Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp75-80)

Budgeting for Information Security and ROI Approach

Akshai Aggarwal *, Vishnu Kanhere. †, Shankar Kanhere ††, Nilesh Bajoria †††

* Computer Science, University of Windsor, Windsor, Ontario, CANADA
† Consultant on e-Security, Software Valuation, Mumbai, INDIA
†† The Bombay Dyeing& Mfg Co. Ltd., Mumbai, INDIA
††† IT Consultant, London, UNITED KINGDOM
akshaia@uwindsor.ca, vkanhere@vsnl.com,
sdkanhere@gmail.com, nileshbajoria@hotmail.com

Abstract: - Information security expenditure involves heavy investment in people, processes and tools. Information system security projects cover a number of non-quantifiable factors not amenable to simplistic cost benefit or ROI analysis. Associated cost/benefits are contingent upon uncertain factors, including level, type, nature and extent of security. Moreover security projects have to comply and deal with statutory issues and differ from case to case. For such projects, the expected productive life, the training period, the periodicity and quantum of benefits/inflows and the expected future outflows required for maintenance, have to be estimated, making quantification complex. The proposed method uses the concept of Total Cost of Ownership, consisting of Direct and Indirect Costs of deploying and maintaining the system for base level security. Option price based ROI method is used to create the second metric for additional level of advanced security. We use the metrics to estimate the net pay offs of the different choices under different probable conditions. The result is a decision matrix to assist stakeholders in decision-making.

Key-Words: - Information security expenditure, non-quantifiable factors in IT Security Projects, cost benefit and ROI analysis, Total Cost of Ownership of IT Security, Option price based ROI, decision matrix to assist stakeholders.

1 Introduction

Expenditure on information security constitutes as much as 10% of the total outlay on information technology. It is a field that is witnessing many changes and challenges. The technology is fast evolving and enterprises need to keep pace with the developments, if they have to maintain an effective level of security.

Admittedly, in the post 9/11 scenario properly implemented Information Security Management Systems (ISMS) can make a vital difference to the very existence of any business. With stringent legislation, which requires companies to secure and protect data and information assets, and with introduction of legislation like Law 1386 in California, the expenditure on information has become a necessity even for the small and medium sized business segment.

Information security, along with ethical practices, objectivity in decision-making, transparency, accountability and social responsibility, is one of the key pillars of corporate governance. With the advent of legislation similar to the Sarbannes Oxley Act in the US, worldwide, it is information security that helps management in performing its key role of protection of assets to ensure productive utilization, without interruption. ISMS also helps prevention and detection of frauds to plug leakages, which water down the net worth of businesses. In today's world, information security has moved from the desks of the CTOs, CSOs, and CIOs to the boardrooms. Information security systems ensure that the confidentiality, integrity and authenticity of data, along with its easy accessibility and transferability comply with the business requirements and with the legislative rules and governance framework.

Information security expenditure depends on and is decided by many intangible factors. It involves heavy investment in people, processes, tools and training. Given the ever-changing scenario it also involves a high degree of uncertainty. The resources at the disposal of an organization are always limited. With the constant pressure on margins and the bottom line due to intense global competition, budgeting for Information Security has become necessary to ensure proper utilization of funds and to get maximum value for money. Moreover carrying out a budgeting exercise for

information security provides a reality check and helps prevent self-delusion and wasteful misdirected effort and expenditure in the battle for information security [1].

Information system security projects by their very nature are not amenable to a simplistic cost benefit or a regular ROI kind of analysis. This stems from the fact that associated cost/benefits are contingent upon a number of non-quantifiable factors and involve considerable uncertainty, making quantification a complex task. Moreover security projects have to comply and deal with statutory issues and differ from case to case. Further, ISMS projects have a high degree of uncertainty in respect of expected productive life, gestation/training/implementation period, periodicity and quantum of benefits, expected future outflows required for maintenance and consequential costs [1]. One school of thought considers ISMS spend as an expenditure rather than an investment, since for ISMS spend, ROI cannot be measured with any degree of certainty [2].

