A new quantitative approach for information security risk assessment

Abbas Asosheh
Department of Industrial Engineering,
Tarbiat Modares University
Tehran, Iran
asosheh@modares.ac.ir

Bijan Dehmoubed, Amir Khani
Department of Information Technology Management,
Faculty of Management, University of Tehran
Tehran, Iran
b.dehmoubed@ashnasecure.com
a.khani@ashnasecure.com

I. INTRODUCTION & BACKGROUND

Today's highly connected IT infrastructures exist in an environment that is increasingly hostile. Attacks are being mounted with increasing frequency and are demanding ever shorter reaction times. Often, organizations are unable to react to new security threats before their business is impacted. Managing the security of their infrastructures and the business value that those infrastructures deliver has become a primary concern for IT departments.

There are so many models for security risk assessment, but most of them are non practical. An effective security risk management process enables enterprises to operate in the most cost efficient manner with a known and acceptable level of business risk. Callio Secura 17799 is a simple, but effective tool for implementing an information security management system, based on the ISO/IEC 27001:2005 standard and has a module for risk assessment. Also Microsoft has a Risk Assessment model.

By studying and implementing the above two models in the real environment, we reach to the point that none of them can fit the business requirements completely. The Callio Secura approach is a very complete model for assessing the Exposure Factor (EF) of a risk, but it doesn't calculate the business impact of a risk. Vice versa the MS risk assessment approach starts from the EF and ends with the calculation of ROSI.

In this poster we introduce a new approach for assessing the security risk of information assets. This new model is composed of the MS risk assessment model and the Callio Secura risk assessment model with some changes.

II. PROPOSED RISK ASSESSMENT MODEL

By combining the two models and make it more complete, we can cover the weak points of each approach. The proposed model is a practical model which can be used in a real business environment. In this model the output of the Callio Secura approach is used as an input for Microsoft risk assessment model with some differences. The goal of this model is to deliver clear, actionable approach on how to implement a security risk management process.

The phases and steps of the proposed model are shown in the Figure 1.

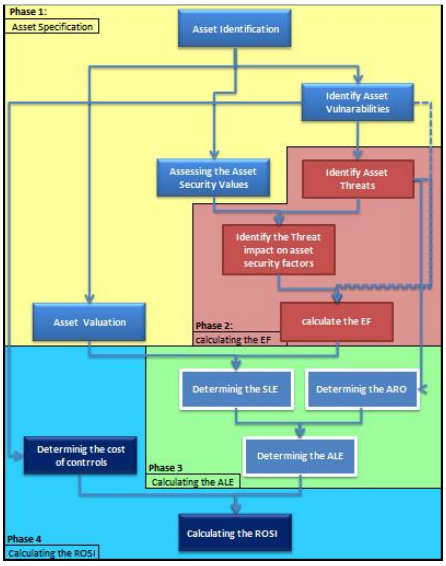

Figure1. The Proposed model phases and steps

As shown above, the proposed model consists of four phases and twelve steps. The steps should be followed for each combination of specific vulnerability and threat per asset.

A. Phase 1: Asset Specification

Step 1: In Asset Identification the assets which are in our scope should be identified and listed. Using predefined categories can help the organization to identify the different assets.

Step 2: Asset Valuation is identifying the monetary value of the asset. The monetary worth of each asset can be defined using the sum of the physical value, business value, indirect value and competitive value.

Step 3: Assessing the asset security values is identifying the asset value from the security aspects. In this step the assets should be assessed against the security factors according to table I. According to the ISO27001:2005, these factors are Confidentiality, Integrity and Availability.

Step 4: Every asset has some vulnerability according to its category. These vulnerabilities should be defined and ranked against their severity for each asset according to table I.

TABLE I. THE IMPORTANCE OF VULNERABILITY SEVERITY/TREAT SEVERITY

Importance of Information Security Values/ Vulnerability Severity/treat severity	Rank
Very high	5
High	4
Medium	3
Low	2
Very low	1
Not Applicable	0

B. Phase 2: Calculating the EF

Step 5: There are so many threats that can target a vulnerability of an asset and exploit that. Like the vulnerabilities, each threat has a severity level according to the environment business context, Security guards, etc. The asset threats should be ranked according to table I.

Step 6: Each threat exploits the vulnerability in order to break the security factors based on the type of the threat. After exploiting, one, two or all of the security factors which were defined in step 3, will be broken.

Step 7: The EF represents the percentage of loss that a realized threat could have on a certain asset using the targeted vulnerability. The EF is calculated by the formula No 1.

$$EF = Vv * Tv * (C + I + A)/375 \quad (1)$$

Vv: is the vulnerability value for the asset.

Tv: is the threat value which can exploit the vulnerability.

C, I and A: are the Confidentiality, Integrity and Availability value of asset. Theses value is defined according to step 3 & 6. If the combination of vulnerability and threat can impact these factors of asset, C, I and A will get their value; otherwise they are 0.

C. Phase 3: Calculating the ALE

Step 8: In determining the SLE, the total amount of revenue that is lost from a single occurrence of the risk, should be calculated.

$$SLE = EF * \text{Asset Value} \quad (2)$$

Step 9: In determining the ARO, the number of times that you reasonably expect the threat to occur during one year, should be estimated.

Step 10: Determining the ALE in the goal of this phase. The ALE is the total amount of money that the organization will lose in one year if nothing is done to mitigate the risk.

$$ALE = SLE * ARO \quad (3)$$

D. Phase 4: Calculating the ROSI

Step 11: Determining Cost of Controls is based on the type and severity of vulnerabilities. The controls will cover the asset vulnerabilities. It requires accurate estimates on how much acquiring, testing, deploying, operating, and maintaining each control would cost.

After determining the security controls and the cost of them, the vulnerability value, threat value and ARO will change. The new EF, SLE and ALE should be calculated according to these changes.

Step 12: Calculating the ROSI is the last step of this approach and will be determined using the formula No 4.

$$ROSI = ALE1 - ALE2 - ACC \quad (4)$$

Where:

ALE1= ALE before control, ALE2= ALE after control, ACC= Annual Cost of Control

At last, the ROSI will be calculated for each asset. If the ROSI is positive, it means that the controls which are selected and implemented are cost effective. If the ROSI is negative, it means that the cost of controls cannot cover the loss of organization for the risk of that asset. Sum of the ROSIs will determine the ROSI of whole organization.

III. CONCLUSION

Assessing the IT security risks is a critical success factor for all today's businesses. In order to assess and manage these risks in a cost efficient way, we need a comprehensive and practical approach. In this article a new approach is introduced, which is based on the most two common and famous risk assessment approaches in the world (Microsoft and Callio Secura). This approach has covered the incompleteness and weak points of those approaches. The new approach composes of twelve steps and starts with asset identification and ends with calculating the return on security investment.