SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies

System Quality Requirements
Engineering (SQUARE) Team

Nick (Ning) Xie
Nancy R. Mead, Advisor

Contributors:
Peter Chen
Marjon Dean
Lilian Lopez
Don Ojoko-Adams
Hasan Osman

November 2004

Networked Systems Survivability Program

Technical Note
CMU/SEI-2004-TN-045

This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Contents

List of Figures

List of Tables

Abstract

Many companies rely on historical data to build predictability models for cost/benefit justification of future projects. Unfortunately, for small companies, which generally do not have a process for collecting security data, the costs and the benefits of information security improvement projects have been very difficult to estimate and justify. In addition, detailed attack data are simply not available to be used as references in cost estimations. Given these difficulties, many small companies choose to ignore entirely the security vulnerabilities in their systems, and many suffer the consequences of security breaches and significant financial loss. Small companies that do implement security improvement projects often have problems understanding the cost structures of their improvement initiatives and how to translate risk exposures into costs that can be passed on to their customers.

To deal with the aforementioned problems, this report describes a general framework for hierarchical cost/benefit analysis aimed at providing acceptable estimations for small companies in their information security improvement projects. The framework classifies misuse cases into categories of threats for which nationally surveyed risks and financial data are publicly available. For each category of threats, costs, benefits, baseline risks, and residual risks are estimated. The framework then generates all permutations of possible solutions and analyzes the most optimal approach to maximize the value of security improvement projects. The framework analyzes the problems from five dimensions: Total Implementation Costs, Total System Value, Net Project Value, Benefit/Cost Ratio, and Risk Exposures. The final proposed system will be derived from the comparisons of these dimensions, taking into consideration each company’s specific situation.

This report is one of a series of reports resulting from research conducted by the System Quality Requirements Engineering (SQUARE) Team as part of an independent research and development project of the Software Engineering Institute.

1 Introduction

The purpose of a cost/benefit analysis is to provide a set of quantitative metrics to assist companies in their decision making. In information security improvement projects, such analysis can provide insights about which vulnerabilities and/or design flaws to fix, in what order of importance, and for how much investment. By associating a calibrated monetary amount with each risk, vulnerability, cost item, and recommendation, a cost/benefit analysis enables companies to compare and contrast available alternatives and to arrive at a sound decision with financial justification.

1.1 The Problem

Information security data has traditionally been very difficult to collect. In small companies, where human resources are especially scarce, the process of collecting data on the annual number of security breaches and their resulting financial losses is typically non-existent. This creates the problem that, on one hand, small companies need reliable data to make good decisions, and on the other hand, they cannot have data when no one has time to collect data. In addition, security risk is often an unknown quantity, because no one can predict the exact time and methods of future security incidents. Businesses can only hope to reduce risk and potential loss by implementing security solutions. At a detailed level, there is often a many-to-many relationship between risks and security improvement measures, and it is difficult to compute the actual risk versus the cost for each specific misuse and attack.

Without reliable historical data and/or comparable third-party data, small companies are usually at a loss about whether to implement their security improvement projects. Many small companies choose to ignore entirely the security vulnerabilities in their systems, and many suffer the consequences of security breaches and significant financial loss when attacks occur. Small companies that do implement the security improvement projects often have problems understanding the cost structures of their improvement initiatives and how to translate risk reduction into costs that can be passed on to their customers.

1.2 A Framework for Cost/Benefit Analysis

To deal with the aforementioned problems, we have devised the Cost/Benefit Analysis Framework, a general framework for hierarchical cost/benefit analysis aimed at providing acceptable estimations for small companies in their information security improvement projects. The framework classifies misuse cases into categories of threats for which nationally surveyed risks and financial data are publicly available. For each category of threats, costs, benefits, baseline risks, and residual risks are estimated. The framework then generates all permutations of possible solutions and analyzes the most optimal approach to maximize the value of security improvement projects. The framework is described in detail in Section 2.

1.3 The Acme Company

Throughout this report we will use the Acme Company as the alias of our real-life client. The Acme Company is a small start-up software company. Its core product has attracted interests from several large prospects. However, before deals can be signed, these prospect companies demand that the Acme Company show them that the product is reasonably secure when deployed in large, heterogeneous enterprise environments. Because of customer demands, the Acme Company is planning to initiate a project to improve the security of its product. Before the project is undertaken, however, its costs must be justified relative to its benefits.

An application of the framework to the Acme Company example is discussed in Section 3.

1.3.1 System Overview

The Acme Company's core product is a web-based n-tier asset management system with browser clients, web servers, application servers, and database components. It has an existing client installation base. Currently it is undergoing a major migration to a new version. It remains to be shown whether the system can be reasonably secure when deployed in a large, heterogeneous enterprise environment.

1.3.2 Business Goals

As with any business, one of the Acme Company's main objectives is to make a profit. In addition to the security objectives presented in this document, Acme wants to keep focus on its business goals of increasing profits and market share in the industry. Hence, incorporating security improvements should work in parallel with the original objectives rather than against them.

1.3.3 Security Objectives

The following are Acme's security objectives for its asset management system. They are listed alphabetically.

Availability: The business purpose of the system can be met, and the system is accessible to those who need to use it [SANS 03].

Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity) [SANS 03].

Integrity: The system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Data in the system are not changed, destroyed, or lost in an unauthorized or accidental manner [Allen 99].

2 Cost/Benefit Analysis Framework

2.1 Terms and Concepts

Terms and concepts used in the Cost/Benefit Analysis Framework are defined in Table 1.

Table 1: Terms and Concepts Used in the Framework

Category of Threats	a set of related misuses and attacks that pose threats to the organization
Category of Preventions	a set of recommendations that sufficiently mitigate a *Category of Threats*. A *Category of Preventions* has a one-to-one relationship with a *Category of Threats.*
Baseline Risk	incident risk to the organization if no security solutions are in place
Bypass Rate	probability that an attack will penetrate a given security solution and result in observable damage. A 100% bypass rate means the security solution does not stop any incidents; a 0% bypass rate means the security solution stops all incidents.[1]
Residual Risk	incident risk to the organization if security solutions are properly installed, utilized, and monitored. *Residual Risk* = *Baseline Risks* x *Bypass Rate*.
Net Present Value (NPV)	the present value of an investment's future net cash flow minus the initial investment

2.2 Methodology

The Cost/Benefit Analysis Framework derives its cost and benefit figures from misuse cases and the architectural and policy recommendations needed to mitigate these misuse cases. We

[1] The authors gratefully acknowledge the ideas expressed by Arora et al. that all security solutions are subject to rate of failures (bypass), which needs to be accounted for in the risk reduction analysis. (Arora, Ashish; Hall, Dennis; Pinto, C. Ariel; Ramsey, Dwayne; & Telang, Rahul. “An Ounce of Prevention vs. a Pound of Cure: How Can We Measure the Value of IT Security Solutions?” Carnegie Mellon CyLab, 2004.)

will not explain in depth how to generate misuse cases and recommendations, since they are very company and project specific. To illustrate our points, we will show examples of misuse cases and recommendations in Section 3.

The framework categorizes related misuses into *Categories of Threats*, which are sets of related misuses and attacks that pose threats to the organization. Examples of *Categories of Threats* include denial of service, system penetration, and sabotage of data. Categorization has several benefits. First, categories are high level and easy to understand by business users. Second, categorization reduces the scope and the dimensions of the problem by aggregating on top of related misuse cases, which themselves are aggregates of incidents. Third, categories are relatively distinct from each other. We are assuming that the effects of mitigating risks in one *Category of Threats* are negligible to other *Categories of Threats*. This assumption allows us to compute independently costs of implementations for each *Category of Preventions* without worrying about overlapping cardinalities. Finally, attack and loss data for *Categories of Threats* can be found in national surveys, which provide reasonable estimates for small companies without forcing them to invest large amounts of human resources in data collection or research.

