International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 1, January-2014, pp: (491-497), Impact Factor: 1.252, Available online at: www.erpublications.com

A Cost / Benefit / Risk (CBR) Analysis Methodology and its Application in a Computing System

Dr. Rajiv Srivastava
Professor & Director, Ph .D (Computer Science Engineering),
Sagar Institute of Research & Technology, Bhopal, M.P., India

ABSTRACT: This paper describes a compound cost/benefit/risk (CBR) analysis methodology and its application in a Computing System for assessing the security threats, vulnerabilities and suggests corrective actions. These factors are analyzed, evaluated and presented in a practical meaningful perspective. The Decision Making Factor which justifies the selection of corrective action with respect to related risk is also calculated. The priority ranking of risk is defined in terms of the likely Consequences of the threat, the Frequency of Exposure of threat and the Probability of threat sequence completion and the Correction Value is defined on the effectiveness and cost of applied counter measures. The methodology employs a mathematical technique that combines both objective and subjective approaches to classical risk analysis.

1. INTRODUCTION

A good management practice demands that when evaluating the security of an information system (IS) supported with a computing environment, use of given resources should be made wisely for maximum effectiveness or profit since computers & peripherals is typically a costly set-up and is vital to economy of an IS. The assessment of risk should follow a set guidelines to maintain consistency and accuracy and it should not be biased on the basis of past incidents to predict what might happen in future as traditionally done in objective risk assessment [15]. This bias may happen due to lack of availability of comprehensive data on computer related risks as many cases normally are not reported to officials. Subjective risk assessment based on the method of best guesses of risks depending on the specified features of the system is often criticized for the results least likely to happen. Expected values of annual loss appear unrealistic and not suit to the organizations every time and proponents to this analysis too often ascribe levels of accuracy that the methodology can not support.

The previous Cost / benefit Analysis and Risk Analysis have played major role in First Generation of information system design and tend to decline in Second and Third Generations [11]. Whereas, a good attention now has started in analyzing the factors like risk, threats and vulnerability affecting to Operating Systems [10]. This paper presents a combined analysis of objective and subjective methods for an information system and operating systems. It is a well known fact that an operating system supporting an information system plays a major role in overall successful functioning, hence we shall be calling both these systems in one term named as Computing System. In our analysis, we mainly concentrate on the first five elements of risk management as reported in [1], i.e. identification of risk factor, assessment of risk effects on computing system, development of strategies to take corrective actions monitoring of risk factors and invoking contingency plans by clearly defining their criteria of selection. We relate the risk with three factors (i) Consequences (ii) Exposure and (iii) Probability of completion of threat sequence and countermeasures with three factors (i) Cost factor of proposed counter measure (ii) Degree of correction and (iii) Time taken in implementing counter measure and analyse them in terms of Risk Value and Correction Value respectively. Finally, a

Decision Making Factor is calculated on the basis of Risk Value and Correction Value which justifies the selection of proposed countermeasure with respect to related Risk Value. Our analysis in this paper appears to offer most meaningful and pragmatic results which provide assessment of losses using the knowledge of various risks and their countermeasures. We present Main Methodology in section 2., whereas section 3. Presents a Case Study. Conclusion and Discussion are given in section.

2. CBR ANALYSIS

The Cost / Benefit / Risk (CBR) analysis incorporates procedures to evaluate Risk Value, Correction Value of countermeasure and a Decision Making Factor which justifies the selection of proposed countermeasure against corresponding risk. These values are evaluated numerically.

2.1 Assessment of Risk :

We asses the risk as the Risk Value (RV), denoted α, which is given by a function $f(\alpha_1, \alpha_2, \alpha_3)$, where α_i, for $i \in \{1, 2, 3\}$ are defined as follows:

α_1 : The value Consequences of a possible event due to a potential threat,

α_2 : The value of Exposure or Occurrence Frequency of threat,

α_3 : The value of Probability of threat sequence completion,

We assume that the function f satisfies the following condition :

C1 : $f(\alpha_1, \alpha_2, \alpha_3) = 0$, if any $\alpha_i = 0$,

Where, $0 <= \alpha_1 <= \eta 1$ (η' are positive integer) ;

$0 <= \alpha_2 <= \eta 2$

$0 <= \alpha_3 <= \eta 3$;

Satisfying condition C1, we consider the linear form of function f in α_1, α_2 and α_3, that is in our case, the Risk Value ; α , is given by :

$$\alpha = \alpha_1 \times \alpha_2 \times \alpha_3, \qquad (2.1)$$

We shall divide the values of α thus obtained from equation (2.1) into five ranges denoted as VH (Very High Value), H (High Value), M(Medium Value), L (Low Value) and VL (Very Low Value) for reference in calculation of Decision Making Factor (section 2.3)

We assume a high value of α bears more risk as compared to a low value of α.

