INFORMATION SECURITY EXPENDITURES and REAL OPTIONS: A WAIT-and-SEE APPROACH

by

Dr. Lawrence A. Gordon, Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance, Smith School of Business, University of Maryland

Dr. Martin P. Loeb, Professor of Accounting and Information Assurance, Deloitte & Touche Faculty Fellow, Smith School of Business, University of Maryland

Mr. William Lucyshyn, Research Director, Defense Advanced Research Projects Agency & Senior Research Scholar, School of Public Affairs, University of Maryland

Stefan, the company's CSO, has spent the last few days working on the security budget for the growing online mortgage provider and is now making his case to the company's CFO. He starts his presentation by noting the growing number of unauthorized intrusions into the company's network, and moves quickly to hardware, software and services he believes the company needs to invest in to prevent the security breaches. He concludes his presentation with a financial analysis that shows the net value (i.e., savings minus costs) from the expenditures on additional in formation security. Mary, the CFO is impressed with Stefan's presentation, but decides to fund only 60% of Stefan's request at this time. Stefan is convinced that Mary is clueless when it comes to security. Mary, on the other hand, is convinced that Stefan does not understand the economics of information security.

I. INTRODUCTION

The information age has created an environment where information is a critical ingredient for the success of most organizations. Indeed, protecting the information assets of an organization is a key concern to modern organizations.

However, information security is more than just a defensive maneuver by organizations. Information security is also a strategic variable that can help organizations gain a competitive advantage in the market place.

The importance of information security has led many organizations to pay much attention to information security investment decisions and, especially to deriving the appropriate level of these investments (e.g., see Gordon and Loeb, 2002). Even with all the focus on security, the numbers of unauthorized intrusions and security breaches are steadily increasing.

There are likely many reasons why security breaches are so common. One explanation could be that most managers just do not understand the economics of investing in information security. This explanation is akin to the argument that managers make decisions regarding information security investments in an *ad hoc* fashion (i.e., in a fly-by-the-seat-of-your-pants manner). This explanation may be true for some managers, but clearly it would not apply to the vast majority of managers in charge of information security. In fact, anyone who has dealt with Chief Security Officers (CSOs) knows that investments in information security investments are usually carefully considered. The data collected Gordon and Loeb (2003) clearly shows that most managers understand, and are attempting to use, economic concepts in making information security investment decisions.

Another explanation for the ubiquitous nature of information security breaches could be that it just does not pay to eliminate them from a cost-benefit perspective. In other words, trying to prevent most, if not all, of an organization's potential security breaches could involve a clear over-investment in such security. This explanation is akin to the belief that many security breaches are just a normal cost of doing business and should not be the basis for much concern. Although obviously true for some breaches, this normal-cost-of-doing-business argument is also unlikely to be the basis for the vast majority of information security breaches.

Given the uncertainties surrounding security breaches and efforts to prevent such breaches, a third explanation for the ubiquitous nature of information security breaches may be that it is economically rational to initially invest a portion of the information security budget and defer remaining investments until security breaches actually occur. In other words, it may pay to take a wait-and-see attitude toward part of the investments made in information security activities. This third explanation is akin to the notion of the deferment option discussed in the modern economics literature on capital budgeting.[1] To the extent that this explanation is correct, we would expect organizations to use security breaches as a critical determinant of their actual (as opposed to budgeted) expenditures on information security.

The purpose of this article is to examine the deferment option explanation for why information security breaches are so prevalent. Our examination will

[1] Another analogy can be taken from the spiral development strategy, which began in the software development community and now has expanded to hardware developments as well. It was developed to provide an incremental capability, which could be improved as risk was reduced and technology advanced.

focus on security breaches within major U.S. corporations and will include some empirical evidence to support our discussion. As will be seen, the evidence presented supports the argument that the ubiquitous nature of security breaches is due, at least in part, to the wait-and-see (i.e., deferment option) approach of many senior managers. This article will also show why such an approach is quite rational from an economics perspective.