Section 2 describes the background analysis required for any ISMS project. This information is also valuable for preparing a budgetary justification for expenses on ISMS projects. Section 3 describes the basic concept of Total Cost of Ownership (TCO), as applicable to security products. The Return on Investment (ROI) calculation method is discussed in Section 4. The annual loss expectancy and the macro and micro level factors that affect security and the budgeting process are given in section 5. Section 6 describes the two stage option-pricing model and the TCO options approach. The procedure for building a business case is described in section 7. At the end, the balanced scorecard framework is worked out in section 8. The conclusions of the study are given in the last section.

2 Setting the Ground work

Before embarking on the idea of a budgetary exercise, an enterprise needs to answer a few questions, so that the process of budgeting may begin.

These questions resolve around what, when, where, whom, which, how and why information security?

What are you trying to protect?
Data information, processes, products,people, assets, reputation.

Upto when are you going to protect?
A minute, an hour, a day, a year, twenty years?

Where are you going to protect?
On the hard disk, in the system, on the Network, in the data base on the laptop/on the main server.

Whom are you going to protect against?
*T*he delinquent *insiders, the malicious hackers against?*
The business competitor? The computer geek/yuppie? The occasional snooper?

Against which attacks/threats do you seek protection? – some of them? Those, which are more frequent? Those, which are more disastrous? Those, which have high visibility? All attacks and threats? Those, which cannot be insured?
How are you going to protect? In house/outsourcing, proprietary solutions, commercial product or customized? Centralized solution or distributed? heavy absolute protection level or workable functional security?
And finally, why are you trying to protect? To avoid monetary loss? To avoid loss of reputation? To ensure business continuity?

The ISMS budgeting exercise involves getting reasonably accurate and reliable numbers for certain key costs and benefits and other incidental ones.

Costs are essentially of two types. Direct costs of security solutions and indirect costs of deploying, maintaining and using them over a period of time. The direct costs of information security would include costs of all the stages of operation starting with risk analyses and evaluation of impact.

In quantification and building up metrics therefrom, the issue of relevance becomes important. Are all these factors relevant? The reliability issue is whether the numbers are reliable and all relevant figures have been reported. The relevance and reliability of numbers can only be determined from the past history of observed trend of major losses and of information security incidents. Hypothetical future projections of probable losses and cost savings may not prove to be reliable. Security consultants have been known to over project potential threats and cost savings leading to a disillusionment and skepticism among managers about expenditure on information security.

The protocol is a structured methodology to budget for IT security based on the above approach. Certain key issues to be considered in implementing the methodology are:

1. Different regulatory and government agencies may not have the same perspective on the business case for security of components of data. Thus the requirements for settlement of credit card fraud cases and the case of security of health information of an individual may be quite different..

2. Security decisions require a tradeoff between cost, convenience and computing performance in terms of flexibility, speed and performance.

3. Retrofitting security to a legacy system v/s designing a new secure system may also be considered in some cases, particularly when a closed system is sought to be converted to a public platform.

4. To be able to protect the right things, the designer has to think like a hacker. Keep the bad guys out but let the good guys in without hassels– is the right philosophy. The only problem is that most of the successful and highly damaging attacks are mounted by insiders.

5. One size does not fit all – a bank, a military installation, a manufacturing company an ISP, a website, a small business – all of them have different needs and each one of them reacts to a security incident in a different way.

6. Cost of gold plating, bells and whistles in IT security can be high. Moreover what should be considered as gold plating may be essential in another case.

7. Insecure computers and networks cost time, money and in some cases reputation and goodwill.

3 Approach: Total Cost of Ownership Concept

A great deal of the value of the approach depends upon the analyst's understanding of the ultimate effectiveness of information security.

To determine the total cost of ownership, the costs, direct and indirect, and associated revenues (cost benefits) associated with implementing information security have to be captured and compared.