The most difficult problem for any small company is the lack of historical data or comparable external data to base its analysis on. Therefore, reasonable assumptions need to be made in the areas of expected probabilities and consequences when the company is subject to misuses and attacks. In most cases, even for large companies, we cannot accurately predict when and how an attack will happen. However, these challenges can be overcome with threat categorization. Annual national surveys have shown that over the period of a year, *Categories of Threats* have average probabilities of occurrences and ranges of financial losses due to exposures to these *Categories of Threats*. Because these *Categories of Threats* are general and encompassing, they can be assumed to include most of the misuses and attacks that a small company is likely to face. By not concentrating on each specific misuse or attack that a company may face, small companies can avoid getting consumed by over-detailed risk modeling that they have no resources or reliable data to do. Instead, by focusing on mitigating *Categories of Threats*, small companies will have reasonable estimations of their expected loss if they were to take no actions against a set of probable misuse cases. From *Categories of Threats* they can quantify and prioritize sets of security improvement measures with respect to their high-level security and business goals. We call these security improvement measures *Categories of Preventions*. They have one-to-one relationships with *Categories of Threats*.

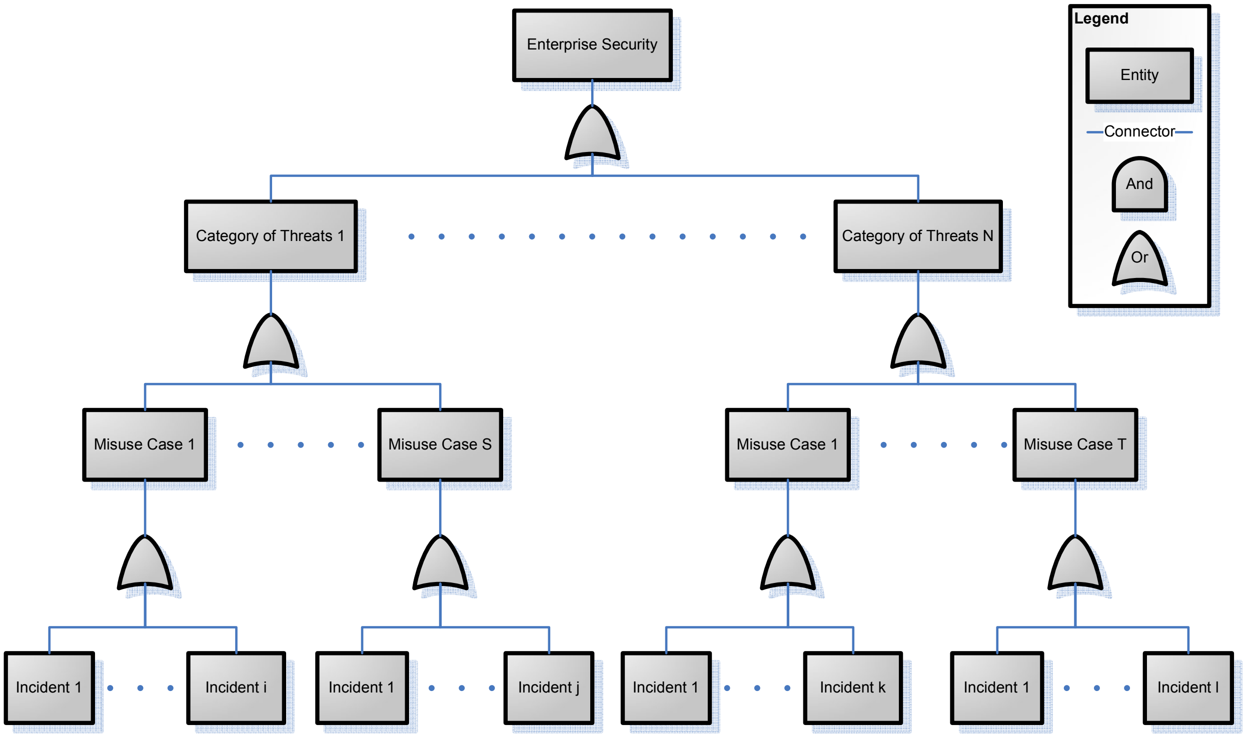

Figure 1: Categorization of Threats, Misuse Cases, and Incidents

The framework takes financial and probabilistic data from annual national surveys for each *Category of Threats*. The principal assumption is that a small company is subject to attacks and misuses at probabilities at or near national average. If the company cannot provide an estimate for the expected loss when misuses happen, lower ends of nationally surveyed loss are used as cost avoidance items for implementing security improvement measures. We use the lower end because small companies typically do not have as many assets to lose as larger companies.

The goal of the framework is to support better decision-making to ensure that resources are effectively allocated in the lifetime of the project. Typically,

- a security improvement project runs for M number of years and
- there are N possible *Categories of Preventions* to implement.

If and only if all the architectural and policy recommendations in a *Category of Preventions* are implemented do we consider the risks in its corresponding *Category of Threats* mitigated; otherwise *Category of Threats* is considered not to have been mitigated. Let's define the following:

X_i = 1 if we are going to implement a *Category of Prevention* (i = 1, 2…N)

= 0 if we are not going to implement a *Category of Prevention* (i = 1, 2 …N)

Using the aforementioned probabilities from the surveys, *Margin of Safety* and *Risk Exposures* of a company's existing system can be calculated. *Margin of Safety* is the probability that none of the categories of threats happen at all within a year. Therefore, it is the accumulative product of (1 – probabilities of a *Category of Threats* happening). The probability of a *Category of Threats* happening will differ depending on whether the given *Category of Threats* has been mitigated. When unmitigated, a particular *Category of Threats* will have *Baseline Risk* (incident risk to the organization if no security solutions are in place) assumed at national average; when mitigated, the same *Category of Threats* will have only *Residual Risk*, which is the incident risk to the organization even if security solutions are properly installed, utilized, and monitored. However, even with proper security solutions in place, an attack still might penetrate the security solutions and result in observable damage. The rate of such occurrence is thus defined as the *Bypass Rate*. A 100% *Bypass Rate* means the security solution does not stop any incidents; a 0% *Bypass Rate* means the security solution stops all incidents. For small companies, which typically do not have voluminous data on their information security, a reasonable estimate of *Bypass Rate* can be used. This is the case in the Acme Company example in Section 3.

For i = 1, 2….N number of possible *Categories of Preventions*:

$$\textbf{\textit{Residual Risk}}_{\,i} = \textit{Baseline Risk}_{\,i} \text{ x } \textit{Bypass Rate}_{\,i}$$

$$\begin{aligned}\textbf{\textit{Margin of Safety}} &\cong \prod_{i=1}^{N}(1 - P\{attacked\}_i) \\ &\cong \prod_{i=1}^{N}(1 - P_i)\end{aligned}$$

$$P_i = \begin{cases} Baseline\_Risk_i & \text{if } X_i = 0 \\ Residual\_Risk_i & \text{if } X_i = 1 \end{cases}$$

$$\textbf{\textit{Risk Exposure}} = 1 - \textit{Margin of Safety}$$

Example 1:

If a company currently has a 60% likelihood of encountering misuse incidents in Category A and a 30% likelihood of encountering misuse incidents in Category B, then:

Baseline Risk (A) = 60%
Baseline Risk (B) = 30%

Margin of Safety = (1-60%) x (1 – 30%) = 28%
Risk Exposure = 1 – 28% = 72%

when no action is taken.