II. INFORMATION SECURITY BREACHES AND REAL OPTIONS

Information security is usually grouped into one of the following three categories: (1) confidentiality (i.e., protecting private information), (2) availability (i.e., making information available to authorized users on a timely basis), and (3) data integrity (i.e., protecting the accuracy, reliability and validity of information).[2] Unfortunately, the ubiquitous nature of information security breaches is well documented. For example, the recent survey conducted by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) points out that 90% of the respondents detected a security breach within the past 12 months (Power, 2002, p.10).[3] According to the latest study by Congressman Stephen Horn, 14 of the 24 federal agencies flunk in terms of their success in

[2] Two other dimensions of information security, that are often discussed, are authentication and non-repudiation. For purposes of this article, we view these dimensions as sub-categories of "availability."

[3] Of course, since a large percentage of security breaches go undetected, this number is probably below the actual percentage.

implementing computer security (Mathews (2002). Although many information security breaches are not serious, many others cause significant financial losses. Some estimates of total economic losses from coping with virus activities unleashed on the Internet in 2001 exceed $10 Billion (Lyman, 2001).

Given the prevalent nature of information security breaches, the relevant question confronting most senior managers is not: Will an information security breach occur in my organization? Instead, managers need to be concerned with the following set of questions: When, where and how will the next information security breach occur? What are the best ways to detect and correct information security breaches? How do we invest our funds related to improving information security in the most efficient manner? It is this last question that is of particular interest to us in this article.

Once we acknowledge that we cannot protect all our systems from security breaches all of the time, it becomes obvious that a strategy is needed for allocating information security expenditures. One aspect of this strategy concerns the value of the information subject to breaches. That is, the level of spending on securing information should correspond to the value of the information being protected.

Another aspect of the strategy concerning the allocation of information security expenditures relates to the uncertainty associated with potential information security breaches. This uncertainty is the result of the potential vulnerabilities and threats associated with security breaches. Due to this uncertainty, it may be rational to take a "wait-and-see" approach toward spending some of the funds earmarked for information security. In other words, it may be wise to wait for some security breaches to actually occur before spending all of the funds available for information security. This approach is analogous to the deferment option often discussed in the literature on real options (e.g., see Pindyck, 1991). Of course, people with a military background will recognize the similarities between this approach and the "two forward, one in reserve" strategy often employed on a battlefield.

According to the real options literature, waiting for key events to occur will often yield higher expected benefits from capital investments than acting as if the investment needs to be made now or never. In essence, this literature shows that before one makes the investment, the net present value (NPV) of making an investment today needs to be greater than the option value associated with deferring the decision until more information is available (see Gordon, 2000, Chapter 12).

