We conducted an empirical study to examine the way corporations make decisions regarding information security expenditures. This study assessed whether firms approach the budgeting process for information security expenditures in a rational economic manner based on cost-benefit analysis. (We view budgeting and financial planning as synonymous in this article.)

Information security is primarily concerned with ensuring the confidentiality (protecting private information from unauthorized individuals), availability (providing timely access to information to authorized users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information. Authentication (ensuring that persons using the system are who they claim to be) and nonrepudiation (ensuring that a legitimate user cannot deny actually using the system) are also concerns of computer security. Additionally, firms must be able to detect and correct information security breaches once they occur. Thus, information security relates to an array of actions designed to protect information and information systems.

Empirical evidence shows that cost-benefit analysis is a sound basis for budgeting information security expenditures.

Despite prevention efforts, information security breaches are common. The largest body of research related to preventing breaches is technical, focusing on such concerns as encryption and access controls. In contrast, the research related to the economic aspects of information security is small but rapidly growing [1, 2, 4–6]. Yet, little is known about the budgeting process used in deciding how much to spend on information security.

The costs associated with information security activities relate to a host of items, including hardware, software, and personnel. Most of these expenditures are best thought of as capital investments, although firms tend to treat such costs as operating expenses within the period incurred. Whether they are treated as capital or operating expenditures, budgeting for information security expenditures is a crucial resource allocation decision. From an economics perspective, firms should invest up to the point where the last dollar of information security investment yields a dollar of savings. That is, information security expenditures should be viewed in cost-benefit terms.
A well-established rational economic process used for budgeting capital investments applies cost-benefit analysis using the net present value (NPV) model. This process consists of estimating and comparing the risk-adjusted discounted present value of expected benefits with expected costs. Although the use of the risk-adjusted discounted cash flow techniques does not guarantee higher firm performance [7], such techniques move organizations toward a more efficient allocation of resources. Accordingly, it seems logical for managers to use the NPV approach in budgeting expenditures for information security. Unfortunately, it is rarely possible to use completely rational economic models of cost-benefit analysis (for example, the NPV model) in budgeting for information security. Although the expected costs related to information security activities can usually be estimated with a reasonable degree of accuracy, the same cannot be said for estimating the expected benefits. Estimating the expected benefits requires users to have information on potential losses from security breaches and the probability of such breaches.

Use of the NPV approach to derive an optimal expenditure level can be regarded as an ideal economic approach for budgeting information security expenditures. This approach is considered ideal because it forces firms to compare (in monetary terms) risk-adjusted expected benefits to anticipated information security expenditures. As long as the monetary value of the anticipated incremental benefits exceeds the incremental expenditures, additional expenditures would be warranted.

Short of this ideal approach, it is possible for firms to take a modified economics approach to planned information security expenditures. For example, managers may quantify the estimated potential benefits from preventing information security breaches without quantifying the probability of such breaches occurring. Alternatively, managers could quantify the probability of security breaches without quantifying the estimated loss resulting from such breaches. Another possibility is that both the potential losses and the probabilities of such losses occurring are considered, but neither is actually quantified. Under these scenarios, the manager could intuitively compare the potential incremental benefits to the incremental costs of information security activities. This intuitive comparison could result in categorizing the expected net payoff from such costs (the difference between the expected benefits and costs) as high, medium, or low.

Some managers may merely adjust the previous period’s budget to derive the next period’s information security budget. Thus, some sort of incremental budgeting approach may be the key factor driving information security expenditures. Alternatively, managers may view information security expenditures as must-do projects to be carried out irrespective of any cost-benefit analysis. This discussion suggests two research issues that should be addressed in order to better understand the process used by firms in planning (budgeting) for expenditures on information security. These issues are posed in two general questions: Do firms use economic analysis in deciding on planned expenditures for information security? What are the key factors driving and impeding the use of economic analysis by firms in deciding on information security expenditures?

