Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2006 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2006

Portfolio approach to information technology security resource allocation decisions

Shivraj Kanungo
The George Washington University, kanungo@gwu.edu

Portfolio approach to information technology security resource allocation decisions

Shivraj Kanungo
Department of Decision Sciences
The George Washington University
Washington DC 20052
kanungo@gwu.edu

Abstract

This paper presents a portfolio optimization approach to information technology (IT) security investment decisions in an organization. This approach has been motivated by the extreme variations that are found in IT security requirements for organizations in addition to the diversity of starting conditions found in organizations that choose to embark on a formal approach to managing their security. Often, a budgetary allocation is made for IT security and IT managers and management are faced with the problem of how to allocate these monies or resources across competing projects and products that can potentially improve or enhance IT security in an organization. Instead of ranking or rating the various alternatives based on their benefits only, it is demonstrated how, by identifying organizational objectives, and then aligning the decisions with the objectives, one can optimally allocate resources across the IT security portfolio. The approach in this paper has been to provide a generic decision framework that can be customized by practitioners and fine-tuned by other researchers. The approach is explained and then the results are discussed using a case study. Both the strengths and weaknesses of this approach are highlighted and suggestions for how this approach can be deployed and enhanced are provided.

Keywords: IT security, resource allocation, decision theory, analytic hierarchy process, optimization

Introduction

Spending on IT security is projected to grow by 24 percent (compounded annually) between 2001 and 2006 (Roberts 2003). Organizations are spending heavily not only on IT security but also on security in general. As the IS function matures, many organizations have a formal information system plan (which may include an IT plan also). This implies that there exists a formal IS strategy that is aligned with the organizational strategy. In such cases, we can assume that the information security plan would be part of the larger IS plan. By implication, since the information security plan would be derived from, and consistent with, the IS plan, it would also be aligned with the organizational strategy. The issue of spending on IT security is well summed up by Levinson (2002) who quotes an IT professional, “we have no fear of spending money, but we have to do it wisely.”

According to Swanson et al. (2003), resource allocation responsibilities, in various forms, reside with the head of the organization, the CIO, the security program manager and the program manager or the system owner. The ultimate responsibility, however, resides with the head of the organization. While Swanson et al. (2003) refer to federal government agencies, this distribution of responsibility holds for any organization in general. The implication of such shared and ultimate responsibility is that every decision maker and (preferably) every organizational stakeholder needs to understand why certain decisions were taken, how they were taken and the implications of such decisions going wrong. The problem for any manager requesting funds is to convince budgetary authorities to allocate the requisite resources (most typically, funds). The problem for the individual(s) who make the allocation decision is to understand the need for such funds and then make decisions well aware of the tradeoffs that may ensue. In essence, information security decisions, like many decisions, need first, a transparent decision process and second, a parsimonious way of communicating the decision framework.

In essence, IT security resource allocation decisions require significant organizational investments. The goal of such decisions is to maximize the value of such investments (whether one time or ongoing). The objective of this paper is to present one such decision making framework that helps organizations analyze and understand their security concerns in addition to helping them leverage their investments in information security.

The paper is presented as follows. First the IT security investment problem is described and definitions of key terms are provided. Then a portfolio optimization approach to the problem is proposed. Such and approach is justified primarily by invoking the contextual and unique nature of IT security needs of an organization. Then the application of this approach is presented using a real life case study to explain how the model was developed and how the results can be interpreted. The paper is concluded by pointing out some weaknesses of this approach as also highlighting the strengths. In addition suggestions for improving this framework are also made.

Problem description

In an organization, information security or information technology security often rears itself as a critical issue. This means that organizations often wake up to security problems when they actually encounter (or expect to encounter) a security-related incident or when a security incident has occurred in another organization that this proximal to itself increasing the likelihood of its happening in that organization. Alternatively, organizations can be mandated by regulatory bodies to meet minimum security standards.

Budgetary processes are instrumental in driving most investment decisions in organizations (OMB 2005). Given that IT security-related decisions fall into the critical category and that there is often a regulatory deadline or high opportunity cost associated with making mistakes with such decisions, there are two, often, conflicting goals in this decision-making situation – (a) take a decision expeditiously and, at the same time, (b) exercise due diligence.

The decision is often compounded by the fact that there always so much to do when it comes to IT security simply because there are so many potential vulnerabilities in any organizational system (not just the information system). Apart from the information technology infrastructure (that, among other things, includes networks, databases and applications), organizational processes have to be made secure just as people have to be trained to change their security related behaviors. Not only does this take high initial investment, it also requires a continuous stream of recurrent investments to reinforce and sustain the existing standards of IT security.

As a result, the IT security investment decision is one that needs to be made every year in order to reassess the IT security goals and realign investments (or spending) with those goals. The nature of organizational decision-making is not perfect. Prevailing organizational biases and tensions due to competing demands for the same set of resources and the lack of perfect information require that tradeoffs be made and in doing so judgments be used. Judgments are subjective and we need to encapsulate such subjectivity in a meaningful way. For instance, when comparing two security products (say, firewall), regardless of how carefully we develop criteria to compare them, there will eventually remain a level of subjectivity when we compare these products based on those criteria. More importantly, when we attempt to evaluate the "value" of an investment in IT security such an evaluation is necessarily multifaceted and complex.