Example 1, continued:

The company can take steps to mitigate Category A and/or Category B. The available solution for A is highly effective (*Bypass Rate* of 5%), but the available solution for B is not effective (*Bypass Rate* of 70%), so:

Residual Risk (A) = 60% * 5% = 3%
Residual Risk (B) = 30% * 70% = 21%

When steps to address both A & B are implemented:

Margin of Safety = (1 – 3%) x (1 – 21%) = 77%
Risk Exposure = 1 – 77% = 23%

The Cost/Benefit Analysis Framework employs the formula of *Annualized Loss* in each category multiplied by *Baseline Risk* in each category to calculate the *Baseline Cost* in each category. The *Baseline Cost* is the amount in dollars that an organization is expected to lose by taking no action against a *Category of Threats*. The *Annualized Loss* is then used to derive the *Tangible Benefits* in the Benefits section (cost avoidance) of the recommendations for each category, if the recommendations were to be implemented. The cost avoided by implementing the security solutions is the amount in dollars reduced from the total possible loss by the effectiveness of the security solutions. The effectiveness of a security solution is essentially the amount of risk reduction a *Category of Preventions* can achieve.

Annualized Loss (AL) **i**

$$\begin{array}{ll} = Surveyed\_Average_i & \text{if no data available} \\ \quad Avg\_Incident\_loss_i \times Est\_Frequency_i & \text{if data or estimation available} \end{array}$$

Baseline Cost **i** $= Baseline\_Risk_i \times AL_i$

Residual Cost **i** $= Residual\_Risk_i \times AL_i$

$$= Baseline\_Risk_i \times Bypass\_Rate_i \times AL_i$$

Tangible Benefit **i**

$$\begin{array}{ll} = 0 & \text{if } X_i = 0 \\ \quad Baseline\_Cost_i - Residual\_Cost_i & \text{if } X_i = 1 \end{array}$$

Intangible Benefit **i**

$$\begin{array}{ll} = 0 & \text{if } X_i = 0 \\ \quad Custom\_Benefit_i & \text{if } X_i = 1 \end{array}$$

Total Benefits

$$= \sum_{i=1}^{N} \mathit{Tangible\_Benefit}_i + \sum_{i=1}^{N} \mathit{Intangible\_Benefit}_i$$

$$= \sum_{i=1}^{N} (\mathit{AL}_i \times \mathit{Baseline\_Risk}_i \times X_i \times (1 - \mathit{Bypass\_Rate}_i\ )) + \sum_{i=1}^{N} (X_i \times \mathit{Custom\_Benefit}_i\ )$$

Example 2:

If the company loses $50,000 for each misuse incident in Category A and there are 10 incidents per year in Category A, and the company loses $100,000 for each misuse incident in Category B and there are 2 incidents per year in Category B:

Annualized Loss (A) = $50,000 x 10 = $500,000
Annualized Loss (B) = $100,000 x 2 = $200,000

Using figures from Example 1:

Baseline Cost (A) = $500,000 x 60% = $300,000
Residual Cost (A) = $500,000 x 3% = $15,000
Baseline Cost (B) = $200,000 x 30% = $60,000
Residual Cost (B) = $200,000 x 21% = $42,000

Tangible Benefit (for mitigating A) = $300,000 - $15,000 = $285,000
Tangible Benefit (for mitigating B) = $60,000 - $42,000 = $18,000

Suppose that the company can get a $50,000 government award for having effectively guarded against misuses in Category A, then:

Intangible Benefit (for mitigating A) = $50,000
Intangible Benefit (for mitigating B) = $0

Total Benefits = ($285,000 + $18,000) + ($50,000 + $0) = $353,000

With stakeholders' feedback, misuse cases in each *Category of Threats* can be identified as high, medium, or low in priority. We found that small companies typically will only have the resources to mitigate high-priority misuse cases. Given such constraints, it is important to note that misuses and attacks with low to medium risk can still occur. Therefore, the B*ypass Rate* shall not be too low when medium- and low-priority risks have not been mitigated. The recommendations that correspond to high-priority misuse cases are used in the calculations of the Cost/Benefit Analysis Framework. *Cost Avoidance* is used as the benefit for each *Category of Preventions*. If there are any other intangible benefits, they should be included as well.

Costs of implementation for each recommendation need to be estimated, checked with stakeholders, and then adjusted based on their feedback. Total System Value, Total

Implementation Costs, Net Project Value, and Benefit/Cost Ratio (B/C) are then calculated. For more details, see Section 2.4, “Evaluation Criteria.”

2.3 Stakeholder Involvement

Stakeholders must be regularly involved in this Cost/Benefit Analysis Framework to ensure reasonably accurate results, especially during the misuse case identification phase and the cost estimation phase for implementing recommendations. After the stakeholders reply with their feedback and suggestions for change, cost/benefit calculations should be updated and improved on in a reiterative process over a span of several weeks. Small companies probably do not have months of time to analyze a project. Therefore, we recommend that the Cost/Benefit Analysis be done with an existing set of templates instead of reinventing the wheel. Also, it is important to keep in mind that the proposed system and alternatives may change, depending on a company’s internal assessment of its assets, vulnerabilities, development timeframes, and risks and their associated costs, among other variables.

2.4 Evaluation Criteria

The criteria for evaluating alternatives are based on five key metrics: Total Implementation Costs, Net Project Value, Total System Value, Benefit/Cost Ratio, and *Risk Exposures*. These five criteria serve different purposes. Total Implementation Costs can help small companies make decisions as to how much money they can spend without jeopardizing growth in other areas of need. Net Project Value demonstrates the extent to which a particular security solution can contribute to the overall system. Total System Value takes into consideration the fact that unmitigated threats still cost a company some amount of money in risks. It accounts for scenarios where the Net Project Value is high while the overall value of the system is low because the solution did not address costly threats. A positive Net Project Value is a strong key indicator that the solution is worthwhile to implement; a large Total System Value suggests that the system will be improved by implementing the project; and a large B/C Ratio relative to other solutions indicates that the solution should be implemented first because it is more cost effective. Combined with *Risk Exposures* after implementing the proposed system versus implementing alternatives, these five criteria form the basis of correlation between benefits of desired security improvement, costs within available fiscal budget, and tolerance of acceptable *Risk Exposures*. The proposed system and the alternatives will be chosen from a finite set of possible solutions that small companies may wish to implement or ignore, based on comparing and analyzing present values of these metrics.

Let’s assume that *Categories of Preventions* have the following characteristics, which we can calculate by doing a cost/benefit spreadsheet on each category. All values are NPV.

Category of Preventions (P_i)	**Baseline Cost (A_i) if X_i = 0**	**Residual Cost (R_i) if X_i = 1**	**Implementation Cost (C_i) if X_i = 1**
1	A_1	R_1	C_1
2	A_2	R_2	C_2
…			
N	A_N	R_N	C_N

Total Implementation Costs

Total Implementation Costs are the present value costs calculated over the length of the project. Because there might be overlapping in costs of implementing architectural and policy recommendations when some recommendations (e.g., good password management) may be necessary to mitigate multiple *Categories of Threats*, total implementation costs are the sum of all present value costs of implementation minus any overlapping costs.

$$\text{Total Implementation Costs } = \sum_{i=1}^{N}(C_i \times X_i) - \sum_{j=1}^{N}\sum_{k=j+1}^{N} Overlap\_Cost_{jk} \times X_j \times X_k$$

Net Project Value

Net Project Value is the present value of savings (loss) from the total benefits of implementing recommendations minus total costs of implementing recommendations. It demonstrates the value that the project can deliver to the overall system. The higher the Net Project Value is, the better.

