• *By* LAWRENCE D. BODIN, LAWRENCE A. GORDON, *and* MARTIN P. LOEB •

Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS

THE ANALYTIC HIERARCHY PROCESS CAN HELP AN ORGANIZATION MAKE INFORMATION SECURITY INVESTMENT DECISIONS.

In today's information-based economy, organizations must avoid costly information security breaches. Unfortunately, organizations cannot make all of their information 100% secure all of the time. There are economic, as well as technical, impediments that prevent perfect information security. Accordingly, organizations usually prepare an annual fixed (limited) budget for the maintenance and improvement of their information security systems. Two key issues confront the chief information security officer (CISO) of an organization: how to spend this limited information security budget most effectively, and how to make the case to the organization's chief financial officer (CFO) for an increase in funds to further

• ILLUSTRATION BY PAUL WILEY •

enhance the organization's information security. The primary objective of this article is to show how to use the analytic hierarchy process (AHP) to address these two information security issues.

Gordon and Loeb [4] provide an economic modeling framework for assessing the optimal amount to invest in information security based on the principle of equating the marginal financial benefits of information security to the marginal financial costs of such security. The Gordon and Loeb model does not consider qualitative or nonfinancial criteria. (This model also does not consider other quantitative concerns, such as real options, as discussed in [5].) Since a big part of information security relates to qualitative and nonfinancial concerns, traditional economic approaches are severely constrained. Many other real-world problems involve the need to combine quantitative measures (including financial measures) with qualitative concerns. Saaty [6, 7] developed the AHP to analyze multicriteria decision problems involving both quantitative and qualitative criteria. Examples of the use of the AHP can be found in Bodin and Epstein [1] and Bodin and Gass [2].

We propose using the ratings method variant of the AHP to determine the optimal allocation of a budget for maintaining and enhancing the security of an organization's information system. Under the ratings method, the organization enumerates the criteria and sub-criteria to be used and employs the AHP to determine weights for each of these criteria and sub-criteria. The organization then evaluates alternative proposals (called alternatives in this article) for maintaining and enhancing their system information security. These alternatives are evaluated individually against each criterion and sub-criterion using intensity (achievement) levels that measure how well an alternative accomplishes a particular criterion or sub-criterion. A score is determined for each alternative. The perfect alternative has a score of 1.0. The score for an alternative always lies between 0 and 1.0 and each score is determined independently of the scores of the other alternatives. Alternatives with identical scores are considered tied or equally close-to-perfect in the evaluation.

The ratings method is carried out as follows:

- The criteria, sub-criteria, and intensity levels for the criteria or sub-criteria are defined.
- The AHP tree containing the criteria, sub-criteria, and intensity levels is drawn.
- The weights to be used for the criteria, sub-criteria, and the intensity levels at each level of the tree using pairwise comparisons are determined. Let C(i,j) be a pairwise comparison that the decision-maker makes between two elements i and j, which are children of a node in the AHP tree (the children are also nodes in the AHP tree). Assume that element i is considered at least as preferable as element j. The larger the value of C(i,j), the more the decision-maker prefers element i to j. C(i,j) = 1 means that the decision-maker regards element i and j as equally important. When C(i,j) = 3, 5, 7, and 9, the decision-maker regards element i as being moderately preferred, strongly preferred, very strongly preferred, and extremely strongly preferred, respectively, to element j.[1] Each pairwise comparison can be interpreted as a ratio scale [2]. For elements i and j on the same level of the tree, C(i,j) can be interpreted as follows:

$$C(i,j) = \frac{\text{The weight the decision-maker would like to assign to element i}}{\text{The weight the decision-maker would like to assign to element j.}}$$

  Thus, C(j, i) = 1/C(i,j) and C(i,j) is well defined, no matter whether the decision-maker finds element i to be more or less important than element j, or equally important to j. The weights for each pairwise comparison matrix defined in this manner are the components of the eigenvector associated with the maximum eigenvalue of the pairwise comparison matrix.
- A spreadsheet is created that shows the evaluation of each alternative using the weights for each criterion, sub-criterion, and intensity determined in the previous step. Alternative i is evaluated in row i of the spreadsheet. Cell(i,j) in the spreadsheet gives the weight for each criterion or sub-criterion j with respect to alternative i.
- The score for each alternative is the sum of the weights of the various cells in row i of the spreadsheet.

In this article, two scenarios are presented for deciding upon an alternative that best enhances an organization's information security system. The AHP tree can involve costs and/or benefits. Since in our example we assume a fixed budget, we do not include costs in our analysis. If the budget were variable, we could include costs in the AHP tree or carry out a cost/benefit analysis.

