International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-2 Issue-3, February 2013

A Cost-Benefit Model for an Enterprise Information Security

Kiran Kumar Kommineni, Adimulam Yesu Babu

Abstract*— *A Cost-Benefit model for an enterprise information security is presented in this paper. Economical analysis of information security investments that enterprises can use as guidance when applying the recommended risk mitigation plans are developed. An enterprises information security risk management associated with economical metrics. An economical analytical model is presented that enables the assessment of the necessary investment in the recommended information security. This model would be useful for both information security professionals and researchers in assessing the cost of the security measures versus the benefit of these measures in reducing the identified information security challenges.

***Keywords*— Cost Benefit Model; Enterprise; Information Security; Risk management.**

I. INTRODUCTION

The increasing complexity of today's computer systems makes security hardening a formidable challenge for security administrators. Although a large variety of tools and techniques are available for vulnerability analysis, the majority work at system or network level without explicit association with human and organizational factors. An analytical model concerned with the analysis of the cost of the recommended protection measures that could be used by enterprises for facing the information security challenges versus the benefits from acquisition and deployment of these protection measures in reducing the effects of these challenges. One of the essential objectives of the proposed EISRM framework on suitable financial metrics and to find the optimal enterprise security budget in the selection of the best-practice controls subset that is appropriate to its needs from the set of all possible best practices security controls.

The information security management, from the perspectives of business managers, is an investment to be measured in saved cost because of reducing loss. In contrary, information security management, from the perspectives of technical managers, is only the technical tools and organizational procedures that should be implemented to reduce the expected risk to an acceptable level. Recently, a number of important surveys indicates that financial metrics start to direct the decision between the alternatives of information security protection measures. The computer crime and security survey started to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the cost and benefits of computer security expenditures.

Manuscript published on 28 February 2013.
***Correspondence Author(s)**
Mr. Kiran Kumar Kommineni, Lecturer, Department of Information Technology, Bapatla Engineering College, Bapatla - 522101, Guntur, AP, INDIA E
Dr. Adimulam Yesu Babu, I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru -534007, West Godavari (Dt), AP.,India.

II. BACKGROUND

Several models were developed by several experts related to a cost-benefit model for an enterprise information security. The important ones are Shuzhen Wang et al [1] presented a middleware approach to bridge the gap between system level vulnerabilities and organization level security metrics, ultimately contributing to cost-benefit security hardening. Romain Jallon et al [2] reviewed and studied the key elements that should foster the use of indirect-cost calculation methods by decision makers. Feng-Ming Tsai and Chi-Ming Huang [3] presented a scenario analysis to evaluate the cost and benefit analysis of implementing the RFID E-seal system in Port of Kaohsiung. Tung Bui and Taracad R. Sivasankaran [4] presented a Cost-Effectiveness Model that determines an optimal program for control of EDP systems. It also determined acceptable levels of potential losses, and identify cost-effective control strategies. Matthew L. Saxton et al [5] investigated the policy issues surrounding the implementation and assessment of 2-1-1 information and referral services. Rok Bojanc et al [6] presented a mathematical model for an optimal security technology investment evaluation and decision-making processes based on a quantitative analysis of the security risks and a digital assets assessment in an organization. Carlos Blanco et al [7] applied the method of systematic review for identifying, extracting and analyzing the principal proposals for security ontologies. C. Ryu et al [8] presented a model deception system with the explicit purpose of enticing unauthorized users and restricting their access to the real system. Michael Workman et al [9] investigated the technical side of this critical issue, but securing organizational systems has its grounding in personal behavior.

III. STANDARD ORGANISATIONS ECONOMIC DIRECTIONS

The ISO/IEC 27002 information security management standard stated that appropriate controls for risk treatment should be selected and implemented to meet not only the requirements identified by the risk assessment, but also to satisfy other requirements including the cost of implementation and operation in relation to the risks being reduced and the need to balance the investment in implementation and operation of controls against the harm that is likely to result from security failures. In addition to the above ISO direction, different other standards and professional organizations also include directions and general guidelines for basing the selection of the information security protection measures on an economical analysis.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Three of such standards and documents will be presented in the following.