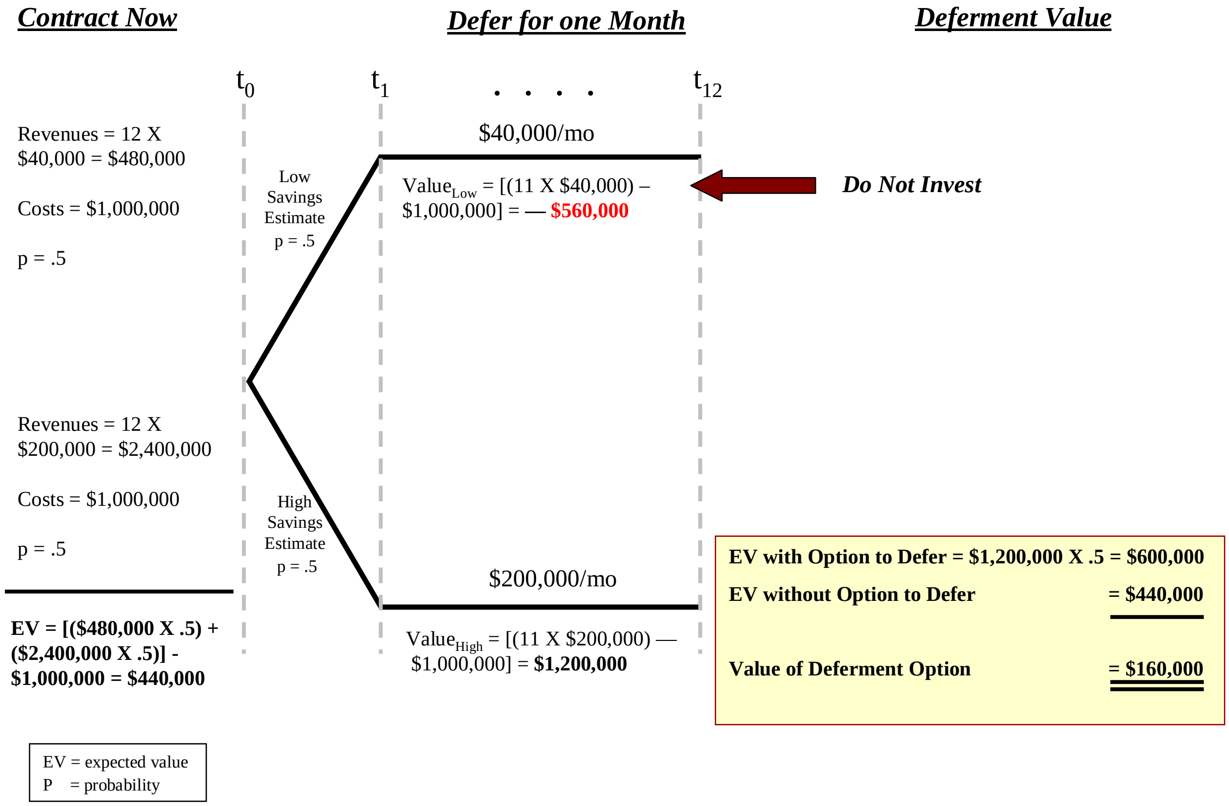
To see how the real options approach applies to expenditures on information security, consider the following example for the GLL Company that is illustrated in Figure 1. The GLL firm has tentatively budgeted next year's expenditures for information security in the amount of $2,500,000. The first $1.5 million is earmarked for basic information security activities (e.g., basic access controls, firewalls and physical protection of the firm's computers) and the firm's CSO is already authorized to use these funds for this purpose. The remaining $1 million is considered discretionary, and needs the firm's CFO's approval before any final commitments can be made to spend this money. The most likely use of the remaining $1 million is to hire an outside firm that specializes in enhancing the information security operations of major organizations. However, the outside company's policy is to contract for one fiscal year, or any part thereof, at a cost of $1 million. In addition, once the contract is signed, it is not reversible for the remainder of the year (or part thereof).

At the beginning of the year, the GLL company estimates that the costs associated with the remaining monthly security breaches, assuming only the basic security is installed, will either average $40,000 or $200,000, depending on the effectiveness of the basic security system. However, if the outside company is hired to enhance GLL's security activities, it is assumed that these breaches can be prevented. In other words, the potential additional cost savings for the year from outsourcing additional information security will either be $480,000 (i.e., 12 x $40,000) or $2,400,000 (i.e., 12 x $200,000). Either one of theses outcomes is considered to be equally likely (i.e., there is a 50% probability of either one occurring). Accordingly, the expected net value of this extra investment in information security would be $440,000 (i.e., [.5 x $480,000] + [.5 x $2,400,000] – [$1,000,000]).[4] The expected return on this extra investment would be 44% (i.e., $440,000/$1,000,000). Hence, under traditional investment decision rules, the

[4] Since the investment and cost savings are all assumed to occur in the same year, the net value is assumed to equal the net present value (i.e., the time value of money is ignored in this example).

decision would be to invest the extra $1 million dollars and the CFO should allow the CSO to spend the extra $1 million immediately (assuming the firm has a cost of capital below 44%). Of course, the actual (*ex post*) savings from this project will be either $480,000 or $2,400,000, and the net value of the investment will be either a positive $1,400,000 (i.e., $2,400,000 - $1,000,000) or a negative $520,000 (i.e., $480,000 - $1,000,000).