In capturing the costs – the key issues would be considered. These are balancing openness v/s security, social engineering, risks of monoculture, myth of perfect security, overprotection vs. under protection, access on need to know – need to do basis, cost of abuse, knowledge of the hacker or sophistication of level of attack and so on.

The next step is to convert the numbers into metrics for decision-making. This is done by analyzing a number of security projects actually implemented, with relative cost benefits assessments.

4 The Mathematics of the ROI Calculation [3]

Three data points are required:

1. The time period.
2. The investment.
3. The return – This is the sum of the cost savings and revenue enhancements gained from the project.

There are three ways to calculate the ROI:

1. As a percentage — If you gain benefits equal to Rs.1 million in 1 year on a total investment of $ 0.25 million in the same time period, the ROI can be calculated as follows:

Return = Payback (P) – Investment (I)
ROI = [(P - I) / I)]*100,

or in this case:
[(1mn -0.25 mn)]/ 0.25 mn * 100
= 300%

2. As a ratio — Divide the return by the investment.

1 mn/ 0.25 mn = 4:1

3. As a time to break-even — Determine the number of days, weeks, or months it will take to break even on the investment, say 12 months in our example.

Time period to break-even = (Investment/Return)*Time Period

(0.25 mn/1 mn) * 12 months = (0.25)*12 = 3 months or 90 days.

Any ROI analysis, to be comprehensive and relevant to IT projects, should include the following categories of potential benefits in determining the return from these projects [4]:

- Hard costs
- Soft costs
- Hard revenue inflow
- Soft competitive benefits

Hard costs are typically quantifiable in financial value terms and can be relatively easily estimated or

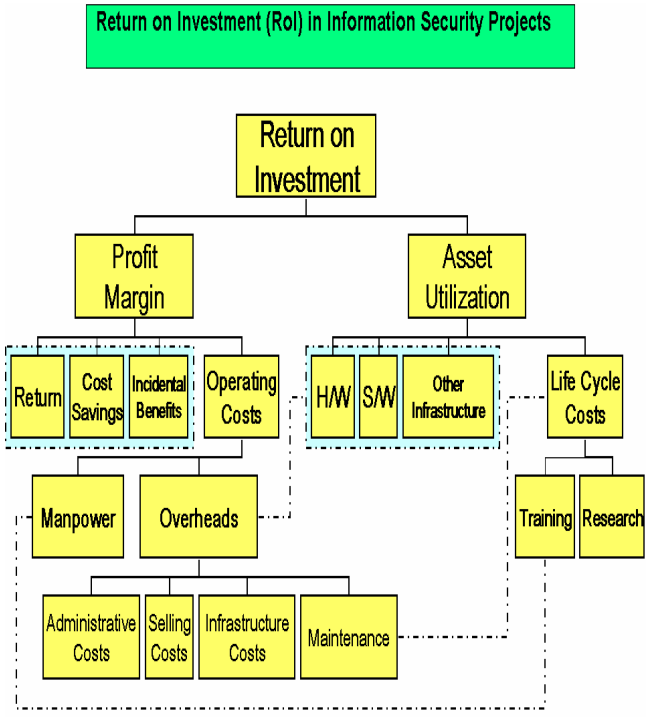

Fig. 1

Measured. For example, the investment in infrastructure and hardware can be estimated easily. However, since the same hardware and infrastructure will in all probability be used for subsequent IT projects, the initial project typically bears a very high investment cost. Only project specific costs are considered for the subsequent projects. Ideally, all projects should be allocated a component of the initial infrastructure cost. The number of projects will be a factor of the expected life of the infrastructure facilities, future uses and the estimated project completion times.

Soft costs would include opportunity costs, i.e., loss of other revenue opportunities, and consequential costs like costs incurred on business reorganisation and cost of modifications to and impact on existing business processes.