Net Project Value (NV) = Total Benefits – Total Implementation Costs

Total System Value

Total System Value is the present value of Net Project Value minus the present value of expected loss from unmitigated threats. It takes into consideration that unmitigated threats still cost companies some amount of money in risks. If a *Category of Threats* is mitigated, then its *Residual Cost* is used; otherwise its *Baseline Cost* is used. Total System Value accounts for scenarios where the Net Project Value is high while the overall value of the system is low because the solution did not address costly threats. It evaluates the system's overall value after implementing the project and provides high-level guidance to the business objective beyond the project itself. The higher the Total System Value is, the better.

Total System Value (TV) = Net Project Value - costs of unmitigated risks

$$= \text{Net Project Value} – (\sum_{i=1}^{N} X_i \times R_i \times + \sum_{i=1}^{N}(1 - X_i) \times A_i)$$

Theoretically the higher TV is, the better; but it needs to be taken into consideration with *Risk Exposures* and other company-specific factors. Because X_i is either 0 or 1 (2 choices) and there are N categories, there are 2^N possible solutions. For small N this can be easily calculated via a computer program (e.g., Microsoft Excel), which is the case in the Acme Company example. In fact, this is where categorization helps out small companies in terms of estimation efforts because it reduces the size of N.

Benefit/Cost Ratio (B/C)

Benefit/Cost Ratio pertains to the ratio between the net benefit in implementing a security solution and the costs of implementation. It demonstrates the capability for the organization to profit (cost savings) from its security investments. The higher the B/C Ratio, the better an investment is.

$$\mathrm{BC} = \frac{Total\_Benefits}{Total\_Implementation\_Costs}$$

Example 3:

If it costs $200,000 to implement solutions for A and $150,000 to implement solutions for B, with $40,000 of overlapping hardware costs, then:

Total Benefits = $335,000 (from Example 2)
Residual Costs (A) = $15,000 (from Example 1)
Residual Costs (B) = $42,000 (from Example 1)

Total Implementation Costs = $200,000 + $150,000 - $40,000 = $310,000
Net Project Value = $335,000 - $310,000 = $25,000
Total System Value = $25,000 – ($15,000 + $42,000) = -$32,000
Benefit/Cost Ratio = $335,000/$310,000 = 108%

2.5 Maximizing System Value Within Real-Life Budget Constraints

We have until now presented a framework that analyzes the proposed system versus the alternatives assuming that there are no limits and no variations to yearly budgets. For the sake of convenience, we assumed that the budget is going to be so large that these variables could be ignored. However, we know from real-life experience that this is often not the case, especially in small companies where capital is at a premium. Companies with little initial budgets and large future budgets will make their decisions significantly different from companies that have large initial budgets but little future budgets. In such cases, to deal with real-life budget constraints, we must find a linear solution in which all constraints are linear functions of the decision variables. Some or all of the decision variables must have integer values (0 or 1, do or not do). In mathematics terms, the model to solve these kinds of problems is called *Integer Model* [Camm 00]. We are able to do so because decisions to implement *Categories of Preventions* are essentially concrete (yes/no), and the options come from a finite set of *Categories of Preventions* that are sufficiently distinct from each other.

Back to the problem, there are N possible *Categories of Preventions* to implement, each of which runs for M number of years, with the following Total System Values and yearly implementation costs.

Category of Preventions **(P_i)**	**Implementation Cost (C_{it})** **if X_i = 1**			
	Y_0	Y_1	…	Y_M
1	C_{10}	C_{11}		C_{1M}
2	C_{20}	C_{21}		C_{2M}
…				
N	C_{N0}	C_{N1}		C_{NM}

And we have available budget for each year: B_0, B_1, … B_M , with B_0 being the initial budget.

Now we have to decide which set of *Categories of Preventions* to implement in order to maximize our returns within the budget constraints. We know that yearly costs for implementations must also be within the yearly budget. The constraints for the *Linear Model* problem are then the linear sum of implementation costs for each category. If a *Category of Preventions* was implemented, then it would contribute its cost against the budget; otherwise it will count as 0.

$$\sum_{i=1}^{N} C_{it} \times X_i \le B_t \qquad \text{(t=0, 1, 2…M)}$$

or

$$C_{10} \times X_1 + C_{20} \times X_2 + ... + C_{N0} \times X_N \le B_0 \qquad \text{(year 0)}$$
$$C_{11} \times X_1 + C_{21} \times X_2 + ... + C_{N1} \times X_N \le B_1 \qquad \text{(year 1)}$$
$$\text{…….} \qquad \text{……}$$
$$C_{1M} \times X_1 + C_{2M} \times X_2 + ... + C_{NM} \times X_N \le B_M \quad \text{(year M)}$$

There could be Z number of solutions to this set of equations, where Z is less than or equal to 2^N.

We can exhaustively apply every set of possible ($X_1, X_2 \dots X_N$) values to calculate financially feasible solutions under the budget constraint. In fact, in most cases we expect the exhaustive method to be used because it is easy to understand and easy to calculate when N is not too large. However, should there be a situation where N is very large, the *Branch and Bound* method may be used. *Brand and Bound* is an algorithmic technique to find the optimal solution by keeping the best solution found so far [NIST 04]. In the *Brand and Bound* method, if a partial solution cannot improve on the best value, it is abandoned. The method systematically enumerates a fraction of feasible solutions, while still guaranteeing that the most optimal integer solution is found.   Several commercially available software packages support the *Brand and Bound* method, including Microsoft Excel.

In the end, we should get a set of *TV* values and a set of ($X_1, X_2 \ldots X_N$), from which we derive the proposed system and possible alternatives. When we analyze them with their associated Benefit/Cost Ratio and *Risk Exposures*, we can find the best paths to take for information security improvement projects in small companies.

3 Cost/Benefit Analysis Framework in Practice

The Cost/Benefit Analysis Framework is applied on the Acme Company to help it determine how to meet its security and business objectives at the same time within reasonable costs.

3.1 Misuse Cases

Before the cost/benefit analysis can be done, misuse cases must be identified in order to accurately access the impact of misuses when they happen. This report will not go into detail about how these misuse cases are generated. The misuse case documentation shown in Table 2 is provided as an example of the level of detail misuse cases need in order to derive comprehensive architectural recommendations and policy recommendations. Attack trees for misuse cases may also be used to ensure that the list of architectural and policy recommendations is complete.

Table 2: Example Misuse Case

Number:	MC-xx	
Name:	Users gain sys admin rights on the server (elevation of privileges).	
Scope:	User Authorization Concerns	
Priority:	___ Low ___ Medium _x_ High	
Deployment Environment:	_x_ Intranet ___ Extranet/Internet	
Mis-actors:	Users	
Access Right Levels:	___ Low-Level System User _x_ Medium-Level System User _x_ High-Level System User ___ Sys-Admin-Level System User _x_ Other Network User	
Point of Entry:	___ Network _x_ Host ___ Application	
Security Attributes affected:	_x_ Confidentiality _x_ Integrity ___ Availability	
Description:	A user attempts to gain sys admin rights on the server and succeeds.	
Sophistication:	___ Low ___ Medium _x_ High	
Pre-conditions:	• The user has unintended logon rights to the Windows 2003 server.	
Assumptions:	• The user is not already a sys admin. • The user does not have expressed permission to gain sys admin rights.	
Post-conditions:	Worst Case Threat:	• The user gains sys admin rights on the server and then tampers with system and/or user data. His/her actions are never caught.
	Wanted Prevention Guarantee:	• Enforce machine access control list (ACL) security policy (role-based user authentication).