The research motivation for this paper was provided by Bodin et al. (2005) who have identified the need for using quantitative measures (like NPV) and Gordon and Loeb (2006) who have identified AHP as one of the approaches to resource allocation in IT security decisions. While both papers attempt to provide a basis to make meaningful investments for IT security, there gaps that can be addressed. For instance, Gordon and Loeb (2006) acknowledge that the ability to accurately estimate benefits is a key factor in using NPV effectively. However, as Rodewald (2005) has observed ROI is a poor metric to use when comparing IT security investments to investments that yield a tangible return. So, in this paper, a multi-attribute measure to evaluate IT security benefits is suggested. Secondly, Bodin et al. (2005) have suggested that the ratio of benefits to costs may be a better metric to employ when making resource allocation decisions in the context of IT security. It is shown that such an approach may not be indeed so and that focusing on benefits is the most optimal approach.

Methodology

Linear programming approach is combined with the analytical hierarchy process to demonstrate how IT security investments can be effectively leveraged by an organization. While every organization has its own specific goals IT-security related objectives, we present a somewhat generic approach (that can be customized by other users) by identifying three broad objectives (G1, G2 and G3) based on security service categories shown in Table 1.

Security service	Category	Description
Security Program (C11)	Management (G1)	Management objectives: are those that have to do with the organization's overall computer security program.
Security Policy (C12)		

Risk Management (C13)		These goals are met based on how well the computer security program and risk are managed within the organization. These could include meeting regulatory compliance and minimize enterprise-wide disruptions.
Security Architecture (C14)		
Certification and Accreditation (C15)		
Security Evaluation of IT Products (C16)		
Contingency Planning (C21)	Operational (G2)	Operational objectives: are focused on controls implemented and executed by people (as opposed to systems). For these goals to be met technical or specialized expertise that rely on management activities and technical controls need to be in place. These goals could include meeting a certain level of diffusion of personal firewalls in the organization and ensuring a certain cycle time for recovering from a virus attack.
Incident Handling (C22)		
Testing (C23)		
Training (C24)		
Firewalls (C31)	Technical (G3)	Technical objectives: have to do with security controls involving a computer system. These goals depend on the proper functioning of the system. These goals could include an upper bound on the number of successful virus attacks or ensuring that a certain minimum number of computers are part of a third-party authentication framework.
Intrusion Detection (C32)		
Public Key Infrastructure (C33)		

Table 1. Security services and goals (Adapted from Grance et al., 2003, p. 5-1)

The logic of the approach is that the resources being invested in IT security have to be *aligned* with the IT security goals. Once the objectives are identified and the alternatives identified (these are projects or initiatives that are shown in Appendix A), the criteria are established to evaluate how well a certain alternatives meets a particular aspect of a goal. These are shown in Table 1 in the first column. For instance the management objective has six components. For instance C23 is the third criterion for the second goal. An alternative is evaluated on how important it is to meeting the requirements of each component. Based on this the decision hierarchy that we develop is shown in Figure 1. The 8 alternatives (A1 through A8) are shown hanging from each of the criteria that have been identified. The decision hierarchy also shows that at each node we have a comparison matrix, the order of which is the number of elements being compared. For instance, at the goal node, the comparison matrix is of order 3, since there are three goals being compared.

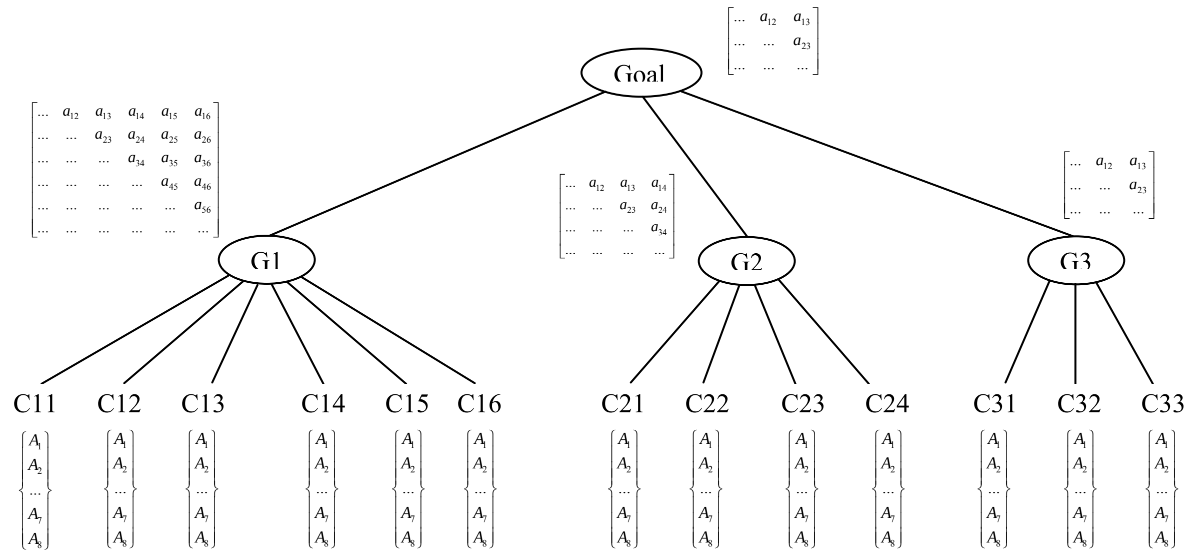


Figure 1. The AHP hierarchy used to generate priorities for the eight projects shown in Appendix A

