Incentives for Improving Cybersecurity in the Private Sector: A Cost-Benefit Perspective

Testimony for the House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

October 31, 2007

By: Dr. Lawrence A. Gordon (http://www.rhsmith.umd.edu/faculty/lgordon/)
Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland, College Park, MD 20742
Affiliate Professor – University of Maryland Institute for Advanced Computer Studies

Thank you for inviting me here today to talk about economic aspects of improving cybersecurity in the private sector. I commend the members of the Subcommittee for focusing on this critical and complicated issue.

Introduction

My comments today will center on ways of encouraging (i.e., providing incentives for) investments that are directed at improving cybersecurity in profit-oriented organizations operating in the private sector. However, much of what I have to say would also apply, with some modifications, to non-profit organizations (in both the private and public sector). My comments are based on an ongoing stream of research on "economic aspects of cyber/information security" that I (along with several colleagues) started in 1998. Part of this research has already been published, as indicated in the reference section at the end of this testimony.[1]

A key concern among profit-oriented organizations is efficiency. This concern is usually thought of in terms of facilitating the generation of profits (i.e., the difference between revenues and costs) for the owners of an organization, with the ultimate goal being to increase the value of the organization. **Indeed, the most powerful incentive for an organization in the private sector to invest in cybersecurity activities is the motivation to increase the organization's value to its owners.** For a publicly traded profit-oriented corporation, this value proposition is usually (or at least primarily) thought of in terms of increasing the stockholders' value.

At the heart of implementing this stockholders' value proposition is the notion of cost-benefit analysis. "*Cost-benefit analysis* compares the costs of an activity to the benefits of that activity, thereby focusing attention on the process of efficiently allocating scarce resources among competing activities. In the context of cybersecurity, the cost-benefit analysis principle means that managers need to compare the costs of an additional

[1]Given the limited nature of this testimony, many facets of the above noted stream of research are not directly addressed in this document (e.g., cybersecurity risk management).

information security activity with the benefits derived from that activity" (Gordon and Loeb, 2006, p. 20-21). When the benefits exceed the costs, the value of the organization will increase. **Thus, in considering a decision to increase spending on cybersecurity activities, it is important that the organization believe that the benefits will exceed the costs.**

A fundamental assumption underlying the above concept of cost-benefit analysis is the fact that organizations have scarce resources that need to be allocated to competing activities, including cybersecurity activities. In other words, cybersecurity activities are competing with other organizational activities (e.g., new product development, R&D, merger and acquisition decisions, fringe benefits for employees, etc.). If an organization invests more in cybersecurity activities, that means less will be available for other initiatives (i.e., organizations have finite resources to invest in competing projects). Accordingly, it is important for profit-oriented organizations to be able to argue that cybersecurity investments represent a more efficient allocation of organizational resources (on a cost-benefit basis) than if such resources were put to an alternative use (e.g., developing a new product). In the vernacular of business, this means it is important to be able to **"make the business case"** for investing in the cybersecurity activities. Generally speaking, there is a well established process for making the business case for an investment, including investments in cybersecurity activities. Figure 1 provides a diagram of that process.

As indicated in Figure 1, **making the business case** starts with specifying the cybersecurity objectives for the organization. Next, various alternative investments for achieving the cybersecurity objectives need to be identified. Once the alternatives have been identified, the data associated with each alternative needs to be specified and analyzed. The next step is to conduct a cost-benefit analysis and to rank the various investment alternatives, followed by the allocation of resources to particular cybersecurity investment(s).[2] The final step in the business case framework is to conduct a post-audit of the investment decision (i.e., evaluate the effectiveness of the cybersecurity investment decision).

Unfortunately, making the business case for cybersecurity investments is often more difficult than making the business case for many other investments. There are at least three separate, albeit related, aspects to this added difficulty. First, the benefits derived from cybersecurity investments are especially difficult to assess. Second, the risks associated with cybersecurity investments are also especially difficult to assess. Third, there are *externalities* (spill-over effects) associated with cybersecurity investments. A brief discussion of each of these concerns is provided below.

In addition to the benefits, risks and externalities associated with cybersecurity investments, there are two other items that are important to any discussion of improving cybersecurity investments in the private sector. These two additional items concern the total amount to spend on cybersecurity activities and the Sarbanes-Oxley Act of 2002. A brief discussion of both of these items is also provided below.