	Wanted Detection Guarantee:	• Logon attempts are logged and viewed by system administrators.
	Wanted Recovery Guarantee:	• Remove users’ unauthorized logon rights on the server.
Potential Mis-actor Profiles:	Highly skilled users with high criminal intent.	
Stakeholders and Threats:	• Acme Company’s client: loss of data integrity and/or confidentiality • Acme Company: loss of reputation, loss of current and potential clients	
Related Use Cases:	UC-06, UC-07, UC-08	
Related Threats:	Elevation of privileges, unauthorized access to administration interfaces, unauthorized access to configuration stores	
Architectural Recommendation:	• Store audit information in a separate location from the servers and the workstations. • Implement a strong role-based authentication control.	
Policy Recommendation:	• Patch applications and operating systems routinely (bimonthly). • Ensure that users do not have rights or access levels beyond those prescribed by their job responsibilities. • Review audit information routinely (monthly). • Store and cross-review configuration changes (monthly). • Enforce strong password policies. • Password protect any necessary shared documents. • Require users to change their passwords periodically (monthly). • Periodically review user activities (bimonthly). • Require users to log out of the system or close their browser as soon as their activities are done. • Require users never to reveal their account names and passwords. • Perform routine system and data backup (weekly).	

3.2 Categories of Threats

The Cost/Benefit Analysis Framework categorizes all misuse cases into seven *Categories of Threats*:

- Denial of Service
- System Penetration
- Sabotage of Data
- Theft of Proprietary Info
- Unauthorized Access by Insiders
- Virus
- Active Wiretapping [Richardson 03]

Financial and probabilistic data are available for these categories from the *2003 CSI/FBI Computer Crime and Security Survey* [Richardson 03]. Given that the Acme Company had not paid much attention to its own security efforts up to this point in time, we assumed that Acme will have *Baseline Risks* at or near national average within each *Category of Threats*. The lower end of reported losses is initially used as the estimate of *Annualized Loss* if attacks were successful in achieving observable damages. Later the Acme Company performs an internal estimation and determines a more precise set of financial numbers that get incorporated in the analysis instead.

3.3 Risk Exposures

The cost/benefit analysis assumes that the *Bypass Rate* is approximately 10%. Subsequent calculations show that when none of the seven *Categories of Threats* are mitigated, the Acme Company's core product's *Risk Exposures* to some combination of misuses are above 90%. Because the probability of misuses/attacks is very high, the cost/benefit analysis is needed in order to manage and mitigate the company's *Risk Exposures* for its core product.

3.4 Architectural Recommendations

From our work, we have discovered that architectural recommendations tend to have costs that are heavily front-loaded (e.g., initial implementation costs). It intuitively makes sense because architectural improvements need to be implemented, tested, and deployed before benefits can be realized over the lifetime of a project. The Acme Company prefers to view the costs of implementation in terms of man-hours of effort. We have no objections to this method of evaluation. In fact, we would recommend the man-hour estimation method to our future clients because it is a standard way of making engineering estimates. We can then multiply man-hours with average hourly wage rates to arrive at a good estimation of total costs. Other than costs of salaries, there are maintenance costs (also calculated via man-hours), third-party software costs, and hardware costs. Table 3 shows the format we used to break down the types of costs that architectural recommendations have.

Table 3: Cost Estimates for Architectural Recommendations

No.	Architectural Recommendation	Related Misuse Cases	Priority	Category of Threat	Implementation Cost ($/ year)	Maint. Cost ($/ year)	Software Cost [Type]/($)	Hardware Cost [Type]/ ($)
AR-01	All shared drives on the network should enforce authentication policies.	MC-01	High	U	$xxx	$xxx	$xxx	$xxx
AR-02	Antivirus software is installed on the server.	MC-17	High	V	$xxx	$xxx	$xxx	$xxx

3.5 Policy Recommendations

Policy recommendations tend to recur over the lifetime of the project. The cost of training and the cost of enforcement are difficult to quantify on the macro level. However, the feedback we gained from the Acme Company is that it is much easier to visualize the efforts in terms of man-hours per user per year. The total costs can then be calculated by multiplying man-hours per user per year with an estimated number of users and with average hourly wage rates. Table 4 shows the format we used to break down the types of costs that policy recommendations have.

Table 4: Cost Estimates for Policy Recommendations

No.	Policy Recommendation	Related Misuse Cases	Priority	Category of Threat	Training Cost ($)	Enforcement Cost ($)	Other Costs [Type]/ ($)
PR-01	All installation must be approved and reviewed by managers.	MC-13, MC-15	High	U, W	$xxx	$xxx	Name/$xxx
PR-02	Applications and operating systems must be patched routinely (bi-monthly).	MC-01, MC-03, MC-13, MC-15, MC-16, MC-17, MC-18, MC-19, MC-20, MC-21, MC-22	High	U, P	$xxx	$xxx	Name/$xxx

3.6 Total System Value Versus Total Implementation Costs

The Total System Value vs. Total Implementation Costs graph in Figure 2 shows us there are optimal and non-optimal solutions among the security solutions that the Acme Company may choose to implement. The solutions with higher Total System Value are better solutions. The four colored boxes (solutions) are better solutions within their respective cost ranges because they have the highest Total System Value compared to other solutions on the same vertical lines in the graph. The pink solution represents the Total System Value of the current system. It has zero total implementation costs. The Blue solution (Alternative 2) represents the total value of the system when every architectural and policy recommendation has been implemented. The brown solution (Alternative 1) and the red solution (Proposed System) have the highest Total System Value, meaning that by implementing either one the Acme Company can obtain the best value for its system over the next three years of project lifetime. From a strictly financial perspective, solutions with higher Total System Value and lower Total Implementation Costs are preferred. Therefore, the graph suggests that Alternative 1 is a better solution than the Proposed System or Alternative 2. However, it is not immediately apparent from this view the extent to which *Risk Exposures* are reduced. We shall examine *Risk Exposures* in later sections. It is worth noting, however, that Alternative 1 is a subset of the Proposed System.