To demonstrate the AHP in action, we examine the case of LBG Manufacturing Inc. (LBG), which has budgeted $1 million for improving computer system information security and has decided to solicit

[1] An even value of C(i,j) means the decision-maker regards element i as being halfway between the two adjacent odd values of C(i,j). For example, if C(i,j) = 4, the decision-maker regards element i as being between moderately and strongly preferred to element j.

proposals from three reputable companies that specialize in information security. In its request for proposal (RFP), LBG notes its $1 million budget. It also specifies the criteria and sub-criteria, and the weights assigned to these criteria and sub-criteria.

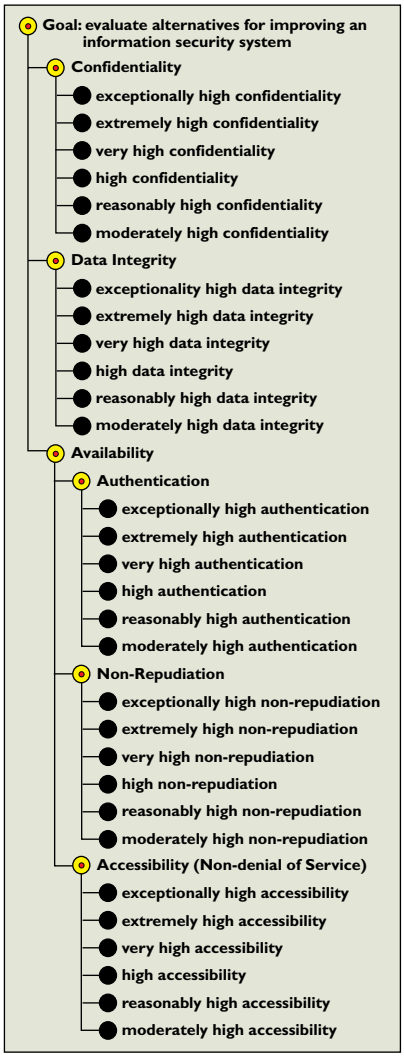
LBG asks each company to give its best proposal for performing this system enhancement under the $1 million budget, as well as under a $1.3 million budget. The CISO hopes to make a case, if it exists, for a budget increase. The CISO deliberately included the weights in Table 1 in the RFP so the vendors know the basis on which their proposals will be evaluated.

The criteria to be used in this evaluation are Confidentiality, Data Integrity, and Availability. These criteria are defined as follows:

Confidentiality. Only authorized individuals have access to the databases and information systems.

Data Integrity. The information in the systems is accurate, complete, and consistent, and only authorized individuals can change such information.

A AHP tree.



Availability. The information is available to authorized users in a timely manner.

The availability criterion is broken down into the following three sub-criteria: Authentication, Non-repudiation, and Accessibility or non-denial of service. The sub-criteria are defined as follows:

Authentication. The system makes sure users are who they claim to be.

Non-repudiation. A user cannot deny using the system, if in fact he or she did actually use it.

Accessibility (non-denial of service). A legitimate user cannot be denied access to the system.

LBG uses the following six intensities for each criterion or sub-criterion: exceptionally high, extremely high, very high, high, reasonably high, and moderately high. As the CISO evaluates the proposals, each criterion and sub-criterion for each proposal will be rated using these intensities.

The sideway view of the AHP tree for this analysis is displayed in the figure here. The Goal node represents the overall purpose of this analysis—determining the best alternative to improve the overall information security of the organization's computer system. The major criteria are Confidentiality, Data Integrity, and Availability. The sub-criteria under Availability are Authentication, Non-Repudiation, and Accessibility.

Since we are using the ratings model of the AHP, the terminus nodes of the AHP tree are the intensities for the criteria or sub-criteria that do not have other sub-criteria emanating below them in the AHP tree. In this example, the Confidentiality and Data Integrity criteria, and the Authentication, Non-Repudiation, and Accessibility sub-criteria

Panel A: Pairwise comparisons for the three criteria from the Goal Node

	Confidentiality	Data Integrity	Availability
Confidentiality	1	5	3
Data Integrity	1/5	1	1/2
Availability	1/3	2	1
Weights	**0.648**	**0.122**	**0.230**

Panel B: Pairwise comparisons for the three sub-criteria from the Availability Node

	Authentication	Non-Repudiation	Accessibility
Authentication	1	4	5
Non-Repudiation	1/4	1	2
Accessibility	1/5	1/2	1
Weights	**0.683**	**0.200**	**0.117**

Panel C: Pairwise comparisons for the six intensities from the Confidentiality Node