Benefits Derived from Cybersecurity Investments

[2] For a detailed explanation on the mathematics underlying cost-benefit analysis, based on discounted cash flows, see Chapter 2 of Gordon and Loeb (2006).

The first difficulty associated with cybersecurity investments has to do with identifying and estimating the benefits derived from such investments. The primary benefits associated with cybersecurity investments are the future "cost savings" derived from the prevention of losses due to cybersecurity breaches.[3] However, if breaches were prevented, the actual losses would not occur and therefore would not be observable. In fact, the better the security, the less an organization will observe the losses resulting from cybersecurity breaches. Thus, organizations need to estimate the potential losses from cybersecurity breaches in order to estimate the benefits derived from cybersecurity investments. These estimates can be based on past experiences, where such experience exists.

A fundamental problem in coming up with estimates of the benefits derived from cybersecurity investments is that the most important potential losses are due to unobservable lost customers resulting from cyber breaches and the potential liabilities associated with cyber breaches. In fact, as shown in the Campbell et al. (2003) study, these costs can be staggering.[4] Unfortunately, even when organizations have data upon which to estimate the explicit losses associated with detecting and correcting past breaches, they rarely have data upon which to estimate the implicit losses associated with lost customers and the potential liabilities.

One way of addressing part of the problem discussed above concerning estimates of the benefits of cybersecurity investments is to take a "wait-and-see" approach to such investments. As pointed out in the Gordon, Loeb and Lucyshyn (2003a) study, this wait-and-see approach is consistent with the "real options" (more specifically, the "deferment option") approach to capital budgeting. Of course, as the name suggests, it also means that it is often best to defer certain investments in cybersecurity due to the problems associated with estimating the potential benefits.

The fact that the benefits derived from cybersecurity investments are essentially "cost savings" raises an additional issue not discussed above. That additional issue has to do with the fact that most corporate executives would prefer to increase profits by increasing revenues rather than by decreasing costs. The reason for this preference is due to the fact that the stock market tends to reward the owners of firms for growth as well as efficiency. Thus, in competing for funds, cybersecurity investments have a built in bias against them relative to "revenue generating" projects.

Risks Associated with Cybersecurity Investments

[3] It can also be argued that cybersecurity investments can create a competitive advantage for an organization, which in turn translates into potential benefits. Although this argument is correct, such benefits are generally considered to be secondary in relation to the potential cost savings from such investments.

[4] The Campbell et al. (2003) study also shows that many cybersecurity breaches are not statistically significant, in an economic sense.

The second difficulty associated with cybersecurity investments deals with the risks (or uncertainty) associated with such investments.[5] It is important to recognize at the onset that 100% security is rarely feasible in a technical sense, and certainly not cost-beneficial in an economic sense. Thus, it is important to realize that cybersecurity investments are intended to reduce the risk (i.e., probability) of cybersecurity breaches. However, determining the reduction in the probability of a particular breach taking place, let alone a string of breaches taking place, as result of a cyber investment is extremely difficult to estimate. Nevertheless, in estimating the benefits from cybersecurity investments it becomes necessary to associate those benefits with the probability of the occurrence of security breaches. In other words, the "expected" cost savings (i.e., expected benefits) from cybersecurity investments are actually derived by multiplying the potential cyber losses by the difference between the probability of the cyber security losses occurring prior to the cybersecurity investment and the probability of the cybersecurity losses occurring after the investment.

Not surprisingly, estimating the before and after probabilities associated with cyber losses is more an art than a science. Thus, many have argued that the entire process of trying to estimate the expected benefits derived from cybersecurity investments is nothing more than an academic exercise. **However, the fact that it is difficult to estimate the risk (uncertainty) associated with cybersecurity breaches should not be used as an excuse for avoiding the determination of such estimates.**

Another aspect of the risk associated with cybersecurity investments deals with the definition of the term risk. In the cybersecurity literature, risk is usually associated with the expected loss from security breaches (i.e., the sum of the product of potential losses multiplied by the probability of such losses). The goal of reducing the risk of a cybersecurity breach, according to this definition of risk, is to reduce the expected loss. However, there are other important notions of risk that should be of interest to those responsible for allocating cybersecurity investments. For example, reducing the variance (i.e., variation) of the potential losses is another valuable facet of risk when discussing cybersecurity investments.[6] Although beyond the scope of the testimony being submitted today, it should be noted that one way for an organization to reduce the risk associated with cybersecurity breaches is to invest in cybersecurity insurance (see Gordon, Loeb and Sohail, 2003).

