Assets Dependencies Model in Information Security Risk Management

Jakub Breier[1,2] and Frank Schindler[3]

[1] Physical Analysis and Cryptographic Engineering, Temasek Laboratories@NTU
[2] School of Physical and Mathematical Sciences, Division of Mathematical Sciences, Nanyang Technological University, Singapore
jbreier@ntu.edu.sg
[3] Faculty of Informatics, Pan-European University, Bratislava, Slovakia
frank.schindler@paneurouni.com

Abstract. Information security risk management is a fundamental process conducted for the purpose of securing information assets in an organization. It usually involves asset identification and valuation, threat analysis, risk analysis and implementation of countermeasures. A correct asset valuation is a basis for accurate risk analysis, but there is a lack of works describing the valuation process with respect to dependencies among assets. In this work we propose a method for inspecting asset dependencies, based on common security attributes - confidentiality, integrity and availability. Our method should bring more detailed outputs from the risk analysis and therefore make this process more objective.

Keywords: Information Security Risk Management, Asset Valuation, Asset Dependency, Risk Analysis.

1 Introduction

Information systems are subject to various threats that can have undesirable effects on them. As information technologies evolve, threats are more sophisticated and harder to detect. Great volumes of valuable data are stored in information systems that are connected to the Internet and therefore it is necessary to use security techniques for their protection.

Information security risk management [2] is a fundamental process conducted for the purpose of securing information assets in an organization. It usually involves asset identification and valuation, threat analysis, risk analysis and implementation of countermeasures. There are few standards that deliberate this process and provide recommendations for security specialists in organizations. The most popular are NIST Special Publication 800-39 [1] and ISO/IEC 27005:2011 standard [3], both provide a high-level overview of the risk management process.

The important part of the risk management process is the asset valuation that, if used properly, will tell us which assets are important for the organization in the meaning of price and necessity in business processes. Works that

Linawati et al. (Eds.): ICT-EurAsia 2014, LNCS 8407, pp. 405–412, 2014.

implement one of these standards usually use simple valuation methods, based on qualitative techniques of measurement. They express value on some discrete scale, consisting mostly of 3 to 5 degrees of precision, for example 'none', 'low', 'medium', or 'high' importance in a meaning of contribution to organization's business processes. Usually, they do not take asset dependencies into consideration, but it can significantly change the results of a risk analysis if two assets are strongly dependent. If is, for example, a storage server in a high risk resulting from its physical placement and the database server running on this physical server has only low level of risk, resulting from risk evaluation, we cannot consider these two entities as independent. The way how dependent are they should be an outcome from asset valuation sub-process.

In this paper we would like to introduce a model for asset valuation that involves inspection of asset dependencies. This inspection is based on examining dependencies from the security attributes point of view - confidentiality, integrity and availability. After evaluation of asset relations we consider risk values, acquired by the preliminary risk assessment, and assign new risk values deliberating the original values and the dependencies.

The rest of this paper is structured as follows. Section 2 provides an overview of a related work dealing with the problem of security risk management techniques with focus on asset dependencies. Section 3 proposes our approach and describes method used for examining dependencies among assets. Finally, section 4 concludes this paper and provides a motivation for further work.

2 Related Work

There exist a number of works in the field of information security risk management. These works implement mostly the ISO/IEC 27005:2011 standard and use various methods in order to automate this process. They usually follow process structure from the standard and propose own methods based on either quantitative or qualitative assessment techniques. We will examine these works from the asset valuation perspective.

Some works do not examine dependencies at all. For example, Vavoulas and Xenakis [9] use five dimensions in asset valuation - value, repair cost, reputational damage, operational damage, and legal or regulatory damage. The consequences of an attack are then equal to the sum of these values. Tatar and Karabacak [8] propose a hierarchy based asset valuation method that express the value in three terms - confidentiality, integrity and availability. Their method is straightforward and needs a security expert to determine these values for each asset. They do not deliberate asset dependence, buying price or operating costs.

Leitner [4] propose his own risk analysis approach called ARiMA (Austrian Risk Management Approach). It uses a configuration management database (CMDB) to identify relevant assets in accordance to the business processes. The assets are classified into five degrees according to the importance for the organization from 'very low' to 'very high'. The corresponding multiplicators that affect the risk value are numbers from 1 to 1.5, with 0.125 granularity. The risks

are computed using standard matrices with impact values for the columns and probability values for the rows. The asset dependencies are modelled by using two logical connection types OR and AND that are used in evaluating asset's security attributes - confidentiality, integrity and availability. If OR is used, the values are computed as an average, if AND is used, the highest number among dependent entities is chosen. It is naturally better to implement at least some technique for examining dependencies, but this approach is very simple and does not provide desired complexity for asset analysis.