The approach to constructing the AHP hierarchy in this paper departs from that adopted by Gordon and Loeb (2005) in that the goal of IT security is designed to be maximally aligned with that of the organizational goals. Hence, one does not necessarily have to limit themselves to technical criteria. Using this approach allows an organization to adopt a more integrative approach toward conceptualizing and budgeting for IT security. Using this tree, relative importance of the goals is measured using pair-wise comparison. This step is repeated for the criteria to evaluate each alternative. After prioritizing the objectives, the IT security alternatives are scored, using either pair-wise comparisons (which can be tedious) or absolute rating scales and utility curves (typically non-linear). Once the final priorities for the alternatives are obtained, they are subjected to sensitivity analysis to ensure that the judgments are valid. The complete set of results are shown in Appendix B.

Following this, the portfolio for benefits subject to funding is optimized based on dependency and other constraints. The typical form for this optimization would be

$$\text{Maximize Expected value of IT security Benefits} = \sum_{i=1}^{n} B_i$$

Subject to

1. Budget constraint
2. Dependency constraint (if x is funded, then y has to be funded or not funded)
3. Some projects can be partially funded while other can not be
4. Specific constraints

Where B_i is the benefit associated with the i^{th} project. B_is can be generated as AHP priorities (since they are generally qualitative) or by some other method. In this study ExpertChoice version 11.1.3628 was used to generate "benefit" priorities using the AHP hierarchy shown in Figure 1. These computations can also be accomplished using Microsoft Excel and the built-in optimizer (the Solver Addin).

Data and Analysis

In this section the data are presented that were be used to allocate resources among IT security alternatives. Issues such as which projects are funded and why, what the tradeoffs are, what the nature of those tradeoffs are, and what are the implications of using different approaches to allocating resources for IT security initiatives are scrutinized. Table 2 shows the benefits derived using the AHP structure shown in Figure 1 (See Appendix B). A1 through A8 are the leaf nodes for the tree shown in Figure 1. The available budget is taken to be $200,000 (See Appendix A).

Project Id	**Project definition**	**Benefit**	**Cost ($)**
A1	End user training (training programs and online material development)	0.082	56000
A2	End user support (firewall and anti virus software)	0.124	24000
A3	Upgrade and maintain server for firewall	0.108	25000
A4	Revise and improve security process audit and quality office process	0.078	43000
A5	Establish IT security task force (for security planning and coordination)	0.053	25000
A6	Establish separate security program office (for SOX and regulatory compliance reporting)	0.123	75000
A7	Security operations group training (5 programs per year)	0.073	59000
A8	Email spam filter enhancement	0.053	12000

Table 2. List of all the projects, their benefits and the associated costs

Three approaches are presented to allocated resources across IT security projects. They include benefit maximization, benefit to cost ration maximization and maximization of benefits using linear programming.

Benefit maximization

When attempting to maximize benefits the project that provides the maximum benefit is chosen and selected to be funded. Then the project with the next highest benefit is picked select to be funded and this process continues till the budget is exhausted or the next project to be funded makes the total cost exceed the available budget. Table 3 shows that if project A4 is funded the total allocation exceeds the budgeted amount of $200,000.

Project Id	**Benefit**	**Cost**	**Cumulative cost**
A2	0.124	24000	24000
A6	0.123	75000	99000
A3	0.108	25000	124000

A1	0.082	56000	180000
A4	0.078	43000	223000
A7	0.073	59000	282000
A5	0.053	25000	307000
A8	0.053	12000	319000

Table 3. Benefits, costs and cumulative costs for the projects sorted by benefits

Total benefits add up to 0.694 and the actual benefits (from the projects that were funded) add up to 0.437. Similarly all the benefits to cost ratios add up to 2.218E-05 and the total of benefits to cost ratios of projects that were actually funded add up to 1.259E-05[1]. Hence the effectiveness of this allocation from a benefit maximization perspective is 63.0%[2]. Similarly, the effectiveness of this allocation from a benefit to cost maximization standpoint is 56.8%.