The professional organizations concerned with information security risk management recommend the use of economical analysis in the selection of the most appropriate protection measures for mitigating the discovered security flaws. Enterprises wanted to manage risks based on economical analysis would be faced with a lack of indicators, rigorous methodologies and standard tools for conducting the suggested economical analysis. Most of the financial metrics are adjusting the overall information security expenditures. The most important financial metrics that could be used in building the required cost benefit model.

3.1 AS/NZS 4360

The AS/NZS 4360 risk management standard states that enterprises should adopted specific cost effective strategies and action plans for risk treatment, development and implementation. The standard also added that the selection of the most appropriate mitigation option involves balancing the costs of implementing each option against the benefits derived from it. Furthermore, the standard suggests that when making such cost versus benefit judgments, the context of the enterprise under consideration should be taken into account considering all direct and indirect costs and benefits whether tangible or intangible and measured in financial.

3.2 NIST SP 800-30

The NIST SP 800-30 document suggests running cost-benefit analysis for each of the proposed controls to determine which control is required and appropriate for the enterprise circumstances. The document emphasizes encompassing the following steps in running cost benefit analysis for the new controls:

- Determining the impact of implementing the new or enhanced controls;
- Determining the impact of not implementing the new or enhanced controls;
- Estimating the costs of the implementation; and
- Assessing the implementation costs and benefits against system and data criticality to determine the importance of implementing the new controls to the enterprise, given their costs and relative input.

3.3 Microsoft

The Microsoft document for information security risk management states that the main goal of conducting decision support in selecting the treatment controls is to identify and evaluate control solutions based on a defined cost-benefit analysis process. The document also suggests considering the acquisition, implementation, ongoing, communication, training of both staff of IT & users, productivity & convenience and auditing & verifying the effectiveness of costs in conducting cost-benefit analysis.

IV. INFORMATION SECURITY FINANCIAL METRICS

There are a number of financial metrics that evolved from the information security risk management literature to assess information security risks. A brief description of each of these metrics and their equations as shown in Table 1, will be discussed in the following sections.

Table 1: Information security financial metrics

	Metric/ Symbol	*Equations*
1	Annual Loss Expected (ALE)	$ALE = \sum_{i=1}^{n} I(O_i) F_i$ $I(O_i)$ the impact of outcome i in monetary value and F_i the frequency of outcome i
2	Return on Investment (ROI)	$ROI = \frac{Benefit}{Cost-of-Safeguards}$
3	Return on Security Investments (ROSI)	$ROSI = \frac{(Risk\ Exposur * \%\ Risk\ Mitigated) - Solution\ Co}{Solution\ Cost}$
4	Net Present Value (NPV)	$NPV = \frac{R_t}{(1+i)^t}$ t is the time of the cash flow; i is the discount rate R_t is the net cash flow
5	Internal Rate of Return (IRR)	$C_o = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t}$ C_0 is the initial cost of an investment C_t respective cost in year t; B_t respective benefit in year t

4.1 Annual Loss Expected (ALE)

ALE metric became a common measure for the risk of a harmful event, which is the product of the yearly rate of occurrence of the event times the expected loss resulting from each occurrence. The main limitation of this metric is that it cannot distinguish between high-frequency, low-impact events and low-frequency, high-impact events. The calculation of the expected loss is by adding the product of each loss with its respective probability. The expected severe loss is focused on the breaches that would put the survivability of the enterprise at risk, and it is calculated by adding together the product of each loss, that is greater than or equal to the specified threshold loss, with its respective probability. The standard deviation of loss represents the dispersion around the expected loss. It is computed by taking the square root of the product of squares of the deviation of each loss from the expected loss with the probability of the loss. The calculation of the frequency of occurrence of loss is not an easy task, especially in different environments and with scarcity of the available data and its suitability to the environment.