2.2 Assessment of Countermeasure :

We assess the value of counter measure as Correction Value (CV), denoted β, which is represented by a function $g(\beta_1, \beta_2, \beta_3)$, where β_i for $i \in \{1, 2, 3\}$ are defined as follows:

β_1 : The value of Cost of proposed countermeasures,

β_2 : The value of Degree of correction provided by the proposed countermeasure,

β_3 : The value of time taken in implementing counter measure,

We assume that the function f satisfies the following conditions :

T1 : $g(\beta_1, \beta_2, \beta_3), = 0$ if any $\beta_i = 0$ $i \in \{1, 2, 3\}$

Where, $0 <= \beta_1 <= \varphi$

$0 <= \beta_2 <= \varphi$ (φ' are positive integers) ;

$0 <= \beta_3 <= \varphi 3$;

Satisfying condition T1, we consider the linear form of function f in β_1, β_2 and β_3, that is in our case, the Correction Value ; β , is given by :

$$\alpha = \beta_1 \times \beta_2 \times \beta_3, \qquad (2.2)$$

We shall divide the values of β obtained from equation (2.2) into five similar ranges as done for α (section 2.1), for reference in calculation of Decision Making Factor (section 2.3).

We assume that a lower value of β corresponds to a better countermeasure.

2.3 Decision Making Factor :

Given a Risk Value; α, and a Correction Value; β, for a tentative countermeasure corresponding to Risk Value, we assume the Decision Making Factor; γ, to be given by function h(α, β) satisfying following conditions:

M1 : $h(\alpha, \beta) = 0$ if $\alpha = 0$,

M2 : $h(\alpha, \beta) = 0$ if $\beta = 0$,

Satisfying conditions M1 and M2, we consider the form of function h as α divided by β, that is in our case, the Decision Making Factor, $\gamma = \alpha/\beta$, (2.3)

Based on our five ranges each for RV and CV [sec 2.1, sec 2.2], we evaluate various values of ϒ and represent these values into five ranges denoted from VH (Very High) to VL (Very Low) same as for RV or CV and display them in γ - Matrix (Table 1). We shall use these ranges to suggest appropriate plan of action as remedy of threat. The proposed criterion of selection of this plan is given in Table2.

Table 1 : γ -matrix

PV \ RV	VH	H	M	L	VL
VL	VH	H	M	L	L
L	L	L	VL	VL	VL
M	VL	VL	VL	VL	VL
H	VL	VL	VL	VL	VL
VH	VL	VL	VL	VL	VL

Remark 1 : In the situation where there is less possibility of making the ranges of values from VH to VL, three ranges can made by merging VH into H to make H and VL into L to make L, thus making H, M and L ranges of values.

Table 2 : Action Plans

γ -values	Proposed plan
VH	• Situation is critical, requires immediate action
H	• Situation is urgent, requires attention within two days
M	• Situation is Poor, requires attention within a week
L	• Situation is Poor, requires attention within two weeks
VL	• Threat is not very harming, but it should be eliminated

3. A CASE STUDY

We consider an information system named: Multilevel Information Protection System (MIPS) which provides relatively higher degree of security to Sensitive Information (SI) in this Case Study. The MIPS provides security to SI with a powerful MIPS Encryption Algorithm (MEA) and a System Run Time Checker (SRTC) : an Authentication module. We apply our CBR analysis (section 2.2) on MIPS and make the assessment of Risk value; α, and Correction Value; β. We analyze all related factors (caused from various threats (sec. 3.1) by Genesis, Time of Introduction and Location [2], including physical and natural disasters) that influence Consequences, Exposure and Probability of threat sequence completion, on which Risk Value is based. We also analyze the factors that influence Cost countermeasure, Degree of Correction and Time taken in correcting the problem. These are the factors on which Correction Value; β, depends. We assign different ratings to these factors as per their degree affecting the system (section 3.1, 3.2). Finally, we evaluate Decision Making Factor ; γ, in section 3.3 to decide upon the appropriate contingency plan from Table 14.