Benefit/cost ratio maximization

The approach to maximizing the total of benefit to cost ratios is identical to the approach for maximizing benefits. The primary difference is that instead of using benefits to select projects, benefits to cost ratios are used to make the selection. Table 4 shows the projects sorted in descending order based on the benefit/cost ratio. The project with the highest benefit to cost ratio (in this case project A1) is chosen to be funded, followed by the project with the next highest benefit to cost ratio and this process continues till the budget is exhausted or till the next project to be funded makes the total allocation overshoot the available budget. Note that by employing this approach one is able to fit in one more projects into the available budget. While, budget utilization was not an explicit goal, this approach has been able to increase benefits in such as way that more projects are funded.

Project Id	**Benefit**	**Cost**	**Benefit / cost**	**Cumulative cost**
A1	0.124	24000	5.167E-06	24000
A8	0.053	12000	4.417E-06	36000
A3	0.108	25000	4.320E-06	61000
A7	0.053	25000	2.120E-06	86000
A5	0.078	43000	1.814E-06	129000
A2	0.123	75000	1.640E-06	204000
A4	0.082	56000	1.464E-06	260000
A6	0.073	59000	1.237E-06	319000

Table 4. Benefits, costs, benefits/costs and cumulative costs for the projects sorted by benefits/costs

[1] *Actual* total benefits are composed of all the benefits above the dashed line in Table 3. Similarly *actual* total benefits to cost ratios are computed from the same set of projects that are above the dotted line.

[2] (0.437/0.694)∗100 = 63.0%

Using this approach and as shown in section 4.1, the effectiveness of allocation from a benefit maximization standpoint is 59.9% and from a benefit to cost maximization standpoint is 80.4%.

Benefit maximization with budget constraints

In this approach linear programming (LP) is used to maximize benefits subject to budget constraints.

The canonical form of the generalized LP formulation becomes

Maximize **IT security benefits** = $\sum_{i=1}^{n} B_i F_i$

Subject to the following constraints

$$\sum_{i=1}^{n} C_i F_i \leq Budget$$

All F_is are integers that can take a value 0 or 1

Where

B_i = benefit associated with alternative i
C_i = cost associated with alternative i
F_i = decision variable associated with alternative i

For this problem, B_is and C_is are obtained from the benefits and cost columns respectively in Table 2. Solving for F_is, we obtain the following solution: $F_1 = F_3 = F_4 = F_5 = F_7 = F_8 = 1$ and $F_2 = F_6 = 0$. This implies that projects/initiatives 2 and 6 are not funded; everything else is. Using this approach the effectiveness of allocation from a benefit maximization perspective is 71.76% and from the benefits to costs ratio standpoint is 87.03%. Table 5 summarizes the results.

Approach	**Effectiveness of allocation with respect to**	
	Benefits	**Benefits/Costs Ratio**
Benefit maximization	63.0%	56.8%
Benefit to cost maximization	59.9%	80.4%
Linear Optimization	71.67%	87.03%

Table 5. Effectiveness of three resource allocation approaches from the benefits and benefits/costs ratio perspectives.

Table 5 clearly shows that the optimization approach is much more effective than the either the benefit maximization or the benefits/costs maximization approach.

Discussion

The issues of how and why one obtains better resource allocation effectiveness when we one uses LP and why it makes sense in the context of IT security investments is taken up for discussion. Subsequently, how this approach has been able to meet the two decision objective that had identified in the beginning of the paper is taken up for discussion.

In terms of IT security portfolio decision effectiveness, it is clear from Table 5 that a singular focus on IT security benefits fails to provide the most effective allocation policy for IT security resources. Figure 2 shows a comparison of IT security resource allocation approaches by using three efficient frontiers for each of the allocation approaches. The numbers above the arrows show the number of projects that can be funded using a particular approach. For instance using the benefits only approach (Section 4.1) we can only fund four projects.

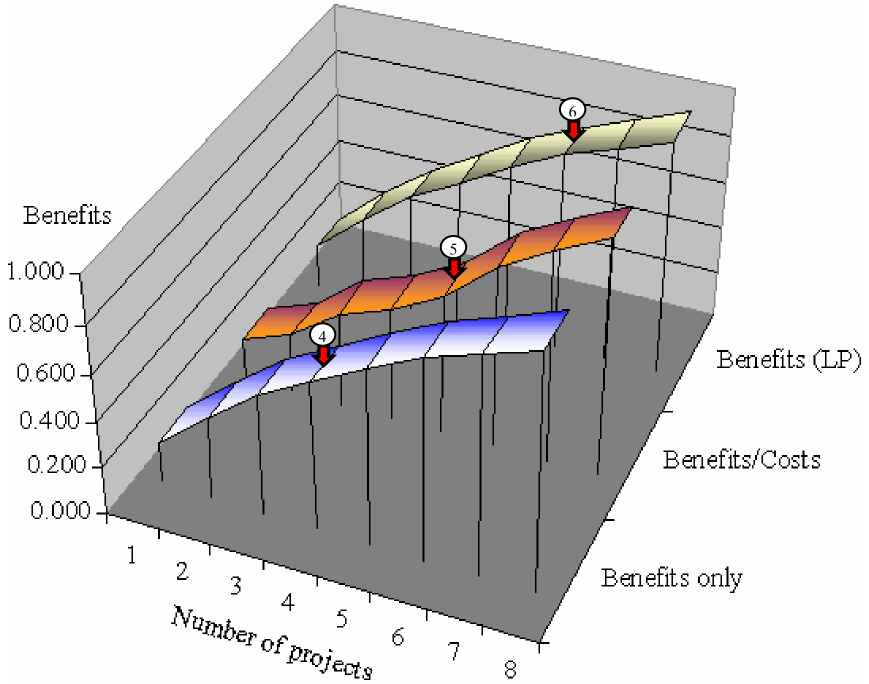


Figure 2. Comparative effectiveness for resource allocation strategies.