Externalities Associated with Cybersecurity Investments

The third difficulty associated with cybersecurity investments relates to the externalities (i.e., spillover effects) associated with such investments. **These spillover effects are largely the result of the inherent interconnectivity associated with computer networks.** In other words, the security of a computer network -- particularly the Internet -- depends on the actions of all users of the network. This creates a problem in the following sense. When a firm invests in information security activities in an effort to improve its cybersecurity, it bears all the costs, but does not reap all the benefits. The

[5] In the early economics literature, a distinction is sometimes made between the terms *risk* and *uncertainty* (see Gordon and Loeb, 2006, p. 96). For purposes of this testimony, no such distinction is made.

[6] The expected loss and reducing the variance of potential losses are only two of the different concepts of risk that could be considered in the context of cybersecurity investments. For a further discussion of various risk concepts applicable to cybersecurity investments, see Chapter 5 of Gordon and Loeb (2006).

larger the share of the benefits that accrue to other firms, the smaller the incentive for a firm to increase its investments in cybersecurity activities. This may result in the firm, and hence society, under-investing in information security. While the government could, in principle, counteract this tendency by creating incentives for information security investments (for example, by offering tax credits for such investments), the government currently does not know the right level of incentives to provide.

The externalities associated with the Internet have resulted in all sorts of efforts to coordinate cybersecurity activities on both a national and international level. The ISACs (Information Sharing Analysis Centers) and the US-CERT (United States Computer Emergency Response Team) are two good examples of efforts to coordinate cybersecurity activities. Both of these efforts rely heavily on information sharing related to computer security, with particular emphasis placed upon protecting the nation's critical infrastructure.

Information sharing has the potential for lowering the cost of cybersecurity for each organization involved in such a program. Unfortunately, the free-rider problem (i.e., the situation where each member of a group shares a little amount of information, in the hope of learning a lot about the other members of the group), is prevalent among information sharing arrangements related to cybersecurity (see Gordon, Loeb and Lucyshyn, 2003b). Thus, unless economic incentives are devised to offset the free-rider problem, much of the potential benefit from information sharing organizations will not be realized.

How much in Total should be Invested in Cybersecurity Activities?

The cost-benefit framework discussed above provides a straightforward way of assessing the benefits and costs associated with incremental investments in cybersecurity activities. If we assume that an organization already has in place some initial level of cybersecurity spending, then the total spending on cybersecurity activities would be this initial spending plus the sum of incremental investments. A more sophisticated approach to deriving the right amount to invest in cybersecurity activities is to assume a zero-base starting position for such investments. In its most rigorous form, a mathematical model can be developed to derive the optimal amount an organization should spend on cybersecurity activities. Although cost-benefit analysis would be embedded within such a model, an optimization approach would be a far more sophisticated (in terms of the mathematics) approach to deriving the right amount to invest in cybersecurity. This model should involve specifying security breach functions, the potential losses associated with security breaches, the probability of such losses, and the productivity of cybersecurity investments.

One model for deriving the optimal amount to invest in cybersecurity activities, which has gained wide acceptance among academicians and many practitioners, is referred to as the **Gordon-Loeb Model.** This model is described in the paper by Gordon and Loeb (2002). It must be emphasized, however, that the Gordon-Loeb Model is best viewed as a "framework" for examining the optimal level of spending on cybersecurity, rather than as an absolute solution to the cybersecurity investment dilemma. Indeed, in the final analysis, determining the right amount to spend on cybersecurity activities requires sound business judgment (based on experience and knowledge related to a particular firm and industry), as well as the application of sound economic principles. In

other words, in the final analysis, there is no silver bullet for deriving the right amount to spend on cybersecurity.

Since cybersecurity investment decisions are made based on expectations of the future, the likelihood of getting the optimal solution to the investment problem is close to zero. However, it is important to realize that on average an organization would be better off by utilizing sound economic principles in making cybersecurity investment decisions than ignoring such principles.

