IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 17-20
www.iosrjournals.org

A Quantitative Measurement Methodology for calculating Risk related to Information Security.

Abhishek kumar srivastav[1,] Irman Ali[2,] Shani Fatema[3]
[1,2]*M.S in Cyber Law & Information Security*
[3]*M.Tech in Software Engineering*
[1,2]*Indian Institute of Information Technology, Allahabad ,India*
[3]*SRMSCET, Bareilly, India*

***Abstract**: Nowadays, technology increases, so the risk related to technology is also increasing. Risk is the possibility of suffering loss. Therefore, we have to adopt some risk management methodology to reduce the number of risks. There are many risks are present in the organization. So it is the primary concern in risk management which risk we have to deal with because reducing every risk is not possible in any way. There is some risk that is always present, which is known as residual risk. Risk Assessment is the part of risk management. In this paper, we are focusing on quantitative approaches for risk assessment related to information security.*
***Keyword**: Risk, information security, risk assessment, quantitative approach.*

I. Introduction:

Information security plays a very important role in any organization even it is non IT organization because every organization has some critical and sensitive information and information security is all about securing the information. The possibility that something could go wrong with information like damage, disclosure, loss, destroy of information is known as risk. Therefore, it is necessary to anticipate and identify all kinds of risk related to information in the organization. Risk management therefore very important for every organization.

Risk Management: The main goal of risk management is to reduce the impact of all types of risk that might affect the business information. Risk Management consists of three important activities.

- Risk Identification
- Risk Assessment
- Risk Containment

1-Risk Identification: risk identification is the process or mechanism of identifying all the dangers and hazards that may affect the business information. It is a procedure of analyzing, reviewing, anticipating all kinds of possible risk. Basically, there are two types of risk

- Systematic Risk
- Unsystematic Risk

Systematic Risk: Systematic Risk are those risks that affect the large set of asset. For example a political event may affect several asset in the organization is a type of systematic risk. Systematic risk is also classified into three categories:

- Interest rate risk
- Market risk
- Inflationary risk

Unsystematic risk: unsystematic Risk is those risks that affect a very small set of asset. It is also known as "specific risk". Unsystematic risk is classified into three categories.

- Financial risk
- Business risk
- Operational risk

2-Risk Assessment: The main goal of risk assessment is to rank or quantify the risk in terms of their damage causing potential. For risk Assessment each risk should be first classifieds in two ways.

- The probability of the risk coming true.
- The consequences or impact if the risk becomes true.

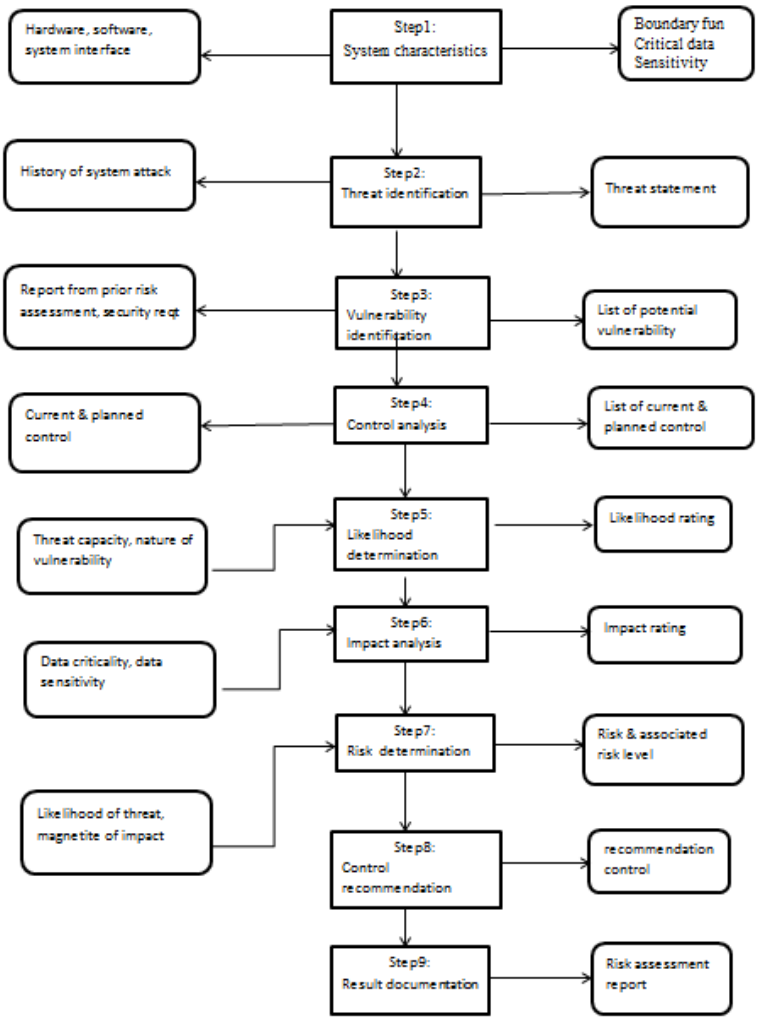
Risk Exposure or Risk Impact can be calculated by the following formula:

Risk Exposure = Probability * severity

Where probability is likely or the frequency with which risk becoming true and.Severity is defined as what is the impact or damage if a particular risk becoming true.