Loloei, Shahriari and Sadeghi [5] propose an asset valuation model, emphasizing dependencies between assets. They define dependencies in terms of security attributes and divide organization's assets into three layers - business, application and technical layer. They use a value propagation graph to represent how assets affect the value of each other, and how an asset value propagates through other assets. Authors claim that the well-known risk management methodologies, such as CRAMM, OCTAVE, or NIST 800-30 show limitations during risk assessment because of lack of considering dependencies among assets. However, the work is missing comparison between different asset valuation methods, therefore it cannot be decided whether the asset dependencies are modelled correctly and contribute in terms of more precise assessment, or not.

Suh and Han [7] propose a risk analysis method based on Analytic Hierarchy Process with more detailed view of asset identification and evaluation. They divided this phase into five sub-processes: asset identification, assignment of assets to business functions, determination of initial asset importance, asset dependency identification, and determination of final asset importance. The dependencies are expressed from the view of asset importance. If asset A depends on assets B,C and D, its importance is maximum of importances of these assets. This value can be then revised by a security analyst and can be further adjusted.

Mayer and Fagundes [6] design a model for assessing the maturity model of the risk management process in information security. This model is aimed to identify weaknesses or deficiencies in the risk management and improve its effectiveness. It examines all the processes measuring their quality. From our point of view, the main disadvantage is that the asset analysis is not deliberated as an individual process, just as a sub-process of risk analysis.

3 Methods

We can examine dependencies among assets on a simplified organization model, depicted in Figure 1. Dependencies are arranged in a tree-based hierarchy, with the building as a top-level node. If the building is destroyed, all the other assets would be lost, if we consider simple model without information backup and alternative information processing facilities in other building(s). As we can see, one entity can be dependent on multiple entities, the Exchange server is dependent both on Physical server 2 and on Active Directory server. If we look at Database server, there is a redundancy - company has one secondary backup server in a case of failure of the primary one. Therefore we have to differentiate a connection between the data stored on these servers.

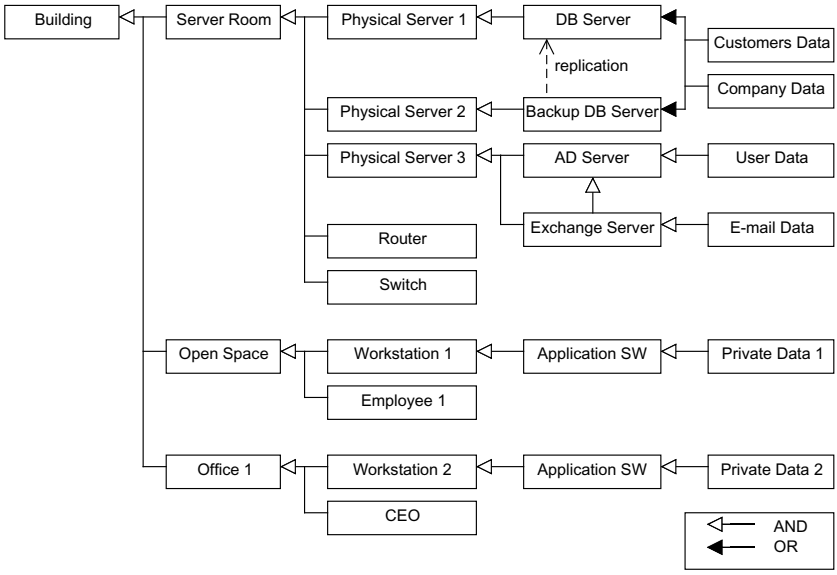

Fig. 1. Dependencies between assets

3.1 Model Assumptions

Now we can make following assumptions for our model:

- We can assume that the business goal of our model company is dependent on all the leaves, therefore we need to ensure confidentiality, integrity and availability of all the other components following the hierarchy. We will call this set of entities 'chain of dependence', for example User data in our picture has four entities in its chain of dependence, beginning with AD server and ending with the building.
- We have to assign dependency weights for each entity in the chain of dependence. These weights will be then used to adjust the process of a risk analysis - if entity N depends on other entity M that has high level of risk, this risk should be distributed on the entity N.
- If we have redundant entities, we will use the 'OR' type of connection. Normal type of connection, 'AND', means that the dependent entity depends exclusively on the superior entity in the hierarchy. The 'OR' connection lowers the risk, distributing it on two or more superior entities.
- Weights cannot be represented as a single value, since dependencies can have different character. For example, Customers data depends on Physical server 1 from the availability point of view mainly, but their confidentiality is strongly influenced by the Database server.