Hard revenue inflow is the total revenue value of the solution that can be estimated or measured. However, when estimating hard revenue inflow, the following factors must be considered:

1. Increased revenue;
2. Cost savings;
3. Increased productivity;
4. Increased efficiency.

Though the decrease in operating costs and increase in revenue are easily determinable, the other two factors often pose serious problems to the IT managers.

Soft competitive benefits like improved business synergy are difficult and sometimes impossible to quantify and measure [7]. IT managers often assign an arbitrary figure to these intangible benefits, by using Figure of Merit Analysis, Delivered System Capability, Polar or Kiviat Graphs or other models, which essentially makes the cost-benefit analysis of IT projects unscientific.

5 Annual Loss Expectancy

Annual Loss Expectancy (ALE) is a simplified theoretical estimation. ALE is defined as the cost of damage done by an attack, multiplied by frequency. Using these estimates, ROI can be reduced to a simple formula:

(ALE x IDS EFFICIENCY) – COST OF IDS = ROI

For example, it is estimated that a network expected to lose $100,000 to attacks. A $40,000 ISMS, which was 85% effective, would yield an ROI of $45,000.

Using quantitative methods, risks analysis and use of empirical data, actual estimates can be developed. This can help in the construction of a reliable estimation method.
The budget expenditure on Information Security can thus be presented using total cost of ownership as an option pricing model under the overall ROI approach [5].

The Macro level factors that have to be considered are corporate governance needs, unforeseen disasters and threats and necessity of IT security. The micro level factors include compliance with

regulations and enterprise level requirements and needs.

At the macro level costs would be dictated by the approach to IT security – choice between good & bad security, under and overprotection, sanitization v/s immunization, honey pot or Fort Knox and the associated costs.

6 Option Pricing two stage model

Stage I – covers the base level of security – the cost of deploying base level security solutions based on discharging governance obligations and statutory responsibilities and providing essential level business protection and continuity.

Stage II – covers additional expenditure on advanced IT security facilities and features. The option to be exercised being in terms of – is additional security required? And if so to what level?

6.1 The TCO – Option Approach

REVENUES

Direct:

No direct income, direct cost savings. Loss deferral determined, saving in downtime costs avoided, benefits of preservation of IS

Non-Quantifiable:

Image, goodwill, preparedness, discipline, approach.

COSTS:

Direct:

Direct costs of acquisition & development,
Cost of deployment

Indirect:

Effect on performance, convenience

Opportunity costs:

Costs of overprotection/under protection

Investments:

Capital Costs, overhead, share of infrastructure – related long term benefits and savings.

7 The Procedure for Building a Business Case

The tools prepared to be used – TCO, option pricing based ROI method, Decision making based on range of values using probability distributions.

First understand the total cost of ownership of ISMS. Next look at legal requirements, baseline costs, resource requirement and inter dependencies to develop cost estimates. Use the metrics developed to estimate the net pay offs of the different choices under different probable conditions or outcomes. Outline the result or the impact in the form of a decision matrix tool and assist top management and IT management in decision making by presenting to them the data for being able to make the right choice.

8 The Balanced Scorecard Framework

Determining the ROI of IT projects helps in crystallizing the intangible benefits and non-quantifiable considerations. This enables the management to weigh all the factors in the right perspective, to arrive at informed decisions rather than relying on instinct alone.

ROI analysis tends to favour proven technologies over cutting-edge solutions. Relying on ROI alone thus may close options and deny the benefit of potential gains by not adopting a technology whose time has come. ROI is a benchmark because it demonstrates that benefits are more than the costs and also indicates the rate of return. However, with interest rates falling, conventional ROI alone is not an appropriate tool for deciding whether or not to go in for IT projects. However ROI would be more appropriate for making a choice between different alternatives.

Hence, ROI should be tempered with assessment of the competitive advantage of IT proposals. A balanced scorecard could be developed with ROI being a key player.