Risk Assessment Steps: these are the following steps to perform risk assessment
• Assets characterization
• Threat identification
• Vulnerability identification
• Analysis of safeguarding
• Frequency or probability determination
• Impact analysis
• Determination of risk
• Safeguard recommendations
• Documentation of result

In this paper we are trying to show risk assessment work flow through a diagram. In the following figure we are trying to evaluate each step of risk assessment, what are Inputs, and Output of each stage in performing risk assessment activities.



3-Risk containment: different risk requires different containment procedures.
There are four main methods used to reduce the risk.

- Accept the risk
- Avoid the risk
- Transfer the risk
- Risk mitigation

Accept the risk: Accepting risk is totally depending upon the management for the cost/benefit analysis of the possible control to reduce that risk and overall impact of that risk if becoming true. It also means that the management has agreed to accept the consequences and the loss if the risk is realized.

Avoid the risk: A final, but unacceptable possible response to risk is to reject risk or ignore risk or avoid the risk. Avoiding a risk that exists, it means the organization is hoping that by ignoring a risk it will never be coming true. [[2]]

Transfer the risk: This methodology involves getting the risky component deployed by a third party, or buying insurance cover etc.

Risk mitigation: This involves planning ways to contain the damage due to a risk. For example, if there is a risk that some key personnel might leave, new recruitment may be planned.

Goal of Risk Assessment
• Identify assets in the organization and their value.
• Identify threat and vulnerabilities.
• Quantify the probability and impact if the threat is exploited.
• Provide a balance between cost/benefit analysis..

II. Methodology:

There are two risk assessment methodologies

- Quantitative Methodology
- Qualitative Methodology

Quantitative Approach to calculate risk: In the rank assessment process, there are mainly three strategies that are conducted.

- Risk identification
- Risk analysis
- Evaluating and ranking of risk

Risk analysis is the core of the risk assessment process.A *quantitative risk analysis* plays a very important role when we have to assign a numerical value to each risk either in terms of money or something else. It is more of a scientific or mathematical approach to risk analysis compared to qualitative. The quantitative method results in concrete probability percentage.

Steps of a Quantitative Risk Analysis: We have identified the assets that are to be assessed, associated a value to each asset, and identified the vulnerabilities and threats that could affect these assets. Now we need to carry out the risk analysis portion, which means that we need to figure out how to interpret all the data that was gathered during the assessment. The most generally used mathematical concepts for this objective are the ***single*** *loss expectancy (SLE)* and the *annual loss expectancy (ALE).*
A single loss expectancy (SLE): The SLE is a cost which relates to a single realized risk against a particular asset. SLE indicates that exact amount of loss a business organization will face if a threat is exploited. And harmed the asset the formula to calculate SLE is as follows.
Asset Value × Exposure Factor (EF) = SLE

Exposure Factor (EF): The exposure factor determines the expected overall asset value loss for a single risk has realized.

Annualized rate of occurrence (ARO)*:* The annualized rate of occurrence (ARO) can be defined as the expected probability or likelihood with which a particular threat or risk will occur.
Annualized loss expectancy (ALE): Annualized loss expectancy is defined as the possible yearly cost of all samples of a particular realized the threat against a particular asset.

The ALE can be determined with the following mathematical formula.

ALE= SLE × ARO(Annualized Rate of Occurrence)

SLE=AV x EF
Thus, finally risk value is defined as follows:

ALE=AV x EF x ARO

Qualitative Risk Analysis: Another method of risk analysis is ***qualitative,*** which does not assign numbers and monetary values of components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. Qualitative analysis techniques include judgment, best practices, intuition, and experience. [[1]]

Matrix to evaluate quantitative and qualitative approach to calculate risk:

Characteristic	Qualitative	Quantitative
Employs complex functions	N	Y
Uses cost/benefit analysis	N	Y
Results in specific values	N	Y
Requires guesswork	Y	N
Supports automation	N	Y
Involves a high volume of information	N	Y
Is objective	N	Y
Users' opinions	Y	N
Requires significant time and effort	N	Y
Offers useful and meaningful results	Y	Y

The benefits of adopting Quantitative approach:

- Risk are stored or measured by their financial impact
- The result of quantitative risk analysis can be presented in specific management terminology.
- Quantitative risk analysis methodology is objective results are same for everyone..
- The security level is much better classified based on the confidentiality, integrity, availability.
- Performance of Management can be monitored accurately
- Data are more accurate as compare to qualitative risk methodology.

III. Conclusion:

It is concluded from the matrix we have drawn that quantitative approach to measuring the risk related to information security is much better than the qualitative approach. Qualitative approach is subjective and is based on person to person, it may be possible that one risk that one person interpret as he may be low for another person may be he/she think from different perspectives. On the other hand quantitative approach for measuring risk related to information security is objective. If one risk is calculated as high, then it will be higher for all other employees that deal with risk management in the organization. When a risk assessment is performed by adopting a quantitative approach, then it is not possible to achieve 100 % quantitative analysis, there is still some subjectivity when it comes to the data. In quantitative risk analysis, we can do our best to assure that all the information is correct and by doing so we will come very close to risk values.

References:

[1]. http://blog.simplilearn.com/it-security-management/qualitative-risk-analysis, date accessed Jan 26.
[2]. http://www.coursehero.com/flashcards/431914/CISSP-Glossary/ data accessed Jan 26.