We will use 4x4 risk matrix [10] for demonstrational purposes. This matrix has threat probability for its columns and impact for its rows. We will define following risk values:

– in interval [1,5] as a *low* risk value,
– in interval [6,9] as a *medium* risk value,
– in interval [10,16] as a *high* risk value.

It is clear that we cannot assign some of these numbers by using the risk matrix below, but we will need the whole intervals in the latter phase.

Let us assume that we have already made the risk analysis using standard methodology. To save the space we will analyze only part of our model company, risk values for particular elements can be seen in Figure 2. These are the average risk values for threats, we will not examine dependencies among individual threats.

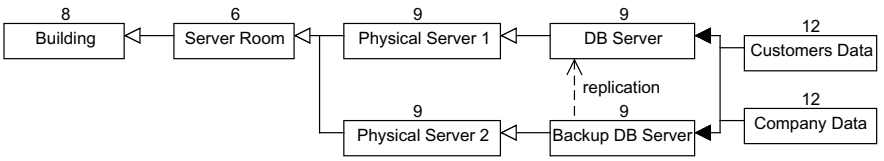

Fig. 2. Risk values

3.2 Model Construction

We can now construct our dependency valuation model based on previous assumptions. The valuation process consists of following steps:

1. Begin with the top level entity (building in our example).
2. Assign dependency component weight values of confidentiality (W_{con}), integrity (W_{int}) and availability (W_{ava}) to each relation in the hierarchy. These values are from interval [0,1] with the granularity of 0.1 points.
3. Adjust the risk value by using the dependency adjustment formula. If there is 'OR' connection between entities, compute the average of the adjusted risk values and divide it by the number of redundant entities. If one entity is directly dependent on more than one entity, we have to adjust the risk value considering all of the superior entities.
4. Continue with the lower level entities until the last level in the hierarchy.

We define an overall dependency weight value W_o as a sum of component weight values.

$$W_o = \sum_{i=con,int,ava} W_i \tag{1}$$

The dependency adjustment formula, used in step 3, is used for adjusting the risk value by examining dependency weight values:

$$W_o \times max(W_{con}, W_{int}, W_{ava}) \times RV \tag{2}$$

The formula depends on three factors. First, we sum the component weight values and multiply it with the maximal value among components. And finally

we multiply this value with the RV, which is the simplified risk value of the upper level entity connected with the dependency relation. If the risk of the asset is low, this value would be 1, if medium, the value is 2 and for the high risk this value is 3.

Table 1. Dependency adjustment formula examples

Dependent Entity	W_o	$max(W_{con}, W_{int}, W_{ava})$	RV	Adjustment Value
Asset 1	0.5	0.2	1	**+1**
Asset 2	1.5	0.8	2	**+2.4**
Asset 3	2.4	1.0	3	**+7.2**

In the Table 1 we can see the example of adjusted risk values. The first asset has low dependency and low risk of the entity on which it depends, in this case the adjustment to the final value would be +1 point. The second asset has medium dependency and medium RV, the original risk will be adjusted by +2.4 points. Finally, we have an asset with high dependency and high RV, so the adjustment in this case will be +7.2 points.

3.3 Model Example

We will now examine our method on the provided example. In Figure 3 we can see part of our model company with assigned dependency component weight values. In Table 2 are listed adjusted risk values corresponding to dependency weights. Redundant entities are stated in one row, because their weights are equal. Notice that after the first assignment we take the adjusted risk values as an input, for example when considering Customers Data, we take high risk value of the DB Server as an input, not medium from the original risk assessment. Also notice that Data are adjusted just by +2.1 risk value because of the DB Server redundancy.

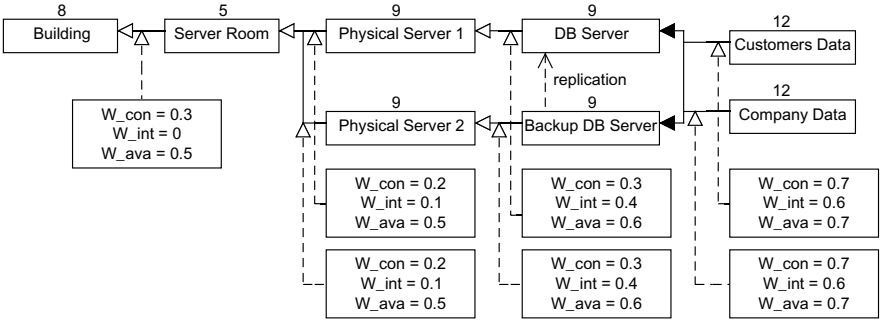

Fig. 3. Dependency component weight values

Table 2. Adjusted risk values

Dependent Entity	W_o	W_{max}	Original Risk Val.	RV	Adjusted Risk Val.
Server Room	0.8	0.5	5	2	**5.8**
Physical Server 1 & 2	0.8	0.5	9	1	**9.4**
DB Server & Backup Server	1.3	0.6	9	2	**10.56**
Customers Data	2	0.7	12	3	**14.1**
Company Data	2	0.7	12	3	**14.1**