	Exceptionally High Confidentiality	Extremely High Confidentiality	Very High Confidentiality	Reasonably High Confidentiality	Moderately High Confidentiality	High Confidentiality
Exceptionally High Confidentiality	1	2	4.5	6.5	8	9
Extremely High Confidentiality	1/2	1	3	5	7	8
Very High Confidentiality	1/(4.5)	1/3	1	3	5	6
High Confidentiality	1/6.5	1/5	1/3	1	3	4
Confidentiality	1/8	1/7	1/5	1/3	1	2
Moderately High Confidentiality	1/9	1/8	1/6	1/4	1/2	1
Weights	**0.428**	**0.286**	**0.146**	**0.075**	**0.038**	**0.027**

Table 1. Pairwise comparisons.

have intensities, whereas Availability does not have intensities. The intensities for a criterion or sub-criterion can be regarded as the user's evaluation of how close an alternative is to perfection with respect to this criterion or sub-criterion. A perfect alternative would have a rating of exceptionally high for each criterion and a score equal to one.

The CISO's pairwise comparisons for the three criteria out of the Goal node are shown in the first three rows of Table 1A. The last row of Table 1A shows the weights of these criteria that are determined by the AHP. The CISO's pairwise comparisons for the three sub-criteria out of the Availability node are given in the first three rows of Table 1B, and the weights for these sub-criteria, calculated by the AHP, are given in the last row. As noted earlier in this article, the weights determined in Table 1 are the eigenvector associated with the maximum eigenvalue of the pairwise comparison matrix. The calculation of these weights can be done directly or via standard AHP software packages.

The CISO's pairwise comparisons for the intensities out of the Confidentiality criterion are given in Table 1C and the weights for these intensities are given in the last row of Table 1C. We assume that the pairwise comparisons for the intensities for the Data Integrity criterion and the Availability sub-criteria (Authentication, Non-repudiation, and Accessibility) are the same as the pairwise comparisons given in Table 1C.

If a criterion has no sub-criterion, then the score for a criterion is the following:

$$\text{criterion score} = \frac{\text{(weight of the criterion) * (weight of the intensity)}}{\text{weight of the exceptionally high intensity for the criterion.}}$$

If a criterion has a sub-criterion, then the score for the sub-criterion is the following:

$$\text{sub-criterion score} = \frac{\text{(weight of the criterion)* (weight of the sub-criterion)* (weight of the intensity)}}{\text{weight of the exceptionally high intensity for the criterion.}}$$

For example, the score for the extremely high intensity for data integrity is computed as .122*.286/.428=.081 where the weight for data integrity is .122, the weight for extremely high intensity is .286, and the weight for an exceptionally high intensity is .428. Similarly, the score for the extremely high intensity for non-repudiation is computed as 230*.200*.286/.428=.030 where the weight for availability is .230, the weight for non-repudiation is .2, the weight for extremely high intensity is .286, and the weight for an exceptionally high intensity is .428. (See [3] for a more detailed analysis of the computation of these weights.)

Assume that three vendors responded to the RFP with proposals for the $1 million and $1.3 million budgets. The three $1 million proposals are labeled 1a, 2a, and 3a, while the $1.3 million proposals are labeled 1b, 2b, and 3b. The CISO's evaluation of the $1 million proposals is given in Table 2A and the scores for these proposals (using the evaluations and the weights given in Table 1) are given in Table 2B. Thus, the AHP suggests that Proposal 3a, with a score of .589 should be selected.

The CISO, being held responsible for the organization's information security, naturally would like the overall score to be greater than the 58.9% of perfection attainable with the $1 million budget. In order to support a request for an increased budget, the CISO examines the $1.3 million proposals. Table 3 illustrates the CISO's evaluation, and the corresponding scores of the $1.3 million proposals using the weights given in Table 1. Proposal 3b has the highest score (.901), even though it has a rating of High in Non-Repudiation, the lowest rating of any criterion or sub-criterion among the three proposals. If $1.3 million were to become available for enhancing the information security system, the AHP suggests that Proposal 3b be selected.