FIGURE 1: OPTION VALUE EXAMPLE



Contract Now
Defer for one Month
Deferment Value
t_0
t_1
. . . .
t_{12}
Revenues = 12 X $40,000 = $480,000
Costs = $1,000,000
p = .5
Low Savings Estimate p = .5
$40,000/mo
$\text{Value}_{\text{Low}}$ = [(11 X $40,000) – $1,000,000] = — $560,000
Do Not Invest
Revenues = 12 X $200,000 = $2,400,000
Costs = $1,000,000
p = .5
High Savings Estimate p = .5
$200,000/mo
$\text{Value}_{\text{High}}$ = [(11 X $200,000) — $1,000,000] = $1,200,000
EV = [($480,000 X .5) + ($2,400,000 X .5)] - $1,000,000 = $440,000
EV with Option to Defer = $1,200,000 X .5 = $600,000
EV without Option to Defer = $440,000
Value of Deferment Option = $160,000
EV = expected value
P = probability

Now let us assume that the true security breaches will reveal themselves after one month. That is, the true cost savings from the incremental security will become obvious at the end of the first month. Furthermore, let us also assume that the outside sourcing contract can be deferred for a month, although the contract price for the remaining 11 months would still be $1million (i.e., by the assumption noted above, the $ 1 million is the cost of the security contract for one year or any part thereof). Thus, at the end of one month the firm will know whether the cost savings for the remaining 11 months are $440,000 (i.e., 11 x $40,000) or $2,200,000 (i.e., 11 x $200,000). If the low cost savings is the right number, the GLL firm would not make the $1million discretionary investment because the extra cost savings is less than the extra investment. If the high cost savings is the right number, it pays for GLL to make the incremental investment because the net value of the investment is a positive $1,200,000 (i.e., $2,200,000 - $1,000,000). Since there is only a 50% probability of this latter scenario occurring, the expected value is actually $600,000 (i.e., .5 x $1,200,000). This $600,000 is greater than the $440,000 expected value if the contract for the additional security were signed immediately. As a result, it pays for the GLL firm to wait-and-see what happens with the actual breaches. In essence, the option value to defer the decision regarding the hiring of the outside security firm for additional security is equal to $160,000 (i.e., $600,000 - $440,000) and it pays to postpone the decision (i.e., to wait and see what the actual breaches look like).

The above example shows how the uncertainties associated with information security breaches may well make it quite rational to take a wait-and-see approach before allocating all funds earmarked for such activities. In other words, by deferring the decision to invest the remaining $1 million, the revelation of actual security breaches provides a clearer picture of whether or not to spend the discretionary funds. Although actual losses are expected to occur while waiting for such revelations, the expected benefits of waiting outweigh the costs in this example.

The discussion above leads us to speculate that, regardless of how the information security budget is initially derived, it may be economically sound to wait for actual breaches to occur before allocating all of the funds available for information security activities. In other words, it seems perfectly rational to expect managers in major corporations to hold back part of their spending on information security activities until actual (i.e., detected) information security breaches take place. The above expectation is based on the belief that managers in major corporations intuitively understand and use the real options approach toward information security expenditures (i.e., formal computation of the actual option value, as done in the above example, is not necessary). Of course, in many companies, the people actually held responsible for security breaches (e.g., CSOs) often prefer to prevent more, rather than less, breaches, even where the economics of the situation argue in favor of the reverse situation. On the other hand, those not held directly responsible for security breaches (e.g., the CFO) may prefer to wait and see. Thus, Stefan and Mary (from our opening story) may have good reason to exhibit differing views about the desirability of spending the extra money on security.

