution controlled by a single robust security policy. Some vendors are capable of offering an entire integrated solution in a single product. Frequently however, a single enterprise-wide system can be put together out of components produced by different security tool vendors. One of the problems the vendors have been dealing with recently is the ability of their tools to interoperate with tools of other vendors by being able to describe detected vulnerabilities and attacks to each other and to report them in a consistent manner to operators or monitoring systems. For example, simple NIDS systems capable of detecting network-based attacks on infrastructure components may need to report detected attacks to a centralized monitoring system so that proper automated or manual actions may be taken to address the new threat.

Having a common vocabulary and format for reporting these events is becoming increasingly important. Efforts have been made in the industry to create such standards, of which the three most commonly mentioned today are CVE (Common Vulnerabilities and Exposures) (CVE, 2005), IDMEF (Intrusion Detection Message Exchange Format) (The Internet Engineering Task Force [IETF], 2005), and SDEE (Security Device Event Exchange) (ICSA Labs, 2005). CVE is essentially a dictionary of known vulnerabilities, in which each vulnerability has a unique name like CVE-1999-0006 and a short description. IDMEF and SDEE, on the other hand, are message protocols that describe how tools should communicate. IDMEF and SDEE messages have a way of including CVE names in them as one of the options, but they also allow tools to use proprietary naming schemes.

The development of CVE, partially funded by DHS, included a wide range of experts from security tool vendors, response teams, academic institutions, and nonprofit organizations and resulted in the creation of a common dictionary for describing security vulnerabilities in cyber infrastructure elements. The CVE project hosted by the MITRE Corporation also includes a continuously updated list of over 3,000 entries currently describing commonly known vulnerabilities, each with a unique name. Each entry contains a brief description of the vulnerability and references to other sources of information (e.g., Bugtraq or CERT databases) where more detailed descriptions can be found. The CVE list is freely available and allows security tools to use a common naming scheme when reporting detected vulnerabilities in the infrastructure. CVE-compliant tools are capable of either generating CVE names when vulnerabilities are detected or allowing users to search for specific CVE entries based on the CVE names. In short, CVE offers a common naming scheme, that security tools and human operators can use to exchange information about vulnerabilities with each other.

An example of a system properly using CVE would be a network scanner capable of detecting known vulnerabilities in systems attached to the network and reporting those vulnerabilities using CVE names to a network monitoring system. This monitoring system may then display this information for the benefit of the network operator or take automated measures.

IDMEF is a protocol for communications between security tools. It was developed by IETF, the organization responsible for standardizing the vast majority of Internet protocols, to standardize the automated reporting of vulnerabilities and attack alarms, so that disparate security tools may be able to communicate with each other in a common format. By its definition, IDMEF subsumes the functionality offered by CVE, which is just a dictionary of vulnerabilities. IDMEF messages can include CVE references, but it goes further by allowing references to other sources of information like Bugtraq and OSVDB (Open Source Vulnerability Database) for describing a detected vulnerability. It also allows security tools to describe attacks that may not have names in vulnerability databases and defines the language that describes the actions taken by the NIDS/IPS in response to an attack.

Finally, a strictly vendor-based effort to define a protocol similar to IDMEF is called SDEE and is being defined by ICSA Labs. Cisco Systems appears to be one of its few large backers. SDEE is similar to IDMEF in many technical respects.

The MITRE CVE Web site lists a large number of security tools that are partially or fully CVE compatible. Security tools compliant with IDMEF and SDEE are beginning to appear on the market as well.

All these serve not only to improve communications between different components of an organizational security system, which in this case does not have to purchase its entire security solution from a single vendor, but they also encourages sharing of incident information with outside organizations like IT-ISAC or any of the regional organizations. This in turn would serve to improve the overall security environment by allowing people to detect and respond to new attacks more quickly.

A.4 EMERGING THREATS

Emergence of certain technologies has led to a number of novel threats whose potential effects are not adequately understood yet. These technologies usually bring lower TCO or better ease of use, so decisions about their adoption are made without a detailed economic analysis of their security impact. Among the threats created by these novel technologies, the following are particularly significant:

- Wireless technologies: Wi-Fi (802.11a/b/g), emerging WiMax (802.16), Bluetooth, and cell phones are all examples of wireless technologies that allow for easier access to networked resources from home, the road, and remote office. All of them, however, have serious security implications, because by moving away from a fixed, physically secure infrastructure of land-based LANs and phone networks they allow hackers easier access to the same infrastructure. The threat introduced by wireless technologies must be assessed very seriously, and the convenience of wireless access must be weighed against the increased susceptibility to attacks on the infrastructure. The relative cryptographic weakness of the currently employed wireless security solutions (WEP, WPA-PSK and WPA-Enterprise) and lack of education among the public regarding the risks posed by running an improperly configured wireless network as well as the increasing pervasiveness of wireless technologies are a big part of the reason for why this threat will be with us for a while.

- Effects of monoculture: Using a single-vendor solution for network hardware components, end-user host operating systems, and/or other applications lowers the TCO; however, this also increases the susceptibility of the infrastructure to a catastrophic failure, because all of the components of such infrastructures usually have common exploitable weaknesses. Thus, an attack by a worm, for example, may bring down the entire network instead of a subset of hosts. Decisions about adopting single-vendor approaches to cyber infrastructure must be carefully weighed against the increased susceptibility of this infrastructure to a single attack.
- Spam (UCE): Spam, as stated above, is more often becoming a significant security threat instead of a nuisance. The latest indications of collaborative efforts between virus writers and spammers suggest that spam must be treated with the same level of cautiousness as other more common security threats, such as viruses, worms, and trojans.
- Phishing—Phishing is becoming increasingly targeted and sophisticated and is no longer strictly the domain of scammers. As recent incidents uncovered in Israel (*New York Times*, 2005) have revealed, even large companies are sometimes involved in phishing to steal their competitors' sensitive information.
- Spyware—Spyware (software installed on a computer without explicit knowledge or consent of the user, monitoring his or her actions and or taking partial control of the computer) is also becoming more sophisticated in avoiding detection and presents a problem even if the reasons for its installation were benign (i.e., the recent SONY DRM debacle). Music CDs from SONY contained spyware software intended to prevent illegal copying; however, bugs in the software actually allowed hackers to abuse it and take control of computers running it. Thus, installing this spyware actually increased the vulnerability of the computer.
- Botnets—Networks of computers (frequently in disparate locations around the world) containing back doors known to a single hacker or group of hackers that can perform functions such as relaying SPAM, performing DoS attacks on a specific host or domain without the knowledge of the owners. Because of the relative homogeneity of home computers' install base (MS Windows), and failure of owners to keep them properly up to date, these botnets frequently comprise large numbers of home computers attached to wide-band (DSL or cable-modem connections) and may present a serious problem to a network administrator under attack because of their distributed nature.