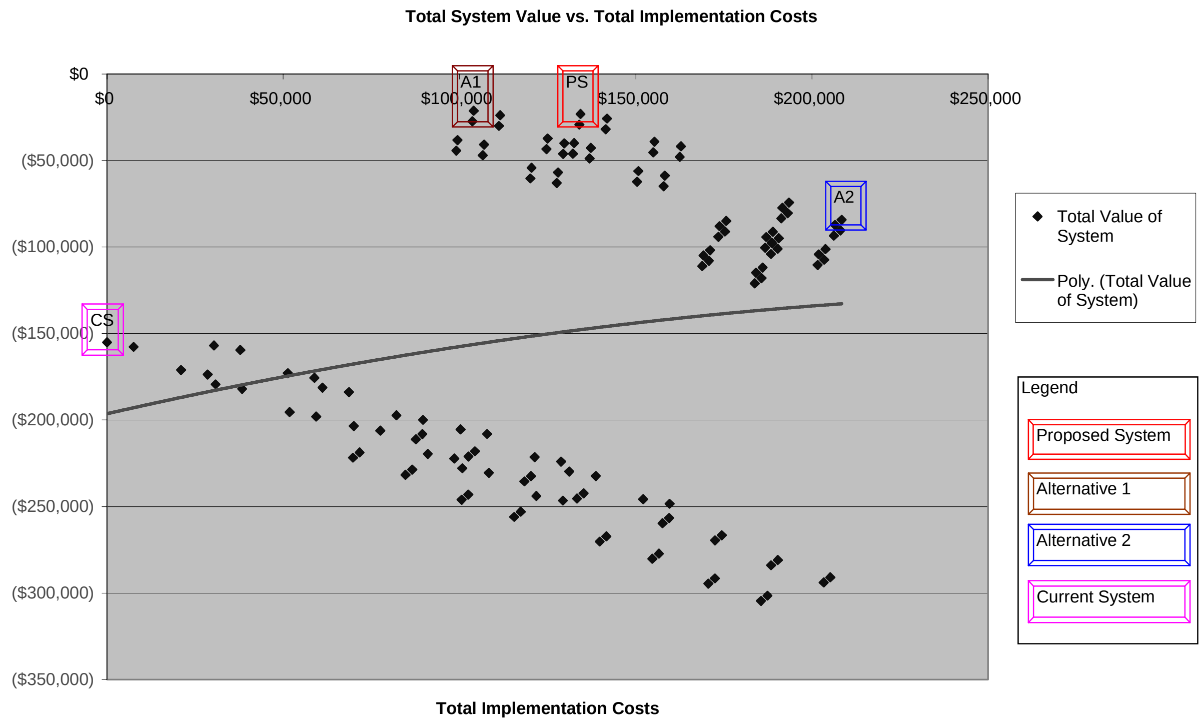

Figure 2: Total System Value vs. Total Implementation Costs

3.7 Benefit/Cost Ratio Versus Total Implementation Costs

How effective are the solutions in delivering results? Benefit/Cost Ratio gives us the trend pattern when compared against the Total Implementation Costs. From the graph, B/C Ratio briefly increases before dropping as costs of implementing security recommendations go up. Small companies often gain significant benefits by implementing a small set of selected security improvement recommendations but then lose the benefits when they start to implement additional security solutions.

The Benefit/Cost Ratio vs. Total Implementation Costs graph in Figure 3 suggests that there are highly cost-effective security solutions that should be implemented first. The Current System is not present on this graph because there is no implementation cost involved with taking no action. Similar to the Total System Value vs. Total Implementation Costs graph, the three solutions with higher Total System Value are more cost effective when compared against other security solutions that have the same implementation cost. Alternative 1 appears to be more cost effective than the red or blue solution. However, when compared to the previous graph, we note that Alternative 1 and the Recommendation have the same total value. This suggests that the additional investment with the Recommendation mitigates the cost of additional risk at or near 100% Benefit/Cost Ratio, which is the case when we see that the Recommendation has approximately 100% Benefit/Cost Ratio. The trend line also suggests that if the Acme Company invests more resources to become more secure, its return on the investment will decline precipitously. Without intangible benefits such as new revenue opportunities, large investments associated with making many security improvements are probably difficult to justify beyond an acceptable level of risk tolerance.

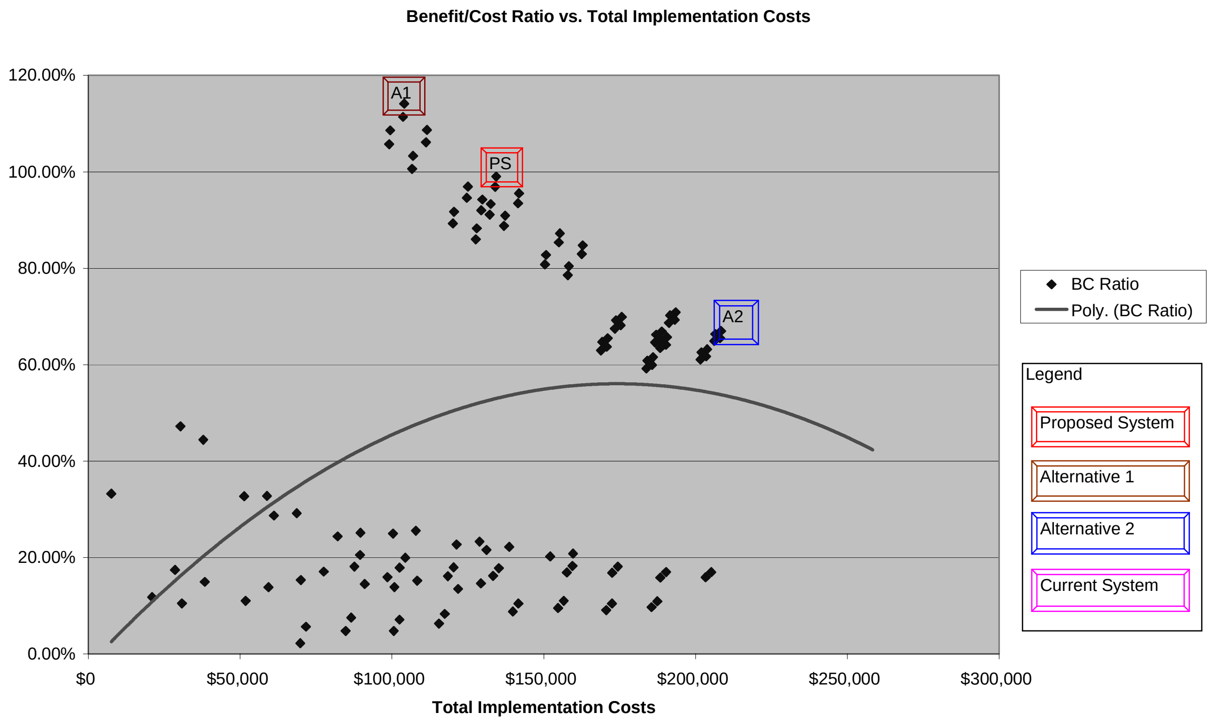

Figure 3: Benefit/Cost Ratio vs. Total Implementation Costs

3.8 Total Implementation Costs Versus Risk Exposures

The Total Implementation Costs vs. Risk Exposures graph in Figure 4 shows us that initially security improvements can be costly. Security improvements may be best when done together with implementing multiple *Categories of Preventions*. The solutions that mitigate more risks with lower costs are better solutions.

There are several things to be noticed with the graph. First, costs go up when *Risk Exposures* go down, which is to be expected. Second, the smallest *Risk Exposure* is not near zero. This is due to the fact that a small company such as the Acme Company may not have the resources to implement and enforce every single recommendation. Therefore, its *Bypass Rates* and *Residual Risks* for security breaches are still high, which causes its *Risk Exposures* to be high. More detailed studies are warranted if the Acme Company needs to reduce its risk exposures further. However, from the trend projection, we can see that the cost goes up significantly as *Risk Exposures* become smaller and smaller. It is an indication that the costs needed to cover edge scenarios may be very expensive and may only be justified with large increases in the benefits (such as new revenue opportunities) that additional security improvements would bring.

The variance around the trend line is extremely high when risks are not mitigated. This suggests a few possible scenarios. First, there are *Categories of Threats* with low rates of return and high costs to fix. Therefore, they should only be implemented after other categories with higher Benefit/Cost Ratio. Second, strategies that focus on mitigating only very small number of *Categories of Threats* may be neither cost effective nor risk averse.