4.2 Return on Investment (ROI)

The ROI metric measures the productivity of an investment. A company's productivity is the ratio between the total outputs and the total inputs. The total inputs being the external and internal resources used by the company to make its activity work and the total outputs being the value of the production. The ROI metric is considered in terms of finance as the most important financial indicators. It identified specific factors concerned with the needed security expenditures and it also introduced related factors concerned with the viability of these expenditures.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

4.3 Return on Security Investment (ROSI)

The ROI metric used in financial arena to be more suitable for information security. The risk mitigation, when security initiatives are concerned, is considered as an important component of the ROI and it is important to include it as an explicit factor in the ROI calculation. According to ROSI equation, measuring risk exposure is conducted by investigating the loss of highly confidential information and the productivity loss associated with a security incident. The mitigated risk, or in other words, the benefits of security solutions could be calculated also by evaluating risk mitigation within the context of the considered problem. In quantifying solution cost, the impact of the solution on the productivity is considered an important factor.

4.4 Net Present Value (NPV)

The NPV metric is defined as the total present value of a time series of cash flows. It is a standard method for using the time value of money in assessing the financial value of long-term projects. The NPV metric is an indicator of how much value an investment or project adds to the value of the enterprise. In financial theory, if there is a choice between two mutually exclusive alternatives, the one yielding the higher NPV should be selected. The problem with using NPV for security investments is that the accuracy is quite critical in obtaining comparatively meaningful results.

4.5 Internal Rate of Return (IRR)

The IRR metric is often used in order to decide in which alternative to invest. Using IRR metric involves calculating the investments expected return, and can be used to compare different investment alternatives. The choice might stand between investing in a machine and simply investing the money in a bank account that gives an interest on the money. The comparison is always done by calculation of the IRR factor between different alternatives using a discount factor compared to the bank account. The outcome of the calculation should equal zero and, therefore the better of the alternatives is then likely to invest in. There is no one perfect discount factor, and therefore different companies use different discount factors as they believe it fits their enterprise and investment best suit their context. The IRR metric is considered as an indicator of the efficiency or quality of an investment, as opposed to NPV, which indicates value or magnitude.

4.6 Costs-Benefit Analysis

Cost-benefit analysis is a technique for comparatively assessing the costs and benefits of an activity or project over a relevant time period. It may also be defined as the process of comparing the various costs of acquiring and implementing an information security system with the benefits which the enterprise derives from the use of the system. The cost-benefit analysis is generally developed to build a business case for the use of a particular technology solution by comparing the investment amount, net benefit, return on investment and cost effectiveness. The framework considers not only the costs of security controls and expected loss from security breaches, but also takes care of the additional profits expected from new opportunities. There is clear limitation to the applicability of this model. This model overstates the reduction in risk resulting from the use of safeguards that act as substitutes for each other. In addition, the model fails to capture the effects of complimentary safeguards. Finally, the model leaves an open question of how to forecast the rate at which loss events will occur, and how to forecast the reductions in these rates that will result from adding safeguards.

V.INFORMATION SECURITY ECONOMICAL ANALYSIS

A generic practical model for assessing the cost of the protection measures versus the benefit from applying these measures in reducing or eliminating the discovered risk. Management practices that are used by enterprises for mitigating discovered information security risks. It protects the important asset of information in IT-based applications; information security is enough for such applications; and to evaluate the resulting security benefits. It provides a background for the target cost-benefit model for information security context.

5.1 Protection of Information

The question of how to protect information in IT-based applications has been answered by professional organizations concerned with IT. They produced information security products including: firewalls, Intrusion Detection Systems (IDS), antivirus programs, cryptographic techniques and other security products and tools. These tools increased very fast and became very sophisticated and powerful in providing different levels of protection to security challenges. The technologies are divided into two groups, proactive and reactive. Each of these groups has three layers of security technologies, network layer, host layer and application layer.

5.2 Required Protection

The question of how much security is enough has been addressed by national and international organizations concerned with IT risk management and information security management standards. These organizations provided risk management methods and information security management standards that recommend the use of various management rules and technical tools for the protection of information security. These recommendations usually provide common, or just enough security protection practices and not necessarily best possible practices. The ISO/IEC 27002 information security management standard is considered as one of the most important example.