Interestingly, the approach that has been advanced by Bodin et al. (2005) is shown to be the least effective. They propose that the ratio of benefits to costs can be used to provide more “bang for the buck.” However, as the second efficient frontier (based on the benefits/costs ratio) shows, the efficiency, in terms of maximizing benefits, is consistently lower than the other two approaches. So, while the effectiveness of this approach is more than that of relying purely on benefits to allocate resources, it is less effective than the LP-based resource allocation approach. While this may not always be so (Forman 2001), the LP-based benefit maximization approach makes sense because our aim is to maximize the benefits associated with IT security. The goal in the approach adopted in this paper is not to spend as much of the budgeted amount as possible. While the latter may be a realistic organizational goal (to avoid budget reductions in subsequent budgeting cycles, especially in organizations that practice zero-based budgeting), it is far more important to "spread" the investment. From an IT security perspective it is more important to provide coverage for all identified areas of vulnerabilities than to optimize one or two selected areas. Therefore, it is more effective to fund two smaller IT security projects, the combined value for which may be (marginally) more than one large project that may send the cumulative cost over budget.

It has been shown that the proposed method for making IT security portfolio decisions is parsimonious. This shows that one of the goals of decision-making in the context of IT security has been met. As mentioned in the beginning of this paper, one of the goals of decision making in the context of IT security is to take decisions expeditiously. This implies that a parsimonious decision making framework is needed – one that helps decision makers take the best decision without investing unreasonable time and resources. While there are alternative approaches as those suggested by Butler (2002), Gordon and Loeb (2006) and Cavusoglu et al. (2004), they are encumbered by the need to collect a large body of information that is either composed of rare events (IT security failures and associated estimates of costs that can be attributed to such failures) or a series of estimates.

The suggested approach is also extensible in that if, the goal was to minimize risk, then instead of assessing benefits, risks could be expressly addressed. In addition, if benefits are combined with risks, one could compute expected benefits. This could done so by computing risks for each alternative using a separate AHP model and use the priorities that are generated as probabilities of failure (p) associated with the different project. The expected value of each of the alternatives could then be obtained by multiplying benefits by (1-p,) the probability of success.

The approach to IT security decisions presented in this paper also meets the objective of ensuring due diligence. Identifying the organizational IT security goals and further by identifying the criteria that are used to evaluate how these organizational security goals are met, not only ensures that the decision problem is fully enumerated (from a completeness perspective), but also ensures that an organization responds to IT security issues that are specific to its context – and not generic security that form part of the "best practices" approach. Neubauer et al. (2005) have identified the criticality of organization-specificity in the context of IT security related investment decisions.

Conclusion

This paper has shown how to formulate the IT security portfolio decision as one where multiple alternatives (initiatives or projects) can to be evaluated based on multiple criteria (some of which may be subjective) in order to meet multiple goals (many of which may conflict with each other). A generic approach to IT security resource allocation has been provided that is flexible and can be customized for any organization. In doing so, it has been demonstrated how IT security investments decisions can be maximally aligned with the organizational security goals. In addition, given the absence of a normative basis to judge how good a decision is, it has been shown how to optimize IT security resource allocation decisions keeping in mind the organizational context and other singularities that are specific to the decision at hand. This work can be extended and enriched by incorporating constraints that are not budgetary. These include those constraints that involve "must fund" projects, dependency constraints (if project A is funded then project B has to be funded or if project A is funded then project B can not be funded) and constraints that allow projects to be partially funded.

In summary, it is believed that the proposed approach to IT security resource allocation will allow an organization to maximize the value of its IT security investments, improve communication and alignment between IT groups, user and managers and allow It security planners to schedule resources more efficiently.

References

Bodin, L. D.; Gordon, L. A. and Loeb, M. P. "Evaluation information Security investments using the Analytic Hierarchy Process," *Communications of the ACM*, (48:2), 2005, pp. 79-83.

Butler, S. A. "Security Attribute Evaluation Method: A Cost-Benefit Approach," *Proceedings of the 24th International Conference on Software Engineering (ICSE 2002)*, Orlando, FL, 2002, pp. 232–240.

Forman, E. H. and Selly, M., A. *Decision by Objectives*, World Scientific Publishing Co: River Edge, NJ, 2001.

Gordon, L. A. and Loeb, M. P. "Budgeting Process for information security expenditures," *Communications of the ACM*, (49:1), 2006, pp. 121-125.

