2012 International Conference on Computer Technology and Science (ICCTS 2012)
IPCSIT vol. 47 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V47.43

Statistical Quantitative Risk Calculator (SQRC)

Upasna Saluja[+], and Dr Norbik Bashah Idris

University of Technology, Malaysia (UTM)

Abstract. Information Security Risk Assessment is still in its infancy and is continually evolving. The sole purpose of Risk Assessment is to identify risks faced by any organization, so that the management can allocate resources towards Risk Mitigation optimally. There are number of Risk Management Standards and methodologies existing; most of which are Qualitative in nature. They are based purely on subjective analysis. Cost benefit analysis is nearly impossible in case of qualitative risk assessment. The most recent and widely accepted Standard for Information Security Risk Management is ISO 27005. There is a dearth of good quantitative Risk Assessment methodology. This paper highlights merits and shortcomings of ISO 27005 and proposes a Quantitative Risk Calculator based on Statistics. In the proposed methodology, SQRC looks into the existing threats and vulnerabilities on the key assets in an organization and the deployed Safeguards to prevent adverse incidents. It calculates the probabilities of a particular safeguard not being effective against various threat vulnerability combinations. SQRC's ability to determine risk in monetary terms can prove to be of great assistance in taking business decisions. The proposed methodology also provides flexibility in accepting qualitative data for certain parameters where the quantitative data cannot be made available.

Keywords: Information Security Risk Assessment; Quantitative Risk Assessment; Statistical Analysis

1. Introduction

Risk Assessment and Management is quite critical for any organisation in order to sustain its business. [5] Risk Assessment is the primary step in managing risks. Risk management aims at implementing different strategies in order to reduce the identified risks to an acceptable level. Risk Management is becoming one of the primary concerns in businesses these days and many companies regard it as a critical but challenging endeavour. Risk Management is now used by small as well as large organisations conducting business in diverse domains such as Finance and Investment, Insurance, Health Care, Government Institutions, Information Technology etc.

2. Information Security Risk Management

Risk management is one of the most integral parts of planning for businesses. The Risk Management process is specifically designed to reduce or eliminate the risk of certain kinds of events happening and impacting the business. Risk management recognises risk, accesses risk, and takes measures to reduce risk, as well as takes measures to maintain risk to an acceptable level.

In information security, a risk can be defined as the probability that a particular threat-source will exploit particular information security vulnerabilities and that the result will have an adverse impact on the organisation. There are different existing standards and methodologies namely CRAMM, NIST SP 800 – 30, ISO 27005 and ISO 31000. Today, ISO 27005 is the latest and most established Risk Management Standard.

3. ISO – 27005: Information Security Risk Management

3.1. Introduction

[+] Corresponding author.
E-mail address:upasnasaluja@gmail.com

The complete name of ISO - 27005 standard is ISO/IEC 27005: 2008 [18], Information Technology – Security Techniques – Information security risk assessment. ISO 27005 Standard is the most widely accepted approach to IT risk management in the world. The global adoption of this standard has made it quite popular. Presently it is being adopted by 156 countries such as US, United Kingdom, Australia, Canada, Japan, Korea, France, etc. Although the ISO 27005 standard provides sufficient details regarding Risk Assessment and Risk Treatment, it remains quite qualitative in nature.

3.2. Strengths of ISO – 27005

ISO 27005 standard is quite simple, systematic and comprehensive. It is a substantial contribution to the development of the information security field. Most of the risk assessment methodologies just focus on the critical assets instead of all of them. ISO – 27005 does not exclude non-critical assets from the risk management framework and instead it assigns a value to each asset. This is one of most significant differences from the OCTAVE's methodology.[3]

3.3. Short Shortcomings of ISO – 27005

ISO – 27005 Standard does not provide any specific methodology to manage risk, rather it just provides generic guidelines for risk management. Key points which merit attention are given below -

- ISO 27005 has very little to do with the actual management of risk. It's more like the risk management framework where risks are identified and then a Plan-Do-Check-Act cycle is tied to that risk. It does very little to address the root cause of risk. Having a control in place does not make us absolutely secure; generally some risk would still be there after deploying safeguards. [1]
- 27005 doesn't really do a good job at helping build a risk management program. It seems more geared to a program to manage Risk rather than focusing on the calculation of
- ISO 27005 does not provide any substantial contribution to the existing Risk Assessment Methodologies which could have helped industry to assess risks more effectively. Its only demonstrative use is for the purposes of auditing to standard compliance. [1]
- It is not easy to implement it as terms and phases are quite confusing for example Risk Estimation vs Risk Evaluation. [2]
- Risk Measurement has not looked into Quantitative Assessment of Risks in-depth. [2]

4. Statistical Quantitative Risk Calculator (SQRC)

4.1. Introduction

The proposed SQRC proposes risk assessment model which is quantitative in nature. SQRC provides a quantitative approach to estimate risk. In case, while performing risk assessment, if quantitative data pertaining to some kind of risk is unavailable, then the model offers the flexibility to accommodate qualitative data even. Therefore SQRC is very simple to use as well as it provides a statistical foundation to conduct practical Risk Assessment. SQRC can be applied to any types of organisations, whether big or small across industries.