**Empirical Study**

An empirical study was conducted using a survey instrument to examine the research questions. Based on a 7-point scale, respondents were asked to indicate their level of agreement (with 1 indicating Strongly Disagree and 7 indicating Strongly Agree) with a series of statements. The survey instrument also included open-ended questions.

The sample firms were selected from InformationWeek.com’s 2000 list of technology-savvy firms, subject to the constraint that the firm was also included in the Standard & Poor’s (S&P) 500 Index. InformationWeek.com’s (publicly available) list of firms pro-
vides the names of the senior IT managers for each of these firms, allowing us to send the questionnaire to specific individuals with decision-making responsibility for information security expenditures. Limiting the sample population to S&P 500 firms guaranteed that all respondents represented large U.S. corporations. The survey was mailed to 212 firms. A cover letter assured anonymity of individuals and firms participating in the study. Three months after the first mailing, a second mailing was conducted. Due to changes in jobs and incorrect addresses, the final sample population was reduced to 199 firms.

A total of 38 responses were received. Given the sensitive nature of the issue under study, a response rate of slightly over 19% is viewed as good. More important, the returned surveys were completed by individuals with firsthand knowledge of their firm’s information security, as evidenced by both their position and time in position. Thirty-five of the respondents provided data on their job title and years of experience. The job titles range from Chief Information Security Officer to Vice-President for Information Security. The mean number of years in their respective positions is 3.2 years, ranging from six months to 14 years. The study participants also provided a rich set of data on the information security expenditures within their firms via the open-ended questions. A check was made for both nonresponse bias and internal reliability of the questionnaire. Statistical tests showed that nonresponse bias was not a problem, and the instrument demonstrated a high degree of internal reliability.

The respondents indicated their firms’ concerns with information security breaches are related to protecting information from unauthorized intrusions (confidentiality); ensuring the availability of information to authorized users; and assuring the integrity of information. Thus, the respondents considered issues at the heart of this study.

Several parts of the survey addressed aspects of the first research question: Do firms use economic analysis, in one form or another, in deciding on planned expenditures for information security?

At the beginning of the instrument, respondents were asked to indicate the extent to which they agree with Statement #1: Our firm usually decides on how much to spend on information security by comparing the present value of future benefits expected from such security to its associated costs. In essence, the respondents were being asked whether their firms use an NPV approach in making information security budgeting decisions.

As illustrated in the figure on the opposite page, some respondents claim to use NPV analysis in their decisions to invest in information security. Considering responses of 5 or higher as representing a respondent’s claim to be using NPV analysis, nine respondents out of 38 made such a claim. The responses to our open-ended questions, for these nine firms, confirm that they tend to take an NPV analysis approach toward infor-
impeding the use of economic analysis by the firms in planning expenditures for information security? Since NPV analysis is viewed as providing a well-established economic process for budgeting information security expenditures (investments), our survey instrument was designed to permit an examination of the following specific question: What drives the use of NPV analysis for information security expenditures? The most likely answer, based on conversations with information security managers and previous case studies, is that the use of NPV analysis is largely driven by the ability to estimate the benefits from information security expenditures.

In order to test this argument, we regressed (see Equation 1) the responses to Statement #1 concerning a firm’s use of NPV analysis on the responses to Statement #2 contained in the survey instrument, regarding a firm’s ability to estimate the future benefits from information security: Statement #2. In our firm, it is not possible to estimate the future benefits expected to be derived from information security investments. Since statements in the survey instrument relate to the inability to estimate future benefits from information security expenditures, we would expect to see a negative relation between X and Y in equation (1):

\[
Y = b_0 + b_1 X, \quad (1)
\]

where 
\[Y = \text{response on Statement } #1\]
\[X = \text{response on Statement } #2\]
\[b_0 \text{ and } b_1 \text{ are parameters of the Equation.}\]

The analysis of the data shows that the use of NPV is negatively correlated (and significant beyond the .01 level) with a firm’s inability to estimate future benefits from information security. Thus, the ability to estimate benefits from expenditures on information security is a key factor driving the use of NPV analysis.