3.1 Assessment of Risk; α : We suppose that for the assessment of Risk Value (RV), the three main components of the RV i.e. Consequences, Exposure and Probability of threat sequence completion are influenced by the following factors (Table 3):

Table 3

Main Component of Risk Value	Factors
Consequences; α_1	• Damage of Resources by Volume. • Cost Impact of Damaged Resources in Dollars, • Period of Denial of Service in days / weeks,
Exposure ; α_2	• Frequency of Occurrence of threat event in days/weeks.
Probability ; α_3	• Probability of threat sequence Completion in days/week.

We now present in the following sections the procedure of rating of the main components of the Risk Value.

3.1.1 Consequences; α : We frame five different Cases (Table 4) based on various ratings of the factors : Damage of resources by volume and Cost Impact of damaged resources in dollars. Based on the period of Denial of Service in days / weeks, we assign different ratings to these Cases (Table 5). A highest rating 50 is assigned to Case A under catastrophic conditions when all resources are damaged, Cost impact is highest and Period of Denial of service is greatest. A lowest rating 2 is assigned to Case E when the Damage of resources is partial, the Cost impact is lowest and the Period of Denial of service is also lowest.

Table 4 : Case Table

Case	Description
A	• Damage : All Resources Cost Impact: Greater than $250,000.00
B	• Damage : Partial Destruction of Resources Cost Impact: Between $175,000.00 to $250,000.00
C	• Damage : Partial Destruction of Resources Cost Impact: Between $100,000.00 to $175,000.00
D	• Damage : Partial Destruction of Resources Cost Impact: Between $25,000.00 to $100,000.00
E	• Damage : Partial Destruction of Resources Cost Impact: Less than $25,000.00

3.1.2 Exposure; α_2 : The second factor, Exposure, is defined, in terms of Frequency of Occurrence of threat event in days / week. A highest rating 20 is assigned to this factor if a threat event occurs many a times in a day and lowest rating 2 is assigned if a threat event has rarely occurred somewhere (Table 6).

3.1.3 Probability ; α_3 : We rate the Probability of threat sequence completion in terms of the extent of completion of the sequence when the threat event occurs. A highest rating 10 is assigned to this factor if a complete sequence is likely to take place and lowest rating 2 is assigned if the sequence is least likely to be completed (Table 7).

Table 5 : Consequences ; α_1

Period of Denial of Service	Case	Rating
• Greater than 4 weeks	A	50
	B	48
	C	46
	D	44
	E	42
• Two to Four weeks	A	40
	B	38
	C	36
	D	34
	E	32
• One to Two weeks	A	30
	B	28
	C	26
	D	24
	E	22
• Less than One Week	A	20
	B	18
	C	16
	D	14
	E	12
• Less than One day	A	10
	B	08
	C	06
	D	04
	E	02

Table 6 : Exposure ; α_2

Exposure	Rating
1. Many a times in a day	20
2. Once per day	18
3. Twice per week	16
4. Once per week	14
5. Once per two weeks	12
6. Once per four weeks	10
7. Once per six weeks	08
8. Once per twelve weeks	06
9. Once per half year	04
10. Rarely have occurred some where	02

Table 7 : Probability ; α_3

Probability of Completion of Threat Sequence	Rating
• Consequence is likely to be completed by 100%	10
• Consequence is likely to be completed by 75%	08
• Consequence is likely to be completed by 50%	06
• Consequence is likely to be completed by 25%	04
• Consequence is likely to be completed	02

On the basis of these ratings (Table 5-7), the values of RV will vary from 10,000 to 8. We divide this range of values into five ranges as follows (Table 8):

Table 8

Range Category	Rating
VH	7500-10000
H	5000-7500
M	2500-5000
L	1000-2500
VL	8-1000

We will use these categories of ranges in the calculation of Decision Making Factor in section 3.3.

3.2 Assessment of Correction Value ; β : For the assessment of Correction Value we assume that the three main components i.e. Cost countermeasure ; β1, Degree of correction of problem; β2, and Time taken in correcting problem ; β3, [sec 2.2] are mainly influenced by the following factors (Table 9):

Table : 9	
Main Component of Correction Value	Factors
Cost ; β1	• Cost of countermeasure in dollars
Degree of Correction ; β2	• Reduction in Consequences of threat in percentage
Time ; β3	• Time taken in correcting the problem in days / weeks

We now explain the procedure of rating of the main components of Correction Value based on above factors.