SQRC provides a holistic risk assessment approach to address Information Security risks. The calculated Risk percentage can be tested, improved and compared as opposed to attributes such as high / medium / low which cannot be quantified numerically for an objective assessment. Therefore, SQRC succeeds in providing results in pure numbers which are easy for management to understand. Steps supporting SQRC are outlined below.

4.2. Step 1 - Identification of Assets under the scope

Identify key assets of the organisation. The different types of assets are generally covered under categories People, Technology (Hardware, Software, Connectivity, Telecommunication), Information and Facility.

4.3. Step 2 - Identification of Threats

Consider each asset one by one and identify all the threats existing to that asset. Identification of threats is important activity as it identifies all the potential risks to an information system that may cause a negative impact on an asset. Some typical examples of threats are theft, loss or destruction of an organizational asset,

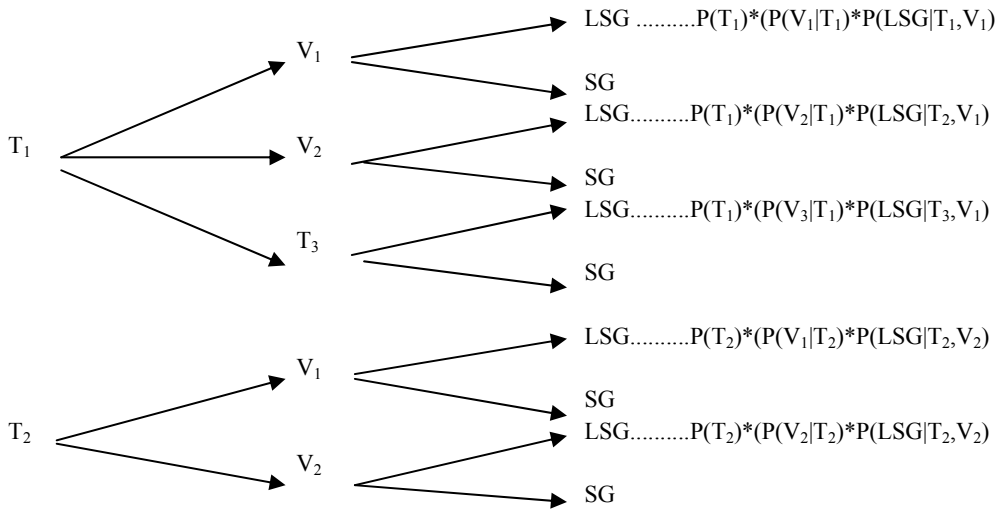
fraud, unauthorized access to the network services, infection with malicious code, disclosure of someone's personal data and identity theft. It is required to identify both accidental and deliberate threats. A threat may arise from within or from outside the organization. None of the threats should be overlooked even the unexpected.

4.4. Step 3- Identification of Vulnerabilities

All the vulnerabilities corresponding to the identified threats are considered in this step. There can be more than one vulnerability corresponding to a single identified threat. Thus, all the identified vulnerabilities are listed beside the corresponding threat. The identified vulnerability is exposed to some kind of risk only, if there is an associated threat existing to exploit that vulnerability otherwise the vulnerability poses no risk to an organisation.

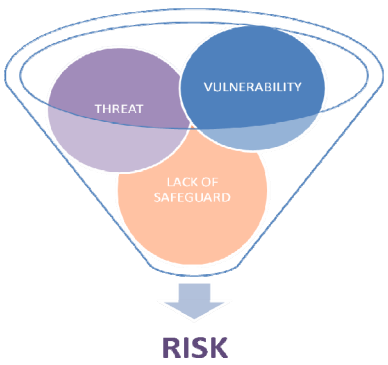
4.5. Step 4 - Construction of Attack Tree Diagram

The considered threats and vulnerabilities are then depicted in the form of an attack tree as shown below. Out of the threats identified, only those vulnerabilities will be depicted in the Attack Tree Diagram that have an associated vulnerability corresponding to them. This is due to the fact the existence of threat alone with no corresponding vulnerability present no risk to the organization.



4.6. Step 5 - Identification of Existing Security Safeguards

All the terms listed above, such as vulnerabilities, threats, safeguards (SG) and Lack of Safeguards (LSG) accept probabilistic values in order to determine the residual risk pertaining to the system. It is relatively quick and easy to determine the probabilistic values for various entities. Therefore the probabilistic foundation of SQRC provides quick and more accurate results when compared against the alternative qualitative risk assessment approach.