5.3 Evaluation of Information Security Benefits

The question of the evaluation of security benefits is of an economic nature. Such benefits usually come as a result of investment, where cost is the major factor. Different researchers have addressed this problem with various considerations. The Incident Cost Analysis Modeling Project (I-CAMP) is an early example in applying the Cost Benefit Analysis (CBA) in computer security. The model is appropriate for situations where the related usage losses are considered to be modest or ignored entirely. The System Quality Requirements Engineering (SQUARE) model is investigated and applied the cost-benefit analysis framework for information security improvement in small companies.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

VI. THE PROPOSED COST-BENEFIT MODEL

The mathematical model presented here provides practical generic tools for the cost benefit analysis of security challenges versus protection measures. The cost of security challenges can be very high if no protection measures are provided. While such measures support reducing the security challenges and their cost, they obviously do not come without cost of their own. In some cases, where many sophisticated protection measures are used, their cost may outweigh the savings they cause to the cost of security challenges. The common problem and concern model is presented in Fig. 1.

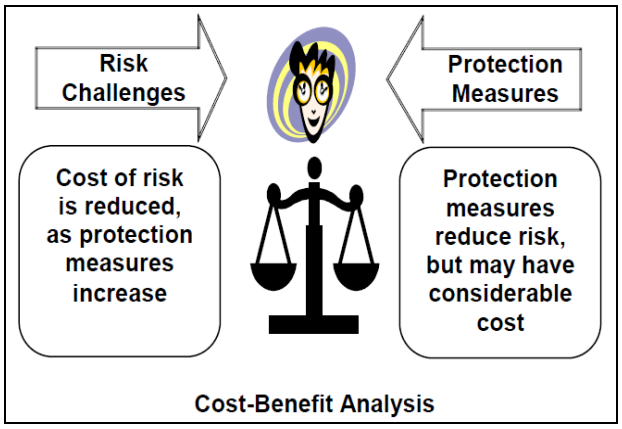

Figure 1: Protection measures versus security challenges: Cost-benefit analysis

The model provides analytical tools for dealing with the cost-benefit assessment tasks shown in the procedure of Figure 2; these tasks are: identifying the security challenges that need to be taken into account; specifying the protection measures that can be considered; estimating the actual protection resulting from the use of the protection measures; finding the saved cost of security challenges resulting from the use of the protection measures; finding the residual cost of security challenges resulting from the saving caused by the use of the protection measures; and finding the cost function that considers the total cost and illustrates the cost-benefit state.

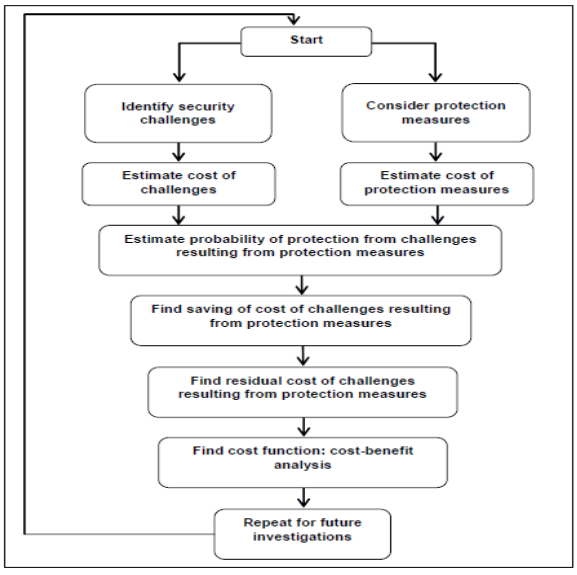

Figure 2: Cost-benefit analysis procedure

6.1 Security Challenges

The number of these challenges is considered to be a variable. For each challenge, it gives its estimated cost if it occurs and it Start Consider protection measures Identify security challenges Estimate cost of protection measures Estimate cost of challenges Estimate probability of protection from challenges resulting from protection measures Find saving of cost of challenges resulting from protection measures Find residual cost of challenges resulting from protection measures Find cost function: cost-benefit analysis Repeat for future investigations. considers its expected annual frequency of occurrence. The same table gives the expected annual cost of each challenge and the annual cost of all challenges.

6.2 Protection Measures

The basic factors concerned with the protection measures and their inter-relationships. The number of these protection measures is considered as a variable. For each measure, it addresses its annual cost. The annual total cost of all protection measures is also taken into account. A point of clarifications is needed here, that is the distinction between a protection measure and a protection tool. The anti-virus software tool may be used with or without information back-up security control leading to two different protection measures.