Grance, T.; Hash, J.; Stevens, M.; O'Neal, K.; and Bartol, N. "Guide to Information Technology Security Services Recommendations of the National Institute of Standards and Technology," *NIST Special Publication 800-35*, 2003, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf (last accessed on March 22, 2006).

Neubauer, T.; Klemen, M. and Biffl, S. "Business process-based valuation of IT-security," *ACM SIGSOFT Software Engineering Notes*, 2005, (30:4), pp. 1-5.

OMB Circular No. A–11. *Information technology and e-government*, 2005, http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf (last accessed on March 22, 2006).

Roberts, P. "Security Spending Swells," *IDG News Service (PC World)*, 2003, http://www.pcworld.com/news/article/0,aid,109221,00.asp. (last accessed on March 22, 2006).

Swanson, M.; Bartol, N.; Sabato, J.; Hash, J. and Graffo, L. "Security Metrics Guide for Information Technology Systems," *NIST Special Publication 800-55*, 2003, http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf. (last accessed on March 22, 2006).

Wheatman. V.; Smith, B.; Schroder, N.; Pescatore, J.; Nicolett, M.; Allan, A. and Mogull, R. "What Your Organization Should Be Spending for Information Security," *The Gartner Group*, March 2005, http://www.gartner.com/DisplayDocument?doc_cd=126733. (last accessed on March 22, 2006).

Appendix A: The security projects or initiatives

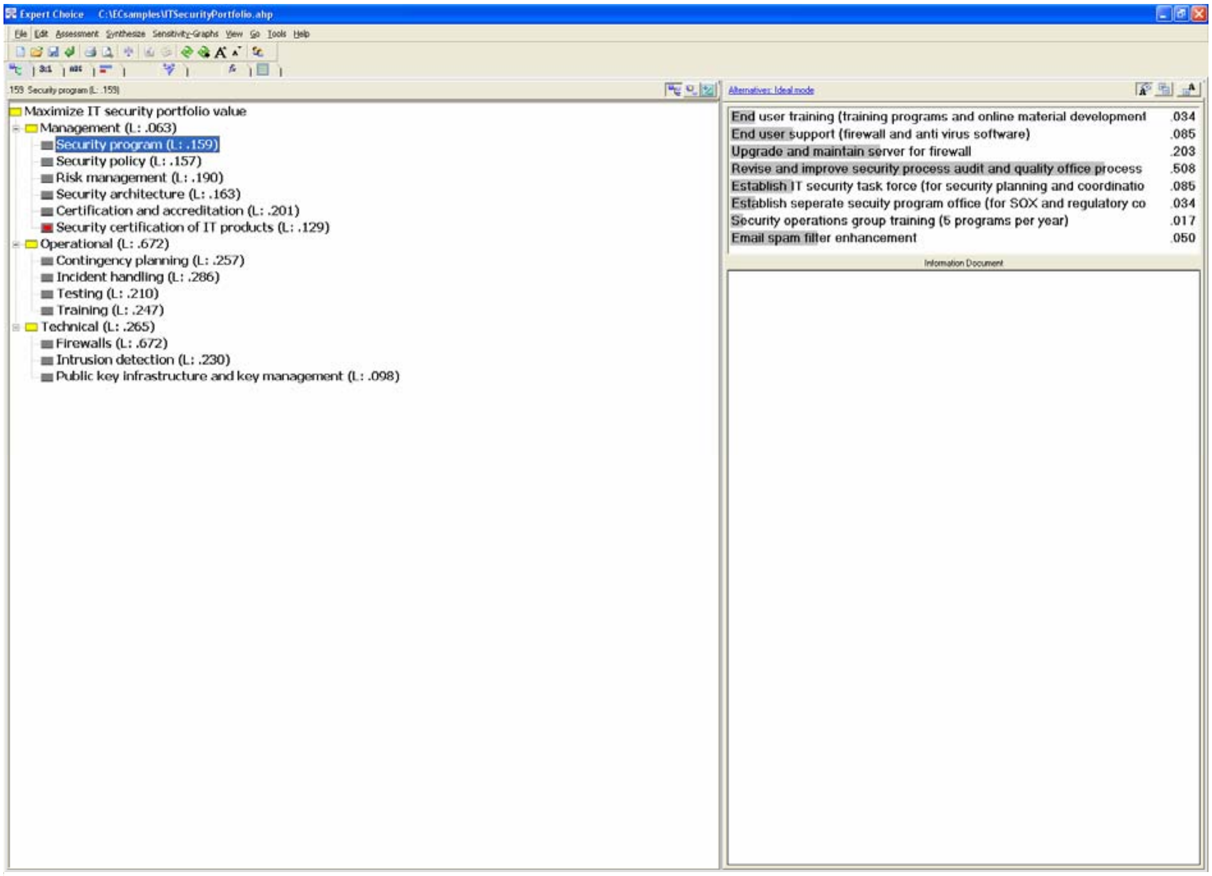
The eight security projects of initiatives are shown below for an operating division of an organization that has a mature IT setup and has been according the highest importance to IT security as a part of its larger security and IT initiative. Since it is financial institution in a large urban setting on the east coast in the US, the $200,000 IT security budget for recurring expenditure items is considered average[3].