In order to calculate the risk the identified assets are analysed for certain period of time such as 2 weeks, 3 weeks, 1 month, etc depending upon the scenario. The analysis of the system for a particular period of time is helpful in determining all the probability values for lack of safeguards, threats and vulnerabilities.

4.7. Step 6 - Determination of Probability Values for Lack of Safeguards

Initially the probability values of safeguards (SG) and Lack of Safeguards (LSG) are determined. The suggested probability values range from 0 to 1.0 (or 0 to 100 percent).

To combat risk, generally, technological safeguards are deployed. It is believed that the attacks are successful only due to lack of some safeguard in place. The obtained probability value for lack of effectiveness of the safeguard deployed (LSG) when subtracted from 1 yield the probability value for safeguard (SG). It implies that the attacks that were not successful in causing harm were unsuccessful due to the presence of some safeguard or security measure in place.

Then the probability values for LSG and SG are calculated according to the formulas mentioned below

$$\textbf{P (Lack of Safeguard)} = \frac{\textbf{Number of Successful Attempts by the Threat}}{\textbf{Total Number of attempts by the Threat}}$$

$$\textbf{P (Safeguard)} = \frac{\textbf{Number of Unsuccessful Attempts by the Threat}}{\textbf{Total Number of attempts by the Threat}}$$

4.8. Step 7 - Determination of Probability Values for Vulnerabilities

Obtain the probability values for the considered vulnerability by back tracking the attack tree diagram. The probability values obtained for the vulnerability would vary from 0 to 1.0.

Let X correspond to total number of unsuccessful attempts by a threat that are prevented by some Safeguard in place and Y correspond to total number of successful attempts of the threat that resulted in a security breach.

Yij = Number of successful attempts of threat j due to vulnerability i
Xij = Number of unsuccessful attempts of threat j due to vulnerability i
j = Corresponds to Vulnerability; i = Corresponds to Threat

It implies that out of Y number of crashes or successful attempts, there were Y11 (T1, V1) counts due to vulnerability V1, Y12 (T1, V2) counts due to vulnerability V2, so on, all stemming from Threat T1. Similarly, Y21 (V2, T1) counts due to threat T1, Y22 (V2, T2) counts due to threat T2, so on, all stemming from vulnerability V2 and so on. Then we can find the probability estimates for the vulnerabilities P(ti,vj) by taking the ratios as follows:

$$\textbf{P}(T_{ij}) = \frac{X_{ij} + Y_{ij}}{(Y_j + X_j)} \quad \textbf{for a given "j"}$$

$$Y_i = \sum_i Y_{ij}\ ,\ X = \sum_i X_{ij}\ ,\ \textbf{for i = 1,2,..... i.}$$

4.9. Step 8 - Determination of the probability values for Threats

The facilitator of the vulnerability is obtained by further back tracking the Attack Tree Diagram. This will yield the threat responsible for the existence of the considered vulnerability. The suggested threat values also range between 0 to 1.0 (or 0 to 100 percent). The probabilistic values for threats correspond to that out of all the considered vulnerabilities, what are the chances that an attack will occur thorough the exploitation of the particular considered threat. Now from the given set of threats the probability P (Ti) of vulnerability i being exploited is given by

$$P(T_i) = \frac{\sum_i (X_{ij} + Y_{ij})}{\sum_i \sum_j (X_{ij} + Y_{ij})} \quad \text{for } i = 1, 2, \ldots I \text{ and } j = 1, 2, \ldots J$$

4.10. Step 9 - Calculation of Risk

Categories	Probabilities
Negligible	0 to 0.1
Extremely Low	0.1 to 0.2
Very Low	0.2 to 0.3
Low	0.3 to 0.4
Medium	0.4 to 0.6
High	0.6 to 0.7
Very High	0.7 to 0.8
Extremely High	0.8 to 0.9
Certain	0.9 to 1

The proposed quantitative (hybrid) Model estimates the residual risk on the considered asset despite the current safeguards in place. The general formula to calculate risk corresponds to (Threat x Vulnerability). Residual risk is what is left of the risk (Threat x Vulnerability) after the safeguards applies to circumvent the risk.

Residual Risk = (Threat x Vulnerability) x Lack of Safeguard

Thus, residual risk is calculated through conditional probability using **Bayesian Technique**. [16] -

$$RR = P(T_1) \times P(T_1/V_1) \times P(LSG/V_1,T_1)$$

$P(T_1)$ = Probability of an attack using Threat T1

$P(T_1/V_1)$ = Probability of the occurrence of attack T_1 when vulnerability V_1 has already being exploited.