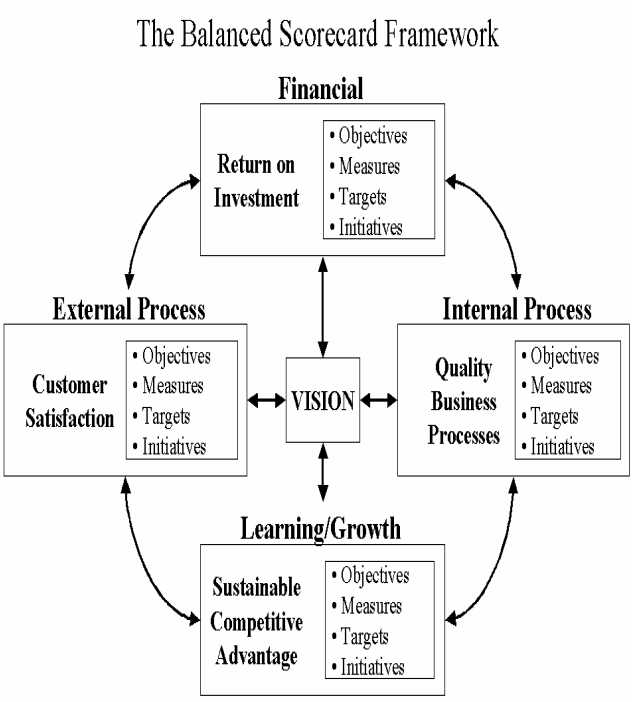

Fig. 2

IT projects depend a lot on software quality metrics, including complexity, effectiveness, modularity, integrity and portability. The human factor coupled with product, system and project attributes also plays a significant role. The intensity and impact of these cost and revenue drivers depend to a large extent on the characteristics of the organisation [8]. Most of the failures of ROI as a good judge are a result of the lack of calibration. The way out is to compare the ROI estimates prior to project implementation with the realised ROI in successive time periods till the end of the productive life of the project. The revised ROI and the trend in its movement will enable prompt rearguard action by redeploying resources.

Thus, projects that initially appeared unattractive and therefore were not given enough allocation could be pursued vigorously, and vice versa. The other more significant benefit is that the process of refining ROI estimates through learning experience (by comparing estimated ROI with realised ROI) will improve with each successive project, resulting in better calibration and better estimates.

Used in this manner, ROI will satisfy the ten criteria of definition (having a clear definition), fidelity (accurate estimation), objectivity (fewer subjective factors), constructiveness (ease of understanding), detail (ability to accommodate all factors), stability (consistency in output vis-à-vis input), scope (applicable to all projects), ease of use, prospectiveness and parsimony [7]. It will thus, become a tool of choice in the hands of IT decision makers, demystifying the whole process.

9 The Conclusion

In this paper, we have developed the method for budgeting of the investment on security through determination of TCO for a 2-stage model. This helps calculate ROI on investments in security. The method can be progressively improved by using the yearly data, if it is used in an organization for a few years. The availability of the data can help in working out common metrics for every industry segment over a period of time.

References:

[1] Strassmann, P.A., "The Business Value Of Computers – An Executive's Guide", The Information Economics Press, Connecticut, 1990.
[2] Hubbard, D., "Everything is Measurable", CIO Magazine, Nov 15, 1997.
[3] Shukla, M.C. & Grewal, T.S., "Advanced Accounts", S. Chand & Co., 1997.
[4] Slater, D., "The Hidden Costs of Enterprise Software", CIO Enterprise Magazine, Jan 15, 1998, Vol. 11 (7), pages 48-55
[5] Surmacz, Jon, "An Ounce of Prevention – Why ROI is the wrong question to ask about Security", CSO Online, May 08, 2002.
[6] "Finally, a Real Return on Security Spending", CIO Magazine, February 15, 2002.
[7] Laudon & Laudon, "Understanding the Business Value of Systems and Managing Change", Prentice-Hall International, 2002
[8] Boehm, B.W., "Software Engineering Economics", Prentice Hall Inc., 1981.