Initiative or project	**Description**	**Budget ($)**
End user training (training programs and online material development)	In-house and outsourced training programs for selected end-users and their representatives. This is an recurring activity that needs to take place every year. The intent is to ensure that all end users are exposed to at least one such training program every two years.	56000
End user support (firewall and anti virus software)	This is part of the overall help desk support system. This is an outsourced activity and 2 FTEs (full time equivalent) are budgeted for this activity.	24000
Upgrade and maintain server for firewall	The bundled cost for the server, installation and testing along with the annual cost of maintaining it is reflected.	25000
Revise and improve security process audit and quality office process	Security processes need to be revised constantly. One half FTE (internal) is budgeted for this activity.	43000
Establish IT security task force (for security planning and coordination)	The IT security task force needs to meet every month and take decisions on the direction of IT security and liaise with external bodies like regulatory agencies, standards bodies and key business partners. The cost reflects coordination, administrative and meeting costs.	25000
Establish separate security program office (for SOX and regulatory compliance reporting)	This requires specific attention to IT security from the standpoint of Sarbanes-Oxley Act. This office will form the interface between IT security, internal audit and the quality group. One FTE and office and administrative expenses are budgeted.	95000

[3] In general, organizations tend to spend 3 percent to 6 percent of total IT spending on IT security (Wheatman et al., 2005).

Security operations group training (5 programs per year)	This is the set of annual training program for the internal IT security group professionals. Five programs attended by five persons each and their travel and expenses are budgeted for.	59000
Email spam filter enhancement.	Email spam has been a source of constant problems. Enhancements of the software and part- manpower are reflected in this budgeted figure.	12000

Appendix B: Screenshots for computing sample priorities


Expert Choice C:\ECsamples\ITSecurityPortfolio.ahp
File Edit Assessment Synthesize Sensitivity-Graphs View Go Tools Help
3:1
ABC
.159 Security program (L: .159)
Alternatives: Ideal mode
Information Document

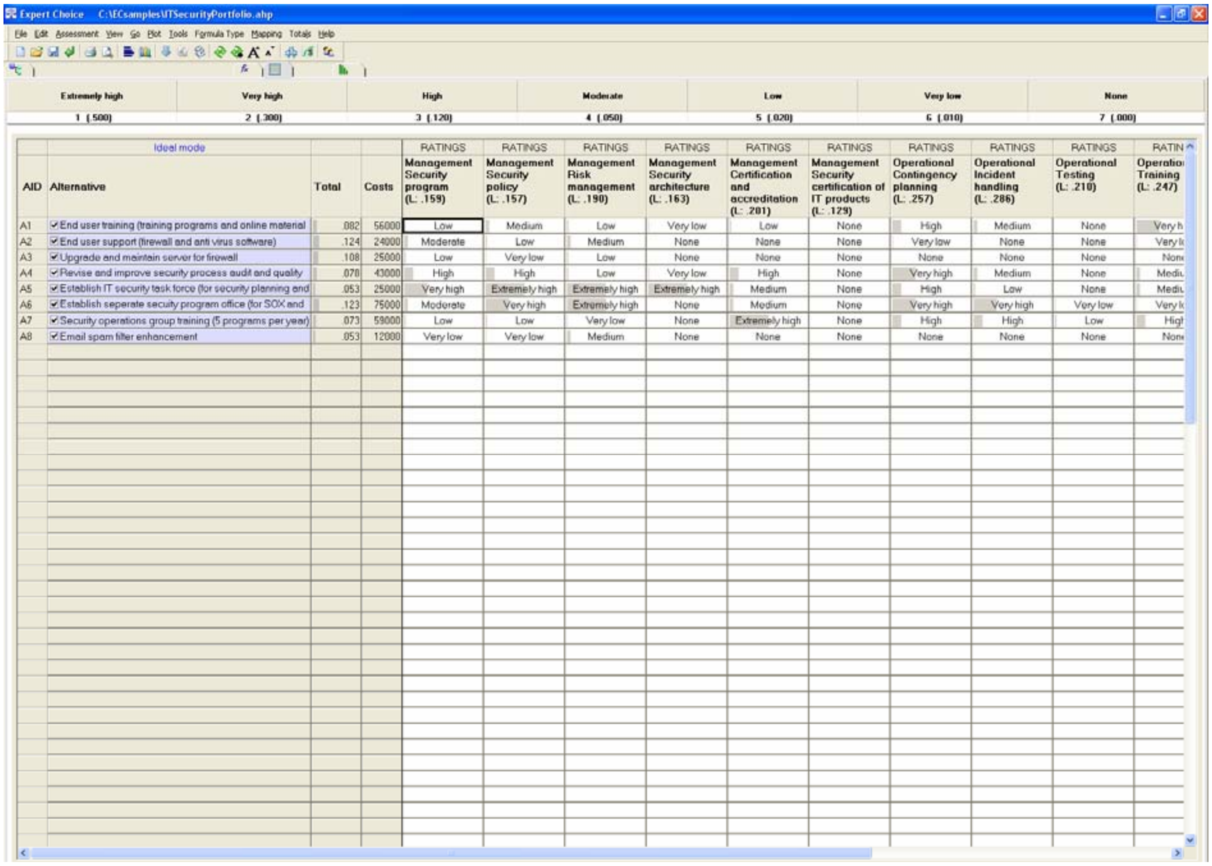
Maximize IT security portfolio value
- Management (L: .063)
  - Security program (L: .159)
  - Security policy (L: .157)
  - Risk management (L: .190)
  - Security architecture (L: .163)
  - Certification and accreditation (L: .201)
  - Security certification of IT products (L: .129)
- Operational (L: .672)
  - Contingency planning (L: .257)
  - Incident handling (L: .286)
  - Testing (L: .210)
  - Training (L: .247)
- Technical (L: .265)
  - Firewalls (L: .672)
  - Intrusion detection (L: .230)
  - Public key infrastructure and key management (L: .098)