Sarbanes-Oxley Act has Created an Incentive to Increase Cybersecurity Activities

The accounting scandals of the late 1990s resulted in the Sarbanes-Oxley Act (SOX) of 2002. A key aspect of this legislation deals with the internal control requirements of SOX under Section 404. In essence, SOX requires firms registered with the U.S. Securities and Exchange Commission to develop sound internal control procedures associated with financial reporting. Given the computer-based nature of modern organizations, it is generally agreed that sound internal controls implies sound information security. Thus, as shown by Gordon, Loeb, Lucyshyn and Sohail (2006), an indirect result of SOX has been to create an incentive for firms to increase their information security activities (and by implication, investments) by firms. **In essence, research suggests that SOX has created a strong incentive for organizations to increase their cybersecurity investments.** Although the above claim has not been directly tested, the findings by Gordon, Loeb, Luchyshyn and Sohail (2006) clearly point to the validity of this claim.

Summary and Recommendations

The above discussion highlights several key aspects of investments directed at improving cybersecurity within profit-oriented organizations operating within the private sector. These aspects can be summarized in terms of the following five points.

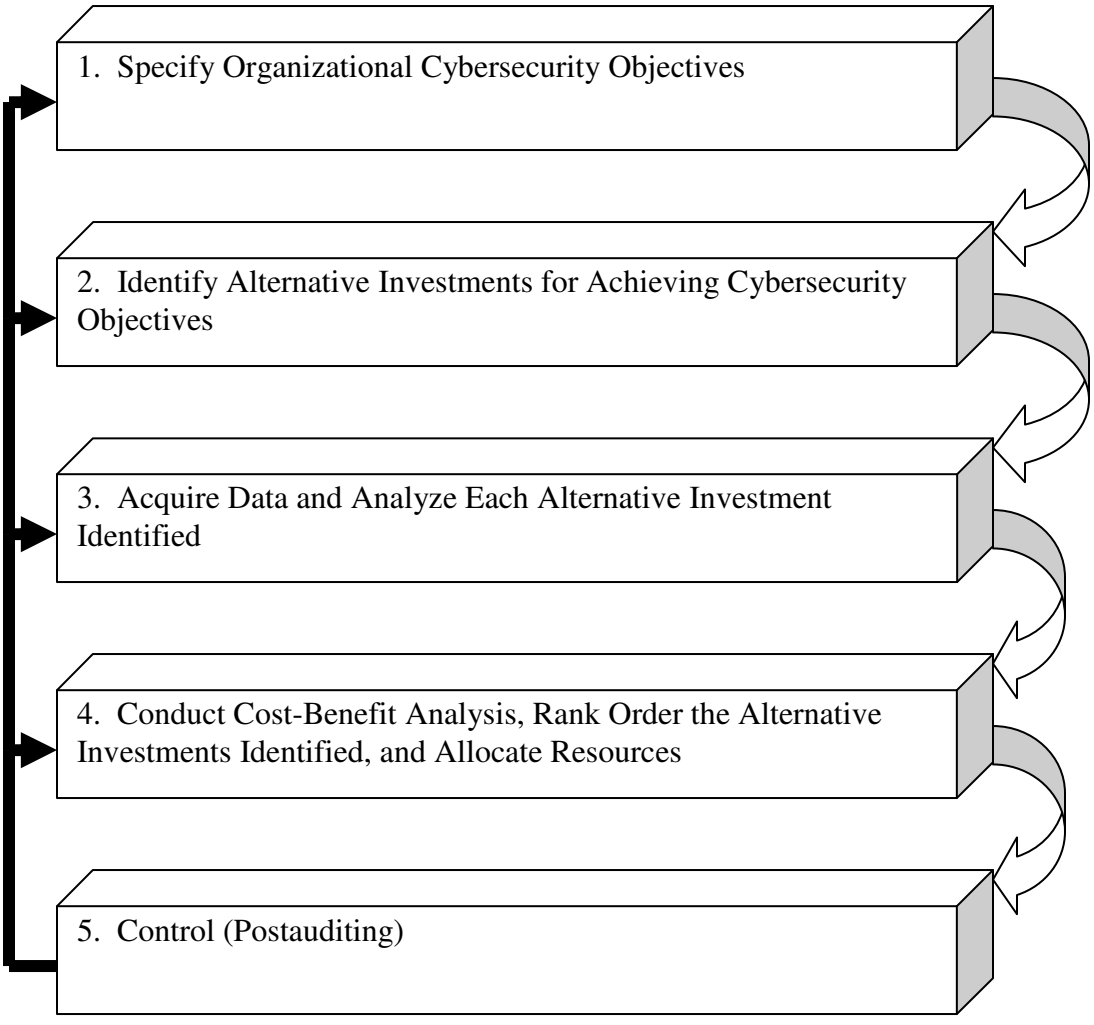
1. T**he most powerful incentive for an organization in the private sector to invest in cybersecurity activities is the motivation to increase the organization's value to its owners.** At the heart of implementing this value proposition is the concept of **cost-benefit analysis**, which falls under the umbrella of **"making the business case"** for cybersecurity investments. The idea of deriving an optimal level of investment in cybersecurity activities is closely associated with this cost-benefit concept. Unfortunately, many (if not most) CIOs (Chief Information Officers) and CSOs (Chief Security Officers) are not well versed in the economic underpinnings of cost-benefit analysis. Accordingly, it is often difficult for those responsible for cybersecurity activities within a firm to make a cogent argument for increasing the firm's spending on such activities. Remember, an increase in spending on cybersecurity activities generally means that less is available for spending on other initiatives (including revenue generating initiatives) within the organization. Thus, my recommendation is for this Subcommittee to initiate an effort to establish training sessions for CIOs and CSOs on how to apply cost-benefit analysis to cybersecurity investment