$P(LSG/V_1,T_1)$ = Probability of Vulnerability V1 exploiting Threat T1 in spite of safeguards in place.

5. Flexibility To Accommodate Qualitative Values In Case Of Absence Of Quantitative Data

In case the quantitative data pertaining to number of attempts made by a particular threat or the number of successful attempts is unavailable, then the subjective judgement can be made regarding the probability of a particular threat occurring after analysing the existing security controls deployed to combat that threat. Thus the probability of the lack of safeguard P (LSG) can be substituted in qualitative terms in the absence of the quantitative data. The scale used to make the subjective judgement can have categories like Negligible, Low, Medium, High.

6. Identification of the Significance Value of an Asset

Since different assets have different value to the organization, Significance value of an asset is calculated. System Significance indicates the degree of how critical or disruptive the entire system is in the event of the entire loss. The value of the Significance factor is assigned within the range of 0 to 1.

SIGNIFICANCE DEFINITION	WEIGHTAGE
Asset's Loss has negligible Impact on organisation's Mission	0
Asset's Loss has Minor Impact on organisation's Mission	0.2
Asset's Loss has Moderate impact on organisation's Mission	0.4
Asset's Loss has Significant Impact on organisation's Mission	0.6
Asset's Loss has Critical Impact on organisation's Mission	0.8
Asset's Loss has Catastrophic Impact on organisation's Mission	1

Significance is low if the residual risk is of little or no significance, such as the malfunctioning of the office printer and Significance is high if the considered asset is very crucial to the organisation such as the server lying within an organisation

Final Risk = Residual Risk x Significance

7. Identification of the Impact of the Residual Risk

Impact of the Residual Risk is calculated in terms of the Expected Monetary Loss in case the organisation takes no steps to mitigate the identified threats. The Expected Monetary Loss is obtained by the product of final risk and the asset value in monetary terms.

Expected Monetary Loss = Final risk x Asset Value

8. Merits of Statistical Quantitative Risk Calculator

- SQRC can supplement ISO 27005 implementation with its focus on quantitative abilities. Since, technology plays an important role in Risk Mitigation; this approach is quite effective in calculating Technological Risks Quantitatively.
- Since SQRC is based on Statistical foundation, it provides more accurate and effective results.
- SQRC succeeds in providing results in monetary figures that the management can understand.

- SQRC is capable for embracing qualitative data also for analysis part along with Quantitative where Quantitative data is not possible.
- Calculated risk percentage can be tested, improved and compared as opposed to attributes such as high, medium, or low, which cannot be quantified numerically for an objective assessment.

9. References

[1] Anderes Gui, Robbyn Kristanto, Hasnah Haron, Ega Adrian, "Information Technology Risk Measurement using NIST", 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2010 IEEE.

[2] Young-Hwan Bang, Sang-Dong Lee, "A Study of System –Based Model for evaluating EF(Exposure Factor) in Quantitative Security Risk Analysis, International Conference on Convergence and Hybrid Information Technology 2008, 2008 IEEE.

[3] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoon-jung Jung, In-jung Kim, "Security Risk Analysis Model for Information Systems," LNCS 3398, Systems Modeling and Simulation: Theory and Applications: Third Asian Simulation Conference, AsianSim 2004.

[4] Zhihu Wang, Xin Wang, "Research on Technologies in Quantitative Risk Assessment and Forecast of Network Security",2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE 2010.

[5] Xiang – Yun Cheng, Ying-Mei Wang, Zi-Ling Xu, "Risk assessment of Human Error in Information Security, IEEE International Conference on Computer Machine Learning and Cybernetics. Pp: 3573-3578.

[6] R.C. Wilcox, B.M. Ayyub, "Uncertainty Modeling of Data and Uncertainty Propogation for Risk Studies", Proceedings of the Fourth International Symposium on Uncertainty Modeling and analysis. IEEE 2003.

[7] Yi-Kun Zhang, Su-yang Jiang Ying-an Cui Bao-wei Zhang Hui, "A Qualitative and Quantitative Risk Assessment Method in Software Security", 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE 2010.

[8] Bob Blakley, Ellen McDermott, Dan Geer, "Information Security is Information Risk Management", in the Proceedings of 2001 workshop on New security paradigms, ACM Digital Library, 2001, New Mexico, USA.

[9] AS/NZS. Risk Management Standard, AS/NZS 4360:2004, Jointly published by Standards Australia International Ltd., Sydney and Standards New Zealand, Wellington, 2004.

[10] NIST – SP 800 – 30, "Risk Management Guide for Information Technology Systems," NIST, July 2002.

[11] ISO Guide 73:2002, Risk Management – Vocabulary – Guidelines for use in standards, Geneva, 2002.