End user training (training programs and online material development	.034
End user support (firewall and anti virus software)	.085
Upgrade and maintain server for firewall	.203
Revise and improve security process audit and quality office process	.508
Establish IT security task force (for security planning and coordinatio	.085
Establish seperate secuity program office (for SOX and regulatory co	.034
Security operations group training (5 programs per year)	.017
Email spam filter enhancement	.050

Figure B2.1. Screen showing the goal, objectives, criteria and alternatives

Figure B2.1 shows how priorities (benefits) associated with alternatives were computed. The screenshot shows a specific scenario (not the one used for computations in the body of the paper). The goal is shown as "Maximize IT security Portfolio." The three objectives have to do with meeting management, operational and technical benefits. The criteria used to assess the extent to which requirements are met (and benefits captured) are shown as the leaf nodes on the tree on the left. The number alongside each of the elements shows the importance of the elements. For instance, in this case, the operational objectives are rated as .672 while the management and technical objectives are rated as .063 and .265 respectively. The advantage of these ratio scales is that we can say the operation objective is 2.5 (.672/.265 = 2.54) times more important than the technical objective and the technical objectives are four times (.265/.063 = 4.21) more important than the management objectives. The criteria for each of the objectives are interpreted the same way. For instance, *from a management perspective*, certification and accreditation is 1.2 (.201/.163 = 1.23) times more important than the security architecture; or from a technical perspective, the benefits of intrusion detection (in general) is computed to be one-third (.230/.672 = .342) as important as firewalls.

In the same way, the items on the right side of the screenshot in Figure B2.1 show the alternatives and their priorities (benefits). The most important project (i.e. the one with the highest relative benefits is “Revise and improve security process audit and quality office process ” followed by “Upgrade and maintain server for firewall.” These final ratings for benefits were produced by providing ratings for each of the alternatives based on each of the criteria as shown in Figure B2.2.


Expert Choice C:\ECsamples\ITSecurityPortfolio.ahp
File Edit Assessment View Go Plot Tools Formula Type Mapping Totals Help

Extremely high	Very high	High	Moderate	Low	Very low	None
1 (.500)	2 (.300)	3 (.120)	4 (.050)	5 (.020)	6 (.010)	7 (.000)

	Ideal mode			RATINGS	RATINGS	RATINGS	RATINGS	RATINGS	RATINGS	RATINGS	RATINGS	RATINGS	RATIN
AID	Alternative	Total	Costs	Management Security program (L: .159)	Management Security policy (L: .157)	Management Risk management (L: .190)	Management Security architecture (L: .163)	Management Certification and accreditation (L: .201)	Management Security certification of IT products (L: .129)	Operational Contingency planning (L: .257)	Operational Incident handling (L: .286)	Operational Testing (L: .210)	Operatio Training (L: .247)
A1	☑ End user training (training programs and online material	.082	56000	Low	Medium	Low	Very low	Low	None	High	Medium	None	Very h
A2	☑ End user support (firewall and anti virus software)	.124	24000	Moderate	Low	Medium	None	None	None	Very low	None	None	Very lo
A3	☑ Upgrade and maintain server for firewall	.108	25000	Low	Very low	Low	None	None	None	None	None	None	None
A4	☑ Revise and improve security process audit and quality	.078	43000	High	High	Low	Very low	High	None	Very high	Medium	None	Mediu
A5	☑ Establish IT security task force (for security planning and	.053	25000	Very high	Extremely high	Extremely high	Extremely high	Medium	None	High	Low	None	Mediu
A6	☑ Establish seperate secuity program office (for SOX and	.123	75000	Moderate	Very high	Extremely high	None	Medium	None	Very high	Very high	Very low	Very lo
A7	☑ Security operations group training (5 programs per year)	.073	59000	Low	Low	Very low	None	Extremely high	None	High	High	Low	High
A8	☑ Email spam filter enhancement	.053	12000	Very low	Very low	Medium	None	None	None	None	None	None	None

Figure B2.2. Screen showing the alternatives and how they were rated based on each criterion