III. EMPIRICAL EVIDENCE

Anecdotal evidence in the popular press clearly supports the above discussion regarding the real options, or "wait-and-see," approach toward information security expenditures. For example, when Microsoft Corp. experienced hacker attacks against its Internet activities in 2001, it immediately hired an outside company to run a backup directory for its major Websites (Bridis, 2001). In order to further examine this real options argument for investments in information security activities, we gathered data from a group of firms to see how actual security breaches affect their actual expenditures on security related activities. In other words, we wanted to see if most organizations use actual security breaches in a manner that is consistent with the real options perspective. Thus, our concern in this study is with the effect of an actual (rather than expected) security breach on the actual expenditures for information security activities.

Based on a survey of senior information security officers from 199 firms, drawn from InformationWeek.com 2000 list of technology-savvy firms, we had 38 senior managers respond to the following statement.[5,6]

> **Irrespective of how much our firm initially planned to spend on information security, a critical determinant of the actual expenditures on information security is the fact that an actual information security breach has occurred.**

The response to the above statement was in terms of a 7-point scale concerning the level of agreement with the statement (i.e., 1 indicating Strong Disagreement and 7 indicating Strong Agreement). In addition, respondents were able to provide responses to open ended questions. As can be seen in the histogram illustrated in Figure 2, the responses to the above statement are quite varied. However, the majority of respondents did indicate that an actual security breach is an important factor driving actual expenditures on information security (i.e., 21 of the 38 respondents circled a 5, 6, or 7 on their level of agreement with the statement provided above). Thus, the findings tend to support the anecdotal evidence that a large percentage of firms increase actual expenditures on information security following a breach. In other words, security breaches are apparently an important driver of actual expenditures on information security activities. Comments from numerous participants on the open-ended questions provided additional confirmation of this point. In fact, based on the responses to

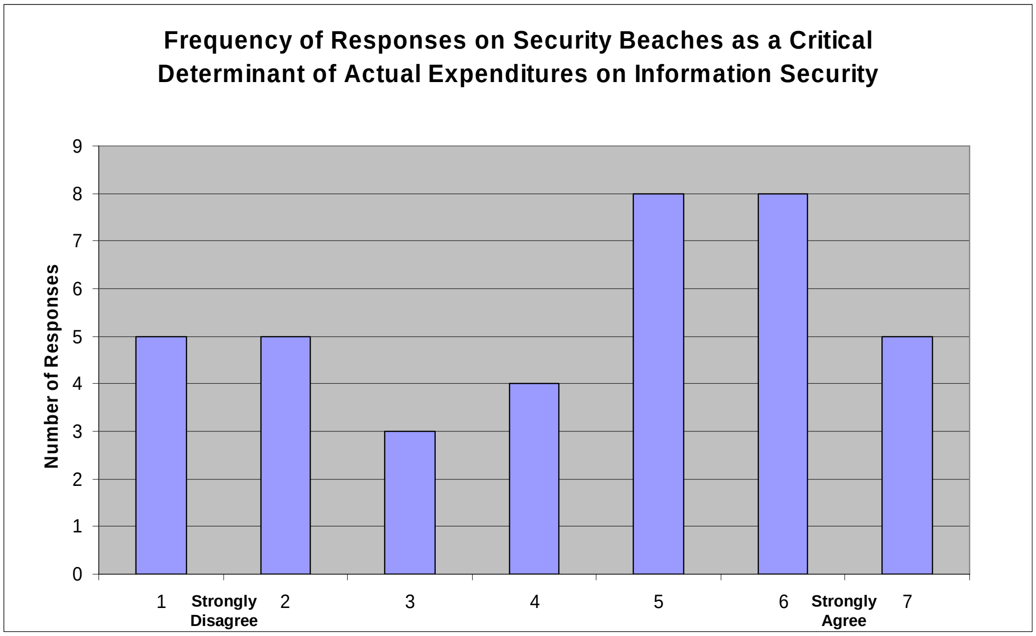
[5] The 38 out of 199 firms represent slightly more than a 19% response rate. Given the confidential nature of the issue under investigation, this is considered a good response. In fact, compared to other studies related to information security, the 19% is quite high (Power, p. 30).