Adjusted values in the whole organization model are listed in Figure 4. Building is the only entity that does not depend on any other entity, therefore its risk value remains the same. Minimal adjustments were made to physical servers, after considering dependencies they have +0.4 risk values. Maximal adjustments were made to both Private Data, their values were raised by +4 points. It is because of double dependency on both AD server and Physical server 3.

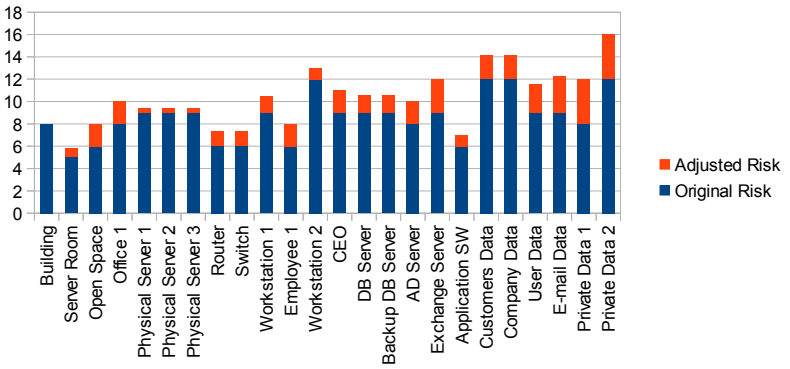

Fig. 4. Adjusted risks in the whole model

4 Conclusions

In this paper we proposed an asset dependency evaluation method that can be used in order to improve results of a risk analysis. Despite the fact that there are not many works dealing with this problem, we find it important to take it in the consideration when assessing risks in an organization.

The ISO/IEC 27005:2011 standard [3] recommends to encompass dependencies of assets in the asset analysis process. It suggests to take the degree of dependency and the values of other assets into account. In our work we inspect this degree from the confidentiality, integrity and availability perspective and instead of the value, we consider the risk value. The dependency valuation model also deals with the situation of dependency on more than one entity and with the dependency on redundant entities. The final risk value is adjusted with respect to these conditions.

It is easy to include our method into the complex risk analysis process, so that the risk values would be adjusted by the terms of asset dependencies. In the future, we would like to provide the whole risk management evaluation model based on quantitative measurement techniques, that would measure security state in an organization and output meaningful results.

References

1. NIST Special Publication 800-53 Managing Information Security Risk - Organization, Mission, and Information System View. NIST (2011)
2. Blakley, B., McDermott, E., Geer, D.: Information security is information risk management. In: Proceedings of the 2001 Workshop on New Security Paradigms, NSPW 2001, pp. 97–104. ACM, New York (2001)
3. ISO. ISO/IEC Std. ISO 27005:2011, Information technology – Security techniques – Information security risk management. ISO (2011)
4. Leitner, A., Schaumuller-Bichl, I.: Arima - a new approach to implement iso/iec 27005. In: 2nd International Logistics and Industrial Informatics, LINDI 2009, pp. 1–6 (2009)
5. Loloei, I., Shahriari, H.R., Sadeghi, A.: A model for asset valuation in security risk analysis regarding assets' dependencies. In: 2012 20th Iranian Conference on Electrical Engineering (ICEE), pp. 763–768 (2012)
6. Mayer, J., Lemes Fagundes, L.: A model to assess the maturity level of the risk management process in information security. In: IFIP/IEEE International Symposium on Integrated Network Management-Workshops, IM 2009, pp. 61–70 (2009)
7. Suh, B., Han, I.: The is risk analysis based on a business model. Inf. Manage. 41(2), 149–158 (2003)
8. Tatar, U., Karabacak, B.: An hierarchical asset valuation method for information security risk analysis. In: 2012 International Conference on Information Society (i-Society), pp. 286–291 (2012)
9. Vavoulas, N., Xenakis, C.: A quantitative risk analysis approach for deliberate threats. In: Xenakis, C., Wolthusen, S. (eds.) CRITIS 2010. LNCS, vol. 6712, pp. 13–25. Springer, Heidelberg (2011)
10. Williams, R., Pandelios, G., Behrens, S.: Software Risk Evaluation (SRE) method description (version 2.0). Software Engineering Institute (1999)