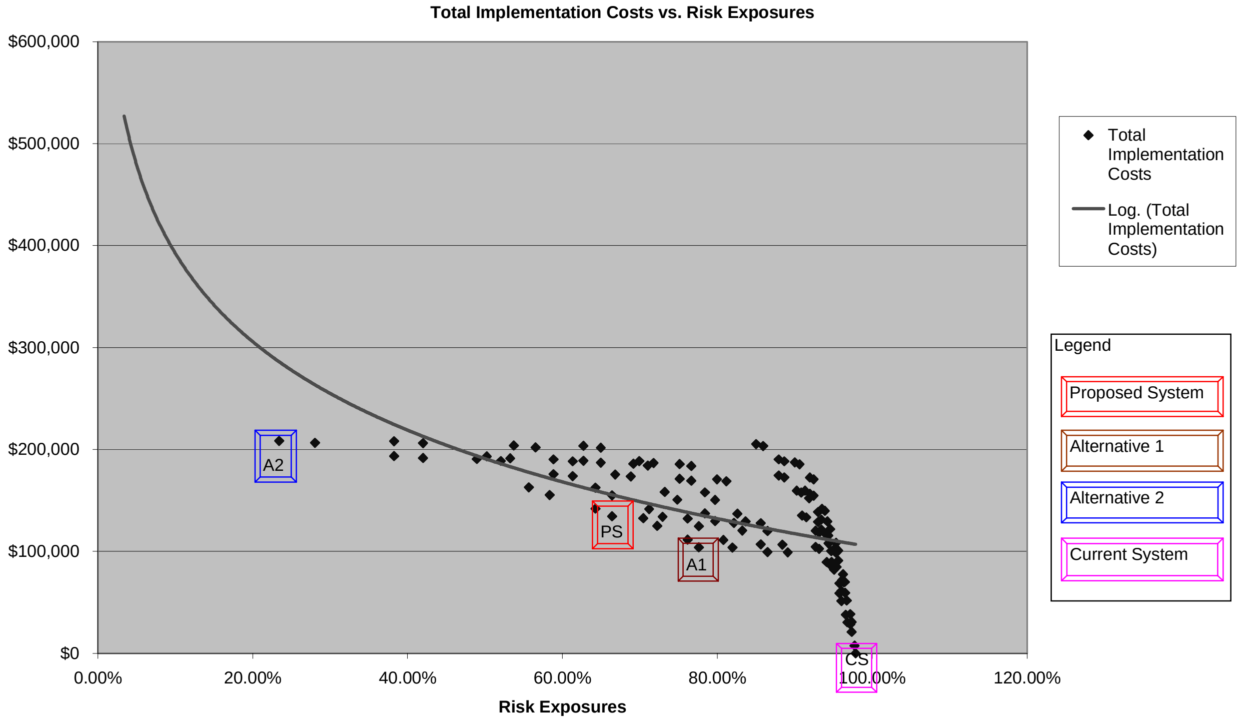

Figure 4: Total Implementation Costs vs. Risk Exposures

3.9 Values Versus Risk Exposures

The Values vs. Risk Exposures graph in Figure 5 shows us what happens when *Risk Exposures* are taken into consideration. The graph shows the relationships between Net Project Value, Total System Value, and *Risk Exposures*. The gap between Total System Value and Net Project Value represents the amount of costs in unmitigated risks the Acme Company is subject to with respect to each possible solution. Because costs of unmitigated risks are the product of multiplying probabilities of occurrence by *Annualized Loss* (when misuses happen), they are essentially approximations of costs of uncertainty. The higher *Risk Exposures* are, the higher the uncertainty and volatility is. As *Risk Exposures* decrease, gaps become smaller and Total System Value becomes more predictable. Therefore, the Proposed System is a much more risk-averse solution that delivers the same results when compared to Alternative 1. So it is a better solution, with same Total System Value, less volatility, higher predictability, and smaller *Risk Exposures*.

Furthermore, the dotted line of Total System Value w/o Residual Costs is shown to demonstrate the extent to which *Residual Risks* can have an affect on the Total System Value.

When security solutions are highly effective (i.e., *Bypass Rate* is small), the gap between the two Total System Values will be small; otherwise the gap will be large. The gap between the two Total System Values represents the costs of the *Residual Risks* that the project's available security solutions cannot mitigate. In order to reduce the *Residual Costs*, the Acme Company needs to consider implementing medium- and low-priority recommendations.

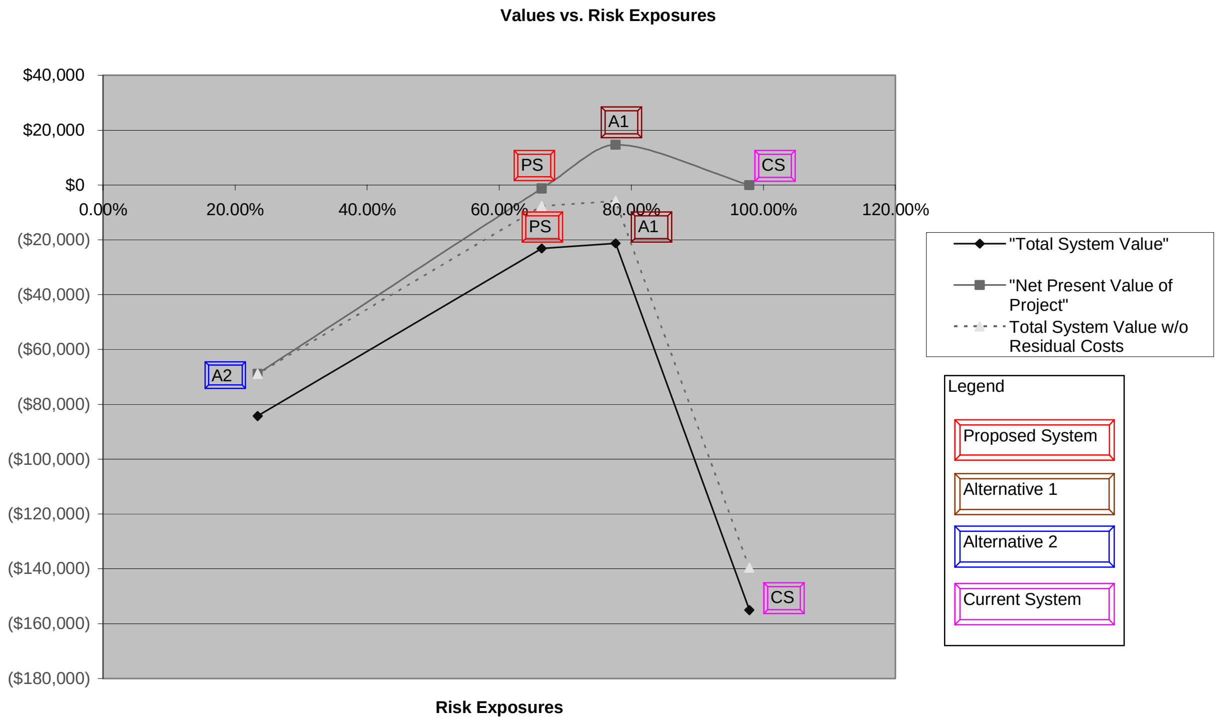

Figure 5: Values vs. Risk Exposures

4 Lessons Learned

4.1 Misuse Cases

The Cost/Benefit Analysis Framework is built on misuse cases. Even though the generation and validation of misuse cases are not discussed in this report, the comprehensiveness of misuse cases will directly impact the accuracy of the results in the cost/benefit analysis. We have discovered that a cost/benefit analysis contributes to more clarification and better understanding of the project's misuse cases. The average probabilities of occurrence and expected loss give insights into the prioritization of misuse cases when costs of risks are ranked. In addition, it provides quantifiable mapping from descriptions to implementation choices for architectural and policy recommendations. Understanding man-hour and capital expenditure requirements helps stakeholders plan the project with respect to their situations.