decisions. The development of these sessions could fall under the auspices of the Department of Homeland Security. In my opinion, such training would go a long way toward improving the allocation of private sector resources toward cybersecurity activities.

2. **A fundamental problem in coming up with estimates of the benefits from cybersecurity investments is that the most important potential losses are due to unobservable lost customers resulting from cyber breaches and potential liabilities associated with cyber breaches.** Until organizations feel more comfortable with their estimates of the benefits from cybersecurity investments, it is unlikely they will make the necessary commitment to such investments. In other words, the tendency will be to treat cybersecurity investments as a necessary evil rather than sound economic investments. Thus, my recommendation is for this Subcommittee to encourage, under the auspices of the Department of Homeland Security, additional research related to estimating the benefits of cybersecurity investments.
3. **The fact that it is difficult to estimate the risks associated with cybersecurity breaches should not be used as an excuse for avoiding the determination of such estimates.** The risks associated with cybersecurity are difficult to estimate. As a result, many view the process of deriving the "expected benefits" from cybersecurity investments as merely an academic exercise. However, there is an extensive body of existing literature on risk that has direct bearing upon cybersecurity investments. To date, this literature on risk has not been well integrated into the cybersecurity literature. Thus, my recommendation is that the cost-benefit analysis training sessions suggested in the first point above should include coverage of this literature on risk.
4. **The inherent interconnectivity associated with computer networks creates externalities (spillover effects).** These externalities revolve around issues related to welfare economics (i.e., a branch of economics associated with improving the welfare of an entire society or economic system, usually based on such principles as the efficiency of resource allocations and equitable income distribution to individuals). Since it is difficult to get organizations to incorporate these externalities into their decisions regarding cybersecurity investments, the development of exogenous government incentives may be appropriate. Thus, my recommendation is for this Subcommittee to encourage research directed at examining the appropriateness of developing incentives to address these externalities.
5. **Research suggests that the Sarbanes-Oxley Act of 2002 has created a strong incentive for organizations to increase their cybersecurity activities.** The fact that there is preliminary evidence that SOX has created a strong incentive for organizations to increase their cybersecurity activities, and by implication their spending on such activities, is worth exploring in greater depth. Indeed, assuming these preliminary findings are correct, there may be ways for the Department of Homeland Security to capitalize on this

development. Thus, my recommendation is for this Subcommittee to facilitate further exploration of this SOX-cybersecurity relation.

Figure 1: The Business Case for Cybersecurity Investments



Source: Gordon and Loeb, 2006 pp. 116 and 131.

References

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." Journal of Computer Security, Vol. 11, No. 3, 2003, pp. 431-448**.**

Gordon, L. A., and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November 2002, pp. 438-457.

Gordon, L. A., and M. P. Loeb, *MANAGING CYBERSECURITY RESOURCES: A Cost-Benefit Analysis*, McGraw Hill, 2006.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait and See Approach." *Computer Security Journal,* Vol. 19, No. 2, Spring, 2003a, pp. 1-7.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn, "Sharing Information on Computer Systems: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003b, pp. 461-485.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail, "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities," *Journal of Accounting and Public Policy*, Vol. 25, No. 5, 2006, pp. 503-530.

Gordon, L. A., M. P. Loeb and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management," Communications of the ACM, Vol. 46, No. 3, March 2003, pp. 81-85.