Regression results show an association rather than a cause-effect relation, and statistical tests cannot prove a hypothesis. Nevertheless, the results support the argument that the ability to estimate benefits is a key factor driving the use of NPV analysis in decisions concerning the level of expenditures on information security.

As discussed earlier, the fact that a firm does not use NPV analysis in deriving the planned expenditure level for information security does not mean complete abandonment of the economic approach to such expenditures (that is, NPV analysis is an extreme form of rational economic analysis). Indeed, firms may use modified forms of economic analysis for such expenditures. Thus, we examined whether the firms explicitly consider the potential losses from security breaches and the probabilities of such losses. This was

The ability to estimate benefits is a key factor driving the use of NPV analysis in decisions concerning the level of expenditures on information security.
accomplished by first separating the responses into three groups based on their level of agreement with the following survey statement related to the potential loss from a security breach: Statement #3. The potential loss (in economic terms) associated with an information security breach is a critical factor in determining the amount spent on information security.

Respondents who circled 5, 6, or 7 (the high end of agreement with this statement) were placed in the first group, and those respondents who circled 1, 2, or 3 (the low end of agreement) were placed in the second group. Respondents in the third group were those who circled 4 as their response to this statement. Respondents were also separated into three similar groups based on the level of agreement with the following survey statement related to the probability of a security breach: Statement #4. The likelihood (that is, probability) that an information security breach will occur is a critical determinant of the planned amount of expenditures on information security in our firm.

For statements 3 and 4, the group of respondents in the high end (the first group) was then compared to the group in the low end (the second group) in terms of their response to the earlier-noted statement on the use of NPV analyses. Respondents were also grouped as high-end users of NPV analysis if they circled a 5, 6, or 7 on the statement concerning use of NPV and as low-end users if they circled a 1, 2, or 3. The respondents circling a 4 on any of the statements discussed here were deleted from the analysis as they did not agree or disagree with the statement. Based on this form of extreme group testing, contingency tables were prepared to examine the relation between the potential loss associated with a security breach and the use of NPV analysis, as well as the relation between the probability that such a loss would occur and the use of NPV analysis (see Panels A and B of the table on page 123).

An analysis of the contingency table data shows that whether they are using NPV analysis or not, a substantial number of respondents consider the potential loss from an information security breach and the probability that such a breach would occur in planning the level of information security expenditures. In fact, 19 of the 22 respondents consider these factors to be important, even though only 7 of the 22 respondents have a high use of NPV analysis. Based on the Fisher Exact test, these results clearly suggest that the potential economic loss and probability of a security breach are important issues in deciding on the planned level of expenditures for information security activities whether or not NPV analysis is used. The responses to the open-ended questions indicate that the key distinction between the users and non-users of NPV analysis appears to be in terms of their reliance on quantifying these factors.

In sum, senior information security managers apparently do use some form of economic analysis in budgeting for information security. Our analysis shows that some of the participants approach information security expenditures with a formal NPV analysis, whereas other respondents approach these expenditures with a modified economic analysis. The modified approach consists of examining the costs and benefits of information security activities, but with less emphasis on formally quantifying the benefits. However, based on the responses to the open-ended questions, there seems to be a movement toward using more economic analysis in evaluating information security activities. However, on the open-ended questions, a few respondents noted the budgeted expenditure level on information security for their firms is largely driven by such items as the past year's budget, best practices in the industry, or a must-do approach.

REFERENCES

This study was partially supported by the DoD, Laboratory for Telecommunications Sciences, through a contract with the University of Maryland Institute for Advanced Computer Studies (UMIACS).

Lawrence A. Gordon (lgordon@rhsmith.umd.edu) is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance in the Robert H. Smith School of Business at the University of Maryland, College Park, MD. Martin P. Loeb (mloeb@rhsmith.umd.edu) is a professor of Accounting and Information Assurance in the Robert H. Smith School of Business at the University of Maryland, College Park, MD.

Gordon and Loeb are the authors of Managing Cybersecurity Resources: A Cost-Benefit Analysis, McGraw-Hill.