4.2 Estimation of Losses

The framework initially used estimated cost figures from the lower end of nationally surveyed losses for each *Category of Threats*. Later on, we worked with the Acme Company to come up with a set of loss figures for each misuse case per incident. We multiplied estimated frequencies (per year) by estimated incident losses (for all misuse cases in a category) to derive the *Annualized Loss* for each *Category of Threats*. Through this process we found that

- Lower ends of nationally surveyed losses may be used as estimations for tangible losses (productivity loss, fixing cost, etc.).
- Surveyed losses cannot sufficiently account for intangible losses (loss of reputation, loss of confidential data, etc.), since these values are highly company and project specific.
- Intangible losses often exceed tangible losses for many *Categories of Threats*.
- For small companies, loss of reputation may be a very important item of interest, and it can contribute significantly to intangible losses.

Therefore, for better accuracy, we highly recommend that losses are estimated for each misuse case.

4.3 Estimation of Costs

Our experience is that the Acme Company strongly prefers the use of man-hours to estimate costs of implementation. Its senior technical and project leads make effort estimations in man-hours. The company provides average cost figures for employees in different roles.

Costs are then calculated on the number of man-hours multiplied by average hourly wage rates. We found this process of cost estimation to be very effective. We will strongly recommend this process in our future work.

4.4 Cost Structures of Security Improvement Projects

We found that the costs of ensuring policy compliance heavily dominate in the costs of implementation for virtually every *Category of Threats*. This suggests that security improvement projects are very human-effort intensive in their cost structures. The costs will be spread over the lifetime of these projects. Such costs are often seen as “hidden costs” that many companies traditionally have difficulties in quantifying. The framework can provide significant insight into the hidden costs of policy compliance by examining and then summing up the efforts for every recommendation. However, because costs are accumulated over multiple years, companies that take on security improvement projects need to look at their investments from a long-term perspective. The cost structures of security improvement projects will be determined primarily by the companies’ willingness to invest in their employees on security awareness and policy enforcement.

4.5 Values of Security Improvement Projects

The Acme Company’s most optimal Total System Value is still negative. There are two possible explanations for this phenomenon. First, *Residual Risks* still cost companies a certain amount. Real-life experiences have shown us that no security solution is 100% secure. Therefore, even the best effort of security improvement may not reduce risks to zero. Second, security improvement may need to be viewed from a lose-less perspective rather than the profit-more perspective that typical IT projects are judged on. Lose-less is another way of profiting by minimizing the risks of having misuses and attacks.

5 Conclusions

The objective of the Cost/Benefit Analysis Framework is to provide a quantifiable financial analysis framework that small companies can apply on their security improvement projects. Within this scope, we show that unmitigated risks can be translated into costs, and we demonstrate the estimation methods for calculating costs of implementation for architectural and policy recommendations. Most importantly, we show through the example of the Acme Company that small companies can obtain optimal results for improving the security of their systems and the optimal results can be achieved with reasonable reductions in *Risk Exposures*. The reductions in *Risk Exposures* in turn enable small companies to have less volatility in their Total System Value. The increase in predictability of results by implementing optimal security solutions will enable small companies to profit from security improvements and to plan for future growth.

6 Future Work

There are several questions that drive future work on the Cost/Benefit Analysis Framework:

- Can the Acme Company’s trend patterns be witnessed in other small companies and their security improvement projects?
- How would the estimate values compare to empirical data if we were to follow through with the Acme Company over the lifetime of its project?
- Are there any other variables that we have not accounted for in the framework? If so, why do they exist and how can we account for them?
- What if *Categories of Threats* cannot be assumed to be independent from each other? So far we have assumed that the effects of mitigating threats in one category are negligible to the risks in other categories. If this assumption no longer holds, how do the resulting interdependencies affect the framework?
- Can the framework be applied to larger companies?

The overall goal of the framework is to provide a way for small companies to be able to accurately estimate the cost of their security improvement projects. By incorporating lessons learned from the Acme Company, we will strive in the future to

- refine the estimation methods to facilitate further analysis
- use the estimation methods with other companies to see if similar trend patterns exist
- develop a general set of cost/benefit profiles and metrics for projects with different types of system architectures
- design a spreadsheet to automate the cost/benefit calculations and to select the most optimal solution
- formalize the relationship between the five metrics we proposed in Section 2.4

References

URLs are valid as of the publication date of this document.

[Allen 99] Allen, J.; Christie, A.; Fithen, W.; McHugh, J.; Pickel, J.; & Stoner, E. *State of the Practice of Intrusion Detection Technologies* (CMU/SEI-99-TR-028, ADA375846). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028app-a.html.

[Camm 00] Camm, Jeffrey D. & Evans, James R. *Management Science & Decision Technology*. South-Western College Publishing, 2000.

[NIST 04] National Institute of Standards and Technology. *branch and bound*. http://www.nist.gov/dads/HTML/branchNbound.html (2004).

[Richardson 03] Richardson, Robert. *2003 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (2003).

[SANS 03] SANS Institute. *SANS Glossary of Terms Used in Security and Intrusion Detection*. http://www.sans.org/resources/glossary.php#top (2003).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE November 2004	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE

SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies

5. FUNDING NUMBERS

F19628-00-C-0003

6. AUTHOR(S)

Nick (Ning) Xie

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

CMU/SEI-2004-TN-045

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Many companies rely on historical data to build predictability models for cost/benefit justification of future projects. Unfortunately, for small companies, which generally do not have a process for collecting security data, the costs and the benefits of information security improvement projects have been very difficult to estimate and justify. In addition, detailed attack data are simply not available to be used as references in cost estimations. Given these difficulties, many small companies choose to ignore entirely the security vulnerabilities in their systems, and many suffer the consequences of security breaches and significant financial loss. Small companies that do implement security improvement projects often have problems understanding the cost structures of their improvement initiatives and how to translate risk exposures into costs that can be passed on to their customers.

To deal with the aforementioned problems, this paper describes a general framework for hierarchical cost/benefit analysis aimed at providing acceptable estimations for small companies in their information security improvement projects. The framework classifies misuse cases into categories of threats for which nationally surveyed risks and financial data are publicly available. For each category of threats, costs, benefits, baseline risks, and residual risks are estimated. The framework then generates all permutations of possible solutions and analyzes the most optimal approach to maximize the value of security improvement projects. The framework analyzes the problems from five dimensions: Total Implementation Costs, Total System Value, Net Project Value, Benefit/Cost Ratio, and Risk Exposures. The final proposed system will be derived from the comparisons of these dimensions, taking into consideration each company's specific situation.

This report is one of a series of reports resulting from research conducted by the System Quality Requirements Engineering (SQUARE) Team as part of an independent research and development project of the Software Engineering Institute.

14. **SUBJECT TERMS** cost/benefit analysis, information security improvement, information security costs, misuse cases			15. **NUMBER OF PAGES** 40
16. **PRICE CODE**			
17. **SECURITY CLASSIFICATION OF REPORT** Unclassified	18. **SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	19. **SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	20. **LIMITATION OF ABSTRACT** UL