3.2.1 Cost of Countermeasure ; β1 : The Cost factor proposed countermeasure is an estimation of cost in dollar and we consider the ratings of this factor equal to the percentage value of system. Cost. These ratings vary from highest value 20 to lowest value 1 (Table 10). In fact, by this criterion more ratings can be assigned to this factor than given in Table 10, depending on the percentage value of the cost of countermeasure.

3.2.2 Degree of correction ; β2 : We estimate the Degree of correction in terms of reduction of threat and its consequences in percentage. We assign a lowest rating 2 under most favourable situation when Consequences of threat is almost eliminated and a highest rating 10 in the most unfavourable situation when consequences of threat are least likely to be eliminated (Table 11).

Table 10 : Cost Factor β_1	
Cost of Proposed Counter Measure	Rating
• 20% of system cost	20
• 15% of system cost	15
• 10% of system cost	10
• 5% of system cost	5
• 1% of system cost	1

Table 11: Cost Factor β_2	
Degree of Correction	Rating
• Threat positively eliminated by 100%	2
• Threat reduced to 75%	4
• Threat reduced to 50%	6
• Threat reduced to 25%	8
• Threat is least likely to be eliminated	10

3.2.3 Time of correction ; β_3: The time of correction, we consider in days/weeks taken in correcting the threat and its consequences by a proposed countermeasure. We assign a lowest rating 2 to this factor under most favourable situations when the threat consequences are corrected in one day. A high rating 10 is assigned in a poor situation when the threat consequences are corrected nearly in 10 weeks (Table 12). The Correction Value thus calculated, based on the ratings of various factors from Table 10-12, vary from 4 to 2000 onward.
Remark 2 : The maximum value of Correction Value can also be greater than 2000 since we are keeping a provision to assign additional ratings to β_1. We divide these ranges of Correction Value into five ranges in Table 13.

Table 12: Correction time of a problem ; β_3	
Time of correction	Rating
• One day	2
• One week	4
• Two weeks	6
• Four weeks	8
• Four to Ten weeks	10

Table 13	
Degree of Correction	Rating
VL	4-100
L	100-250
M	250-500
H	500-1000
VH	1000 onwards

We shall be using these ranges of values in section 3.3 for calculation of Decision Making Factor.

3.3 Decision Making Factor ; γ : Once we analyse a threat and its consequences and decide upon a tentative countermeasure, then we use the Decision Making Factor; γ, to determine whether the estimated Correction Value of proposed countermeasure is justified to corresponding Risk Value. We calculate the values of γ for five ranges of α and β each (Table 8, 13).

A recommended course of action based on the γ value is suggested in Table 14. Any γ value greater than 100 implies that the threat has high risk and its countermeasure is easily affordable. Thus in this situation it is recommended to correct this threat and its consequences immediately. Likewise a γ value between 50 to 100 it implies that the threat and its consequences have caused an alarming situation and its countermeasure may be undertaken, therefore it is recommended to take a sooner action. A γ value less than 50 shows that there exists a non serious threat with its consequences to the system but it should be corrected.

Table 14 : Decision making factor γ	
γ – value	Action
• Greater than 100 • 50-100 • Less than 50	• Situation is Critical, Requires immediate action, • Situation is Urgent, requires sooner action within a week. • Situation is not very harming, but threat should be eliminated.

4. Conclusion and Discussion

The present work includes an analysis of Cost / Benefit / Risk assessment for a computing system. The previous analytical methods are normally based on subjective or objective approach. Whereas our method combines both the approaches together. The previous studies have not stressed on the time taken in correcting the threats and its consequences, which has been introduced by us in the calculation of the Correction value of countermeasure. By Introduction of this factor the CBR analysis gains a wider perspective. We calculate the Risk Value (RV) and Correction Value (CV) and divide them into five ranges each. These ranges of values we use in the calculation of Decision Making Factor ; Which justifies the selection of countermeasure corresponding to related risk. Finally, we illustrate the application of MIPS by a Case Study (section 3). We assign different ratings to RV and PV by considering their severity and friendliness with the system. We calculate the values of Decision Making Factor for the five specific ranges of RV and PV.