To support his argument for a budget increase, with the corresponding selection of Proposal 3b rather than 3a, the CISO computes the performance/cost ratios and the incremental performance/cost ratio as follows:

$$\text{performance/cost ratio} = \text{score of a proposal/cost of a proposal.}$$

$$\text{Incremental performance cost ratio} = \frac{\text{score of Proposal 3b-score of Proposal 3a}}{\text{cost of Proposal 3b-cost of Proposal 3a}}$$

Panel A. Evaluation

			Availability			
Alternative	Confidentiality	Data Integrity	Authentication	Non-Repudiation	Accessibility	
Proposal 1a	Extremely High	Extremely High	High	Reasonably High	High	
Proposal 2a	Extremely High	Extremely High	Very High	Moderately High	Reasonably High	
Proposal 3a	Extremely High	Exceptionally High	Reasonably High	Moderately High	Moderately High	

Panel B. Scoring

			Availability			
Alternative	Confidentiality	Data Integrity	Authentication	Non-Repudiation	Accessibility	**Total Score**
Proposal 1a	0.433	0.081	0.028	0.004	0.005	**0.551**
Proposal 2a	0.433	0.081	0.054	0.003	0.0024	**0.573**
Proposal 3a	0.433	0.122	0.014	0.003	0.0017	**0.589**

Table 2. Evaluation and rating model scoring of $1 million proposals.

THE AHP HELPS ORGANIZE THE THOUGHTS OF THE CISO AND PROVIDES A MECHANISM TO CAREFULLY COMPARE CRITERIA, SUB-CRITERIA, AND ALTERNATIVES.

Panel A. Evaluation

			Availability			
Alternative	Confidentiality	Data Integrity	Authentication	Non-Repudiation	Accessibility	
Proposal 1b	Exceptionally High	Extremely High	Very High	Very High	Extremely High	
Proposal 2b	Extremely High	Exceptionally High	Exceptionally High	Extremely High	Exceptionally High	
Proposal 3b	Exceptionally High	Exceptionally High	Extremely High	High	Extremely High	

Panel B. Scoring

			Availability			
Alternative	Confidentiality	Data Integrity	Authentication	Non-Repudiation	Accessibility	**Total Score**
Proposal 1b	0.648	0.081	0.054	0.016	0.018	**0.817**
Proposal 2b	0.433	0.122	0.157	0.030	0.027	**0.769**
Proposal 3b	0.648	0.122	0.105	0.008	0.018	**0.901**

Table 3. Evaluation and rating model scoring of $1.3 million proposals.

Since the performance/cost ratio for Proposal 3a is .589/$1 million = .589 and the performance/cost ratio for Proposal 3b is .901/$1.3 million = .693, the CISO argues that Proposal 3b gives more "bang for the buck" than Proposal 3a. The Incremental Performance/Cost ratio of Proposal 3b to Proposal 3a equals (.901-.589)/(1.3-1) = 1.04.

Thus, the CISO argues to the CFO that the expenditure of an extra $300,000 has an increasing benefit per dollar spent versus the first $1 million spent on improving the system.

Conclusion

The AHP methodology is a useful tool for assisting an organization in making information security investment decisions, but does not replace the decision-maker. The decision-maker must decide upon the criteria, sub-criteria, and intensities and make numerous evaluations to derive a ranking of the alternatives. The AHP helps organize the thoughts of the CISO and provides a mechanism to carefully compare criteria, sub-criteria, and alternatives. The AHP can be a valuable tool used by itself or combined with other analytic approaches and can facilitate the team approach to decision making. C

References

1. Bodin, L. and Epstein, E. Who's on first—with probability .4. *Computers & Operations Research 27* (1999), 205–215.
2. Bodin, L. and Gass, S. On teaching the analytic hierarchy process. *Computers and Operations Research 30*, 10 (2003), 1487–1497.
3. Bodin, L., Gordon, L.A., and Loeb, M.P. *Making Security Investment Decisions Using the Analytic Hierarchy Process*. Working Paper, University of Maryland, 2003.
4. Gordon, L.A. and Loeb, M.P. The economics of investment in information security. *ACM Transactions on Information and System Security 5*, 4 (Nov. 2002), 438–457.
5. Gordon, L.A., Loeb, M.P., and Lucyshyn, W. Information security expenditures and real options: A wait and see approach. *Computer Security Journal 19*, 2 (Spring 2003), 1–7.
6. Saaty, T.L. *The Analytic Hierarchy Process*. McGraw-Hill, New York, 1980.
7. Saaty, T.L. A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology 15,* 3 (1977), 234–281.

Support for this research was provided in part by the DoD, Laboratory for Telecommunications Sciences, through a contract with the University of Maryland Institute for Advanced Computer Studies.

LAWRENCE D. BODIN (lbodin@rhsmith.umd.edu) is currently Professor Emeritus in the Robert H. Smith School of Business at the University of Maryland, College Park.
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.
MARTIN P. LOEB (mloeb@rhsmith.umd.edu) is Professor of Accounting and Information Assurance, and a Deloitte & Touche Faculty Fellow in The Robert H. Smith School of Business at the University of Maryland, College Park.