[6] The data gathered for examining the real options argument discussed in this paper was part of a larger study concerned with the process used by firms in making decisions regarding information security expenditures.

the open-ended questions, it would appear that actual breaches provide a clear path for a quick, and often large, infusion of funds for information security activities in many firms. Some of the respondents went so far as to note that security breaches represent the easiest way to get senior management's attention regarding the need to increase expenditures on information security related activites.

The findings discussed above are consistent with the real options argument presented earlier. It is interesting to note that some of our respondents pointed out in the open-ended questions that the breach need not be real to generate quick, and large, infusions of new funding for security activities. A mock breach, based on an authorized auditor security attack, was sufficient. Of course, auditors and consultants have long recognized the importance of such penetration tests. However, our study points out the immediate impact that such tests can have on the information security expenditures of a firm. Indeed, as noted in an informal conversation with the CFO of a major corporation (one that not included in the study described above), the very purpose of a penetration test is to see if, and where, the firm needs to revise its approach toward expenditures on information security activities. A fertile area for future research is to conduct a controlled study of such penetration tests across a large number of firms. Such a study could focus on the key expenditure reactions firms have to security breaches, as well as ways to prevent such breaches in an economically feasible manner.

FIGURE 2: SECURITY BREACHES AS A DRIVER OF EXPENDITURES ON INFORMATION SECURITY



Although not directly examined in this study, the respondents clearly alluded to the fact (in the open ended questions) that all breaches are not the same. In other words, there is a high correlation between the amount of additional expenditures approved for information security activities and the severity (in terms of impact on the firm) of the breach. In essence, the respondents seem to be taking a sequential approach to the deferment option.

As breaches are detected, a carefully measured level of incremental expenditures on information security takes place. Of course, this approach is also consistent with the real options view of expenditures on information security.

IV. CONCLUDING COMMENTS

It is well documented that information security breaches have been growing rapidly and are now common among most organizations. The growth in these breaches is due largely to the expanding use of the Internet and the related interconnectivity among information systems.

Expenditures to prevent information security breaches have also been growing rapidly in recent years. However, a large portion of these expenditures seem to be made on a "wait-and-see" basis. More to the point, the empirical evidence provided in this paper supports the argument that one key driver of actual expenditures on information security activities is the occurrence of actual security breaches. This reactive, as opposed to proactive, approach toward a significant portion of information security expenditures is consistent with the real options view of capital investments. Hence, such behavior on the part of senior managers (including CSOs) is consistent with a rational economic perspective toward preventing security breaches in a cost-efficient manner.

Bibliography

Bridis, T., "E-Business: Microsoft Takes Steps to Thwart Hacker Attacks," *The Wall Street Journal* (January 29, 2001, B4).

Gordon, L. A., Managerial Accounting: Concepts and Empirical Evidence (McGraw-Hill, Inc., N.Y., 5th Ed., 2000).

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

Gordon, L.A. and M.P. Loeb, "Budgeting Process for Information Security Expenditures: Empirical Evidence," (Working paper, 2003).

Horn, W. Matthews, "Feds Still Fail Security," *Federal Computer Week*, Dec. 2, 2002, http://www.fcw.com/fcw/articles/2002/1202/pol-horn-12-02-02.asp

Lyman, J, "In Search of the World's Costliest Virus," *NewsFactor Network*, February 21, 2001, viewed at http://www.newsfactor.com/perl/printer/16407/

Pindyck, R. S., "Irreversibility, Uncertainty and Investment," *Journal of Economic Literature* (September 1991), pp. 1110-1148.

Power, R., "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Journal*, Vol. 18, No. 2 (Spring 2002), pp. 7-30.