6.3 Resulting Protection

The use of the protection measures would lead to reducing the effect of the challenges and consequently to saving their cost, partially or fully. The probability of protection provided by the protection measures considered, individually and collectively, that is with regards to each identified challenge.

6.4 Cost Saving

Achieving a certain level of protection would lead to a certain level of saving of the cost of the challenges. The table considers the saving caused by each protection measure and associated with each challenge. The accumulated savings are also taken into account.

6.5 Residual Cost

The protection measures cannot fully eliminate challenges. Therefore, the challenges will keep certain residual cost. Various residual costs are given in the same table, both individually and collectively.

6.6 Cost Function

The cost functions can be developed at different levels. A cost function would combine the cost of the protection measures with the residual cost of the challenges. This can be viewed at each protection measure and challenge level and can also go up to the overall level of all protection measures and challenges. The analytical tools given above are of comprehensive nature, and can be applied to a wide variety of case-studies. The above cost-benefit model that considers the available protection tools and recommendations associated with ISO standards.

VII. SUMMARY

The main aim is to develop a practical model for economical analysis of information security investments that enterprises can use as guidance when applying the recommended risk mitigation plans.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The economical metrics associated with enterprises information security risk management are also presented. An economical analytical model is presented that enables the assessment of the necessary investment in the recommended information security. This model would be useful for both information security professionals and researchers in assessing the cost of the security measures versus the benefit of these measures in reducing the identified information security challenges.

REFERENCES

1. Shuzhen Wang., Zonghua Zhang., Youki Kadobayashi "Exploring attack graph for cost-benefit security hardening: A probabilistic approach" Computers & Security, Volume 32, February 2013, pp 158–169.
2. Romain Jallon., Daniel Imbeau., Nathalie de Marcellis-Warin "Development of an indirect-cost calculation model suitable for workplace use" Journal of Safety Research, Volume 42, Issue 3, June 2011, pp 149–164
3. Feng-Ming Tsai., Chi-Ming Huang "Cost-Benefit Analysis of Implementing RFID System in Port of Kaohsiung" Procedia- Social and Behavioral Sciences, Volume 57, October 2012, pp 40 -46.
4. Tung Bui and Taracad R. Sivasankaran "Cost-effectiveness modeling for a decision support system in computer security" Computers & Security, Volume 6, Issue 2, April 1987, pp 139–151
5. Matthew L. Saxton., Charles M. Naumer., Karen E. Fisher "Information services: Outcomes assessment, benefit–cost analysis, and policy issues" Government Information Quarterly, Volume 24, Issue 1,2007, pp 186–215
6. Rok Bojanc., Borka Jerman-Blažič., Metka Tekavčič "Managing the investment in information security technology by use of a quantitative modeling" Information Processing & Management, Volume 48, Issue 6, Novr 2012, pp 1031–1052
7. Carlos Blanco., Joaquín Lasheras., Eduardo Fernández-Medina., Rafael Valencia-García., Ambrosio Toval "Basis for an integrated security ontology according to a systematic review of existing proposals" Computer Standards & Interfaces, Vol. 33, Issue 4, 2011, pp 372–388
8. C. Ryu., R. Sharman., H.R. Rao., S. Upadhyaya "Security protection design for deception and real system regimes: A model and analysis" European Journal of Operational Research, Volume 201, Issue 2, March 2010, pp 545–556.
9. Michael Workman., William H. Bommer., Detmar Straub "Security lapses and the omission of information security measures: A threat control model and empirical test" Computers in Human Behavior, Volume 24, Issue 6, September 2008, pp 2799–2816

AUTHOR PROFILE

Mr. Kiran Kumar Kommineni Pursuing PhD in Computer Science & Engineering from CMJ University, Meghalaya. Received Master of Engineering in Computer Science & Engineering from RMK Engineering College, Chennai affiliated to Anna University. Working as a Lecturer in Information Technology Department of Bapatla Engineering College, Bapatla, Guntur (Dt), AP

Dr. Adimulam Yesu Babu received Ph. D in Computer Science & Systems Engineering from Andhra University, Visakhapatnam. Dr. Babu having 23 years of Academic & Academic Administration experience and presently working as a I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru -534007, West Godavari (Dt), AP.

.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)