The important outcome of our Case Study is that an immediate action is needed if the γvalue is greater than 100. In case γ value is lying between 50 to 100 then the situation is urgent and requires sooner quick action. In other cases when γ value is below 50; the situation is not very alarming but it should be eliminated (Table 14). One may argue in picking up values of Exposure of threat from Table 6, on the basis Frequency of Occurrence of threat or the possible period of time after which a threat can hit the system. We explain this with a case when a threat may effect the system many a times in a day and as a Consequence the system denies its services for two days. If we pick up the rating corresponding to Exposure of this threat from Table 6, it comes out to be 20, whereas when the system is out of order for two days then infact threat can effect the system only after two days with rating 18 (Table 6). We handle such discrepancies by recommending the plans of action for the ranges of γ values. The accuracy of assessment of various factors in this method will depend upon the judgment and experience of the analyst making the calculations, therefore the ratings of different factors may vary from analyst to analyst and system to system.

REFERENCES

[1]. Dunn, William N. (2009). Public Policy Analysis: An Introduction. New York: Longman. ISBN 978-0-13-615554-6.
[2]. Boardman, N. E. (2006). Cost-benefit Analysis: Concepts and Practice (3rd ed.). Upper Saddle River, NJ: Prentice Hall.ISBN 0-13-143583-3.
[3]. Weimer, D.; Vining, A. (2005). Policy Analysis: Concepts and Practice (Fourth ed.). Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 0-13-183001-5.
[4]. Campbell, Harry F.; Brown, Richard (2003). "Valuing Traded and Non-Traded Commodities in Benefit-Cost Analysis".Benefit-Cost Analysis: Financial and Economic Appraisal using Spreadsheets. Cambridge: Cambridge University Press.ISBN 0-521-52898-4. Ch. 8 provides a useful discussion of non-market valuation methods for CBA.
[5]. Newell, R. G. (2003). "Discounting the Distant Future: How Much Do Uncertain Rates Increase Valuations?". Journal of Environmental Economics and Management 46 (1): 52–71.doi:10.1016/S0095-0696(02)00031-1.
[6]. Campbell, Harry F.; Brown, Richard (2003). "Incorporating Risk in Benefit-Cost Analysis". Benefit-Cost Analysis: Financial and Economic Appraisal using Spreadsheets. Cambridge: Cambridge University Press. ISBN 0-521-52898-4. Ch. 9 provides a useful discussion of sensitivity analysis and risk modelling in CBA.
[7]. "History of Benefit-Cost Analysis". Proceedings of the 2006 Cost Benefit Conference.
[8]. Guess, George M.; Farnham, Paul G. (2000). Cases in Public Policy Analysis. Washington, DC: Georgetown University Press. pp. 304–308. ISBN 0-87840-768-5.
[9]. Richard Fairley, “Risk Management for Software Projects”, IEEE Software, May 1994, pp 57-66.
[10]. Carl E. Landwehr, Et al., “ A Taxonomy of Computer Program Security Flaws”, ACM Computing Surveys, Vol. 26, No. 3, Sept. 1994, pp 211-214.
[11]. Richard Baskerville, “Information System Security Design Methods : Implications for Information Systems Development”, ACM Computing Surveys, Vol. 25, No. 4, Dec. 1993, pp 376-414.
[12]. K. Pullen, “Uncertainty Analysis with Cocomo”, Proc Cocomo User’s Group, Software Engineering Institute, Pitsburgh, 1987.
[13]. B. Boehm, “ Software Engineering Economics”, Prentice Hall, Eaglewood Cliffs, N.J., 1987.
[14]. Stanely, Y.W.Su, “ A cost-Benefit Decision Model : Analysis Comparison and Selection of Data Management System”, ACM Trans on Data Base System, Vol. 12, No. 2, Sept. 1987.
[15]. John Miguel, “A Composite Cost/Benefit/Risk Analysis Methodology”, Proc IFIP/Sec 84, Canada, Sept. 1994, pp 307-311.
[16]. Rabbe Wrede, “The SBA Method : A method for Testing Vulnerability”, Proc IFIP/Sec 84, Canada, Sept. 1994, pp 313-319.
[17]. S.T. Smith, J.J. Lim, “ An Automated Method for Assessing the Effectiveness of Computer Security Safeguards”, Proc IFIP / Sec 84, Canada, Sept. 1994, pp 321-328.